

OFFICIAL MICROSOFT LEARNING
PRODUCT

6426A

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



Be sure to access the extended learning content on your Course Companion CD enclosed on the back cover of the book.

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 web casting 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.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Technical Reviewer: John Policelli

Product Number: 6426A

Part Number: X14 - 71604

Released: 06/2008

MICROSOFT LICENSE TERMS

OFFICIAL MICROSOFT LEARNING PRODUCTS - TRAINER EDITION – Pre-Release and Final Release 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. DEFINITIONS.

- "Academic Materials"** means the printed or electronic documentation such as manuals, workbooks, white papers, press releases, datasheets, and FAQs which may be included in the Licensed Content.
- "Authorized Learning Center(s)"** means a Microsoft Certified Partner for Learning Solutions location, an IT Academy location, or such other entity as Microsoft may designate from time to time.
- "Authorized Training Session(s)"** means those training sessions authorized by Microsoft and conducted at or through Authorized Learning Centers by a Trainer providing training to Students solely on Official Microsoft Learning Products (formerly known as Microsoft Official Curriculum or "MOC") and Microsoft Dynamics Learning Products (formerly known as Microsoft Business Solutions Courseware). Each Authorized Training Session will provide training on the subject matter of one (1) Course.
- "Course"** means one of the courses using Licensed Content offered by an Authorized Learning Center during an Authorized Training Session, each of which provides training on a particular Microsoft technology subject matter.
- "Device(s)"** means a single computer, device, workstation, terminal, or other digital electronic or analog device.
- "Licensed Content"** means the materials accompanying these license terms. The Licensed Content may include, but is not limited to, the following elements: (i) Trainer Content, (ii) Student Content, (iii) classroom setup guide, and (iv) Software. There are different and separate components of the Licensed Content for each Course.
- "Software"** means the Virtual Machines and Virtual Hard Disks, or other software applications that may be included with the Licensed Content.
- "Student(s)"** means a student duly enrolled for an Authorized Training Session at your location.

- i. **"Student Content"** means the learning materials accompanying these license terms that are for use by Students and Trainers during an Authorized Training Session. Student Content may include labs, simulations, and courseware files for a Course.
- j. **"Trainer(s)"** means a) a person who is duly certified by Microsoft as a Microsoft Certified Trainer and b) such other individual as authorized in writing by Microsoft and has been engaged by an Authorized Learning Center to teach or instruct an Authorized Training Session to Students on its behalf.
- k. **"Trainer Content"** means the materials accompanying these license terms that are for use by Trainers and Students, as applicable, solely during an Authorized Training Session. Trainer Content may include Virtual Machines, Virtual Hard Disks, Microsoft PowerPoint files, instructor notes, and demonstration guides and script files for a Course.
- l. **"Virtual Hard Disks"** means Microsoft Software that is comprised of virtualized hard disks (such as a base virtual hard disk or differencing disks) for a Virtual Machine that can be loaded onto a single computer or other device in order to allow end-users to run multiple operating systems concurrently. For the purposes of these license terms, Virtual Hard Disks will be considered "Trainer Content".
- m. **"Virtual Machine"** means a virtualized computing experience, created and accessed using Microsoft® Virtual PC or Microsoft® Virtual Server software that consists of a virtualized hardware environment, one or more Virtual Hard Disks, and a configuration file setting the parameters of the virtualized hardware environment (e.g., RAM). For the purposes of these license terms, Virtual Hard Disks will be considered "Trainer Content".
- n. **"you"** means the Authorized Learning Center or Trainer, as applicable, that has agreed to these license terms.

2. OVERVIEW.

Licensed Content. The Licensed Content includes Software, Academic Materials (online and electronic), Trainer Content, Student Content, classroom setup guide, and associated media.

License Model. The Licensed Content is licensed on a per copy per Authorized Learning Center location or per Trainer basis.

3. INSTALLATION AND USE RIGHTS.

- a. **Authorized Learning Centers and Trainers: For each Authorized Training Session, you may:**
 - i. either install individual copies of the relevant Licensed Content on classroom Devices only for use by Students enrolled in and the Trainer delivering the Authorized Training Session, provided that the number of copies in use does not exceed the number of Students enrolled in and the Trainer delivering the Authorized Training Session, **OR**
 - ii. install one copy of the relevant Licensed Content on a network server only for access by classroom Devices and only for use by Students enrolled in and the Trainer delivering the Authorized Training Session, provided that the number of Devices accessing the Licensed Content on such server does not exceed the number of Students enrolled in and the Trainer delivering the Authorized Training Session.
 - iii. and allow the Students enrolled in and the Trainer delivering the Authorized Training Session to use the Licensed Content that you install in accordance with (i) or (ii) above during such Authorized Training Session in accordance with these license terms.

- i. **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.
 - ii. **Third Party Programs.** The Licensed Content may contain third party programs. These license terms will apply to the use of those third party programs, unless other terms accompany those programs.
- b. Trainers:**
- i. Trainers may Use the Licensed Content that you install or that is installed by an Authorized Learning Center on a classroom Device to deliver an Authorized Training Session.
 - ii. Trainers may also Use a copy of the Licensed Content as follows:
 - 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 solely for your own personal training Use and for preparation of an Authorized Training Session.
 - B. **Portable Device.** You may install another copy on a portable device solely for your own personal training Use and for preparation of an Authorized Training Session.
- 4. PRE-RELEASE VERSIONS.** If this is a pre-release (“beta”) version, in addition to the other provisions in this agreement, 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 each Authorized Training Session 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 and/or in the possession or under the control of any Trainers who have received copies of the pre-released version.
- 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 such distribution, you will follow any additional terms that Microsoft provides to you for such copies and distribution.

5. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. Authorized Learning Centers and Trainers:

i. Software.

ii. **Virtual Hard Disks.** The Licensed Content may contain versions of Microsoft XP, Microsoft Windows Vista, Windows Server 2003, Windows Server 2008, and Windows 2000 Advanced Server and/or other Microsoft products which are provided in Virtual Hard Disks.

A. If the Virtual Hard Disks and the labs are launched through the Microsoft Learning Lab Launcher, then these terms apply:

Time-Sensitive Software. If the Software is not reset, it will stop running based upon the time indicated on the install of the Virtual Machines (between 30 and 500 days after you install it). You will not receive notice before it stops running. You may not be able to access data used or information saved with the Virtual Machines when it stops running and may be forced to reset these Virtual Machines to their original state. You must remove the Software from the Devices at the end of each Authorized Training Session and reinstall and launch it prior to the beginning of the next Authorized Training Session.

B. If the Virtual Hard Disks require a product key to launch, then these terms apply:

Microsoft will deactivate the operating system associated with each Virtual Hard Disk. Before installing any Virtual Hard Disks on classroom Devices for use during an Authorized Training Session, you will obtain from Microsoft a product key for the operating system software for the Virtual Hard Disks and will activate such Software with Microsoft using such product key.

C. These terms apply to all Virtual Machines and Virtual Hard Disks:

You may only use the Virtual Machines and Virtual Hard Disks if you comply with the terms and conditions of this agreement and the following security requirements:

- You may not install Virtual Machines and Virtual Hard Disks on portable Devices or Devices that are accessible to other networks.
- You must remove Virtual Machines and Virtual Hard Disks from all classroom Devices at the end of each Authorized Training Session, except those held at Microsoft Certified Partners for Learning Solutions locations.
- You must remove the differencing drive portions of the Virtual Hard Disks from all classroom Devices at the end of each Authorized Training Session at Microsoft Certified Partners for Learning Solutions locations.
- You will ensure that the Virtual Machines and Virtual Hard Disks are not copied or downloaded from Devices on which you installed them.
- You will strictly comply with all Microsoft instructions relating to installation, use, activation and deactivation, and security of Virtual Machines and Virtual Hard Disks.
- You may not modify the Virtual Machines and Virtual Hard Disks or any contents thereof.
- You may not reproduce or redistribute the Virtual Machines or Virtual Hard Disks.

ii. Classroom Setup Guide. You will assure any Licensed Content installed for use during an Authorized Training Session will be done in accordance with the classroom set-up guide for the Course.

iii. Media Elements and Templates. You may allow Trainers and Students to use images, clip art, animations, sounds, music, shapes, video clips and templates provided with the Licensed Content solely in an Authorized Training Session. If Trainers have their own copy of the Licensed Content, they may use Media Elements for their personal training use.

iv. iv Evaluation Software. Any Software that is included in the Student Content designated as "Evaluation Software" may be used by Students solely for their personal training outside of the Authorized Training Session.

b. Trainers Only:

i. Use of PowerPoint Slide Deck Templates. The Trainer Content may include Microsoft PowerPoint slide decks. Trainers may use, copy and modify the PowerPoint slide decks only for providing an Authorized Training Session. If you elect to exercise the foregoing, you will agree or ensure Trainer agrees: (a) that modification of the slide decks will not constitute creation of obscene or scandalous works, as defined by federal law at the time the work is created; and (b) to comply with all other terms and conditions of this agreement.

ii. Use of Instructional Components in Trainer Content. For each Authorized Training Session, Trainers may customize and reproduce, in accordance with the MCT Agreement, those portions of the Licensed Content that are logically associated with instruction of the Authorized Training Session. If you elect to exercise the foregoing rights, you agree or ensure the Trainer agrees: (a) that any of these customizations or reproductions will only be used for providing an Authorized Training Session and (b) to comply with all other terms and conditions of this agreement.

iii. Academic Materials. If the Licensed Content contains Academic Materials, 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:

© 2007 Reprinted for personal reference use only with permission by Microsoft Corporation. All rights reserved.

Microsoft, Windows, and Windows Server 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.

- 6. 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.
- 7. 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
- install more copies of the Licensed Content on classroom Devices than the number of Students and the Trainer in the Authorized Training Session;
 - allow more classroom Devices to access the server than the number of Students enrolled in and the Trainer delivering the Authorized Training Session if the Licensed Content is installed on a network server;
 - copy or reproduce the Licensed Content to any server or location for further reproduction or distribution;
 - 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, in whole or in part, to a third party;
 - access or use any Licensed Content for which you (i) are not providing a Course and/or (ii) have not been authorized by Microsoft to access and use;
 - rent, lease or lend the Licensed Content; or
 - use the Licensed Content for commercial hosting services or general business purposes.
 - 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.
- 8. 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.
- 9. NOT FOR RESALE SOFTWARE/LICENSED CONTENT.** You may not sell software or Licensed Content marked as “NFR” or “Not for Resale.”
- 10. 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.
- 11. TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of these license terms. In the event your status as an Authorized Learning Center or Trainer a) expires, b) is voluntarily terminated by you, and/or c) is terminated by Microsoft, this agreement shall automatically terminate. Upon any termination of this agreement, you must destroy all copies of the Licensed Content and all of its component parts.
- 12. 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.**
- 13. APPLICABLE LAW.**
- 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.
 - Outside the United States.** If you acquired the Licensed Content in any other country, the laws of that country apply.
- 14. 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.
- 15. 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.**

16. 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 des consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit local, 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.

MCT USE ONLY. STUDENT USE PROHIBITED

Contents

Module 1: Exploring IDA Solutions

Lesson 1: Overview of IDA Management	1-3
Lesson 2: Active Directory Server Roles in IDA Management	1-14
Lesson 3: Overview of ILM 2007	1-27
Lab 1: Exploring IDA Solutions	1-40

Module 2: Configuring AD CS

Lesson 1: Overview of PKI	2-3
Lesson 2: Deploying a CA Hierarchy	2-14
Lesson 3: Installing AD CS	2-26
Lesson 4: Managing CA	2-35
Lab 2: Configuring AD CS	2-43

Module 3: Deploying and Managing Certificates

Lesson 1: Deploying Certificates by Using AD CS	3-3
Lesson 2: Deploying Certificates by Using Autoenrollment	3-15
Lesson 3: Revoking Certificates	3-19
Lesson 4: Configuring Certificate Templates	3-30
Lesson 5: Configuring Certificate Recovery	3-42
Lab 3: Deploying and Managing Certificates	3-53

Module 4: Configuring AD LDS

Lesson 1: Installing and Configuring AD LDS	4-3
Lesson 2: Configuring AD LDS Instances	4-15
Lesson 3: Configuring AD LDS Replication	4-32
Lesson 4: Configuring AD LDS Integration with AD DS	4-42
Lab 4: Configuring AD LDS	4-50

Module 5: Configuring AD FS

Lesson 1: Overview of AD FS	5-3
Lesson 2: AD FS Deployment Scenarios	5-14
Lesson 3: Deploying AD FS	5-26
Lesson 4: Implementing AD FS Claims	5-38
Lab 5A: Configuring AD FS for Federated Web SSO by Using Forest Trust Scenario	5-49
Lab 5B: Configuring Active Directory Federation Services by Using Federated Web SSO Scenario	5-64

Module 6: Configuring AD RMS

Lesson 1: Overview of AD RMS	6-3
Lesson 2: Installing and Configuring AD RMS Server Components	6-18
Lesson 3: Administering AD RMS	6-33
Lesson 4: Implementing AD RMS Trust Policies	6-44
Lab 6: Configuring AD RMS	6-54

Module 7: Maintaining Access Management Solutions

Lesson 1: Supporting AD CS	7-4
Lesson 2: Maintaining AD LDS	7-16
Lesson 3: Maintaining AD FS	7-27
Lesson 4: Maintaining AD RMS	7-36
Lab 7: Maintaining Access Management Solutions	7-44

Module 8: Troubleshooting IDA Solutions

Lesson 1: Troubleshooting AD CS	8-3
Lesson 2: Troubleshooting AD LDS	8-19
Lesson 3: Resolving AD FS Issues	8-28
Lesson 4: Solving AD RMS Issues	8-37
Lab 8: Troubleshooting IDA Solutions	8-42

MCT USE ONLY. STUDENT USE PROHIBITED

About This Course

Course Description

This three-day instructor-led course provides in-depth knowledge on configuring Identity and Access (IDA) management solutions in Windows Server® 2008.

Audience

The audience for this course includes IT professionals interested in IDA management solutions in their enterprise environment. Most students will be Microsoft® Certified Architects (MCAs), IT professionals, or developers who are responsible for integrating applications and platforms with enterprise directory and security services while increasing access to a growing number of customers and partners.

Student Prerequisites

This course requires that you meet the following prerequisites:

- Technical knowledge equivalent to 6424A: Fundamentals of Windows Server® 2008 Active Directory®
- Technical background knowledge and hands-on experience of Active Directory® Domain Services (AD DS). This includes technical knowledge equivalent to 6425A: Configuring Windows Server® 2008 Active Directory® Domain Services

Course Objectives

After completing this course, students will be able to:

- Explore IDA solutions.
- Configure Active Directory® Certificate Services (AD CS).
- Deploy and manage certificates.
- Configure Active Directory® Lightweight Directory Services (AD LDS).
- Configure Active Directory® Federation Services (AD FS).
- Configure Active Directory® Rights Management Services (AD RMS).
- Maintain access management solutions.
- Troubleshoot IDA solutions.

Course Outline

This section provides an outline of the course:

Module 1, "Exploring IDA Solutions" introduces Identity and Access Management (IDA Management) solutions. You will learn to identify Active Directory® server roles in IDA Management. The module will also describe the concept of Identity Lifecycle Manager (ILM).

Module 2, "Configuring AD CS" explains the concepts of public key infrastructure (PKI). You will also learn to deploy a certification authority (CA) hierarchy and install AD CS. Finally, the module describes how to configure AD CS.

Module 3, "Deploying and Managing Certificates" describes the deployment of certificates by using AD CS. In addition, the module elaborates on usage of autoenrollment to deploy certificates, certificate revocation, and configuration of certificate template and certificate recovery.

Module 4, "Configuring AD LDS" elaborates on the installation of AD LDS, and the configuration of AD LDS, its instances, replication, and integration with AD DS.

Module 5, "Configuring AD FS" presents the concept of AD FS and its deployment scenarios. The module also describes how to deploy AD FS and implement AD FS claims.

Module 6, "Configuring AD RMS" explains the concept of AD RMS. The module describes how to install and configure AD RMS server components. The module also explains the administration of AD RMS and implementation of AD RMS trust policies.

Module 7, "Maintaining Access Management Solutions" explains the maintenance of AD CS, AD LDS, AD FS, and AD RMS.

Module 8, "Troubleshooting IDA Solutions" describes how to troubleshoot AD CS, AD LDS, AD FS, and AD RMS.

Course Materials

The following materials are included with your kit:

- *Course Handbook*. The Course Handbook contains the material covered in class. It is meant to be used in conjunction with the Course Companion CD.
- *Course Companion CD*. The Course Companion CD contains lab answer keys, topical and categorized resources and Web links. It is meant to be used both inside and outside the class.

- *Course evaluation.* At the end of the course, you will have the opportunity to complete an online evaluation to provide feedback on the course, training facility, and instructor.

To provide additional comments or feedback on the course, please send an e-mail message to support@microsoft.com. To inquire about the Microsoft® Certification Program, send an e-mail message to mcphelp@microsoft.com.

Virtual Machine Environment

This section provides the information for setting up the classroom environment to support the business scenario of the course.

Virtual Machine Configuration

In this course, you will use Virtual Server 2005 R2 with the Microsoft® Lab Launcher (Oxford) to perform the labs.

Important: At the end of each lab, you must close the virtual machine and must not save any changes. To close a virtual machine without saving the changes, close the virtual machine window and then select **Turn off machine and discard changes**.

The following table shows the role of each virtual machine used in this course.

Virtual machine	Role
6426A-CHI-DC1	Domain controller for the Northwind Traders domain
6426A-NYC-CL1	Woodgrove Bank client
6426A-NYC-DC1 6426A-NYC-DC1-B	Woodgrove Bank Domain Controller
6426A-NYC-SVR1	Woodgrove Bank Member Server

Software Configuration

The following software is installed on each VM:

- Windows Server® 2008 Enterprise

- Windows Vista®

Classroom Setup

Each classroom computer will have the same virtual machine configured in the same way.

Course Hardware Level

To ensure a satisfactory student experience, Microsoft® Learning requires a minimum equipment configuration for trainer and student computers in all Microsoft® Certified Partner for Learning Solutions (CPLS) classrooms in which Official Microsoft® Learning Product courseware are taught. This course requires a computer that meets or exceeds hardware level 5, which specifies a 2.4-gigahertz (minimum) Pentium 4 or equivalent CPU, at least 2 gigabytes (GB) of RAM, 16 megabytes (MB) of video RAM, and a 7200 RPM 40-GB hard disk.

Module 1

Exploring IDA Solutions

Contents:

Lesson 1: Overview of IDA Management	1-3
Lesson 2: Active Directory Server Roles in IDA Management	1-14
Lesson 3: Overview of ILM 2007	1-27
Lab 1: Exploring IDA Solutions	1-40

Module Overview

- Overview of IDA Management
- Active Directory® Server Roles in IDA Management
- Overview of ILM 2007



Identity and access (IDA) management solutions enable you to simplify and centralize the management of user identities and access permissions. IDA solutions use directory services such as Active Directory® Domain Services (AD DS) and server roles to manage user identities and entities such as computers and security groups. With solutions such as, Microsoft® Identity Lifecycle Manager (ILM) 2007, you can manage the entire life cycle of user identities.

Lesson 1

Overview of IDA Management

- Need for IDA Management Solutions
- What Is IDA Management?
- Directory Management by Using IDA Solutions
- Enhancing Security with IDA Management
- IDA Management Technologies



IDA management includes various technologies to address identity management challenges such as maintaining multiple identity stores in an organization, securely authenticating and authorizing users, enhancing security for shared information, and managing the entire identity life cycle. AD DS assists in an IDA management solution by simplifying directory management and providing a unified view of user information. Technologies such as ILM 2007 enhance security for identity management, access management, and confidential data.

Discussion: Need for IDA Management Solutions

- List a few data sources that store identity information.
- Suggest a few procedures to provision a new employee to be fully productive.
- What are the security issues that confront individual access to user-sensitive data?
- Discuss a few conventional methods to securely share information or collaborate with external partners.

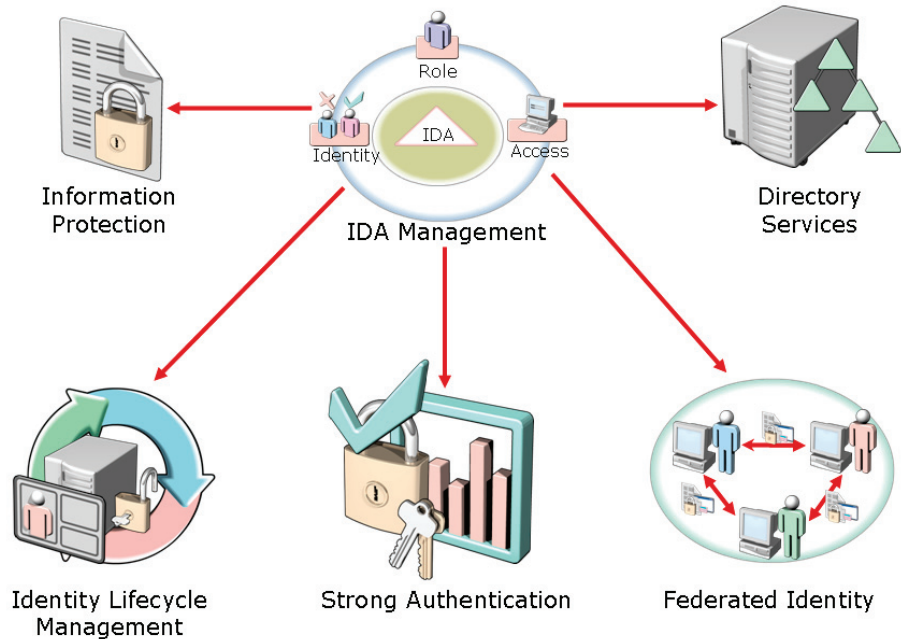
Key Points

IDA management solutions help you manage various identities that users may have. Some of the uses for IDA solutions include:

- **Maintaining multiple identity stores in an organization.** IDA solutions help you maintain multiple identity stores including:
 - AD DS
 - Active Directory® Lightweight Directory Services (AD LDS)
 - Lotus Notes
 - Novell eDirectory
 - HR databases
 - Proprietary directories

- **Determining the current and authoritative identity information.** IDA solutions help you synchronize, maintain, and update identity information across multiple identity stores.
- **Provisioning and deprovisioning user accounts.** IDA solutions can be used to automate the provisioning process. Automation ensures data consistency, integrity, and enhanced security as compared to manual processes.
- **Authenticating and authorizing users.** IDA solutions ensure that a user's identity is authenticated and authorized as access control information, such as an access control list (ACL).
- **Securing shared information.** IDA solutions help you to secure exchange of confidential information across various networks.
- **Securing collaboration of partners and vendors.** With IDA solutions, you can use domain trusts, forest trusts, and federation for vendors, external partners, and other divisions to access the organization's data.
- **Securing access and distribution of sensitive data.** With IDA solutions, you can safeguard confidential business details from unauthorized access and distribution.

What Is IDA Management?



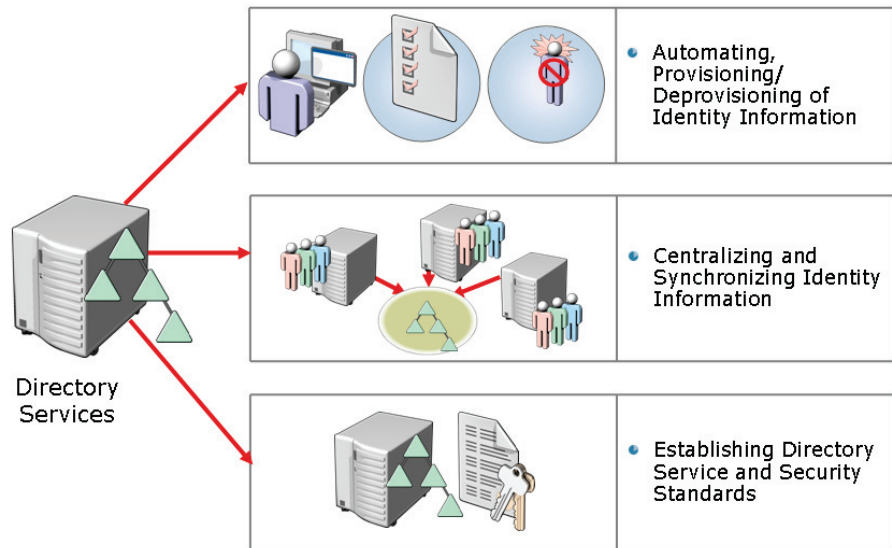
Key Points

IDA management is a set of products and technologies that help you manage user identities and access permissions. Some of the important features provided by IDA solution are tabulated here.

Feature	Description
Information protection	This feature safeguards confidential business information from unauthorized access and distribution.
Directory services	This feature stores and manages details about users and entities such as computers, security groups, and printer objects. Lightweight Directory Application Protocol (LDAP) can be used for interaction between IDA solutions and certain applications and services.
Identity lifecycle	This feature automates identity management through its

Feature	Description
management	entire life cycle. With IDA solutions, you can integrate identities across diverse environments.
Strong authentication	This feature provides enhanced authentication methods, in addition to using user names and passwords.
Federated identity	This feature provides the ability to securely share identities across organizational boundaries, to access other applications and information.

Directory Management by Using IDA Solutions



Key Points

IDA management solutions help simplify and secure directory management. They provide an integrated view of all user information provided by directory services such as AD DS. Some of the ways in which IDA solutions simplify directory management include the following:

- **Automating provisioning and deprovisioning of identity information.** IDA solutions update and synchronize all data sources simultaneously as per changes in user identities.
- **Centralizing and synchronizing identity information.** IDA solutions combine and synchronize information from multiple data sources into a single component to display identity details from multiple data sources.
- **Establishing directory service and security standards.** IDA solutions automate and manage information centrally, to maintain standards and security of a directory service.

Enhancing Security by Using IDA Management



Security and Access Policies



Password Management



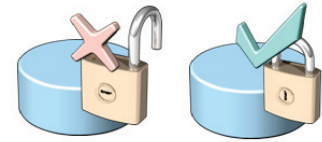
Strong Authentication



Security Audit Policies



Identity Aware Applications



Reducing Information Leaks

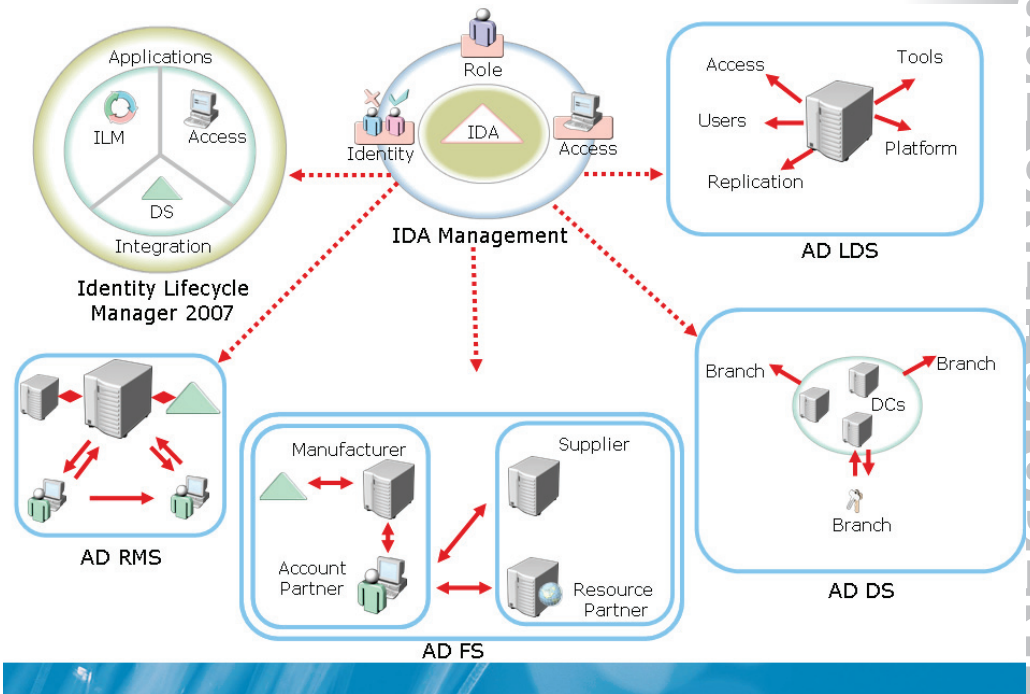
Key Points

IDA management solutions can help simplify IDA management. Additionally, these solutions help secure confidential information by using various mechanisms. Some of the IDA solutions that enhance security are tabulated here.

Feature	Description
Establishing security and access policies	This feature includes policies such as password policy, account lockout policy, remote access policy, and access restrictions policy. For example, you can specify the time when users can log on to the system.
Improving password management	This feature simplifies end-user password management by enabling a simple, secure, and cost-effective password-change solution.
Strengthening	This feature supports trusted protocols such as Secure

Feature	Description
authentication mechanisms	Socket Layer (SSL), Transport Layer Security (TLS), and trusted public key certificates. IDA solutions can use certificates stored in AD DS, or smart cards to securely authenticate users.
Establishing a security audit policy	This feature supports an organization's security needs by creating an auditing policy for specific event categories.
Developing identity-aware applications	This feature facilitates applications such as .NET Web applications to use secure access control mechanisms and meet the authentication, authorization, and audit requirements of the organization. Applications can use the directory and security services of the Microsoft® Windows® operating system.
Reducing the risk of information security leaks through the persistent data protection	This feature helps you to apply specific and persistent rights to sensitive data by using Active Directory® Rights Management Services (AD RMS) to create persistent policies that move alongside the data.

IDA Management Technologies



Key Points

IDA solutions can facilitate new business initiatives such as improved operational efficiency and security, collaboration, and increased compliance. Microsoft® IDA solutions include the following technologies:

- **Identity Lifecycle Management** - Microsoft® ILM 2007
- **Directory Services** - AD LDS and AD DS
- **Federated Identity** - Active Directory® Federation Services (AD FS)
- **Information Protection** - AD RMS
- **Strong Authentication** - Active Directory® Certificate Services (AD CS) and Microsoft® Certificate Lifecycle Manager (CLM) 2007

The following table gives the new names of products and server roles.

Product or Server Role	New Name
Microsoft® Identity Integration Server (MIIS) 2003	Microsoft® ILM 2007
Microsoft® CLM 2007	Bundled as another feature under the Microsoft® ILM 2007
Active Directory® Application Mode (ADAM)	AD LDS
Windows® Rights Management Services (RMS)	AD RMS
Windows® Certificate Services (CS)	AD CS
Windows® Federation Services (ADFS)	AD FS

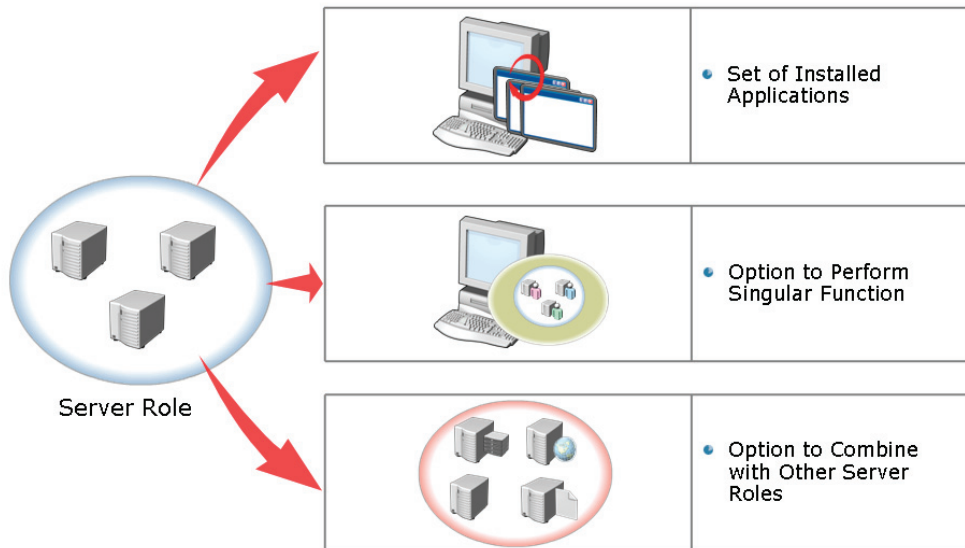
Lesson 2

Active Directory® Server Roles in IDA Management

- What Is a Server Role?
- Configuring a Server Role in Windows Server® 2008
- Directory Services Roles for IDA Management
- Strong Authentication Roles for IDA Management
- Federated Identity Roles for IDA Management
- Information Protection Roles for IDA Management

The first step in planning the implementation of IDA management is to evaluate the requirement of Windows Server® 2008 IDA-related server roles. A directory service manages and stores information about users and other entities such as computers, security groups, and printer objects. Windows Server® 2008 provides a complete IDA solution through strong authentication roles, secure federated identity roles, and information protection roles.

What Is a Server Role?



Key Points

A server role is a unit that logically groups the features and components required to perform a specific function. Windows Server® 2008 consists of various server roles such as AD DS, Web server, Dynamic Host Configuration Protocol (DHCP) server, Domain Name System (DNS), File server, and Print server. Some of the advantages of deploying server roles include:

- **Security management.** Server roles help you reduce the attack surface and maintain security by enabling only necessary services and features. Server roles use the same binaries across multiple systems by making their update and security management easier.
- **Simple installation.** Server roles offer a simple installation and the ability to customize a server.

- **Easy deployment.** By default, the recommended security settings configure server roles. You can immediately deploy server roles that are correctly installed and configured.
- **System Alignment.** Server roles align themselves according to the deployment and distribution of the systems.

Demonstration: How To Configure a Server Role in Windows Server® 2008

- To configure a server role in Windows Server® 2008 by using Server Manager

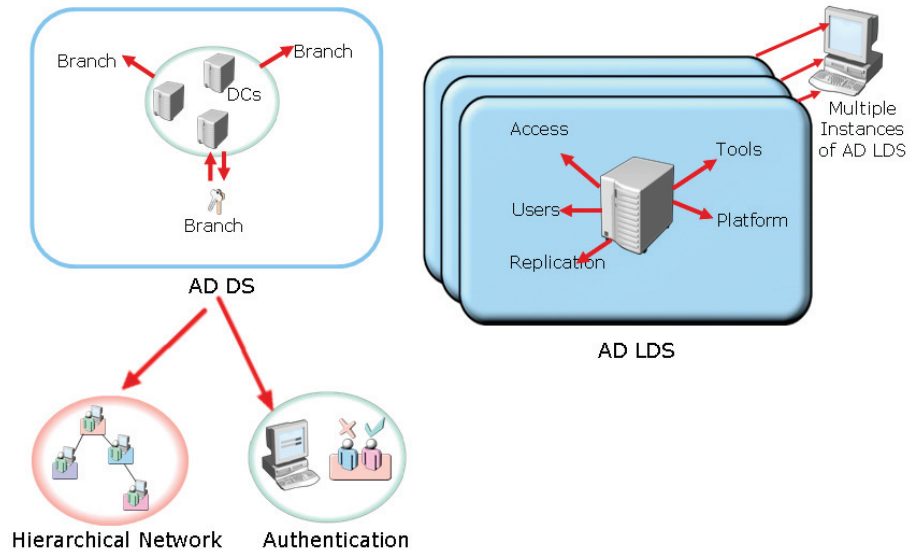


The instructor will provide a demonstration to show how you can configure a server role in Windows Server® 2008.

Questions:

- What is the purpose of AD RMS?
- 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?
- Which server role provides the Certification Authority (CA) infrastructure?
- List some of the advantages of the AD LDS server role compared to AD DS.
- Which server role is a prerequisite for the installation of other server roles?

Directory Service Roles for IDA Management



Key Points

Directory Services enables you to centrally manage and track information about users and other devices such as computers and security groups. In addition, Directory Services supports LDAP to interoperate on certain applications and services.

Some of the key aspects of AD DS and AD LDS server roles are:

- **Manages information securely.** AD DS helps you manage information about users, computers, and other devices securely.
- **Provides directory service.** AD LDS provides directory services for directory-enabled applications without the dependencies that are required for AD DS, such as the need for domains and forests, or a requirement for a single schema throughout a forest as compared to manual processes.

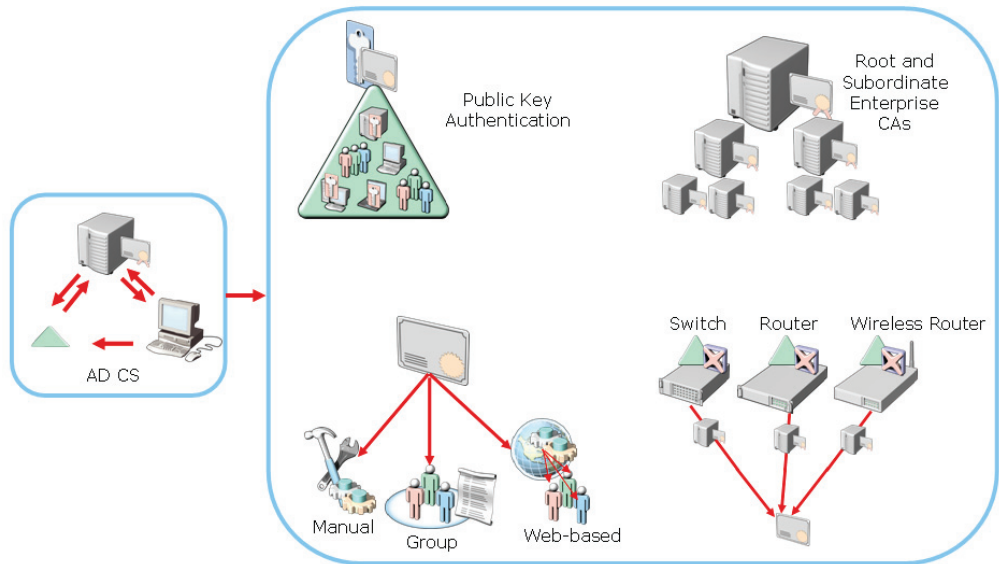
- **Allows data synchronization.** You can synchronize data from an AD DS forest to a configuration set of an AD LDS instance. To synchronize the data, you can use an Active Directory® to ADAM Synchronizer tool known as adamsync.exe.
- **Facilitates resource sharing.** AD DS helps share resource and establishes collaboration between users.
- **Allows storage of application data.** AD LDS allows storage of an organization's application data without its deployment on a domain controller.



For more information, see:

- AD LDS
- Active Directory® Services

Strong Authentication Roles for IDA Management



Key Points

Organizations require authentication solutions to provide an efficient process to authenticate credentials and control access to resources based on trust and identity. The following table describes some of the uses of strong authentication server roles.

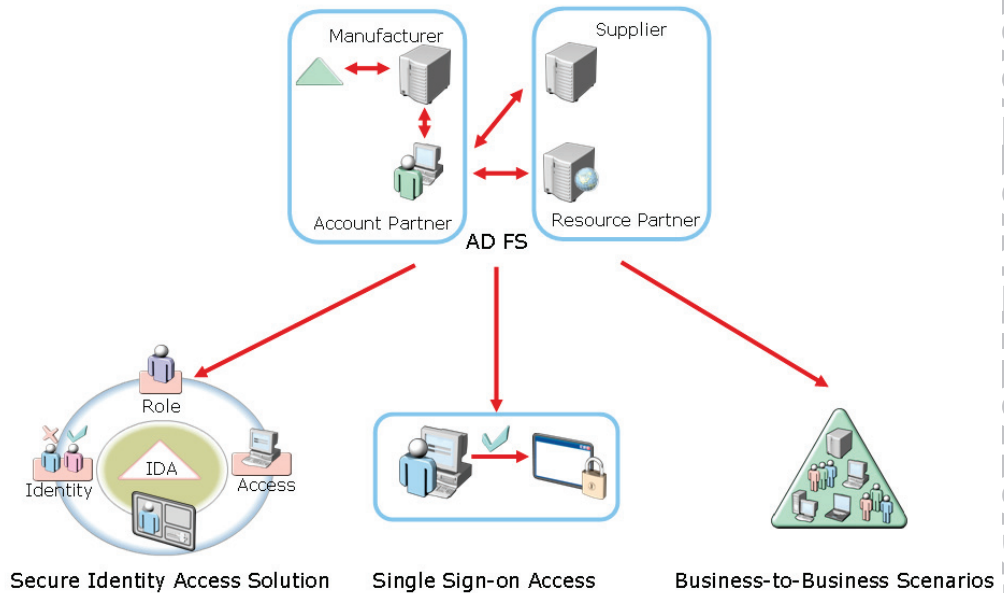
Feature	Description
Ensures access security	Strong authentication provides a secure access method to authenticate users and devices as compared to the user name and password method.
Ensures secure exchange of information	Certificates establish identity and create trusts for the secure exchange of information.

Feature	Description
Enhances organizational security	AD CS enhances security by binding the identity of a person, device, or service to a corresponding private key.
Manages the distribution and use of certificates	AD CS provides tools and services to manage the distribution and use of certificates and certificate revocation in various environments.



For more information, see AD CS

Federated Identity Roles for IDA Management



Key Points

AD FS is a server role that allows organizations to share a user's identity information within an organization and across federated organizations.

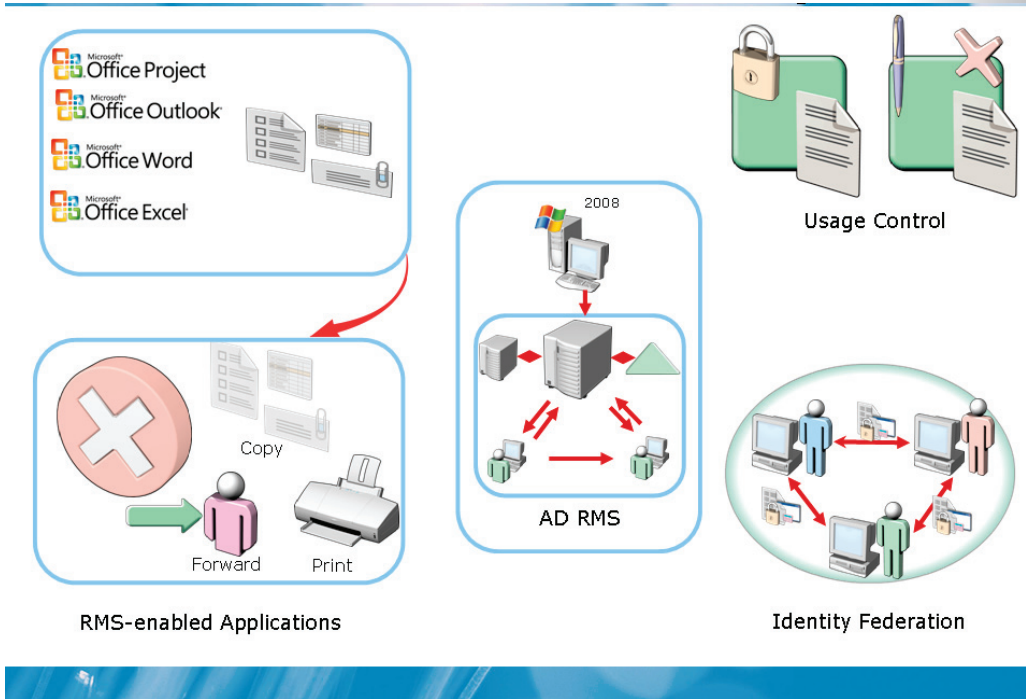
- AD FS scenarios include:
 - Web-based, single-sign-on (SSO) to support business-to-business (B2B) scenarios.
 - Federated Web SSO with Forest Trust to support business-to-employee (B2E) scenarios.
 - Web SSO to support customer access to applications in business-to-consumer (B2C) scenarios.
- AD FS requires an account store to authenticate users (AD DS or AD LDS).
- AD FS supports Web applications such as Windows® NT token-based and claims-aware applications.

- AD FS supports the following types of claims used for authorization purposes in an application:
 - Identity claims such as user principal name (UPN), e-mail, and common name
 - Group claims
 - Custom claims



For more information, see Microsoft® AD FS

Information Protection Roles for IDA Management



Key Points

Information protection helps eliminate unauthorized viewing and distribution of sensitive corporate data. AD RMS technology manages and enforces access policies to safeguard sensitive electronic information from unauthorized use and distribution as compared to existing security solutions such as ACLs and firewalls, where the privacy of data is lost once it is accessed and received.

AD RMS helps you protect various forms of digital assets such as sensitive documents, e-mail messages, and other content regardless of where and when the access occurs. You can deploy AD RMS for internal and external use. AD RMS rights policy templates specify the rights and conditions to protected content such as Copy, Edit, and Print. You can integrate AD RMS with AD FS to share the rights-protected content between organizations without the deployment of AD RMS in both organizations. AD RMS-enabled client computers must have an AD RMS-enabled browser such as Internet Explorer®, or an application such as Microsoft® Word®, Outlook®, or PowerPoint® in Microsoft® Office 2007.



For more information, see AD RMS

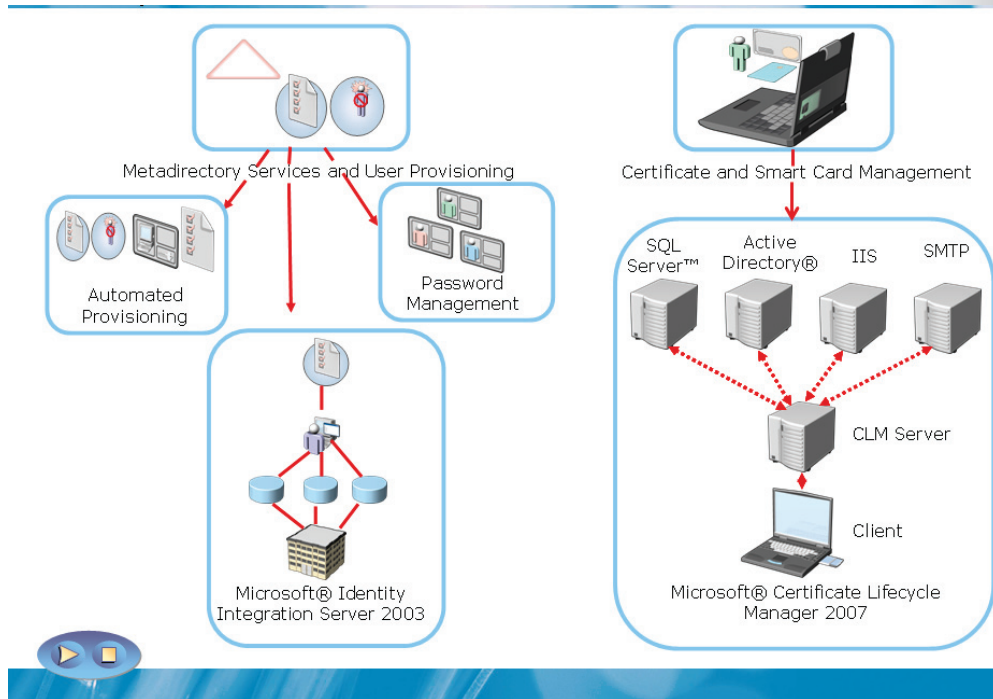
Lesson 3

Overview of ILM 2007

- Components of ILM 2007
- Infrastructure Requirements for ILM 2007
- Identity Integration by Using MIIS
- Identity Management Process by Using MIIS
- Working of CLM 2007
- The Smart Card and Certificate Life Cycle

Microsoft® ILM 2007 simplifies managing the life cycle of a user's digital identity by using various built-in components. ILM 2007 is comprised of Microsoft® Identity Integration Server (MIIS) 2003 and CLM 2007. Before you use ILM 2007, you must have the necessary infrastructure in place. You can use MIIS 2003 for identity integration and management. You can also use Microsoft® Certificate Lifecycle Manager (CLM) 2007, for smart card and certificate life cycle management. smart card

Components of ILM 2007



Key Points

- ILM 2007 provides an integrated, comprehensive product that builds on MIIS 2003.
- MIIS 2003 and CLM 2007 are packaged in a common product called ILM 2007.
- ILM 2007 simplifies management of a user's digital identity by keeping identity information synchronized. This information remains constant across a wide range of directories, databases, and proprietary identity systems.
- In addition, ILM 2007 provides a place to manage the entire life cycle of user credentials such as certificates and smart cards.
- Key features of ILM 2007 include identity synchronization, provisioning or deprovisioning, and certificate and smart card management.



For more information, see Microsoft® ILM 2007.

Infrastructure Requirements for ILM 2007

Hardware Requirements



- 1 GHZ or Faster Processor; Pentium IV Recommended
- 512 MB of RAM or Higher; 1 GB or More Recommended
- 8 GB of Available Hard-disk Space on an NTFS Partition

Software Requirements



- Windows Server® 2003 Enterprise Edition or later
- .NET Framework 2.0
- CLM 2007 Requires Certificate Services
- SQL Server™ 2005 Standard or Enterprise Edition or Later Recommended



Key Points

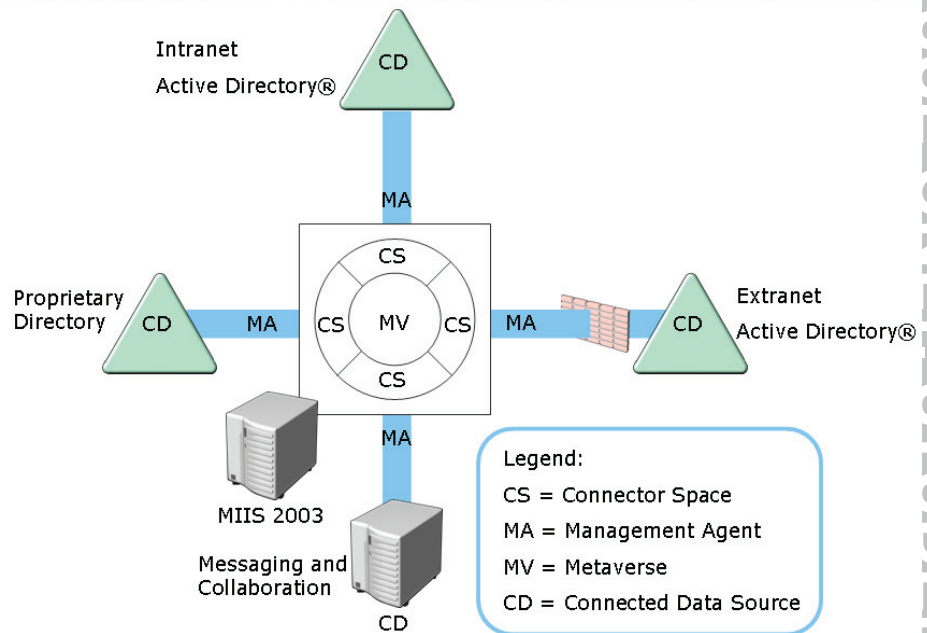
- Software requirements:
 - Windows Server® 2003 Enterprise Edition
 - Windows Server® 2003 Client Access Licenses (CALs)
 - Microsoft® SQL Server™ 2005 or 2000, Standard or Enterprise Edition Service Pack 3 (SP3)
 - .NET Framework 2.0
 - CLM 2007 requires certificate services
 - Microsoft® Visual Studio® development system—to customize rules extensions

- Hardware requirements:
 - 1 gigahertz (GHz) processor, or faster processor such as Pentium 4, recommended
 - 512 MB of RAM or higher; 1 GB or more recommended
 - 350 MB of hard-disk space or more for the default installation and an additional 1 GB of hard disk space recommended for the log file
 - 8 GB of hard disk space on the partition that contains the database files for ILM 2007 metadirectory services and user provisioning
 - Certificate and smart card management hardware requirements include CLM-compatible smart cards and smart card readers



For more information, see Microsoft® ILM 2007 Frequently Asked Questions.

Identity Integration by Using MIIS



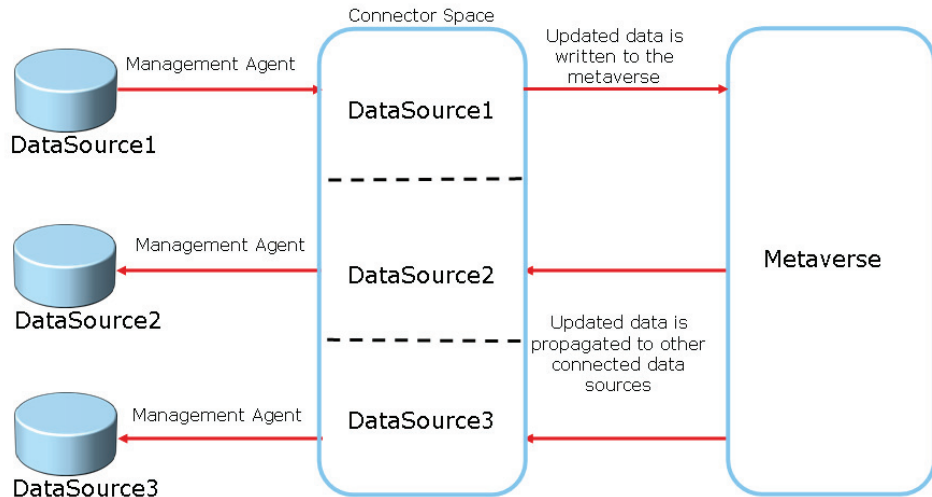
Key Points

MIIS 2003 can help synchronize and integrate identity information between similar and dissimilar data sources. The following table describes the components of MIIS.

Components	Description
Connected Data Source (CDS)	This component provides extensibility to develop additional connectors. There are 25 connectors to external identity stores out of the box.
Metaverse (MV)	This component is a data store that helps contain the aggregated identity information from multiple connected data sources. MV provides a single, global, integrated view of identity data staged in

Components	Description
	the connector spaces.
Connector Space (CS)	This component is a staging area that contains representations of the designated objects from a connected data source and the attributes specified in the attribute inclusion list. CS determines the change in the connected data source. In addition, it helps stage incoming changes.
Management Agent (MA)	This component links specific connected data sources to MIIS 2003. MA is responsible for moving data between a connected data source and MIIS.

Identity Management Process by Using MIIS



Key Points

MIIS 2003 uses state-based processing. This is the processing of the state or condition of identity information in MIIS 2003 at a particular time. MIIS 2003 organizes identity information that allows it to calculate the current state of identity information at any specified point in the identity management process.

Identity Management Process

Identity management process is divided into the following three processes:

- **Staging process.** Various data sources request identity information. MIIS 2003 compares received data to the data that is already staged in the connector space. If MIIS 2003 detects any changes, it either creates new staging objects or updates existing staging objects in the connector space for synchronization.
- **Synchronization process.** MIIS 2003 uses inbound and outbound synchronization rules to apply updates to identity information. During the

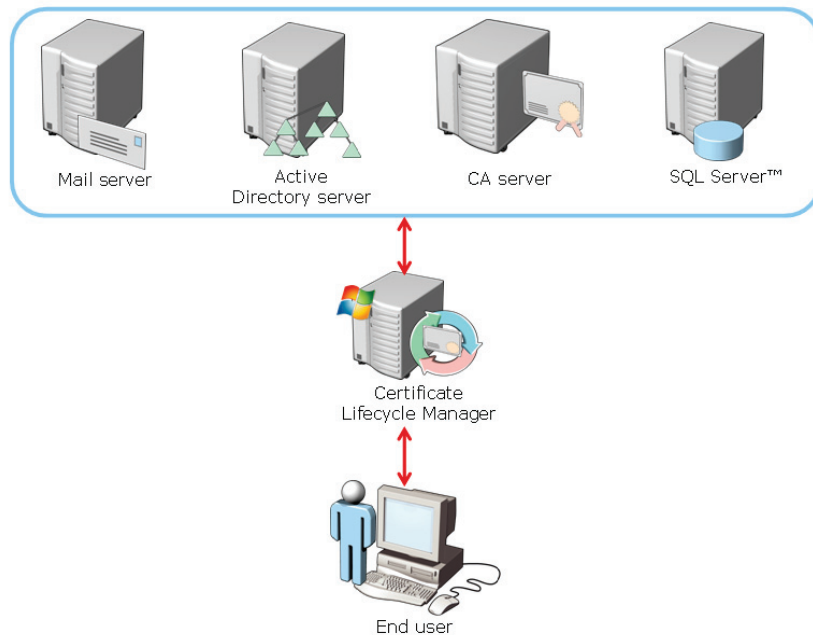
synchronization process, MIIS 2003 updates the metaverse to reflect changes that have occurred in the connector space. It then updates the connector space to reflect the changes that have occurred in the metaverse.

- **Export Process.** The connected data source imports the identity information. During the export process, MIIS 2003 pushes out changes that are staged on staging objects and are flagged as pending export.



For more information, see State-Based Processing in MIIS 2003.

Components of CLM 2007



Key Points

Microsoft® CLM 2007 is an identity-assurance management solution. CLM 2007 maximizes the trust and flexibility associated with digital certificates and smart cards. CLM 2007 manages all smart card functions and digital certificate functions after it is installed in the organization.

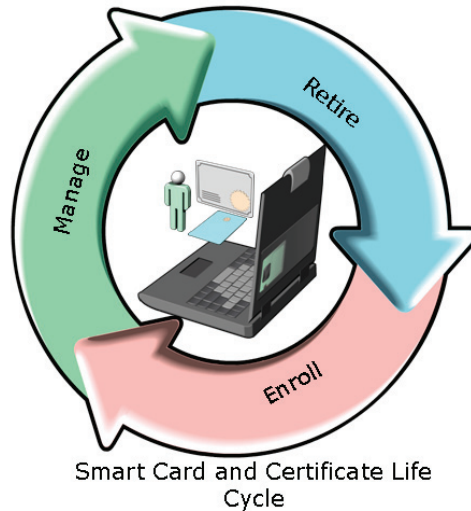
CLM 2007 provides certificate management for a specific CA. This solution also provides an aggregate view of multiple CAs by managing communication with managed CAs. CLM 2007 uses the following components to manage certificates:

- **CLM server-side components.** The server provides a Web interface and is the focal point of administrative functions. It implements all CLM functionality, and communicates with the CLM database, Active Directory®, and all managed CAs. The CLM server can exist as a dedicated server, can be shared with a CA server, or can be shared by other applications.
- **CLM certificate authority plug-in.** A CLM policy module and an exit module must be installed and configured locally on each CA server to actively manage

a CA. These modules communicate with the CLM server, control the behavior of the CA, and provide centralized logging and auditing.

- **CLM client-side components.** End-users and administrators can manage smart cards by providing a connection from a computer to a smart card. The user can manage smart cards by using the CLM client. The CLM client includes the following components:
 - **Smart card self-service control.** This component provides certificate management capabilities.
 - **Smart card personalization control.** This component provides Java card management.
 - **Bulk smart card issuance tool.** This component centralizes large scale smart card deployment scenarios.

Smart card and Certificate Life Cycle



Supported operations include:

- Smart card and certificate enrollment
- Recovery / card replacement
- Temporary card issuance
- Smart card PIN unblocking
- Manager approvals
- Smart card PIN change

Key Points

Smart cards are programmable devices that contain a built-in processor with secure storage space for data. The data can include private keys and public key certificates. Smart cards can be authenticated by using mechanisms such as personal identification numbers (PINs). They can be authorized to access only particular data on the card, or to carry out a particular range of activities by using the card. You can use Microsoft® CLM 2007 to manage smart cards and digital certificates.

CLM 2007 can automatically create a renewal request for certificates that are within the renewal time specified in a certificate template. You can also configure CLM 2007 to issue one-time passwords. If CLM 2007 is configured to issue one-time passwords, users automatically receive e-mail messages reminding them to renew their certificates. CLM 2007 performs all administrative tasks including smart card management through the CLM Web site. You can use CLM 2007 to perform the following management tasks:

- Search for a user, certificate, or certificate revocation list based on a specified search criterion.
- Find or unblock a smart card by searching for a specific smart card.
- View smart card details by using a smart card reader
- Approve pending requests, view the status of a pending request, or distribute passwords for one-time use to complete a request.
- Issue and print smart cards and distribute PINs to users.
- Issue and retire temporary smart cards.
- Change smart card PIN numbers.
- Manage and configure applications written specifically for use on smart cards.

Lab 1: Exploring IDA Solutions

- Exercise 1: Explore how Active Directory® Server Roles will provide IDA Management solutions

Estimated time: 60 minutes

Objectives

After completing the lab, you will be able to:

- Identify business requirements
- Determine server roles and solutions required to meet the business requirements

Scenario

NorthWind Traders is a large multinational corporation with office locations around the world. The company has recently implemented Windows Server® 2008 and an AD DS environment.

The organization is expanding its deployment of custom directory-enabled applications. One of the applications has unique identity requirements and uses custom attributes created in the directory service schema. Application developers

want to ensure that these applications can be tested without affecting the AD DS schema deployed within the production environment.

By using the implementation of directory-enabled applications, it is important that users only have a single network identity and password. This identity must be easily provisioned between the directory-enabled applications, the corporate HR database, and the production Active Directory® domain.

NorthWind Traders has recently started collaboration with a new business partner, Contoso, Ltd. NorthWind Traders has an intranet SharePoint® portal, and has developed a Web-based claims-aware application. Selected Contoso, Ltd. users need to access these applications securely. Contoso, Ltd. has an Active Directory® Domain Services (AD DS) infrastructure deployed and their entire user population logs on to AD DS. There are no external or forest trusts between NorthWind Traders and Contoso, Ltd. Both the organizations have perimeter networks.

The management of NorthWind Traders has expressed a concern that important documents and e-mail messages are not properly protected. This is true for e-mail messages both inside the enterprise network, and also when they leave the corporate network. As a result, being the system administrator, you need to explore options for providing additional security for managing digital content. The security team at NorthWind Traders has mandated the use of secure logon technologies, such as smart cards for specific scenarios that require strong authentication techniques, such as Virtual Private Network (VPN) or secure server access.

Consolidation requirements:

A system administrator, consider the following requirements when consolidating the design of Identity and Access (IDA) solutions:

- Identify business requirements to design the identity and access management solutions for NorthWind Traders.
- Determine solutions that are available to simplify and automate user provisioning.
- Determine a solution to help secure the use of digital content such as corporate documents and email.
- Determine a solution to synchronize identities between AD DS and the corporate HR database.

Exercise 1: Explore How Active Directory® Server Roles will Provide IDA Management Solutions

In this exercise, you will identify the server roles needed to satisfy the objectives for NorthWind Traders and Contoso, Ltd.

The main tasks for this exercise are as follows:

1. Identify business requirements.
2. Determine server roles and solutions required to meet the business requirements.

► Task 1: To identify business requirements

Question:

1. Identify the business requirements for NorthWind Traders.

► Task 2: To determine server roles and solutions required to meet the business requirements

Questions:

1. What server role or roles provide developers with an application test platform that allows schema changes independent of AD DS?
2. What server role or roles provide access to Web applications for an external partner organization without creating the trusts?
3. What account store works best when you implement Active Directory® Federation Services (AD FS)?
4. What server role or roles would you install to provide secure communication and access to the NorthWind Traders SharePoint® portal and the custom Web application?
5. What server role or roles would protect the confidential data of important corporate documents and e-mail messages?
6. What technology can help you to simplify and automate user provisioning?

7. What technology can you implement to synchronize identities from multiple identity stores, such as AD DS and custom HR databases?
8. What server role or roles are required for the implementation and management of smart cards?

Lab Review: Exploring IDA Solutions

In this lab, you have:

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

Lab Resources

There are no additional lab resources for this lab.

Module 2

Configuring AD CS

Contents:

Lesson 1: Overview of PKI	2-3
Lesson 2: Deploying a CA Hierarchy	2-14
Lesson 3: Installing AD CS	2-26
Lesson 4: Managing CA	2-35
Lab 2: Configuring AD CS	2-43

Module Overview

- Overview of PKI
- Deploying a CA Hierarchy
- Installing AD CS
- Managing CA

Public key infrastructure (PKI) is a set of technologies that help you secure corporate communications and transactions. Certification Authorities (CAs) are one of the components of a PKI infrastructure. You can use CAs to manage, distribute, and validate digital certificates that are used to secure information. You can install Active Directory® Certificate Services (AD CS) as a root CA or a subordinate CA in your organization. You can use certificate revocation lists (CRLs) to manage the validity of certificates within an organization.

Lesson 1

Overview of PKI

- What Is PKI?
- Managing IDA and Enhancing Security by Using PKI
- Components of a PKI Solution
- Validating Certificates by Using PKI Solutions
- How AD CS Supports PKI

PKI helps verify and authenticate the validity of each party involved in an electronic transaction. It also helps establish trust between the computers and the corresponding applications hosted on application servers. A common example includes the use of PKI technology in the security of electronic commerce Web sites. Digital certificates are key PKI components that contain electronic credentials used to authenticate users or computers. Moreover, certificates can be validated by using certificate discovery, path validation, and revocation checking processes. Windows Server® 2008 supports PKI by setting up and configuring Active Directory® Certificate Services (AD CS) components.

What Is PKI?

A Public Key Infrastructure (PKI):

- Is the combination of software, encryption technologies, processes, and services that enable an organization to secure communication and business transactions
- Relies on the exchange of digital certificates between authenticated users and trusted resources

PKI enhances infrastructure security by providing:

- Confidentiality
- Integrity
- Authenticity
- Nonrepudiation

Key Points

PKI is a combination of software, encryption technologies, processes, and services that facilitate an organization to secure its communications and business transactions.

The advantages of using PKI include:

- **Confidentiality.** PKI gives you the ability to encrypt both stored and transmitted data.
- **Integrity.** You can use a PKI to digitally sign data. A digital signature identifies if any data was modified while communicating information.
- **Authenticity and Nonrepudiation.** Authentication data passes through hash algorithms such as Secure Hash Algorithm 1 (SHA1), to produce a message digest. The message digest is then digitally signed by using the sender's private key to prove that the message digest was produced by the sender.

Nonrepudiation is digitally signed data, in which the digital signature provides both proof of the integrity of signed data, as well as proof of the origin of data.



For more information, see [Windows Server® 2008 technical library](#).

Discussion: Managing IDA and Enhancing Security by Using PKI

- What benefit would a PKI solution provide to your organization?
- Give a few examples of services that can use certificates to enhance security.
- How does PKI solution support IDA Management?

Key Points

The following table lists some applications of a PKI.

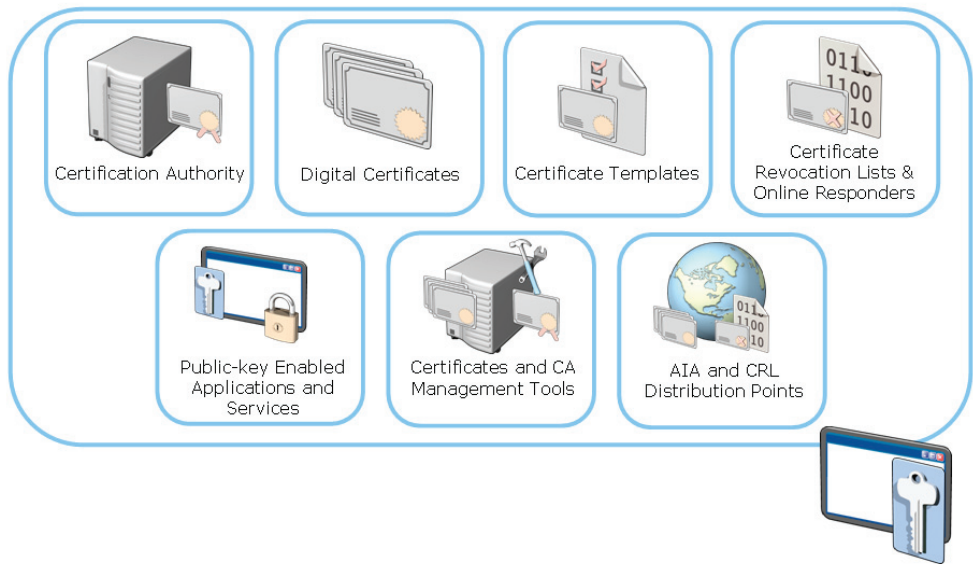
Application	Description
Smartcard logon	This application implements two-factor authentication.
Secure e-mail	This application provides confidential communication, data integrity, and nonrepudiation for e-mail messages.
Encrypting File System	This application allows users to store their data on the disk in an encrypted form.
Internet authentication	This application authenticates the client and server for transactions of a client-server transmission.
802.1X	This application allows only authenticated users to access

Application	Description
	a network. In addition, this application protects the transmitted data across a network.
Internet Protocol security (IPsec)	This application allows encrypted and digitally signed communication to pass between: <ul style="list-style-type: none"><li data-bbox="644 401 843 430">• Two computers.<li data-bbox="644 435 1182 465">• A computer and a router over a public network.



For more information, see **Windows Server® 2008 technical library.**

Components of a PKI Solution



Key Points

- **CA.** This component issues and manages certificates to users, services, and computers.
- **Digital certificates.** This component comprises electronic credentials associated with a public key and a private key that are used to authenticate users. Digital certificates are also used to validate computers and can even be used to ensure that software or code is being run from a trusted source.
- **Certificate templates.** This component describes the content and purpose of a digital certificate.
- **CRLs.** This component lists the certificates that are revoked by a CA before expiry.
- **Public key-based applications and services.** This component supports public key encryption for implementation of public key security.

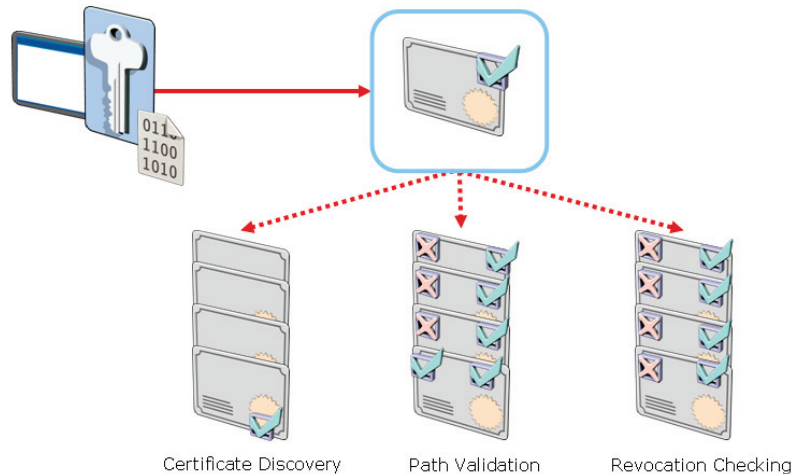
- **Certificate and CA Management tools.** This component provides command-line and GUI-based tools to:
 - Configure CAs.
 - Recover archived private keys.
 - Import and export keys and certificates.
 - Publish CA certificates and CRLs.
 - Manage issued certificates.
- **Authority Information Access (AIA) and CRL distribution points.** This component provides publication locations of certificates and CRLs.



For more information, see Windows Server® 2008 technical library.

Validating Certificates by Using PKI Solutions

- PKI-enabled applications use CryptoAPI to validate certificates.



Key Points

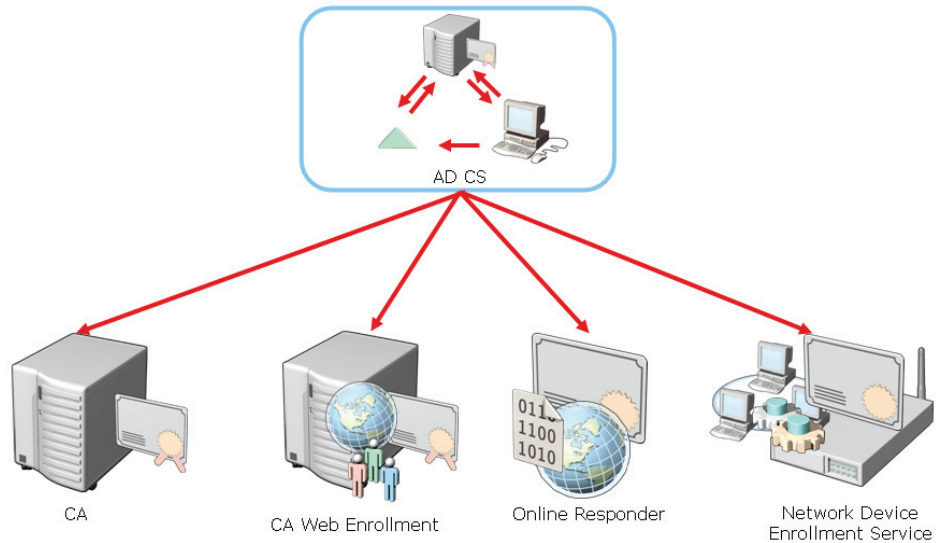
CryptoAPI is a set of application programming interfaces (APIs) that perform cryptographic operations, implement additional cryptographic providers, and create, store, and retrieve cryptographic keys. This API helps validate certificates in a PKI solution. The three distinct but interrelated processes of CryptoAPI include:

- **Certificate discovery.** In this process, all certificates are cached when the certificates are selected from a store or from a URL.
- **Path validation.** In this process, all certificates in a certificate chain are validated. It validates the certificates until the certificate chain terminates at a trusted, self-signed certificate.
- **Revocation checking.** In this process, each certificate in the certificate chain is examined. This examination helps verify that none of the certificates have been revoked.



For more information, see [Windows Server® 2008 technical library](#).

How AD CS Supports PKI



Key Points

AD CS allows setup and configuration of the following components:

Components	Description
CA	This component issues certificates to users, computers, and services. In addition, it manages certificate validity. Multiple CAs can be chained to form a PKI.
CA Web enrollment	<ul style="list-style-type: none"> This component enables users to connect to a CA by means of a Web browser to: <ul style="list-style-type: none"> Request and renew certificates. Retrieve CRLs. Download Root Certificate.
Online Responder	<ul style="list-style-type: none"> This component decodes revocation status requests for specific certificates, evaluates the status of these certificates,

Components	Description
	and returns a signed response containing the requested certificate status information.
Network Device Enrollment Service	<ul style="list-style-type: none">• This component allows routers and other network devices that do not have domain accounts to obtain certificates.



For more information, see [Windows Server® 2008 technical library](#).

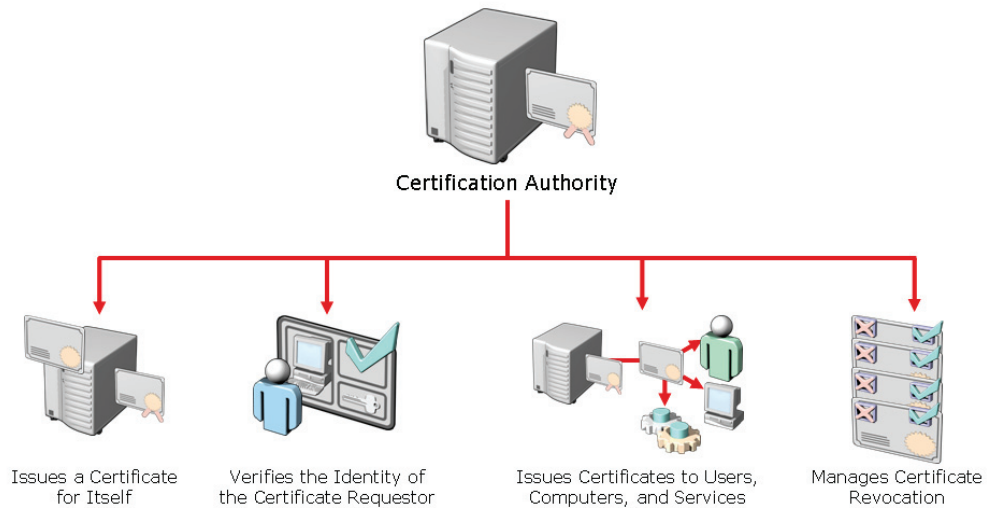
Lesson 2

Deploying a CA Hierarchy

- Overview of CA
- Options for Implementing CA
- Types of CAs
- Stand-Alone vs Enterprise CAs
- Usage Scenarios in CA Hierarchy
- What Is a Cross-Certification Hierarchy?

To deploy a CA hierarchy you need to be familiar with various management tasks that a CA provides to a Windows Server® 2008 network. Most organizations will deploy a CA using one of two ways; by using an internal private CA or an external public CA. Root CAs and subordinate CAs can be used for various scenarios such as increasing hierarchy scalability. CAs can also be categorized as either stand-alone CAs or enterprise CAs. You can use cross-certification to interoperate between businesses and between PKI and certificate-enabled products.

Overview of CA



Key Points

On a Windows Server® 2008 network, a CA is a computer that has the AD CS server role installed. A CA can sign and revoke certificates and can also publish AIA and CRL information about revoked certificates to ensure that users, services, and computers are issued certificates that can be validated.

On a Windows Server® 2008 network, a CA provides several management tasks including:

- Verifying the identity of the certificate requestor.
- Issuing certificates to requesting users, computers, and services.
- Managing certificate revocation.



For more information, see Windows Server® 2008 technical library.

MCT USE ONLY. STUDENT USE PROHIBITED

Discussion: Options for Implementing CA

- What are the advantages and disadvantages of using an external public CA?
- What are the advantages and disadvantages of using an internal CA?

Key Points

You can configure a CA for your company by using an internal private CA such as AD CS. Alternatively you can use an external third-party CA. Both have advantages and disadvantages as specified in the following table.

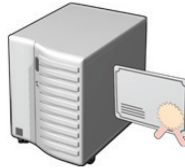
CA Type	Advantages	Disadvantages
Internal CA	<ul style="list-style-type: none">• It provides greater control over certificate management.• It is capable of using customized templates.	<ul style="list-style-type: none">• It is not as trusted as an external CA, by external clients.
External public CA	<ul style="list-style-type: none">• It is trusted by more external clients.• It requires minimal administration.	<ul style="list-style-type: none">• May have a higher cost as compared to an internal CA.



For more information, see [Windows Server® 2008 technical library](#).

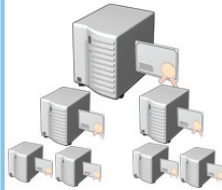
Types of CAs

Root CA



- Is the most trusted type of CA in a PKI infrastructure
- Is a self-signed certificate
- Issues certificates to other subordinate CAs
- Possesses physical security and the certificate issuance policy that are typically more rigorous than subordinate CAs

Subordinate CA



- Is issued by another CA
- Addresses specific usage policies, organizational or geographical boundaries, load balancing, and fault tolerance
- Issues certificates to other CAs to form a hierarchical PKI infrastructure

Key Points

The root CA is the one that is trusted by all other CAs in the hierarchy. The subordinate CAs are those that trust the root CA or any other parent CA. A trust is created when a subordinate server receives a certificate from a server that is hierarchically above the subordinate server. You can create a hierarchy of CAs to:











- Create CAs that specialize in generating certain types of certificates, or certificates for a specific purpose.
- Meet the needs of several divisions within an organization that might require various CA policies or specific administrator access.
- Improve performance.
- Restrict administrative access.

The root CA produces and signs its own certificate. The subordinate CA receives its CA certificate from the root CA or parent CA. Subordinate CAs work on activities

such as issuing certificates and implementing policies on a daily basis. Some of the benefits of creating a CA hierarchy include:

- Enhanced security and scalability.
- Flexible administration for the CA hierarchy.
- Support for commercial CAs.
- Support for most applications.

Stand-Alone vs. Enterprise CAs

Stand-Alone CAs		Enterprise CAs	
 <p>A stand-alone CA must be used if any CA (root or intermediate/ policy) is offline. This is because a stand-alone CA is not joined to an AD DS domain.</p>			Requires the use of Active Directory®
			Requires AD DS
			Can use Group Policy to propagate certificate to Trusted Root CA certificate store
	Users provide identifying information and specify type of certificate		Publishes user certificates and CRLs to AD DS
	Does not require Certificate templates		Issues certificates based upon a certificate template
	All certificate requests kept pending till administrator approval		Supports autoenrollment for issuing certificates

Key Points

As with other Active Directory® server roles, AD CS can be tightly integrated with AD DS. There are two main types of servers running AD CS, stand-alone and enterprise. The following table describes their characteristics.

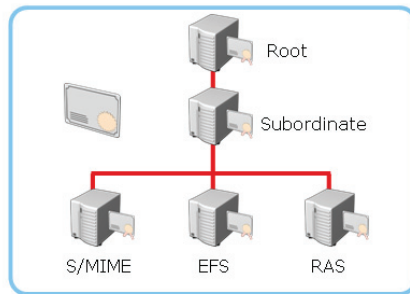
Stand-Alone CA	Enterprise CA
A stand-alone CA is typically used for offline CAs, but can be used for a CA that is consistently available on the network. An offline CA is a CA that is taken off the network to prevent a compromise of the keys that are used to sign certificates.	An enterprise CA is typically used to issue certificates to users, computers, and services.
This does not depend on the use of Active Directory® directory service and can be deployed in non-Active Directory®	This requires Active Directory®, and it can be used as a configuration and registration database and provides a publication point

Stand-Alone CA	Enterprise CA
environments or in network segments where Active Directory® cannot be contacted.	for certificates issued to users and computers.
By default, users can request certificates from a stand-alone certification authority only by using Web pages.	You can use the Certificate Request Wizard (which is started from within the Certificates snap-in), as well as certification authority Web pages, to request certificates from an enterprise certification authority. Certificates can also be issued automatically through group policy and autoenrollment.
By default, all certificate requests received by the stand-alone CA must be issued or denied by a certificate manager.	At an enterprise CA, certificate requests are issued or denied based on the Discretionary Access Control List (DACL) of the requested certificate template.

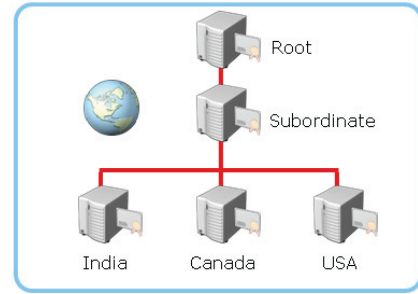


For more information, see Windows Server® 2008 technical library.

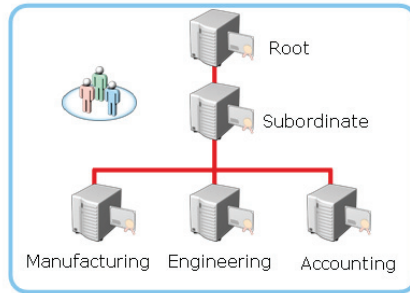
Usage Scenarios in a CA Hierarchy



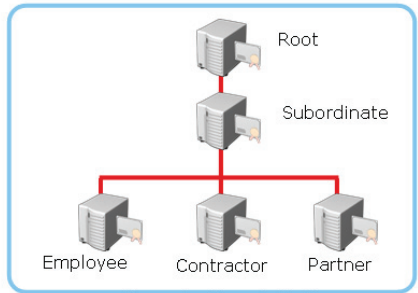
Certificate Use



Location



Departments



Organizational Unit

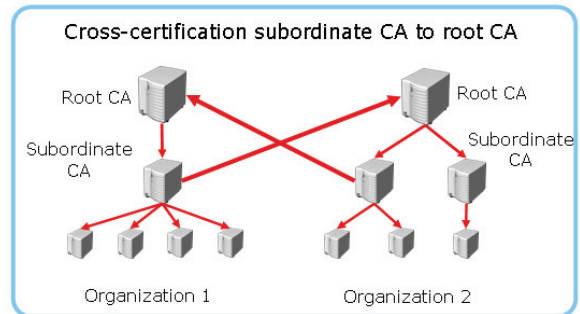
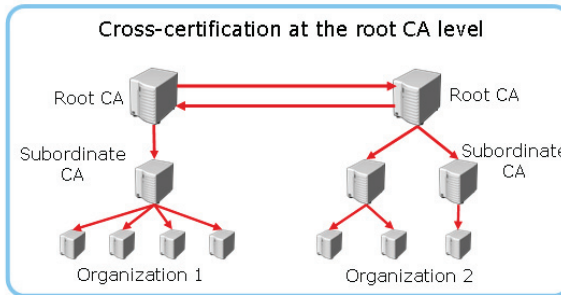
Key Points

The following points describe some usage scenarios in a CA hierarchy.

You can deploy subordinate CAs to:

- Service client certificate needs based on certificate usage such as Encrypting File System (EFS), Secure/Multipurpose Internet Mail Extension (S/MIME), and Remote Access Service (RAS).
- Help enhance performance of the hierarchy in geographically disparate network infrastructures.
- Service certificate needs of departmental users such as manufacturing and engineering.
- Service certificate needs of certain organizational unit users such as contractors, partners, and employees.

What Is a Cross-Certification Hierarchy?



Key Points

Cross-certification implies that each CA hierarchy's root CA provides a cross-certification certificate to the other CA hierarchy's root CA. The other hierarchy root CA installs the supplied certificate. By doing so, the trust flows down to all the subordinates CAs below the level where the cross-certification certificate was installed.

A cross-certification hierarchy provides the following benefits:

- Provides interoperability between businesses and between PKI products
- Joins disparate PKI organizations
- Assumes complete trust of a foreign CA hierarchy

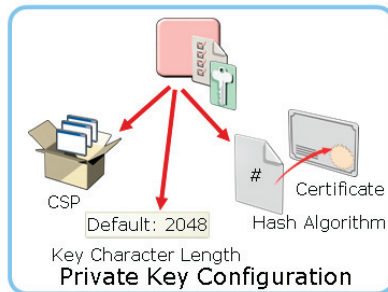
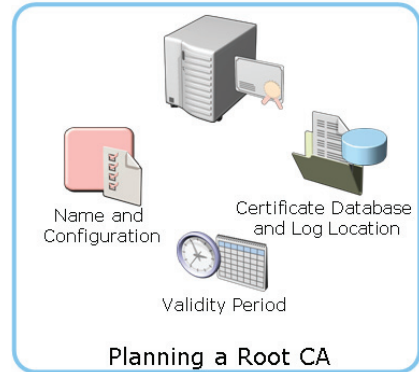
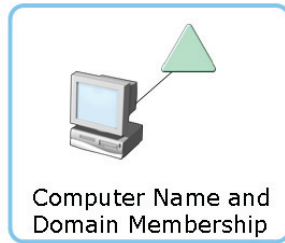
Lesson 3

Installing AD CS

- Considerations for Installing Root CA
- How To Install AD CS as Root CA
- Installing Subordinate CA
- How CAPolicy.inf File Is Used for Installation
- Overview of CA Administration Console

You can install AD CS as a root CA in an organization. After the root CA is installed, you can install a subordinate CA to apply policy restrictions and distribute certificates. You can also use a CAPolicy.inf file to help automate a CA installation and provide additional configuration settings that are not available with the Graphical User Interface (GUI)-based installation.

Considerations for Installing Root CA



Key Points

You must determine the computer's name and domain membership before installing a CA, which should be in the workgroup mode. This is because you cannot change the computer name or domain membership after installing the CA. You must plan for a number of configuration parameters before installing a root CA. You must plan the cryptographic configurations for a private key by using the considerations in the following table.

Consideration	Details
A cryptographic service provider (CSP) that is used to generate the new key	<ul style="list-style-type: none"> The default CSP is Microsoft® Strong Cryptographic Provider. Any provider that starts by using a number sign (#) in the name is a Cryptography API: Next Generation

Consideration	Details
	(CNG) provider.
The key character length	<ul style="list-style-type: none"> The default key length for Microsoft® Strong Cryptographic Provider is 2,048 characters. This is the recommended value for a root CA.
The hash algorithm used to sign certificates issued by a CA	<ul style="list-style-type: none"> The default value of the hash algorithm is SHA-1.
The validity period for certificates issued by a CA	<ul style="list-style-type: none"> The default value for certificates is five years.
The status of the root server—online or offline	<ul style="list-style-type: none"> The root certificate should be deployed as an offline CA. This enhances security and safeguards the root certificate.



For more information, see CNG.

Demonstration: How To Install AD CS as a Root CA

- To install the AD CS server role as an Enterprise Root CA

The instructor will provide a demonstration to show how you can install AD CS as a root CA.

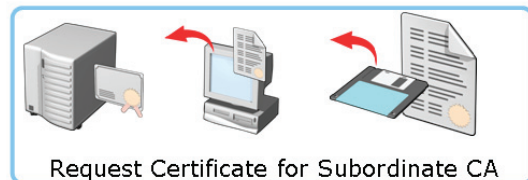
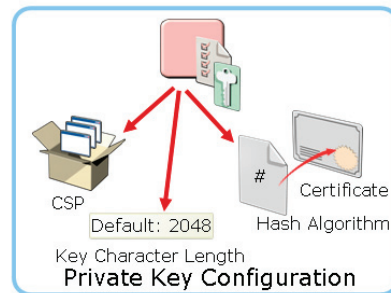
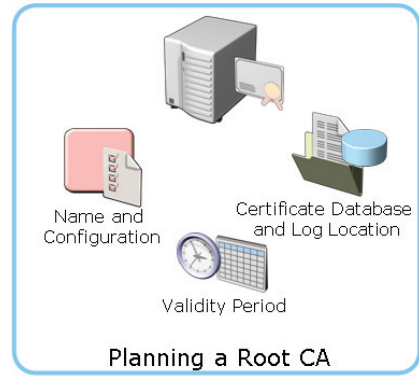
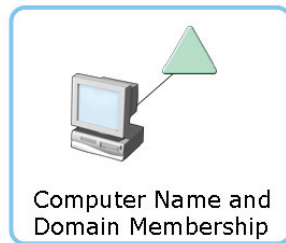
Questions:

1. Where does the root CA get its own certificate from?
2. If you desire an offline root CA, would you choose to install a stand-alone root or an enterprise root CA?



For more information, see CNG.

Considerations for Installing a Subordinate CA



Key Points

You can use a subordinate CA to implement policy restrictions for PKI and distribute certificates to clients. After you install a root CA for the organization, you can install one or more subordinate CAs.

If you use a subordinate CA to distribute certificates to users or computers who have an account in an Active Directory® domain, you can install the subordinate CA as an enterprise CA. You can then use the data of the client account in AD DS to distribute and manage certificates, and to publish certificates to AD DS.

You must be a member of the local administrators group or have equivalent permissions to complete this procedure. If the subordinate CA is an enterprise CA, you also need to be a member of the Domain Administrators group, or have equivalent permissions.



For more information, see CNG.

How CAPolicy.inf File Is Used for Installation

The CAPolicy.inf file is stored in the %Windir% folder of the root or subordinate CA. This file defines:

- Certification Practice Statement (CPS)
- Object Identifier (OID)
- CRL Publication Intervals
- CA Renewal Settings
- Key Size
- Certificate Validity Period
- CDP and AIA Paths

Key Points

You can use the CAPolicy.inf file when you install AD CS to define the following:

- **Certification Practice Statement (CPS).** Describes the practices that the CA uses to issue certificates
- **Object Identifier (OID).** Identifies a specific object or attribute
- **CRL publication intervals.** Defines the interval between publications for the base CRL
- **CA renewal settings.** Defines renewal settings such as the key length and the certificate validity period for an offline CA
- **Key size.** Defines the length of the key pair that you use during the root CA renewal
- **Certificate validity period.** Defines the validity period for a root CA

- **CRL Distribution Point (CDP) and AIA paths.** Provides the path that you use for root CA installations and renewals



For more information, see `CAPolicy.inf` syntax.

Demonstration: Overview of the CA Administration Console

- To open the CA administrative console and review the available options



The instructor will provide a demonstration to show how you can open the CA console and review the available options.

Questions:

1. Using the CA management tool, how would you manage a CA located on a different server?
2. How would you manage a remote AD CS server from a Windows Vista® client?

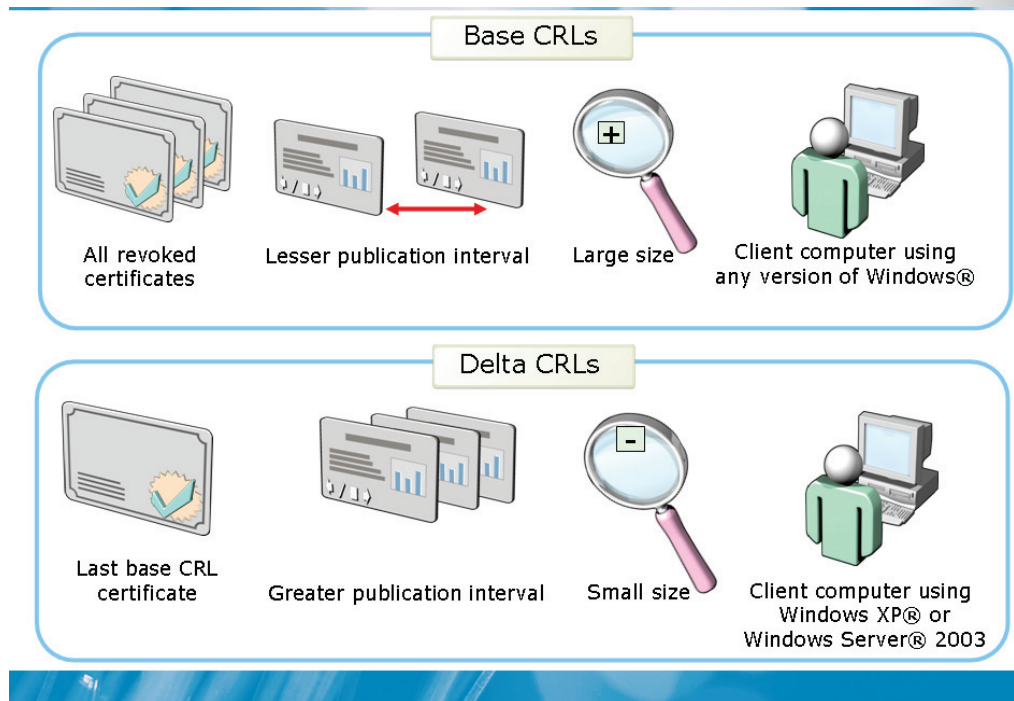
Lesson 4

Managing CA

- What Are CRLs?
- How CRLs Are Published
- Where to Publish AIAs and CDPs?
- Configuring AIA and CRL Availability

Managing a CA includes tasks such as publishing a CRL or configuring AIA and CRL availability. A CRL provides a list of every digital certificate that has been revoked within the PKI infrastructure. A CA can publish an updated CRL based on a configurable CRL publish schedule. If you plan to implement an offline Root CA, you might need to consider how you will ensure availability of the AIA and CDP extensions and apply the settings to all certificates that your root CA issues.

What Are CRLs?



Key Points

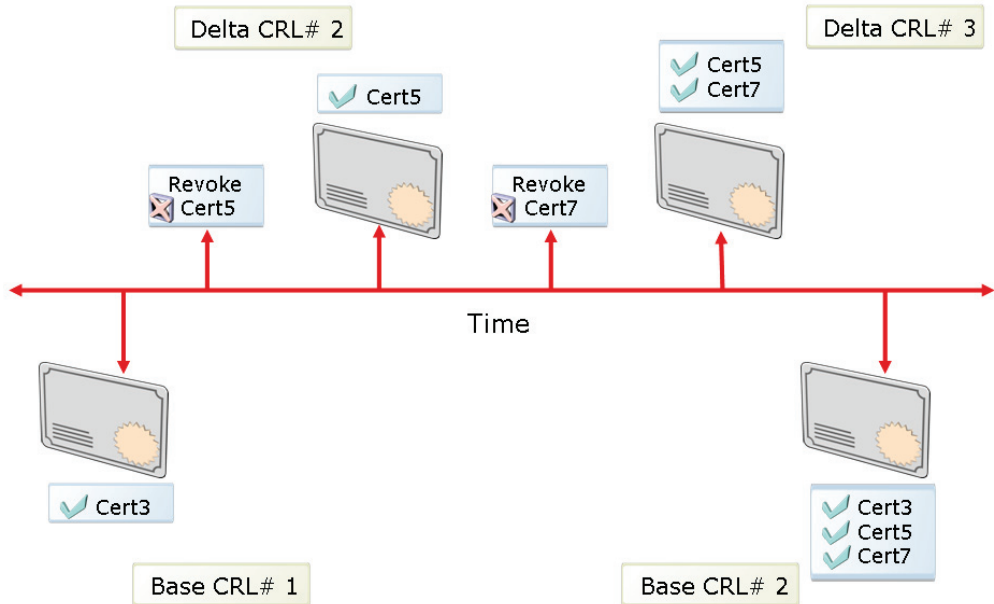
A CRL is a complete, digitally signed list of revoked certificates. Clients can retrieve and cache these lists on the basis of the configured lifetime of the CRL. You can use these lists to verify the revocation status of a certificate.

You can publish base CRLs periodically. If the CA issues and revokes many certificates, you might have to publish a large base CRL. To avoid publishing large base CRLs, you can publish delta CRLs. Delta CRLs are smaller, interim CRLs that contain only the certificates revoked since the last base CRL was published. Clients can retrieve the delta CRL and quickly build a complete list of revoked certificates. You can transfer delta CRLs faster than base CRLs. You can also use the delta CRLs to publish revocation data frequently.



For more information, see Windows Server® 2008 technical library.

How CRLs Are Published



Key Points

You can configure a CRL publication setting or a CRL publish period. The CRL publish period defines when a CA must automatically publish an updated CRL. When you first install a CA, the CRL publish period is set to one week. Later, you can configure the CRL publish period manually. The CA publishes the CRLs in the following sequence:

1. The CA publishes the initial base CRL (Base CRL#1) with one revoked certificate (Cert3).
2. The CA then revokes a certificate, Cert5.
3. The CA publishes the delta CRL (Delta CRL#2). The delta CRL includes Cert5.
4. The CA then revokes another certificate, Cert7.
5. When the CA publishes the updated delta CRL (Delta CRL#3), the delta CRL includes Cert5 and Cert7.

6. Finally, the CA publishes the next base CRL. The base CRL (Base CRL #2) contains the serial numbers for Cert3, Cert5, and Cert7.

7. Any new delta CRLs now include only certificates that have been revoked after the CA issued the base CRL, CRL#4.

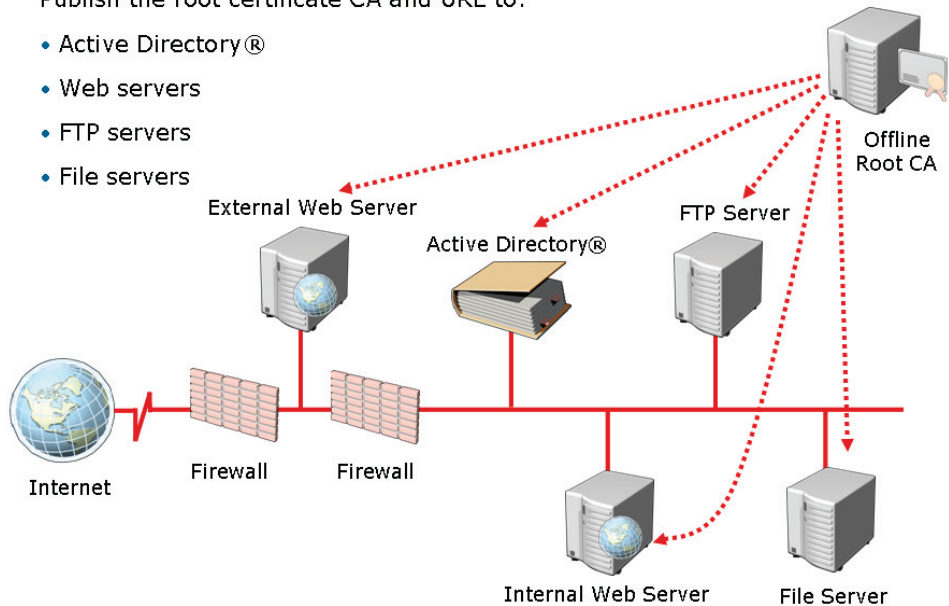


For more information, see [Revoking certificates and publishing CRLs](#).

Where to Publish AIAs and CDPs

Publish the root certificate CA and URL to:

- Active Directory®
- Web servers
- FTP servers
- File servers



Key Points

After you install a root CA, and if you plan to take this CA offline, you need to configure two X.509 version 3-extension fields. These extensions are known as the AIA and the CDP extensions and apply to all certificates that the root CA issues. These extensions define where client applications can locate AIA and CDP information for the root CA. The formatting and publishing of AIA and CDP extension URLs are generally the same for root CAs and subordinate CAs. You can publish the root CA certificate and the CRL to the following locations:

- Active Directory®
- Web servers
- File Transfer Protocol (FTP) servers
- File servers

Demonstration: How To Configure AIA and CRL Availability

- To configure AIA and CDP settings
- To publish the latest version of the CRL
- To publish the CRL and CA certificate for the offline root CA to an HTTP location
- To view the CRL
- To publish the CRL and CA certificate to Active Directory®

The instructor will provide a demonstration to show how you can specify CA certificate access points in issued certificates.

Questions:

1. How do you manually publish the CRL?
2. How would you schedule the publication of the certificate revocation list?



For more information, see [Checklist: Creating a certification hierarchy with an offline root CA](#).

Lab 2: Configuring AD CS

- Exercise 1: Installing the AD CS Server Role
- Exercise 2: Issuing and Installing a Subordinate Certificate
- Exercise 3: Publishing the CRL

Logon information

Virtual machine	6426A-NYC-DC1 6426A-NYC-SVR1
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 40 minutes

Objectives

After completing the lab, you will be able to:

- Install the AD CS server role
- Issue and install a subordinate certificate
- Publish the Certificate Revocation List (CRL)

Scenario

Woodgrove Bank is a multinational corporation with offices located in five countries. The organization is currently running Windows Server® 2003 but is planning to implement Windows Server® 2008. The bank has decided to deploy a

Public Key Infrastructure (PKI) solution by using Windows Server® 2008 Active Directory® Certificate Services (AD CS).

Consolidation requirements:

As the corporate server technology specialist, you have to install and configure Windows Server® 2008 computers in the organization to support certificate services. To do so, you must perform the following actions:

- Install and configure the AD CS server role on a Windows Server® 2008 server
- Configure the server as a root Certification Authority (CA)
- Install a subordinate server and configure the server to distribute certificates by using a Web interface
- Change the default CRL publishing metrics, manually publish the CRL, and then view the CRL for the WoodGroveCA Certificate Authority

Exercise 1: Installing the AD CS Server Role

In this exercise, you will use the available virtual computer environment. Before you begin the exercise, you must:

- Start the 6426A-NYC-DC1 and 6426A-NYC-SVR1 virtual computers.
- Log on to both computers using the user name **Administrator** and the password **Pa\$\$w0rd**.

The main task for this exercise is as follows:

1. Install the AD CS server role with the CA role service.

► Task 1: To install the AD CS server role and configure it as a Standalone Root CA

- On the 6426A-NYC-DC1 virtual computer, install and configure AD CS by using appropriate selections in the Add Roles Wizard of the Server Manager. The following options should be selected for the CA role service:
 - Specify Setup Type: Standalone
 - Specify CA Type: Root CA
 - Set Up Private Key: Create a new private key
 - Configure Cryptography for CA: default settings for all configurations except for key character length set to 4096
 - Common name for this CA: WoodgroveCA
 - Validity Period: default
 - Configure Certificate Database: default

Exercise 2: Issuing and Installing a Subordinate Certificate

The main tasks for this exercise are as follows:

1. Install an enterprise subordinate CA with the Web enrollment role service.
2. Issue and install the subordinate certificate.
3. Install and verify the subordinate certificate.



▶ Task 1: To install an enterprise subordinate CA with the Web enrollment role service

- On the 6426A-NYC-DC1 virtual computer, install and configure AD CS by using appropriate selections in the Add Roles Wizard of the Server Manager. The following options should be selected:
 - Select Role Service: Certification Authority and Certification Authority Web Enrollment
 - Specify Setup Type: Enterprise
 - Specify CA Type: Subordinate CA
 - Set Up Private Key: Create a new private key
 - Configure Cryptography for CA: default settings for all configurations
 - Common name for this CA: WoodgroveIssuingCA
 - Request Certificate from Parent CA: WoodgroveCA
 - Configure Certificate Database: default

▶ Task 2: To issue and install the subordinate certificate

- On the 6426A-NYC-DC1 virtual computer, issue the pending subordinate certificate by using the **Certification Authority** console.

▶ Task 3: To install and verify the subordinate certificate

- On the 6426A-NYC-SVR1 virtual computer, start the **Certification Authority** console.
- Right click **WoodgroveIssuingCA**, click **All Tasks**, and then click **Install CA Certificate**.
- On the **Select file to complete CA installation** page, click **Cancel**.

- In the **CA Certificate Request** dialog box, click **OK** to send an online request to the parent CA.
- Trust the root certificate and then start the certificate service.
- Open **WoodgroveIssuingCA** Properties and view the certificate. Notice the certificate was issued to **WoodgroveIssuingCA** by WoodgroveCA.

Exercise 3: Publishing the CRL

The main tasks for this exercise are as follows:

1. Examine the default Continuous Data Protectors (CDPs) and configure the CRL publication interval.
2. Publish the CRL manually.

► **Task 1: To examine the default CDPs and configure the CRL publication interval**

- On the 6426-NYC-SVR1 virtual computer, in the **Certification Authority** console, refer to properties of WoodGroveIssuingCA.
- By using the **Extensions** tab, examine the default CRL publication intervals.
- Use the Revoked Certificates properties to configure the CRL publication interval to be 1 Month and configure the Publish Delta CRL interval to be 3 days.



► **Task 2: To publish the CRL manually**

- On the 6426A-NYC-SVR1 virtual computer, right-click **Revoked Certificates** and publish the CRL.
- Open the intranet site <http://nyc-svr1/certenroll/WoodGroveIssuingCA.crl> address.
- Add the site to the Trusted Sites.
- Open and view the CRL.
-



After completing this exercise, turn off all virtual computers and Discard Undo disks.

Lab Review: Configuring AD CS

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

Lab Resources

There are no additional lab resources for this lab.

Module 3

Deploying and Managing Certificates

Contents:

Lesson 1: Deploying Certificates by Using AD CS	3-3
Lesson 2: Deploying Certificates by Using Autoenrollment	3-15
Lesson 3: Revoking Certificates	3-19
Lesson 4: Configuring Certificate Templates	3-30
Lesson 5: Configuring Certificate Recovery	3-42
Lab 3: Deploying and Managing Certificates	3-53

Module Overview

- Deploying Certificates by Using AD CS
- Deploying Certificates by Using Autoenrollment
- Revoking Certificates
- Configuring Certificate Templates
- Configuring Certificate Recovery

Active Directory® Certificate Services (AD CS) is used to deploy and maintain certificates within your public key infrastructure (PKI). You can use AD CS along with Web enrollment, Group Policy, autoenrollment, and network device enrollment service (NDES) to automatically enroll users and computers with certificates. You can distribute Certificates Revocation Lists (CRLs) or use online certificate status protocol (OCSP) to communicate certificate status for revocation. Certificate templates can be configured to use the appropriate types of keys and cryptographic service providers (CSPs) that are required for your PKI implementation. Finally, certificate recovery can be implemented by configuring a key recovery agent (KRA) certificate, and establishing KRA policies.

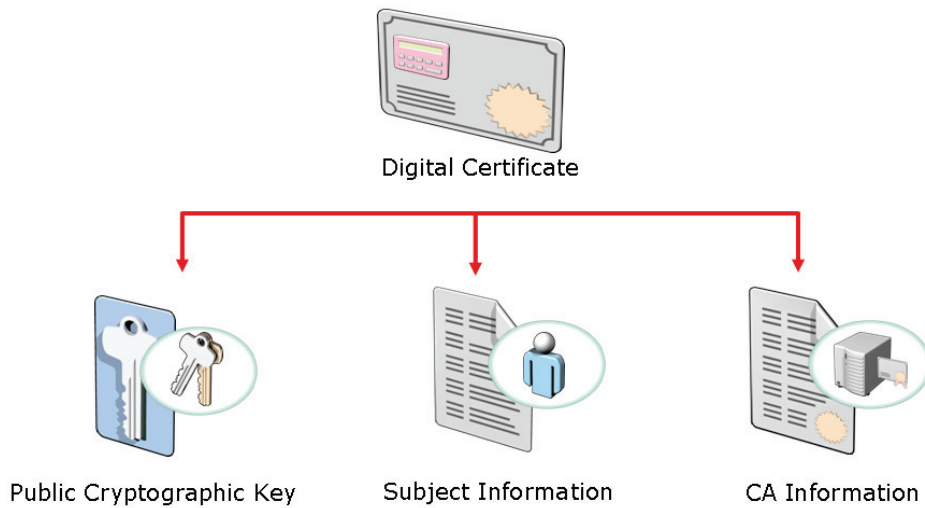
Lesson 1

Deploying Certificates by Using AD CS

- What Is a Digital Certificate?
- Overview of Certificate Life Cycle
- Certificate Enrollment Methods
- Obtaining Certificates by Using Web Enrollment
- Obtaining Certificates by Using Manual Enrollment
- How To Manually Obtain a Certificate for a Web Service
- What Is NDES?

Digital certificates are electronic credentials associated with public keys and a private key. Each certificate that you deploy goes through the cycle of request, generation, distribution, usage with application, and expiry, renewal, or revocation. To assist in your certificate deployment, you can select your choice of certificate enrollment method. To automatically deploy certificates, autoenrollment involves the configuration of technologies such as certificate templates and Group Policy. Therefore, in the absence of these technologies, you might decide to use manual or Web enrollment methods for obtaining certificates. If your infrastructure contains devices that support PKI, you may also consider the use of NDES to enroll certificates for those devices.

What Is a Digital Certificate?



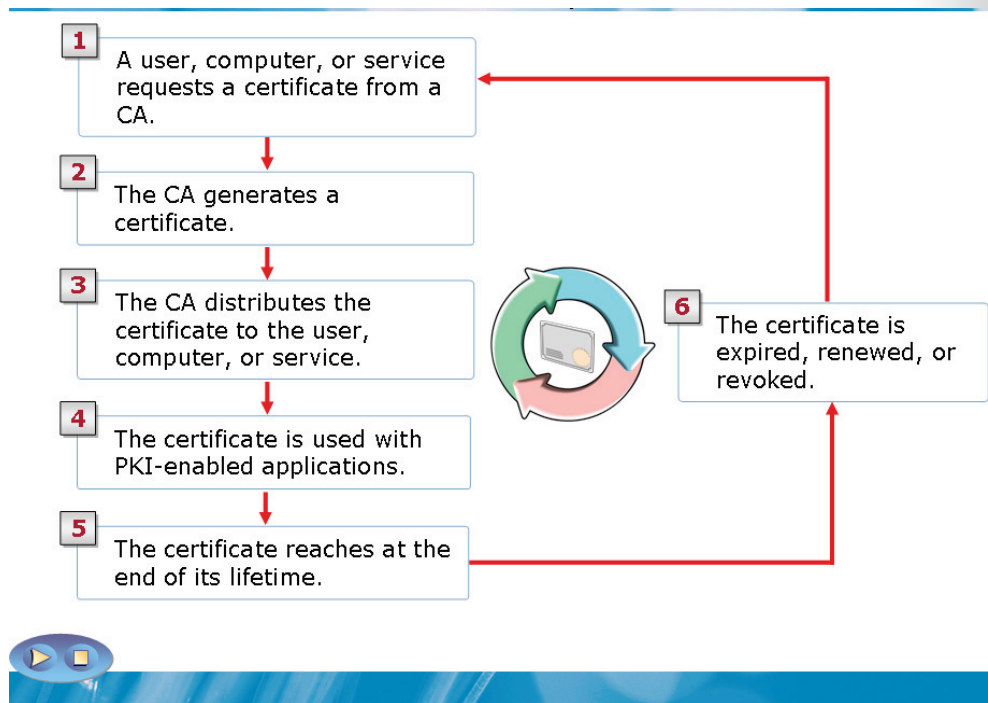
Key Points

Digital certificates are electronic credentials associated alongside a public key and a private key. You can use digital certificates to authenticate users. However, the possession of a digital certificate does not guarantee possession of the associated private key. You can also use digital certificates to validate computers and to ensure that any software runs from a trusted source.



For more information, see [Certificates](#).

Overview of Certificate Life Cycle



Key Points





1. The Certification Authority (CA) receives a certificate request.
2. The CA generates a certificate.
3. The requested certificate is issued to the corresponding user, computer, or service.
4. The certificate is utilized when the user, computer, or service works on a PKI-enabled application.
5. The used certificate expires.
6. The certificate at this point might:
 - **Expire.** If the validity period of the certificate is terminates, the certificate expires.

- **Renew.** The certificate is renewed and may or may not use the existing key pair.
- **Revoke.** You can revoke a certificate before the certificate reaches the end of the validity period. You can renew the certificate to start its validity period again.



For more information, see [Certificate life cycle](#).

Certificate Enrollment Methods

Method	Use
 <p>Autoenrollment</p>	<ul style="list-style-type: none"> To automate the request, retrieval, and storage of certificates for domain-based computers
 <p>Manual Enrollment</p>	<ul style="list-style-type: none"> To request certificates by using the Certificates console or Certreq.exe, when the requestor cannot communicate directly with the CA
 <p>Web Enrollment</p>	<ul style="list-style-type: none"> To request certificates from a Web site located on a CA To issue certificates when autoenrollment is not available
 <p>Enrollment Agents</p>	<ul style="list-style-type: none"> To provide a CA administrator the right to request certificates on behalf of another user

Key Points

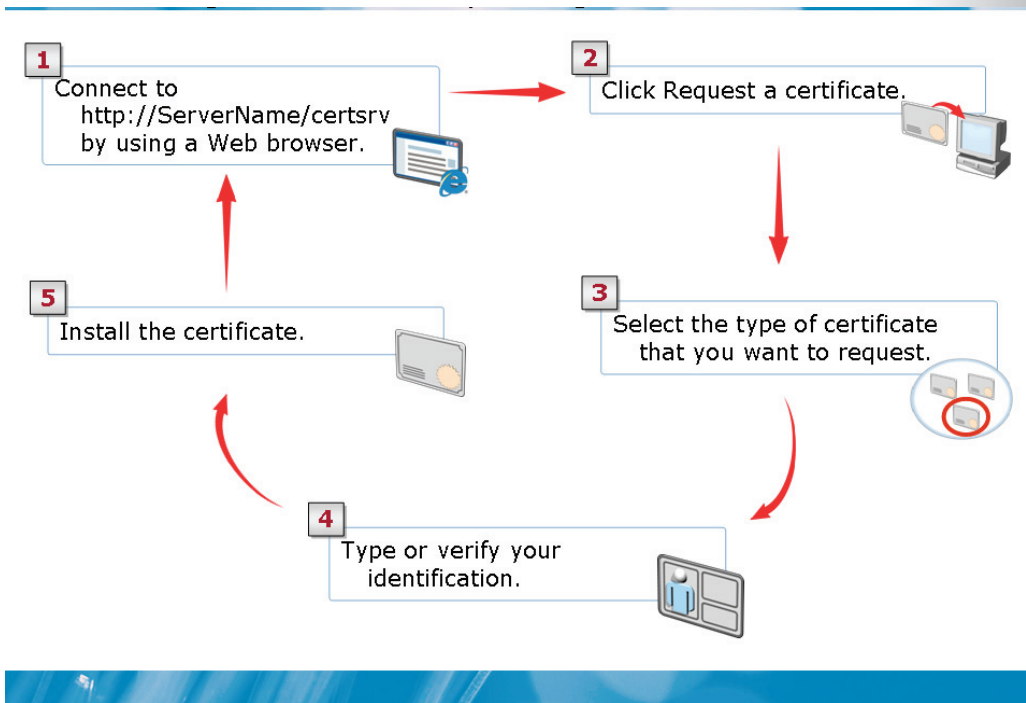
Enrollment method	Description
Autoenrollment	By using this method, the administrator defines the permissions and the configuration of a certificate template. These definitions help the requestor to automatically request, retrieve, and renew certificates without end-user interaction. This method is used for Active Directory® Domain Services (AD DS) domain computers. Autoenrollment settings in Group Policy must be configured. The certificate must be configured for autoenrollment through group policy.
Web enrollment	By using this method, you can enable a Web site CA so that users can obtain certificates. To use Web enrollment, you must first install Internet Information Services (IIS) and Web enrollment role on the CA of AD CS. To obtain a certificate, the requestor can log on to the

Enrollment method	Description
	<p>Web site, select the appropriate certificate template, and then submit a request. The certificate is automatically issued if the user has the appropriate permissions to enroll for the certificate.</p> <p>The Web enrollment method should be used to issue certificates when autoenrollment is cannot be used. This can happen in case of an Advanced Certificate request. However, there can also be cases where autoenrollment can be used for certain certificates, but not for all.</p>
Manual enrollment	<p>By using this method, the private key and a certificate request is generated on a device, such as a Web service or a computer. The certificate request is then transported to the CA to generate the certificate that is requested. The certificate is then transported back to the device for installation.</p> <p>This method is used when the requestor cannot communicate directly with the CA or if the device does not support autoenrollment.</p>
Enrollment agents	<p>By using this method, a Windows® CA administrator creates an enrollment agent account for a user. The user with enrollment agent rights can then enroll for certificates on behalf of other users.</p> <p>For example, if you need to allow a manager to preload logon certificates of new employees on smart cards.</p>



For more information, see [Selecting a certificate enrollment and renewal method](#).

Obtaining Certificates by Using Web Enrollment



Key Points

The Web enrollment Web site is located on the path, `http://ServerName/certsrv`. You can use the following steps to request a certificate by using the Web enrollment Web site:

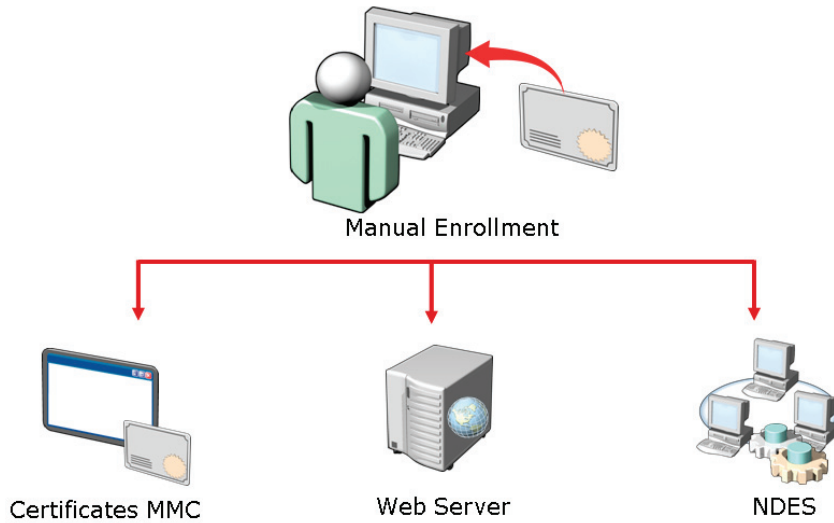
1. In Internet Explorer, in the Address bar, type **`http://ServerName/certsrv`**. Here, `ServerName` is the name of the Web server running Windows Server® 2008 that hosts the CA.
2. Click **Request a certificate**.
3. On the **Request a Certificate** page, do one of the following:
 - a. To enroll a user certificate, click **User Certificate**.
 - b. To enroll any other certificate, click **Advanced Certificate Request**. On the **Advanced Certificate Request** page, you can submit a request to the CA that indicates the certificate template, CSP, and other attributes of the requested certificate.

4. Type the required identification information.
5. On the **Certificate Issued** Web page, click **Install this certificate**.



For more information, see [How to obtain a digital certificate using the Web enrollment form](#).

Obtaining Certificates by Using Manual Enrollment



Key Points

Enrollment Method	Description
Certificates Microsoft® Management Console (MMC)	<p>The certificates snap-in is a multipurpose tool to manage certificates for a user, computer, or service. You can use the snap-in tool to determine what certificates stored on a computer, the stored location of the certificates, and the certificate configuration options.</p> <p>In addition, you can use the snap-in tool for the following tasks to:</p> <ul style="list-style-type: none"> • Enroll for new certificates • Renew existing certificates • Find certificates • Import certificates • Export or back up certificates

Enrollment Method	Description
Requesting a Certificate for services such as Web Servers	If IIS is installed on the CA of AD CS, you can enable a Web site on the CA. The CA-enabled Web site provides a single Web interface for users to obtain certificates, renew certificates, and retrieve certificate revocation lists.
NDES	The NDES is a communication protocol that is the implementation of the Simple Certificate Enrollment Protocol (SCEP). You can use SCEP to access routers and switches firmware that cannot be authenticated on the network and cannot enroll for X.509 certificates from a CA.

Demonstration: How To Manually Obtain a Certificate for a Web Service

- To use IIS and perform Web site enrollment by using one of the manual enrollment methods

The instructor will provide a demonstration to show how you can use IIS and perform Web site enrollment by using a manual enrollment methods.

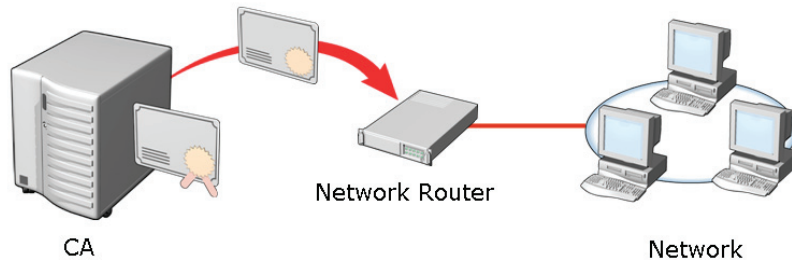
Questions:

1. When you enable Web enrollment on the certificate server, how will you use the Web interface to obtain certificate services?
2. When will you prefer to use Web enrollment method to issue certificates?



For more information, see [How to obtain a digital certificate using the Web enrollment form](#).

What Is NDES?



NDES:

- Uses simple certificate enrollment protocol to communicate with compatible network devices such as routers and switches
- Implements IPsec typically
- Functions as an Active Directory® Certificate Services Role Service
- Requires Internet Information Services

Key Points

Some devices, such as routers and switches, may contain software that uses SCEP to enroll for X.509 certificates from a CA. NDES implements SCEP. You can use NDES as an Internet Server Application Programming Interface (ISAPI) filter on IIS that performs the following functions:

- Creates and provides one-time enrollment passwords to administrators
- Retrieves awaiting requests from the CA
- Collects and processes SCEP enrollment requests for the software that run on network devices



For more information, see Windows Server 2008 technical library.

Lesson 2

Deploying Certificates by Using Autoenrollment

- Benefits and Uses of Autoenrollment
- Functioning of Autoenrollment

One of the most common methods for deploying certificates is to use autoenrollment. This method provides an automated way to deploy certificates to both users and computers within the PKI infrastructure. Autoenrollment can be used in environments that meet specific requirements such as the use of certificate templates and Active Directory® Group Policy.

Discussion: Benefits and Uses of Autoenrollment





- How can autoenrollment simplify certificate management in your organization?
- What are the examples of applications that can benefit from autoenrollment?



Questions:

- How does autoenrollment simplify certificate management in your organization?
- What are the examples of applications that can benefit from autoenrollment?

Functioning of Autoenrollment

 <p>Certificate Template</p>	<p>A certificate template is configured to allow, enroll, and autoenroll permissions for users who receive the certificates.</p>
 <p>Certificate Authority</p>	<p>The CA is configured to issue the template.</p>
 <p>GPO</p>	<p>An Active Directory® Group Policy Object (GPO) is created to enable autoenrollment. The GPO is linked to the appropriate site, domain, or organizational unit.</p>
 <p>Client Machine</p>	<p>The client machine receives the certificates during the next Group Policy refresh interval.</p>

You can use autoenrollment to automatically deploy public key-based certificates to users and computers in an organization. The Certificate Services administrator duplicates a certificate template and configures the permissions to allow Enroll and Autoenroll permissions for the users that will receive the certificates. Domain-based group policies, such as computer-based and user-based policies, can activate and manage autoenrollment.

By default, the Group Policy is applied when you restart computers, or at logon for users. By default, the Group Policy is also refreshed periodically. This Group Policy setting is named as Certificate Services Client - Auto-Enrollment.

An internal timer triggers autoenrollment every eight hours after the last autoenrollment activation. The certificate template might specify user interaction for each request. For such a request, a pop-up balloon appears approximately 60 seconds after the user logs on.



For more information, see [Certificate autoenrollment in Windows Server® 2003](#).

Lesson 3

Revoking Certificates

- Reason Codes for Revoking a Certificate
- How To Revoke a Certificate
- What Is an Online Responder?
- How Online Responders Work
- Steps to Configure an Online Responder
- How To Configure an Online Responder

During your certificate management process, there will be times that you may need to revoke certificates. There may be a number of reasons for revoking certificates such as if a key becomes compromised, or if someone leaves the organization. You need to ensure that network clients are able to determine which certificates are revoked before accepting authentication requests. To ensure scalability and high availability, you can deploy the AD CA Online Responder, which can be used to provide certificate revocation status.

Reason Codes for Revoking a Certificate

Reason Code	Description
Key Compromise	A computer is stolen or a smart card is lost.
CA Compromise	A CA certificate is compromised.
Challenge of Affiliation	An employee is terminated or suspended.
Superseded	An issued certificate is replaced.
Cease of Operation	A smart card has failed or the legal name of a user has changed.
Certificate Hold	A certificate is put on hold temporarily.
Unspecified	A certificate is revoked without providing a reason.

Key Points

Reason Code	Description
Key compromise	You use this reason code when an unauthorized user can access a token or disk location for a private key of a certificate. For example, you can use this reason code when a laptop is stolen or a smart card is lost.
CA compromise	You use this reason code when an unauthorized user can access the token or disk location for the private key of a CA. When you revoke a CA's private key, all certificates that the CA signed by using the private key are revoked.
Affiliation change	You use this reason code when the user resigns from, or is terminated by the organization. The reason code is indicated in the distinguished name (DN) attribute of the certificate. You do not have to revoke a certificate when a user changes

Reason Code	Description
	departments, unless your security policy requires that the departmental CA issue a different certificate.
Superseded	You use this reason code when you issue a replacement certificate to a user. The superseded code must also not include earlier reasons for certificate revocation. For example, you can use this reason code when a smart card fails or when a user forgets the password for a token. In addition, you can use the superseded code when the legal names of users have been modified.
Cessation of operation	You use this reason code when you decommission a CA. You should not revoke a CA's certificate if the CA does not issue new certificates, but still publishes CRLs for the currently issued certificates.
Unspecified	You can use this reason code to revoke a certificate without providing a reason. However, it is not recommended because this reason code does not provide the reason for certificate revocation.



For more information, see [Certificate revocation and status checking](#).

Demonstration: How To Revoke A Certificate

- To revoke a certificate that has been issued previously

The instructor will provide a demonstration to show how you can revoke a certificate.

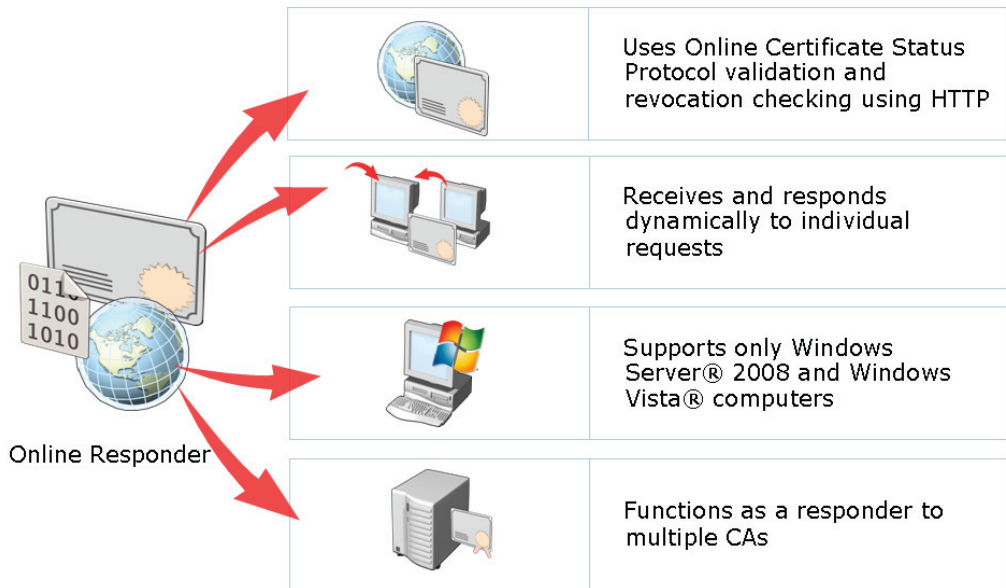
Questions:

1. What are some reasons that you would need to revoke an issued certificate?
2. Is it possible to reverse a revocation on a certificate?



For more Information, see [Revoke an issued certificate](#).

What Is an Online Responder?



Key Points

By using OCSP, an Online Responder provides clients an efficient method to determine the revocation status of a certificate. OCSP submits certificate status requests by using HTTP.

Clients access CRLs to determine the revocation status of a certificate. CRLs might be large and clients might utilize a large amount of time to search through these CRLs. An Online Responder can search these CRLs for the clients and respond only to the requested certificate.

You can use a single Online Responder to determine revocation status information for certificates issued by a single CA or multiple CAs. However, you can use more than one Online Responder to distribute CA revocation information.

You can install an Online Responder on any computer that runs Windows Server® 2008 Enterprise or Windows Server® 2008 Datacenter. A CA on a computer that runs Windows Server® 2008 or Windows Server® 2003, or a non-Microsoft® CA

issues the certification revocation data. An Online Responder and a CA should be installed on different computers.

For scalability and high availability, you can deploy the Online Responder on a single computer or on a software cluster that contains one or more computers. In addition, you can configure arrays of multiple linked computers that host Online Responders and process certificate status requests. You can monitor and manage each member of the Array independently. To configure the Online Responder, you must use the Online Responder management console.

You must configure the CAs to include the Online Responder's URL in the authority information access extension of issued certificates. The OCSP client uses this URL to validate the certificate status. You must also issue the OCSP Response Signing certificate template so that the Online Responder can enroll that certificate.



For more information, see [AD CS Online Responder](#).

How Online Responders Work



An application verifies a certificate that contains locations to OCSP responders.



The Online Responder receives a request through HTTP, if a cached OCSP response is not found.



The Online Responder Web proxy component decodes and verifies the request.



The Online Responder takes the request and checks a local CRL.



The Web proxy encodes and sends the response back to the client.

Key Points

The following steps describe the working of an Online Responder:

1. An application validates a certificate containing OCSP responders' locations. Initially, the client component locates a cached OCSP response that contains the revocation data in the local memory and disk caches.
2. If the client component does not locate a cached OCSP response, the Online Responder receives a request through HTTP.
3. The Online Responder Web proxy component decodes and validates the request. If the request is valid the required revocation information is searched for in the Web proxy cache. If the required information is not in the Web proxy cache, the request is send to the Online Responder.
4. The Online Responder accepts the request and searches a local CRL. If the certificate is not listed in the local CRL, the revocation provider obtains an

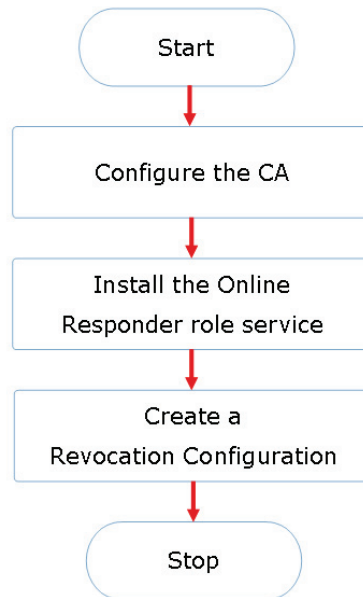
updated CRL from the revocation configuration locations. The Online Responder is then provided the status.

5. The Web proxy sends an encoded response to the client and stores a copy of the response for a limited time interval.



For more information, see [AD CS Online Responder](#).

Steps to Configure an Online Responder



Key Points

To configure an Online Responder, you need to perform the following steps:

1. To configure the CA to support the Online Responder:
 - Enable the OCSP response signing certificate.
 - Configure autoenrollment.
 - Configure the Authority Information Access (AIA) to support the OCSP extension.
2. Install the Online Responder Role Service.
3. To create a revocation configuration:
 - Link the CA with the Online Responder.
 - Select a signing certificate.



For more information, see [AD CS Online Responder](#).

Demonstration: How To Configure an Online Responder

- To configure the CA to support the Online Responder
- To install and configure the Online Responder role service

The instructor will provide a demonstration to show how you can configure an Online Responder.

Questions:

1. Which tool can you use to configure the Online Responder?
2. Which server operating systems support installation of the Online Responder?
3. Can you use non-Microsoft® CAs with the Online Responder role service?



For more Information, see AD CS Online Responder.

Lesson 4

Configuring Certificate Templates

- What Are Certificate Templates?
- Certificate Template Versions
- Certificate Template Categories and Purposes
- Configuring Certificate Template Permissions
- Methods for Updating a Certificate Template
- How To Modify and Enable a Certificate Template



Certificate templates help define how a certificate is used and how it provides specific security. Windows® 2000 Enterprise CAs use version 1 certificate templates, Windows Server® 2003 supports version 2 templates, and Windows Server® 2008 supports version 3 certificate templates. Certificate template categories, users and computers can be used for single purpose and multiple purposes. You can assign Full Control, Read, Write, Enroll, and Autoenroll permissions to certificate templates. Moreover, you can update certificate templates by modifying the original certificate template or superseding existing certificate templates.

What Are Certificate Templates?

Certificate templates define the:

- Format and contents of a certificate
- Process of creating and submitting a valid certificate request
- Security principles that are allowed to read, enroll, or autoenroll for a certificate
- Permissions to read, enroll, autoenroll, or modify a certificate template



Key Points

- Enterprise CAs use certificate templates to define the format and content of certificates. The CAs use the certificate template to specify which users and computers can enroll for which types of certificates. They also use the certificate templates to define the enrollment process, such as auto-enrollment, enrollment only with authorized signatures, and manual enrollment.
- 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 auto-enroll for certificates based on the template.
- The certificate templates and their permissions are defined in Active Directory® through a forest-wide validity.
- If more than one Enterprise CA is running in the Active Directory® forest, permission changes have an impact on all Enterprise CAs.



For more information see, Active Directory® certificate server enhancements in Windows Server® 2008.

Certificate Template Versions

Version 1:

- Provided for backward compatibility
- Created by default when a CA is installed
- Cannot be modified or removed but can be duplicated to become Version 2 or 3 templates

Version 2:

- Allows customization of most settings in the template
- Several preconfigured templates are provided when a CA is installed

Version 3:

- Supports advanced Suite B cryptographic settings
- Includes advanced options for encryption, digital signatures, key exchange, and hashing
- Only supports Windows Server® 2008 and Windows Vista®

Key Points

- Windows® 2000 Enterprise CAs use version 1 certificate templates. You cannot modify these default certificate templates. However, you can change permissions for these templates to allow enrollment of the certificate template. When you install an Enterprise CA, the version 1 certificate templates are created by default.
- Windows Server® 2003 provides version 2 templates. You can customize several settings in these templates. The default installation provides several preconfigured version 2 templates. You can add version 2 templates based on the requirements of your organization. Alternatively, you can duplicate a version 1 certificate template to create a version 2 certificate template. You can then separately modify and secure the newly created version 2 certificate templates.
- Windows Server® 2008 provides version 3 certificate templates. These certificate templates support several features of Windows Server® 2008 CA,



such as specify 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 CNG encryption and hash algorithms for:
- Certificate requests
- Issued certificates
- Protection of private keys for key exchange and key archival scenarios
- To configure support for these new features, you can use the template property sheets in the certificate templates MMC of Windows Server® 2008.



For more information see, [Certificate template overview](#).

Certificate Template Categories and Purposes

Category	Single Purpose	Multiple Purpose
 <p>Users</p>	<ul style="list-style-type: none"> • Basic EFS • Authenticated Session • Smart Card Logon 	<ul style="list-style-type: none"> • Administrator • User • Smart Card User
 <p>Computers</p>	<ul style="list-style-type: none"> • Web Server • IPSec 	<ul style="list-style-type: none"> • Computer • Domain Controller

Key Points

Windows® Enterprise CAs use certificate templates to define the certificates that can be issued. These templates also define the intended use of the certificate. The certificate template is associated with a DACL that defines the security principals that have permissions to read, enroll, and configure the certificate template.

Certificate templates are the sets of rules and settings that define the:

- Format and content of a certificate based on the certificate's intended use. The intended purpose of a certificate may relate to users or computers, based on the types of security implementations required to use the PKI infrastructure.
- Process of creating and submitting a valid certificate request.


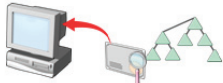
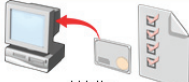


You need to configure the certificate templates on a CA. The CA then applies these templates against the incoming certificate requests. Windows Server® 2008 provides many default certificate templates for user and computer authentication, file encryption and Web server authentication.

In addition, you can use several preconfigured templates, such as code-signing, Internet Protocol security (IPSec) and enrollment agent's certificates, by adding them to the certificates templates folder. For example, if you need to configure a template for your needs, you can duplicate the template and customize its configuration.



For more information, see [AD CS certificate templates in Windows Server® 2008 whitepaper](#).

Configuring Certificate Template Permissions

Permission	Description
 <p>Full Control</p>	Allows a security principle to modify all attributes
 <p>Read</p>	Allows a security principle to find the certificate in Active Directory® when enrolling
 <p>Write</p>	Allows a security principle to modify all the attributes except permissions
 <p>Enroll</p>	Allows a security principle to enroll for a certificate based on the certificate template
 <p>Autoenrollment</p>	Allows a security principle to receive a certificate through the autoenrollment process

Key Points

To configure certificate template permissions you need to define the DACL, for each certificate template, in the Security tab. The permissions that you assign to a certificate template will define which security principals can be read, modified, enrolled, or auto-enrolled for that certificate template.

You can assign the following permissions to certificate templates:

- **Full Control.** The Full Control permission allows a security principal to modify all attributes of a certificate template, which includes permissions for the certificate template.
- **Read.** The Read permission allows a security principal to view the certificate template when enrolling for certificates. The security principal must enroll or auto-enroll a certificate. The Read permission is also required by the certificate server to find the certificate templates in Active Directory®.

- **Write.** This permission allows a security principal to modify the attributes of a certificate template, which includes permissions assigned to the certificate template.
- **Enroll.** This permission allows a security principal to enroll for a certificate based on the certificate template. However, to enroll for a certificate, the security principal must also have Read permissions for the certificate template.
- **Autoenroll.** This permission allows a security principal to receive a certificate through the auto-enrollment process. However, autoenrollment permission requires the user to have both Read and Enroll permissions for a certificate template.

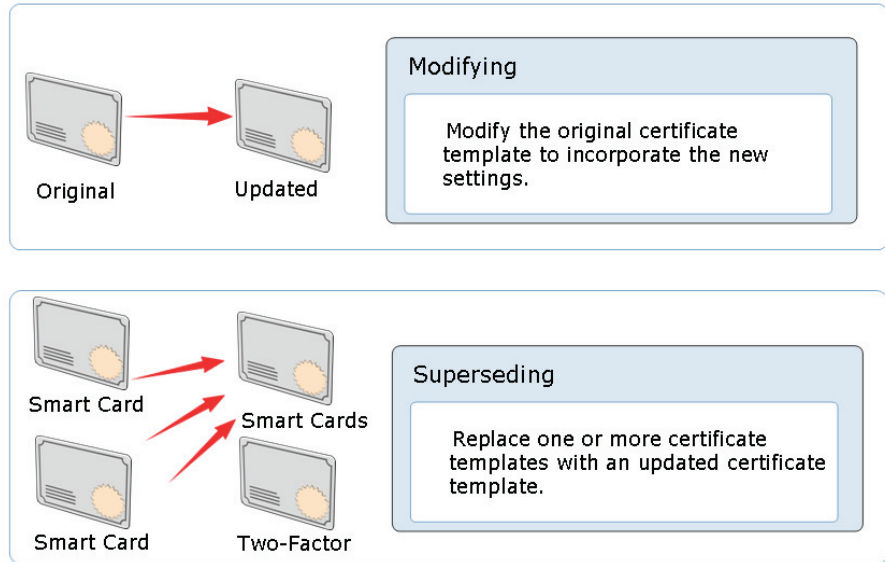
It is recommended that you assign certificate template permissions to global or universal groups only. This is because the certificate template objects are stored in the Configuration naming context in Active Directory®. You cannot assign permissions by using domain local groups found within an Active Directory® domain. You should never assign certificate template permissions to individual user or computer accounts. This will help you simplify administration.

As a best practice, you should keep Read permission assignment for the Authenticated Users group. This permission assignment will allow all users and computers to view the certificate templates in Active Directory®. This permission assignment will also allow the CA running under the SYSTEM context of a computer account, to view the certificate templates when assigning certificates.



For more information, see [AD CS certificate templates in Windows Server® 2008 whitepaper](#).

Methods for Updating a Certificate Template



Key Points

The CA hierarchy in most organizations has one certificate template for each job function. For example, there may be a certificate template for file encryption or code signing. Additionally, there may be a few templates that cover functions for most of the common groups of subjects.

As an IT administrator, you may need to modify an existing certificate template because of incorrect settings that were defined in the original certificate template. You may also need to merge multiple existing certificate templates into a single template. You can upgrade a certificate template in the given ways:

- **Modifying the original certificate template.** To modify a version 2 certificate template you need to make changes and apply them to that template. After this, any certificate issued by a CA based on that certificate template, will include the modifications you had made.
- **Superseding existing certificate templates.** The CA hierarchy of an organization may have multiple certificate templates providing the same or

similar functionality. In such a scenario, you can supersede or replace the multiple certificate templates by using a single certificate template. You can make this replacement by designating that a new certificate template supersedes, or replace, the existing certificate templates.



For more information, see [Certificate templates](#).

Demonstration: How To Modify and Enable a Certificate Template

- To create, modify, and supersede a template
- To issue a certificate to be used by a CA

The instructor will provide a demonstration to show how you can modify and issue a certificate template.

Question:

- Why would you need to modify a certificate template?
- What is the difference between modifying an original certificate template and superseding an existing certificate template?



For more information, see [Advanced features](#).

Lesson 5

Configuring Certificate Recovery

- Importance of Key Archival and Recovery
- Manually Exporting Certificates and Private Keys
- Configuring Automatic Key Archival
- How To Configure Key Archival
- Recovering a Lost Key
- How To Recover a lost key

Certificate or key recovery is one of the most important management tasks throughout the certificate life cycle. A key archival and recovery agent is used for data recovery when you lose your public and private keys. You can also use automatic or manual key archival and key recovery methods to ensure that you can gain access to data in the event that your keys are lost.

Importance of Key Archival and Recovery

Keys get lost when:

- User profile is deleted
- Operating system is reinstalled
- Disk is corrupted
- Computer is stolen



Data recovery methods that use:

- Key archival and key recovery agents
- Manual key archival and recovery



Key Points

- When you lose your public and private keys, you will not be able to access any data encrypted by using the certificate's public key, which can include Encrypting File System (EFS) and Secure/Multipurpose Internet Mail Extension (S/MIME). Therefore, archival and recovery of public and private keys are important.

Conditions for Losing Keys

- You may lose the key pair under following conditions:
- **User profile is deleted or corrupted.** A CSP encrypts a private key and stores it in the local file system and registry into the user profile folder. The encrypted private key is stored in the local file system and registry in the user profile folder. The case of deletion or corruption of the profile results in the loss of the private key material.

- **Operating system is reinstalled.** When you reinstall the operating system, the previous installations of the user profiles are lost, including the private key material.
- **Disk is corrupted.** If the hard disk gets corrupted and the user profile is unavailable, the private key material is automatically lost.
- **Computer is stolen.** If the computer of a user is stolen, the user profile with the private key material is unavailable.

Key Archival and Recovery Agent

Key archival and recovery agent are used for data recovery. You can ensure that CA administrators can recover private keys only by archiving them. KRAs are able to retrieve the original certificate, private key, and public key that were used to encrypt the data from the CA database.

When you enable key archival in a version 2 certificate template, the CA encrypts and stores that private key in its database.

In the case when the CA has stored the subject's private key in the CA database, you can use key recovery to recover a corrupted or lost key.

During the key recovery process, the certificate manager retrieves the encrypted file that contains the certificate and private key from the CA database. Then, a KRA decrypts the private key from the encrypted file and returns the certificate and private key to the user.

Security for Key Archival

- When you have a configured CA to issue a KRA certificate, any user with Read and Enroll permission on the KRA certificate template can enroll and become a KRA. Domain and Enterprise Admins gets permission. It is then that a KRA Domain and Enterprise Admins get these permissions by default. You must ensure that:
 - Only trusted users are allowed to enroll for this certificate.
 - The KRA's recovery key is stored in a secure manner.
 - The server from where the keys are archived is secure



For more information, see AD CS key archival and recovery in Windows Server® 2008 whitepaper .

Manually Exporting Certificates and Private Keys

You can use the following to export certificates:

- Certificates MMC snap-in
- Certification Authority MMC snap-in
- Certutil.exe
- Outlook®
- Internet Explorer®

The tool used depends upon the certificate template upon which the certificate is based.

Key Points

Manual key archival is one of the methods used for data recovery. It is supported in AD CS as a separate operation from enrollment while it still offers centralized key archival. The procedure to export private keys manually from a Windows® client is useful so that the private keys may be manually archived on the CA. This is especially useful for users who have enrolled by using the third-party CAs that do not support key archival.

You can export keys and certificates by one of the three methods.

- 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.
- PKCS #12 (*.pfx file) export from the Outlook® 2003 or 2007 client.
- *.epf file format from the Outlook® 2000 or Outlook® 2002 client.

If a user has enrolled for Exchange Advanced Security with version 1 certificates that is first offered with Exchange 5.0 Key Management Server, direct export from Outlook® into the *.epf file format will be necessary. X.509 version 1 certificates and keys may not be exported into PKCS #12 format on the Windows® client.









If only X.509 version 3 certificates have been used, the PKCS #12 format may be used.



For more information, see [Key archival and recovery in Windows Server® 2008 whitepaper](#).

Configuring Automatic Key Archival

To configure automatic key archival:

- 
Configure and issue the Key Recovery Agent certificate template.

- 
Designate a person as the Key Recovery Agent and enroll for the certificate.

- 
Enable Key Archival on the CA.

- 
Modify and enable required certificate templates for key archival.


Key Points

Steps to configure automatic key archival	Description
Configuring the certificate templates (certificates can be installed in the Active Directory® by default)	You install CA and upgrade certificate templates to the Windows Server® 2008 or Windows Server® 2003. <ul style="list-style-type: none"> • Only Enterprise Administrators or Domain Administrators requests a KRA certificate. This is because, by default, they are configured with the Enroll permission on the template.
Configuring certificate managers	<ul style="list-style-type: none"> • CA enforces a person to be a Certificate Manager, if defined. Certificate Manager holds a private key for valid KRA certificates. It is a best practice to separate these two roles. • By default, the CA Administrator is a Certificate Manager for

Steps to configure automatic key archival	Description
	<p>all users, except for cases with another explicit definition.</p> <ul style="list-style-type: none"> • A KRA is not necessarily a CA Officer or a Certificate Manager. They may be segmented as separate roles. A KRA is a person who holds a private key for a valid KRA certificate. • A CA Officer is defined as a Certificate Manager that has the security permission to issue and manage certificates. The security permissions are configured on a CA by using the Security tab from the CA Properties dialog box in the Certification Authority MMC snap-in.
Enabling a KRA	<ol style="list-style-type: none"> 1. Log on as Administrator of the server or CA Administrator, if role separation is enabled. 2. On the Administrative Tools menu, click Certification Authority, and select CA. 3. Right-click the CA name, click Properties, click the Recovery Agents tab, and then click Archive the key, to enable key archival. 4. By default, the CA uses one KRA. However, you must first select the KRA certificate for the CA to begin archival by clicking Add. 5. The system finds valid KRA certificates and displays available KRA certificates. These are generally published to Active Directory® by an Enterprise CA during enrollment. KRA certificates are stored under the KRA container in the Public Key Services branch of the configuration partition in Active Directory®. Since, CA issues multiple KRA certificates, each KRA certificate will be added to the multi-valued user attribute of the CA object. 6. Select one certificate, and click OK. Ensure that you have selected the intended certificate. 7. After you have added one or more KRA certificates, click OK. KRA certificates are only processed at service start.
Configuring user templates	<ol style="list-style-type: none"> 1. In the Certificate Templates MMC, right-click the key archival template, and select Properties. 2. On the Request Handling tab, select the Archive subject's encryption private key check box to always enforce key archival for the CA.. In Windows Server® 2008 CAs, select the Use advanced symmetric algorithm to send the key to the CA

Steps to configure automatic key archival	Description
	option.

Demonstration: How To Configure Key Archival

- To configure and issue the Key Recovery Agent certificate template
- To designate a person to be the Key Recovery Agent and enroll for the certificate
- To enable Key Archival on the CA
- To modify and enable required certificate templates for Key Archival



The instructor will provide a demonstration to show how you can configure key archival.

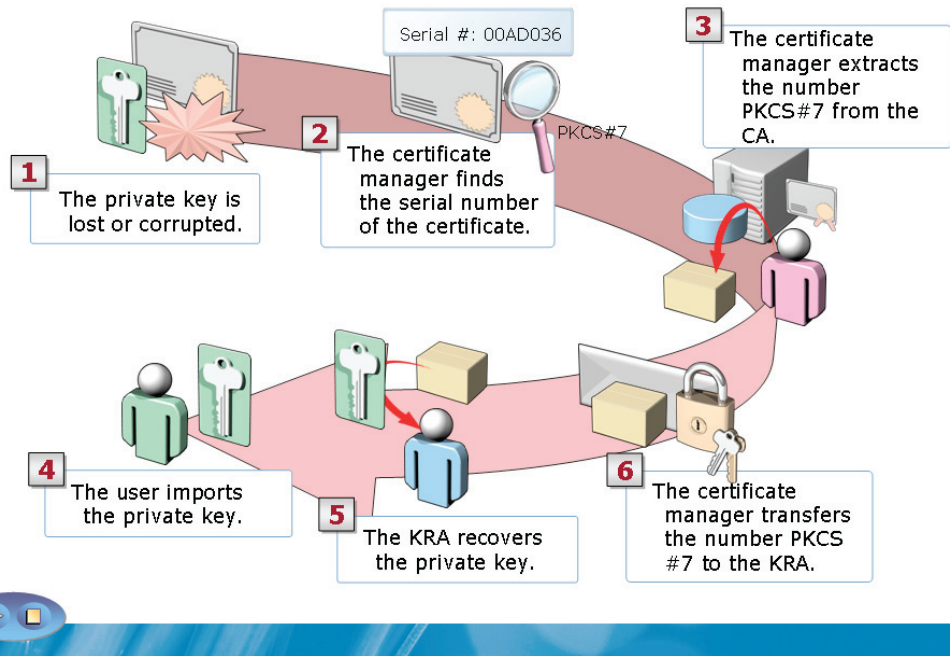
Questions:

1. What groups by default are authorized to request a KRA certificate?
- 2. Where by default in Active Directory® are KRA certificates normally published?



For more information, see [AD CS key archival and recovery in Windows Server® 2008 whitepaper](#).

Recovering a Lost Key



Key Points

- 1. Finding recovery candidates.** You will require two pieces of information to perform key recovery. First, the certificate manager or the CA administrator locates the correct certificate entry in the CA database and. Then, the certificate manager or the CA administrator obtains the serial number of the correct certificate entry and the KRA certificate required for key recovery.
- 2. Retrieving PKCS #7 BLOB from the database.** This is the first half of the key recovery step. A certificate manager or a CA administrator retrieves the correct Binary Large Object (BLOB) from the CA database. The certificate and the encrypted private key to be recovered, are present in PKCS #7 BLOB. The private key is encrypted alongside the public key of one or more KRAs.
- 3. Recovering key material and saving to PKCS #12 (.pfx).** This is the second half of the key recovery step. The holder of one of the KRA private keys decrypts the private key to be recovered. In addition, the holder generates a password-protected .pfx file that contains the certificate and private key.


4. **Importing recovered keys.** The password-protected .pfx file is delivered to the end-user. This user imports the .pfx file into the local user certificate store. Alternatively, the KRA or an administrator can perform this part of the procedure on behalf of the user.



For more information, see [AD CS archival and recovery in Windows Server® 2008 whitepaper](#).

Demonstration: How To Recover a Lost Key

- To recover an archived certificate and a key from an Active Directory®



The instructor will provide a demonstration to show how you can use IIS and perform Web site enrollment by using one of the manual enrollment methods.

Questions:

1. What piece of information will be most important to you while recovering lost keys?
2. 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?

Lab 3: Deploying and Managing Certificates

- Exercise 1: Configuring AD CS Web Enrollment
- Exercise 2: Configuring Certificate Autoenrollment
- Exercise 3: Configuring AD CS Certificate Revocation
- Exercise 4: Configuring AD CS Certificate Templates
- Exercise 5: Managing Key Archival and Recovery

Logon information

Virtual machine	6426A-NYC-DC1-B
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 110 minutes

Objectives

After completing the lab, you will be able to:

- Configure AD CS Web enrollment
- Configure Certificate autoenrollment
- Configure AD CS certificate revocation
- Configure AD CS certificate templates
- Manage key archival and recovery

Scenario

Woodgrove Bank is a large multinational corporation with offices located in five countries. The organization currently runs Windows Server® 2003, but now has to implement Windows Server® 2008. The bank has decided to deploy a PKI solution by using Windows Server® 2008 Active Directory® Certificate Services (AD CS).

Consolidation requirements:

- As the corporate server technology specialist, you must install and configure Windows Server® 2008 computers to support certificate services in the organization. To do so, you must perform the following consolidation activities:
- Install and configure Web Enrollment for Certificate Services.
- Configure the associated Web site to use Secure Socket Layer (SSL).
- Configure Autoenrollment features in Group Policy for Certificate Services.
- Configure certificate revocation and the Online Responder functionality of Certificate Services.
- Implement custom certificate templates and a key archival and recovery solution.

For this lab, you will use the available virtual computer environment. Before you begin the lab, you must:

- Start the 6426A-NYC-DC1-B virtual computer.
- Log on by using the user name **Administrator** and the password **Pa\$\$w0rd**.

Exercise 1: Configuring AD CS Web Enrollment

In this exercise, you will configure AD CS Web Enrollment.

The main tasks for this exercise are as follows:

1. Install the Certification Authority Web Enrollment role service.
2. Configure permissions on the Web Server certificate template.
3. Enroll a Web Server certificate.
4. Configure the Web enrollment site to use SSL.
5. Request and install basic Encrypting File System (EFS) certificate by using Web Enrollment.

► **Task 1: To install the Certification Authority Web Enrollment role service**

- Use Server Manager to install the Certification Authority Web Enrollment role service and its supporting services.
-

► **Task 2: To configure permissions on the Web Server certificate template**

- Open the Certification Authority console, and then access the Certificate Templates console.
- Configure permissions on the Web Server certificate template so that Authenticated Users can utilize the Enroll permission.

► **Task 3: To enroll a Web Server certificate**

1. Open a new MMC console and add the Certificates snap-in for the computer account to the console.
2. Request a new certificate in the personal certificates store.

3. In the **Certificate Enrollment** wizard, click **Web Server**, and then click **More information is required to enroll for this certificate**.
4. In the **Certificate Properties** dialog box, in the **Subject Name** area, under **Type**, click the drop-down arrow, and then select **Common name**.
5. In the **Value** box, type **NYC-DC1**, and then click **Add**.
6. On the **General** tab, in the **Friendly name** box, type **Woodgrove Bank Web Server**, and then enroll for the certificate.
7. Open the certificates folder and examine the new Web server certificate.
-

► **Task 4: To configure the Web enrollment site to use SSL**

1. Open the Internet Information Services (IIS) Manager console, and then click **Default Web Site**.
2. In the Actions pane, click **Bindings**.
3. In the **Site Bindings** dialog box, click **Add**.
4. In the **Add Site Bindings** dialog box, click the **Type** arrow, and then select **HTTPS**.
5. In the **SSL certificate** box, click the **Size** arrow, and then select the **Woodgrove Bank Web Server** certificate.
6. Expand the **Default Web Site** node, and then click **CertSrv**.
7. In the Details pane, scroll down, and then double-click **SSL Settings**.
8. On the **SSL Settings** page, select the **Require SSL** check box, and then click **Apply** in the Actions pane.
9. Close the Internet Information Services (IIS) Manager console.

► **Task 5: To request and install basic EFS certificate by using Web Enrollment**

1. Open Internet Explorer, in the address bar, type **https://NYC-DC1/Certsrv**, and then press ENTER.
2. Authenticate as **Woodgrovebank\Administrator** and use **Pa\$\$w0rd** as password.
3. Create and submit an advanced certificate request for a **Basic EFS** certificate.

4. Install the certificate. You will receive a message that the certificate has been successfully installed.

Exercise 2: Configuring Certificate Autoenrollment

In this exercise, you will configure certificate autoenrollment.

The main tasks for this exercise are as follows:

1. Duplicate and configure the user certificate template permissions to enable autoenrollment.
2. Configure the template to be issued by the CA.
3. Configure group policy to enable autoenrollment for users.
4. Verify that autoenrollment works for a user account.

► Task 1: To duplicate and configure the User certificate template permissions to enable autoenrollment

1. Start the Certification Authority console, right-click **Certificate Templates**, and then click **Manage**.
2. In the Certificate Templates console, duplicate the **User** certificate template as a Windows Server® 2008 compatible version, and then name the new template as **Woodgrove User**.
3. On the **Subject Name** tab, clear the **Include e-mail name in subject name** check box, and then clear the **E-mail name** check box.
4. On the **Security** tab, configure the Enroll permission and the Autoenroll permission for Authenticated Users.
5. Close the Certificate Templates console.

► Task 2: To configure the template to be issued by the CA

- Use the Certification Authority console to issue the **Woodgrove User** certificate template.

► Task 3: To configure group policy to allow autoenrollment for users

1. Open the Group Policy Management console and configure the default domain policy, user configuration, security settings, and the public key policy to allow autoenrollment for users.

2. Use the **Gpupdate /force** to refresh group policy.
3. Log off from the 6426A-NYC-DC1-B virtual computer.

► **Task 4: To verify that autoenrollment works for a user account**

1. Log on to the 6426A-NYC-DC1-virtual computer as **Administrator** with the password of **Pa\$\$wOrd**.
2. Open a new MMC console and add the Certificates snap-in for your user account.
3. Open the Personal Certificates store. Examine the client authentication certificate issued to administrator based on the Woodgrove User template.



The time duration for the certificate issuance is approximately a minute. Refresh the console periodically until the certificate is displayed.

Exercise 3: Configuring AD CS Certificate Revocation

In this exercise, you will configure AD CS certificate revocation.

The main tasks for this exercise are as follows:

1. Examine the default CDPs and configure the CRL publication interval.
2. Install the online responder component on a Web server.
3. Configure CA to include the online responder location in the AIA.
4. Issue the OCSP Response Signing template.
5. Configure the Online Responder.
6. Revoke a certificate.
7. Publish the CRL.
8. Ensure the CRL is downloaded onto the client computer.

► **Task 1: To examine the default CDPs and configure the CRL publication interval**

1. In the Certification Authority console, open the **WoodgroveBankCA Properties** dialog box.
2. On the **Extensions** tab, examine the CRL distribution points, and then close the **Woodgrove BankCA properties** dialog box.
3. Open the **Revoked Certificates folder properties** dialog box.
4. Set the CRL Publishing interval to **1 Month**.
5. Set the Publish Delta interval to **3 Days**.

► **Task 2: To Install the online responder component on a Web server**

- Use Server Manager to install the Active Directory® Certificate Services Online Responder role service.

- ▶ **Task 3: To configure CA to include the online responder location in the AIA**
 1. In the Certification Authority console, open the **WoodgroveBankCA properties** dialog box.
 2. On the **Extensions** tab, add **http://nyc-dc1/ocsp** as an AIA location. Also enable the **Include in the AIS extension of issued certificates** and the **Include in the online certificate status protocol (OSCP) extension** check boxes.

- ▶ **Task 4: To issue the OCSP Response Signing template**
 1. Use the Certificate Templates console to set the permissions on the OCSP Response Signing template so that you allow Enroll permission for the authenticated users.
 2. Use the Certification Authority console to issue the template.

- ▶ **Task 5: To configure the Online Responder**
 1. Launch the Online Responder management console.
 2. Right-click **Revocation Configuration**, and then click **Add Revocation Configuration**.
 3. Use the wizard to create a new revocation configuration named **WoodgroveBankCA. Online Responder**
 4. Browse to, and select the WoodgroveBankCA certificate.
 5. After you run the wizard, the revocation configuration status is set to **Working**.
 6. Close the Online Responder console.

- ▶ **Task 6: To revoke a certificate**
 1. Open the Certification Authority console, and then click **Issued Certificates**.
 2. Locate and revoke the **Basic EFS** certificate that was issued in the last exercise. Select **Change of Affiliation** as the reason.

3. Click the **Revoked Certificates** folder, and then ensure that the revoked certificate appears.

▶ **Task 7: To publish the CRL**

1. Right-click the **Revoked Certificates** folder.
2. Point to **All Tasks** and click **Publish**.
3. Publish a new CRL.

▶ **Task 8: To ensure the CRL is downloaded onto the client computer**

1. Create a Certificates MMC console for the user account.
2. Under the **Certificates –Current User** node, expand the **Intermediate Certification Authorities** node, and then click **Certificate Revocation List**. Notice the CRL from WoodGroveBankCA.
3. Open the Properties for one of the WoodGroveBankCA lists and then click the Revocation List tab. Notice that the certificate that was previously revoked is listed.

Exercise 4: Configuring AD CS Certificate Templates

In this exercise, you will configure AD CS certificate templates.

The main tasks for this exercise are as follows:

1. Duplicate and supersede the Woodgrove User template with a new template that includes smart card logon.
 2. Configure the new template to be issued by the CA.
 3. Verify the certificate is updated.
-
- **Task 1: To duplicate and supersede the Woodgrove User template by using a new template that includes smart card logon**
1. In the Certification Authority console, right-click **Certificate Templates**, and then click **Manage**.
 2. Duplicate the **Woodgrove User** certificate template as a version 3 template.
 3. Name the new template as **Woodgrove Smart Card User**.
 4. On the **Extensions** tab, edit Application Policies to include Smart Card Logon.
 5. On the **Superseded templates** tab, add the **Woodgrove User** template.
 6. On the **Security** tab, and then ensure that the Authenticated Users have Enroll and Autoenroll permissions.
-
- **Task 2: To configure the new template to be issued by the CA**
1. In the Certification Authority console, issue the Woodgrove Smart Card User certificate template.
 2. Close all windows and log off.
-
- **Task 3: To verify the certificate is updated**
1. Log on to the 6426A-NYC-DC1-B virtual computer as Administrator.
 2. Create an MMC console, and then add the Certificates console snap-in for the user account.

3. Open the Personal Certificates store. Examine the client authentication certificate issued to the administrator. Ensure that the certificate is based on the Woodgrove Smart Card User template.



The time duration for a certificate issuance is approximately a minute. Refresh the console periodically until the certificate is displayed.

Exercise 5: Managing Key Archival and Recovery

In this exercise, you will manage key archival and recovery.

The main tasks for this exercise are as follows:

1. Remove the requirement for CA Manager approval and verify who can enroll the KRA certificate.
2. Configure the WoodgroveBankCA to issue KRA certificates.
3. Acquire the KRA certificate.
4. Configure the CA to allow key recovery.
5. Configure a custom template for key archival.
6. Add a user to the Server Operators group.
7. Verify key archival functionality.

► **Task 1: To remove the requirement for CA Manager approval and verify who can enroll the Key Recovery Agent certificate**

1. On the 6426A-NYC-DC1-B virtual computer, in the Certification Authority console, right click the **Certificates Templates** folder, and click then **Manage**.
2. In the Certificates Templates console, open the **Key Recovery Agent** certificate properties dialog box.
3. On the **Issuance Requirements** tab, clear the **CA certificate manager approval** check box.
4. On the **Security** tab. Notice that only Domain Admins and Enterprise Admins groups have the Enroll permission.

► **Task 2: To Configure the WoodgroveBankCA to issue Key Recovery Agent certificates**

1. Right-click the **Certificates Templates** folder.
2. Issue the **Key Recovery Agent template**.

- ▶ **Task 3: To acquire the Key Recovery Agent certificate**
 1. Create an MMC console window that includes the Certificates snap-in loaded.
 2. Use the wizard to request a new certificate and enroll the Key Recovery Agent certificate.
 3. Refresh the console window and view the Key Recovery Agent in the personal store.

- ▶ **Task 4: To configure the CA to allow key recovery**
 1. In the Certification Authority console window, open the **WoodgroveBankCA properties** dialog box.
 2. On the Recovery Agents tab, click **Archive the key**, and then add the certificate using the Key Recovery Agent Selection dialog box.

- ▶ **Task 5: To configure a custom template for key archival**
 1. Open the Certificates Templates Console window.
 2. Duplicate the User template for Windows Server® 2008 Enterprise Edition and name it **Archive User**.
 3. On the Request Handling tab, set the option for the Archive subject's private key. By using the archive key option, the Key Recovery Agent can obtain the private key from the certificate store.
 4. Add the Archive User template as a new certificate template to issue.

- ▶ **Task 6: To add a user to the Server Operators group**
 1. Open the Active Directory® Users and Computers console.
 2. From the **Executives** OU, add the users **Tony Wang**, to the **Server Operators** group.
 3. Open Tony's properties dialog box and configure the e-mail address as **tony@WoodgroveBank.com**.
 4. Log off from the 6426A-NYC-DC1-B virtual computer.

► **Task 7: To verify key archival functionality**

1. Log on to the 6426A-NYC-DC1-B virtual computer as **Tony** and use **Pa\$\$w0rd** as the password.
2. Create an MMC console window that includes the Certificates snap-in.
3. Request and enroll a new certificate based on the Archive User template.
4. From the personal store, locate the Archive User certificate.
5. Open the properties of the certificate and note down the certificate serial number. You will use this for recovery of the private key.
6. Log off the 6426A-NYC-DC1-B virtual computer and then log on as **woodgrovebank\administrator**. Use **Pa\$\$w0rd** as the password.
7. On the 6426A-NYC-DC1-B virtual computer, at the command prompt, type **certutil -getkey <serial#> outputblob**



Note: Replace <serial#> with the serial number that you noted down.

8. To convert the outputblob file into an importable PFX file, on the 6426A-NYC-DC1-B virtual computer, at the command prompt, type **Certutil -recoverkey outputblob tony.pfx**
9. Verify the creation of the recovered key in the C:\Users\Administrator directory.



After completing this exercise, turn off all virtual computers and discard undo disks.

Lab Review: Deploying and Managing Certificates

In this lab, you have:

- Installed the Certification Authority Web Enrollment roles 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 configure 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 the CRL is downloaded to client computer
- Duplicated and superseded the Woodgrove User template with a new template that includes smart card logon
- Configured the new template to be issued by the CA
- Verified the certificate updated
- Removed the requirement for CA Manager approval and verified who can enroll the Key Recovery Agent certificate
- Configured the WoodgroveBankCA to issue Key Recovery Agent certificates
- Acquired the Key Recovery Agent 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' Certificate Serial Number
- Recovered the Private key for the Archive User certificate

Lab Resources

There are no additional lab resources for this lab.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

Module 4

Configuring AD LDS

Contents:

Lesson 1: Installing and Configuring AD LDS	4-3
Lesson 2: Configuring AD LDS Instances	4-15
Lesson 3: Configuring AD LDS Replication	4-32
Lesson 4: Configuring AD LDS Integration with AD DS	4-42
Lab 4: Configuring AD LDS	4-50

Module Overview

- Installing and Configuring AD LDS
- Configuring AD LDS Instances
- Configuring AD LDS Replication
- Configuring AD LDS Integration with AD DS

The Active Directory® Lightweight Directory Services (AD LDS) role was previously known as Active Directory® Application Mode (ADAM). AD LDS is a Lightweight Directory Access Protocol (LDAP) directory service that supports directory-enabled applications. The main components of AD LDS include databases, instances, schema, and partitions. Configuring multiple instances is beneficial to provide database redundancy and increased availability. You can configure replication to synchronize directory data associated with any AD LDS instance. In addition, you can integrate AD DS with AD DS to provide access to additional users within your network environment.

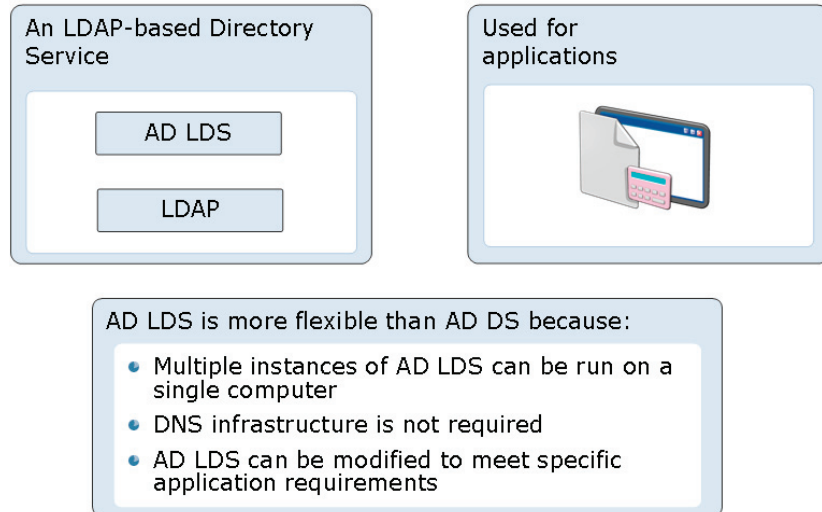
Lesson 1

Installing and Configuring AD LDS

- What Is AD LDS?
- AD DS Deployment Scenarios
- AD LDS Components
- How To Install AD LDS Server Role
- AD LDS Administration Tools
- How Clients Connect to AD LDS

The AD LDS role supports directory-enabled applications and performs many of the functions that typically have been associated with AD DS. You can use AD LDS to function as an application directory store, extranet authentication store, identity systems consolidation, and development environment. You can use different AD LDS administrator tools to serve purposes such as to manage AD LDS instances, to manage AD LDS schema objects, and to synchronize AD LDS to AD DS.

What Is AD LDS?

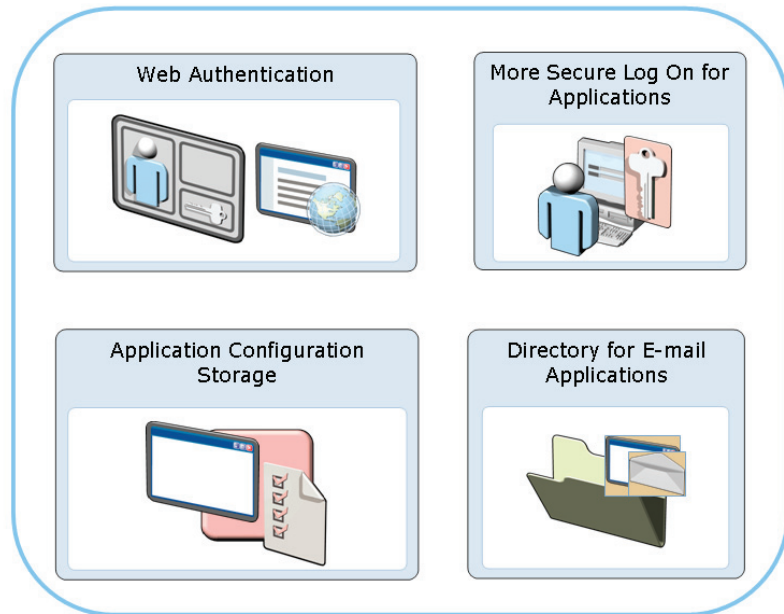


Key Points

The AD LDS role is a LDAP directory service that supports directory-enabled applications. AD LDS was previously called ADAM.

You can use AD LDS to perform most of the functions that AD DS offers. The advantage of AD LDS is that it does not require the dependencies required by AD DS, such as, the deployment of domains or domain controllers. When AD LDS and AD DS co-exist in the same environment, AD LDS can use AD DS to authenticate Windows®-based security principals. You can deploy AD LDS on any computer running Windows Server® 2008, including a domain controller, because each AD LDS instance runs as a self-contained server service.

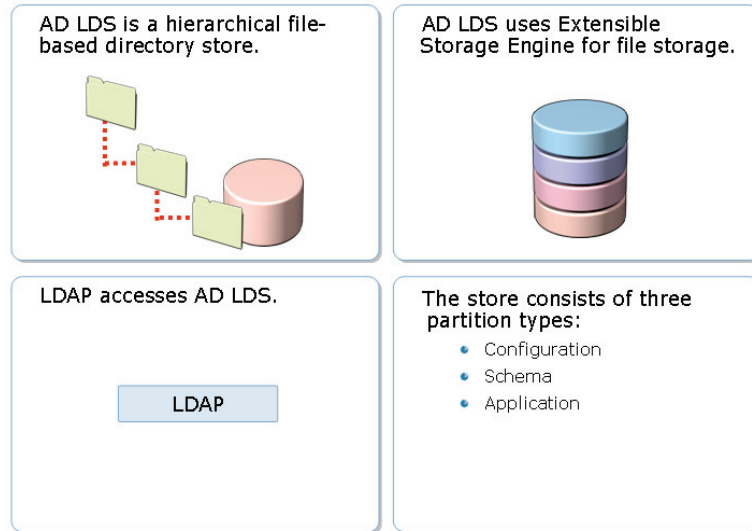
AD LDS Deployment Scenarios



Key Points

- **Directory store.** All directory-enabled enterprise applications can use AD LDS as their directory store. AD LDS can store directory data that pertains to the application in a local directory service.
- **Extranet authentication store.** AD LDS can provide an extranet authentication store. For example, a Web portal application that manages extranet access to corporate applications can use identities that are external to the corporate AD DS.
- **Identity systems consolidation.** You can use AD LDS to store a unified view of all known identity information. This information can be about enterprise users, applications, and network resources.
- **Development environment.** You can use AD LDS as a prototype or pilot environment to test the schema compatibility of applications, before deploying them by using AD DS as their directory store.

AD LDS Components



Key Points

AD LDS provides a hierarchical directory store by using the Extensible Storage Engine (ESE) for storing files. AD DS also uses the same ESE file storage technology.

Component	Description
Database	A database file and its associated transaction logs function as AD LDS data stores.
Instance	AD LDS instances hold copies of the same directory partition or partitions. These partitions form a logical grouping called a configuration set.
Schema	A schema directory partition stores a unique configuration schema of each AD LDS configuration set.

Component	Description
Partitions	An AD LDS directory store is composed of three partitions—configuration partition, schema partition and application partition. A configuration partition and a schema partition are almost identical to an AD DS partition. However, the application partition is akin to application directory partition in the AD DS.

AD LDS supports both LDAP connections and secure LDAP (LDAPS) connections. All LDAP connections use Transmission Control Protocol (TCP) port 389, by default. However, all LDAPS connections use TCP port 636 by default.



For more information, see:

- [Step-by-Step Guide for Getting Started with AD LDS](#)
- [AD LDS](#)

Demonstration: How To Install AD LDS Server Role

- To install AD LDS server role

The instructor will provide a demonstration to show how you can install an AD LDS server role.

Question:

1. Can AD LDS be installed on a member server?
2. Can a single machine hold multiple AD LDS instances?
3. Is an instance created automatically when the server role is installed?
4. What may be some of the reasons for implementing AD LDS replication?



For more information, see:

- Step-by-Step Guide for Getting Started with AD LDS

- AD LDS

AD LDS Administration Tools

Active Directory® Lightweight Directory Services Wizard

- Creates a new instance of AD LDS
- Creates a new replica of an AD LDS instance

LDP

- Creates application partition instances
- Modifies data
- Views data

AdamSync

- Synchronizes an instance of AD DS to AD LDS

ADSIEdit

- Modifies data
- Views data

Dsacls

- Views or sets permissions

Ldifde or Csvde

- Imports and exports data

ADSchemaAnalyzer

- Migrates the Active Directory® schema to ADAM



Key Points

An AD LDS instance primarily provides a service. Therefore, you can start, stop, and restart an AD LDS instance. The following table describes various built-in tools to administer AD LDS.

AD LDS Administration Tool	Description
AD LDS Wizard	This tool helps create a new: <ul style="list-style-type: none"> • Instance of AD LDS • Replica of an AD LDS instance
LDP.exe	This tool provides administration of any LDAP service.
AdamSync.exe	This tool helps synchronize AD LDS to AD DS.

AD LDS Administration Tool	Description
ADSIEdit snap-in	This tool helps manage AD LDS instances.
Dscls.exe	This tool can be used to view and set object permissions.
Ldifde or Csvde	These tools help import and export of data to and from AD LDS.
ADSchemaAnalyzer	This tool helps copy the schema from AD DS and then imports the schema into AD LDS.
Dsdbutil	This directory service management tool helps: <ul style="list-style-type: none"> • Back up and perform authoritative restores of AD LDS data • Move the AD LDS data files • Change the AD LDS service account and port numbers • List the AD LDS instances running on a server
Active Directory® Schema snap-in	This tool helps to view and manage AD LDS schema objects.
Active Directory® Sites and Services snap-in	This tool helps administer the replication of directory data among all sites in an AD LDS configuration set.

How Clients Connect to AD LDS

To connect to an AD LDS server client computer, you:

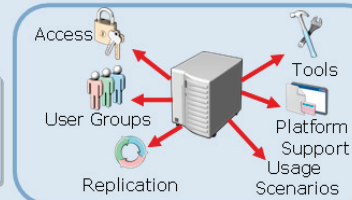
- Can use LDAP or LDAPS
- Must use the port numbers assigned to the AD LDS instance
- Must be configured with the IP address or DNS name of the AD LDS server



Client Computer

To secure the client connections to AD LDS:

- Install a digital certificate on the server
- Configure the clients to use LDAPS to connect to the server



AD LDS

Key Points

Unlike AD DS, AD LDS does not use or register SRV records in DNS. Therefore, you must configure the clients by using the AD LDS server IP address or DNS name. If the clients use the DNS name, you must add the appropriate host record to DNS.

You can use LDAP to read from and write to AD LDS. By default, LDAP data is not transmitted securely. You can secure LDAP data transmission by using the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) technology.

To secure LDAP data transmission, you can also use certificates assigned by internal Active Directory® Certificate Services (AD CS) or by public certification authorities. After you obtain the certificate from a trusted Certification Authority (CA), you must install or import it onto the server that runs AD LDS. You must store the certificate in the AD LDS service's personal store. If you want to use the certificate for applications other than AD LDS, you must store this certificate in the

local computer's personal certificate store. In addition, you must ensure that the service account under which the AD LDS instance is running has Read access to the certificate that you have installed or imported.



For more information, see AD LDS.

Lesson 2

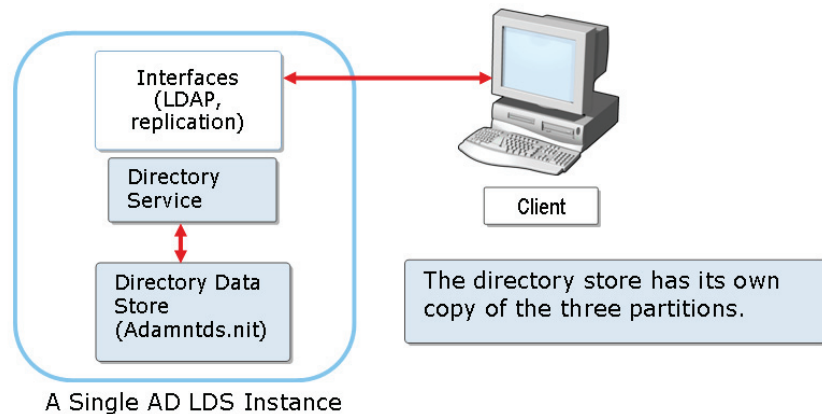
Configuring AD LDS Instances

- What Is an AD LDS Instance?
- What Is an AD LDS Schema?
- How To Modify an AD LDS Schema
- What Is an Application Partition?
- How To Configure an AD LDS Instance and Application Partition
- AD LDS Users and Groups
- How Access Control Works in AD LDS
- How To Configure Access Control in AD LDS

You can configure an AD LDS instance to use as a single running copy of the AD LDS directory service. A schema defines every object and attribute in the AD LDS directory service. Further, application data is stored in the application partition of the instance. You can customize your application to meet business requirements by creating users and groups. You can use AD LDS access control to authenticate users and to determine if the user has permissions to access specific objects.

What Is an AD LDS Instance?

An AD LDS Instance is a running copy of an AD LDS service that contains its own communication interface and directory store.



Key Points

- An AD LDS instance is a single running copy of the AD LDS directory service.
- AD LDS instances that hold copies of the same directory partition or partitions form a logical grouping are called configuration set.
- Each AD LDS configuration set will have a specific and independent schema stored in the schema directory partition.
- Multiple application partitions can be deployed in a single AD LDS instance if they have compatible schemas.
- Multiple copies of the AD LDS directory service can run concurrently on the same computer, each by using a separate directory data store, and a unique service name.
- Creating multiple instances is better than creating multiple application partitions. This is because, multiple applications:

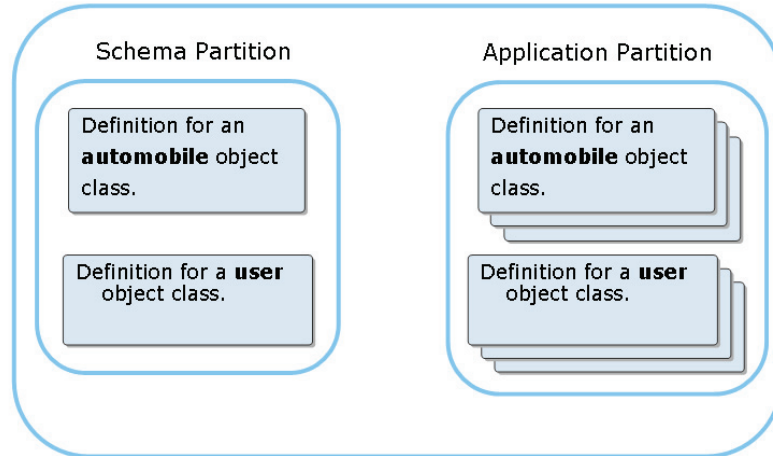
- Must maintain separate or incompatible schema
- Need various replication settings
- Should have administrators that should not have access to each other's AD LDS data



For more information, see Windows Server® 2008 Technical Library.

What Is an AD LDS Schema?

AD LDS Schema defines the types of objects, and data that can be created and stored in an AD LDS instance by using object classes and attributes.



Key Points

A schema defines every object and attribute in a directory. For creating an object type in the directory, you must first define it in the schema.

- An AD LDS schema defines the object types, by using the data that you create and store in an AD LDS instance with object classes and attributes.
- For creating an object type in the directory, you must first define it in the schema. The schema defines every object and attribute in a directory.
- Each AD LDS configuration set has a unique and independent schema that is stored in the schema directory partition. By default, the AD LDS schema contains only the classes and attributes that are needed to start an instance.
- You can extend a schema such that AD LDS can keep specific data needed to run a particular application. When applications require various schemas, a separate AD LDS instance needs to be deployed for each application.

- AD LDS directories can support applications that depend on schema extensions that are not desirable in the AD DS directory. For example, schema extensions those are useful to a single application.
- You need to import only the required schema definition files for each instance. You can also customize the schema modifications for applications that require a custom schema. Similar to AD DS schema, you can extend the AD LDS schema by importing of LDAP Data Interchange Format (LDIF) (.ldf) files into the schema.



For more information, see AD LDS.

Demonstration: How To Modify an AD LDS Schema

- To import a Lightweight Data Interchange Format (LDIF) file to modify the schema

The instructor will provide a demonstration to show how you can modify an AD LDS schema.

Questions:

1. What is LDIF?
2. Which Windows Server® 2008 utility can be used to modify the schema?
3. What is defined in the AD LDS schema?

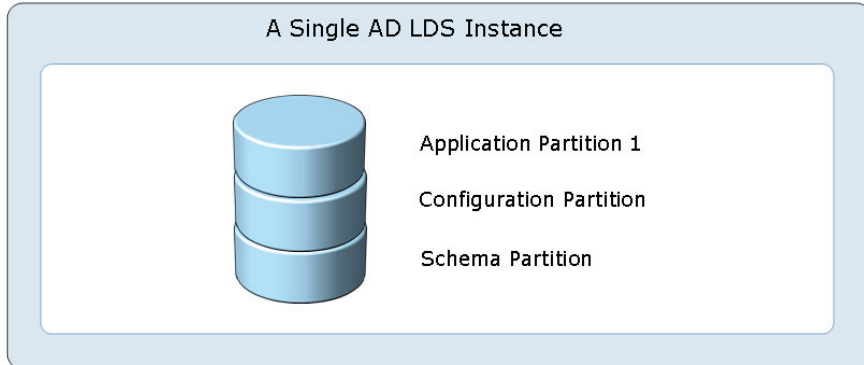


For more information, see

- AD LDS Overview
- AD LDS.

What Is an Application Partition?

The AD LDS application partition holds the data that is used by the application.



Multiple application directory partitions can be created in each LDS instance. However, each partition would share a single set of configuration and schema partitions.

Key Points

AD LDS provides flexible support for directory-enabled enterprise applications, without any AD DS restrictions. You can create an application partition during an AD LDS server role set up or after completing the setup. Before creating any object, the object needs to be defined in the schema. Following are the key aspects of an AD LDS application partition:

- An AD LDS application partition holds the data used by the application.
- The application partition can be easily identified by its fully qualified unique name assigned while creating the partition.
- An AD LDS top-level directory partition supports both DNS-style and X.500-style names. Unlike AD DS, that supports only DNS-style (DC=) names for top-level directory partitions.
- An AD LDS instance supports multiple application partitions sharing the same schema partition independently. This implies that a change in schema to

support an application partition, also affects each of the other applications in that instance.

- In many cases, you can manage data in a particular application's directory partition by using your application. For example, any changes made in the directory-enabled application, such as creating a new user account or modifying the application configuration, are written by the application in the application directory partition.



For more information, see [AD LDS Overview](#).

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

- To configure an AD LDS instance and an application partition

The instructor will provide a demonstration to show how you can configure an AD LDS instance and an application partition.





Questions:

1. Does each AD LDS instance have its own directory store?
2. Do the instances, that are part of the same configuration, set run on the same or separate computers?
3. You have created a new AD LDS instance and you forgot to create an application partition. How can you create an application instance without recreating the instance?



For more information, see **AD LDS**.

AD LDS Users and Groups

Permission	Default Members		Default Access
	Configuration Partition	Application Partitions	
 Administrators	AD LDS administrators that are assigned during AD LDS setup	The administrators group from the configuration partition	Full access to all partitions
 Readers	None	None	Read access to the partition
 Users	Transitively, all AD LDS users	Transitively, all AD LDS users that are created in the partition	None
 Instances	All instances	All instances	None

Key Points

When creating an AD LDS instance a set of users and groups are created by default. These default users and groups provide basic functionality of user and administrative permissions to the AD LDS instance. However, you can create additional users and groups to customize application to meet the requirements.

You can use Windows® security principals for authentication and access control. You can also add local Windows® users and groups, and domain users and groups, to AD LDS groups as members by using AD LDS. You can create AD LDS users by importing default user object class definitions provided with AD LDS in the MS-AdamSyncMetadata.LDF file. You can alternatively create AD LDS users by supplying your own user object definitions.

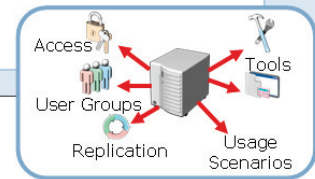
How Access Control Works in AD LDS

Access control is used to limit the information that users can access in the AD LDS partitions.



AD LDS users can be authenticated by using:

- A Simple LDAP bind or bind redirection
- A local Windows® account or AD DS account



AD LDS uses access control lists to restrict access to AD LDS data.



• Key Points

- Access control in AD LDS restricts users to access information.
- Access control in AD LDS is very similar to access control in AD DS.
- AD LDS provides access control that:
 - **Authenticates the identity of all users.** When a user tries to log on to or access the data in the AD LDS directory, the user must first be authenticated. A user is granted a security token that includes the security identifier (SID). Then, the SID is assigned to the user and to all AD LDS groups of which the user is a member.
 - **Uses Access Control Lists (ACLs) to determine if the user has permissions to access specific objects.** When the user tries to access the object, the client computer presents the security token created during authentication. If the SIDs in the security token matches the permissions assigned in the ACL, the user is granted access to the object.



For more information, see AD LDS.

Demonstration: How To Configure Access Control in AD LDS

- To configure user accounts and groups
- To configure access control lists

The instructor will provide a demonstration to show how you can configure access control in AD LDS.

Questions:

1. Which security principals are available in AD LDS?
2. Which tool can be used to customize access control in AD LDS?
3. What are the default role-based groups in AD LDS?



For more information, see AD LDS.

Lesson 3

Configuring AD LDS Replication

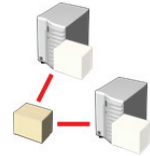
- Why Implement AD LDS Replication?
- How AD LDS Replication Works
- What Is a Configuration Set?
- How To Configure AD LDS Replication
- AD LDS Replication Topology

AD LDS replication provides high availability, load balancing, and data redundancy. It prevents conflicts in replication by using change tracking information. You can use a configuration set to configure all AD LDS instances to replicate one or more application directory partitions. However, each configuration set maintains its own replication topology by using topology information stored as site objects and site link objects.

Why Implement AD LDS Replication?

AD LDS Replication:

Enables multiple copies of an AD LDS instance to be stored on different servers



Provides high availability for critical applications



Provides load balancing



Enables geographically distributed applications



Key Points

You can deploy multiple AD LDS servers and configure replication between instances that run on different servers. AD LDS uses a type of replication known as multimaster replication. By using multimaster replication, you can modify directory data on any AD LDS instance.

By using replication, AD LDS copies data updates for a directory partition. AD LDS copies these updates for an AD LDS instance to another AD LDS instance that contains copies of the same directory partition.

You can use AD LDS replication for the following reasons:

- **High availability.** You can use and distribute multiple replicas of an AD LDS instance on multiple servers at the same locations. This usage and distribution of AD LDS instances improves the availability of business critical applications.
- **Load balancing.** A single server might not be able to handle many requests for an application. So, you can create multiple AD LDS replicas to be stored on

multiple servers. You can then configure the application to balance the load between multiple AD LDS replicas.

- **Geographic limitations.** You can use AD LDS replication to improve the response of applications that users access from different geographic locations. Users need to target a local AD LDS replica which is then replicated to other locations.

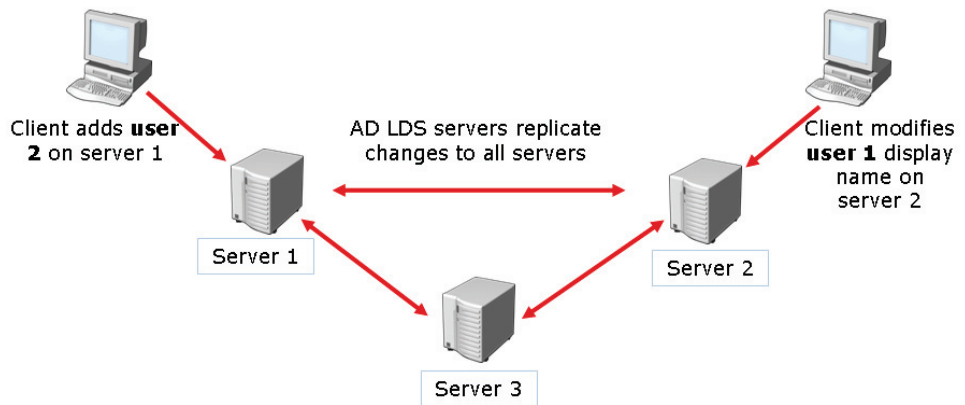


For more information, see AD LDS.

How AD LDS Replication Works

AD LDS uses multimaster replication where:

- All instances are writable
- Changes on one instance are replicated to the other instances



Key Points

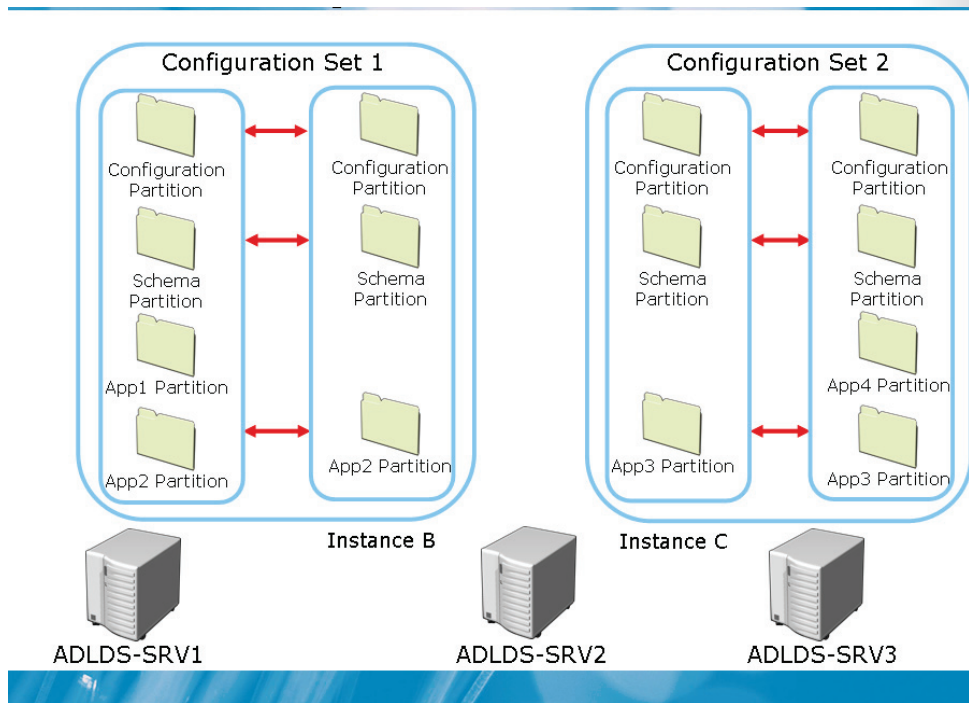
- If you modify directory data for any of the AD LDS instances, the modifications are replicated across all the instances that contain copies of the same directory partition.
- An AD LDS instance replicates data based on participation in a configuration set. You can include an AD LDS instance in a configuration set only when you install the AD LDS instance.
- AD LDS prevents replication conflicts by using change tracking information. The replication partners that receive conflicting changes examine the attribute data that is contained in the changes.
- Each change to the directory data contains a version and a time stamp. AD LDS instances accept only the change that is marked with the latest version. The instances then reject the other changes. If the versions are identical, AD LDS instances accept the change that contains the latest time stamp.

- An AD LDS configuration set maintains its own replication topology. This topology is independent of any AD DS replication topology that may exist. In addition, you cannot replicate directory partitions between AD LDS instances and domain controllers.



For more information, see AD LDS.

What Is a Configuration Set?



Key Points

A configuration set is a group of AD LDS instances that replicate a common schema and configuration partition. You can configure all AD LDS instances in a configuration set to replicate one or more application directory partitions. However, you cannot configure replication between application directory partitions in different configuration sets.

Each configuration set maintains its own replication topology. You can include an AD LDS instance in a configuration set only when you install the AD LDS instance. After you create an AD LDS instance, you cannot add the instance to a configuration set. You also cannot remove the AD LDS instance from a configuration set after you create the instance.



For more information, see AD LDS.

Demonstration: How To Configure AD LDS Replication

- To configure replication for an AD LDS instance

The instructor will provide a demonstration to show how you can configure AD LDS replication.

Questions:

1. What tool provides the ability to create an AD LDS replica?
2. What information do you require to create an AD LDS replica?
3. What is the type of replication that AD LDS uses?



For more information, see **AD LDS**.

AD LDS Replication Topology

The knowledge consistency checker (KCC) automatically creates the AD LDS replication topology on each AD LDS server in a configuration set. AD LDS replication is based on AD LDS sites and site links.

AD LDS replication is based on the following AD LDS sites and site links:

- The Default-First-Site-Name site and the DefaultIPSiteLink are created by default.
- Active Directory® Sites and Services configure sites and site links.
- The intersite topology generator (ISTG) builds the replication topology between sites.
- Inter-site replication can be scheduled.

Key Points

AD LDS, like AD DS, uses topology information to build an efficient replication topology for a configuration set. The topology information for AD LDS is stored as site objects and site link objects in the configuration directory partition.

AD LDS instances replicate data based on participation in a configuration set. All AD LDS instances that are joined to the same configuration set must replicate a common configuration directory partition and a common schema directory partition. An AD LDS configuration set maintains its own replication topology. This replication topology is independent of other AD DS replication topologies.

You can use sites in AD LDS to represent the physical structure or topology of the network. In addition, you can use the ADSIEdit tool to define site objects and site link objects for the AD LDS replication topology.



For more information, see AD LDS.

Lesson 4

Configuring AD LDS Integration with AD DS

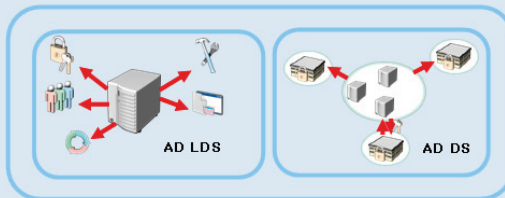
- Options for Integrating AD LDS and AD DS
- How To Add AD DS Users to AD LDS Groups
- Synchronizing AD DS Accounts to AD LDS
- How To Implement AD DS Synchronization

AD LDS uses basic set of security concepts similar to AD DS such as authentication, authorization, users, groups, ACLs, and security tokens. Hence, you can integrate AD LDS with AD DS by adding AD DS users to AD LDS groups. The Active Directory® to ADAM Synchronizer (adamsync) tool can be used to synchronize data from an AD DS forest with a configuration set of an AD LDS instance.

Options for Integrating AD LDS and AD DS

To integrate AD LDS and AD DS:

- Add AD DS user accounts to AD LDS groups and grant access to the AD LDS groups, if the AD LDS server is a member of an AD DS domain.
- Synchronize AD DS information to AD LDS.



Key Points

AD LDS and AD DS use the same basic set of security concepts, such as authentication, authorization, users, groups, ACLs, and security tokens. AD LDS also uses groups to provide access to directory data. Like AD DS, AD LDS contains its own set of default groups that are created during installation.

After you install AD LDS, a set of default groups exist in each directory partition. In addition, you can create your own custom groups.

You can assign a Windows® security principal permission for objects in AD LDS. You can also include Windows® security principals as members in AD LDS groups.

AD LDS does not authenticate Windows® security principals. Instead, AD DS or the Local Security Authority (LSA) on the local computer authenticates these principals.

To obtain access to applications, a user might attempt to authenticate against, or bind to AD LDS. Depending on the type of user who attempts the bind, AD LDS, LSA, or AD DS authenticates the user.



For more information, see [AD LDS](#).

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

- To add AD DS Users to AD LDS groups
- To verify that the AD DS users are granted the appropriate access



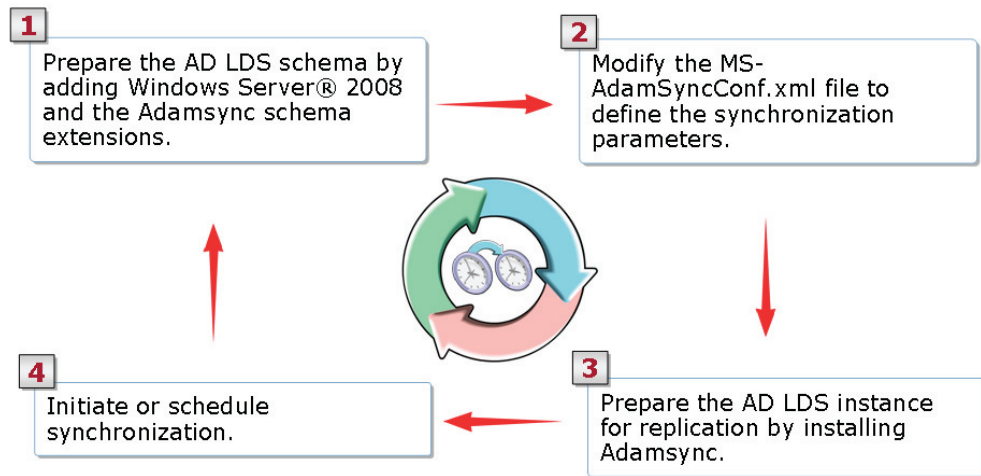
- The instructor will provide a demonstration to show how you can add AD DS users to AD LDS groups.
- **Question:**
 1. What are the user types that you can add to AD LDS groups?
 2. What are the default AD LDS groups that are present in the application partition?
 3. What tool can you use to manage AD LDS users and groups?



For more information, see AD LDS

•

Synchronizing AD DS Accounts to AD LDS



Key Points

- You can use the Active Directory® to ADAM Synchronizer (adamsync) tool to synchronize data from an AD DS forest with a configuration set of an AD LDS instance. For synchronization of data for complex scenarios, you can use the Identity Integration Feature Pack (IIFP) or Identity Lifecycle Manager (ILM) 2007.
- To migrate the Active Directory® schema to AD LDS, you can use the ADSchemaAnalyzer tool. In addition, you can use the ADSchemaAnalyzer tool to migrate the Active Directory® schema from one AD LDS instance to another. You can also use the ADSchemaAnalyzer tool to migrate the Active Directory® schema from any LDAP-compliant directory to an AD LDS instance.
- You can use the ADSchemaAnalyzer tool to run a target schema. You can then mark the elements you want to migrate and export these elements to the base AD LDS schema. In addition, you can use the ADSchemaAnalyzer tool to compare the two schemas. Further, you can use the ADSchemaAnalyzer tool to

create .ldf files from the modified schema. You can then import these files to AD LDS before you implement the adamsync tool.



For more information, see:

- Using the ADAM Administration Tools
- AD LDS

Demonstration: How To Implement AD DS Synchronization

- To Implement AD DS Synchronization with AD LDS

- The instructor will provide a demonstration to show how you can synchronize AD DS with AD LDS.

Questions:

1. What tools are required to prepare AD LDS instance for synchronization?
2. What tool is required to perform synchronization of AD DS objects to an AD LDS instance?
3. What is the purpose of MS-AdamSyncConf.xml?



For more information, see AD LDS.

Lab 4: Configuring AD LDS

- Exercise 1: Configuring an AD LDS instance and an application partition
- Exercise 2: Configuring AD LDS Access Control
- Exercise 3: Configuring AD LDS Replication
- Exercise 4: Configuring AD DS and AD LDS synchronization

Logon information

Virtual machine	6426A-NYC-DC1, 6426A-NYC-SVR1
User name	Administrator
Domain	woodgrovebank
Password	Pa\$\$w0rd

Estimated time: 60 minutes

Objectives

After completing the lab, you will be able to:

- Configure an AD LDS instance and an application partition
- Configure AD LDS access control
- Configure AD LDS replication
- Configure AD DS and AD LDS synchronization

Scenario

Woodgrove Bank has offices located in several cities across the globe. By deploying Active Directory® Lightweight Directory Services (AD LDS), the bank plans to

implement directory services for various organizational applications that require access to directories. These directories store user and application data.

Consolidation Requirements:

To deploy an application, you must configure the AD LDS server role. Configuring AD LDS server role involves creating a new AD LDS instance known as WoodgroveApp1 and creating an application partition. You must perform the following activities to consolidate a solution:

- Provide support for AD LDS user class and related classes.
- Create and configure user accounts, groups and configure access control for the WoodgroveApp1 instance as follows:

Class	Object
Organizational Unit (OU) name	Security
User name	User1
Group name	Group1
Group members	User1
Access required	Grant Group1 permissions to only view the new container
Location	Create User(s) in the new container. Create Group(s) in the Roles container.

To avoid single point of failure, you need to create a second replica of the WoodgroveApp1 instance, and configure AD LDS replication.

Use the LDIFDE tool to add the following:

- Windows Server® 2008 schema to the AD LDS instance
- The schema extensions required to implement AD DS to AD LDS synchronization.

Users must be able to connect to the AD LDS instance by using Lightweight Directory Application Protocol (LDAP) port 6636 and secure LDAP (LDAPS) port 6389. To run the AD LDS instance, you need to configure the AD LDS instance by

using the NT AUTHORITY\NetworkService account. You also need to setup the WOODGROVEBANK\Administrator account to administer AD LDS.

Exercise 1: Configuring an AD LDS instance and an application partition

In this exercise, you will use the available virtual machine environment. Before you begin the exercise, you must:

1. Start the 6426A-NYC-DC1 virtual computer and log on using the user name **woodgrovebank\Administrator** and the password **Pa\$\$wOrd**.
2. Start the 6426A-NYC-SVR1 virtual computer and log on using the user name **woodgrovebank\Administrator** and the password **Pa\$\$wOrd**.

The main tasks for this exercise are as follows:

1. Add the AD LDS server role by using Server Manager.
2. Create an AD LDS instance known as WoodgroveApp1 by using AD LDS wizard.

► Task 1: To add the AD LDS server role by using Server Manager

1. On the 6426A-NYC-SVR1 virtual computer, install the AD LDS server role.
2. On the 6426A-NYC-DC1 virtual computer, install the AD LDS server role.

► Task 2: To create an AD LDS instance known as WoodgroveApp1 by using AD LDS Wizard

1. On the 6426A-NYC-SVR1 virtual computer, create a new AD LDS instance known as **WoodgroveApp1**.
2. Set the **LDAP port number** to **6389** and the **SSL port number** to **6636**.
3. Create an application directory partition known as **OU=App1,dc=woodgrovebank,dc=local**.
4. Configure the AD LDS instance to run by using the **NT AUTHORITY\NetworkService** account and set up the **WOODGROVEBANK\Administrator** account to administer AD LDS.
5. Import **MS-User.LDF**.

Exercise 2: Configuring AD LDS Access Control

The main tasks for this exercise are as follows:

1. Open ADSI Edit and connect to the created instance.
2. Create a container with the distinguished name “CN=Security,OU=App1,dc=woodgrovebank,dc=local”.
3. Create User1 in the created application partition.
4. Create Group1 in the Roles container of the application partition and add User1 to Group1.
5. Use Dsacls to grant Group1 List Only Special Permissions to only view the Security container.
6. Use ADSIEdit to connect to the instance and verify permissions.

► Task 1: To open ADSIEdit and connect to the created instance

1. On the 6426A-NYC-SVR1 virtual computer, use **ADSI Edit** to connect to the newly created instance.
2. Set the default **Connection Settings** name to **WoodgroveApplication**.
3. Connect to **OU=App1,dc=woodgrovebank,dc=local** on NYC-SVR:6389

► Task 2: To create a container with the distinguished name “CN=Security,OU=App1,dc=woodgrovebank,dc=local”

1. Use ADSI Edit to create a container object known as Security.

► Task 3: To create User1 in the created application partition

1. Use **ADSI Edit** to create a **user** object named **User1** located in the **Security** container.
2. Change User1 password to **Pa\$\$w0rd** and set the object’s **msDS-UserAccountDisabled** attribute value to **Not set**.

- ▶ **Task 4: To create Group1 in the Roles container of the application partition and add User1 into Group1**
 1. Create a **group** object known as **Group1** situated in the **Roles** container by using **ADSI Edit**.
 2. Add **User1** as a **Group1** member.

- ▶ **Task 5: To use Dsacls to grant Group1 List Only Special Permissions to only view the Security container**
 1. Use **dsacls** to grant Group1 the **List Only** Special Permissions to only view the Security container. Hint the command is:
dsacls \\NYC-SVR1:6389\CN=Security,OU=App1,dc=woodgrovebank,dc=local /G CN=Group1,CN=Roles,OU=App1,dc=woodgrovebank,dc=local:LO
 2. Review the output from the command to ensure that Group1 has list object permission to the partition.

- ▶ **Task 6: To use ADSI Edit to connect to the instance and verify permissions**
 1. Use **ADSI Edit** to connect to the instance by using User1 credentials.
 2. Select the **Simple bind authentication** check box when connecting.
 3. Verify that User1 has read access to objects in the Security OU.

Exercise 3: Configuring AD LDS Replication

The main tasks for this exercise are as follows:

1. Create a replica of WoodgroveApp1 by using the AD LDS wizard
2. Connect to the application partition on NYC-DC1 and verify initial replication by using ADSI Edit.

► **Task 1: To create a replica of WoodgroveApp1 by using the AD LDS wizard**

1. On the 6426A-NYC-DC1 virtual computer, create a replica of an existing instance by using the **AD LDS Setup Wizard**.
2. Set **LDAP port number 6389**, and **SSL port number 6636**.
3. Copy the **OU=App1,dc=woodgrovebank,dc=local** application directory partition.
4. Use the **Network service account** credentials and ensure that the **Currently logged on user** check box is selected when prompted.

► **Task 2: To connect to the application partition on NYC-DC1 and verify initial replication by using ADSI Edit**

1. On the 6426A-NYC-DC1 virtual computer, connect to the instance by using **ADSI Edit**.
2. Verify that the local replica contains the previously created data.

Exercise 4: Configuring AD DS and AD LDS synchronization

The main tasks for this exercise are as follows:

1. Add AD DS users to an AD LDS group.
2. Verify access to AD LDS for Windows® Users.
3. Configure synchronization between AD DS and AD LDS.
4. Verify AD DS to AD LDS synchronization.

► Task 1: To add AD DS users to an AD LDS group

1. On the 6426A-NYC-SVR1 virtual computer, add the user **woodgrovebank\administrator** as a member of **Group1** by using ADSI Edit.

► Task 2: To verify access to AD LDS for Windows® Users

1. Connect to the instance by using **ADSI Edit** and the **woodgrovebank\administrator** credentials.
2. Select the **Simple bind authentication** check box when connecting.
3. Verify that the **woodgrovebank\administrator** account has read access to objects in the Security OU.

► Task 3: To configure synchronization between AD DS and AD LDS

1. On the 6426A-NYC-SVR1 virtual computer, run **ldifde -i -u -f ms-adamschemaw2k8.ldf -s NYC-SVR1:6389 -j . -c "cn=Configuration,dc=X" #configurationNamingContext** to add the Windows Server® 2008 schema to the AD LDS instance.
2. Run **ldifde -i -f MS-AdamSyncMetadata.ldf -s NYC-SVR1:6389 -j . -c "cn=Configuration,dc=X" #configurationNamingContext** to add the schema extensions required to implement AD DS to AD LDS synchronization.
3. Open **MS-AdamSyncConf.xml** in Notepad and make the appropriate modifications as follows:
 1. In the <source-ad-name> line, change **fabrikam.com** to **woodgrovebank.com**.

2. In the <source-ad-partition> line, change dc=fabrikam,dc=com to dc=woodgrovebank,dc=com.
 3. In the next line, after <source-ad-account>, type Administrator.
 4. In the next line, after < account-domain >, type WoodgroveBank.com.
 5. In the <target-dn> line, change dc=fabrikam,dc=com to ou=app1,dc=woodgrovebank,dc=local.
 6. In the <base-dn> line, change dc=fabrikam,dc=com to OU=NYC,DC=Woodgrovebank,DC=com.
4. Save file as C:\Windows\Adam\WoodgroveSync.xml.
 5. Run `adamsync /install NYC-SVR1:6389 .\WoodgroveBank.xml`
 6. Run `adamsync /sync NYC-SVR1:6389 OU=App1,dc=woodgrovebank,dc=local /log Adamsynclog.txt.`

► **Task 4: To verify AD DS to AD LDS synchronization**

1. On the 6426A-NYC-SVR1 virtual computer, verify that the OU=NYC container was created in the application partition by using ADSIEdit.



After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review: Configuring AD LDS

In this lab, you have:

- Configured AD LDS instances and application partitions
- Configured AD LDS Access Control
- Configured AD LDS Replication
- Configured AD DS and AD LDS synchronization

Lab Resources

There are no additional lab resources for this lab.

Module 5


Configuring AD FS

Contents:

Lesson 1: Overview of AD FS	5-3
Lesson 2: AD FS Deployment Scenarios	5-14
Lesson 3: Deploying AD FS	5-26
Lesson 4: Implementing AD FS Claims	5-38
Lab 5A: Configuring AD FS for Federated Web SSO by Using Forest Trust Scenario	5-49
Lab 5B: Configuring Active Directory Federation Services by Using Federated Web SSO Scenario	5-65

Module Overview

- Overview of AD FS
- AD FS Deployment Scenarios
- Deploying AD FS
- Implementing AD FS Claims



Configuring Active Directory® Federation Services (AD FS) is one of the key aspect in configuring Identity and Access (IDA) solution with Windows Server® 2008 Active Directory®.

To configure AD FS, you should be familiar to the concept of AD FS and its various deployment scenarios. In addition, you know how to deploy AD FS in your organization and implement AD FS claims.

Lesson 1

Overview of AD FS

- What Is Identity Federation?
- Identity Federation Scenarios
- Identity Federation Business Requirements
- What Is a Federation Trust?
- AD FS Components

To deploy AD FS, you need to identify the key aspects of AD FS. Identify various identity federation scenarios and the requirements of an identity federation business. In addition, you will be taken through the concept of Federation Trust and AD FS components.

What Is Identity Federation?

Identity Federation:

Enables user access to resources between different organizations or different server platforms

Allows an organization to retain control over who can access resources

Requires an identity federation partnership to provide a form of trust between two organizations

Provides an agreement to define which resources will be accessible to the other organization and how access to the resources will be enabled

Key Points

Identity federation is a process that enables the distribution of identification, authentication, and authorization across organizational and platform boundaries. You can implement identity federation between two organizations that have a relationship of trust between them. As a part of the trust, the organizations define the resources that can be accessed by the other organization, and the process to enable such an access.

You can use the AD FS server role to implement identity federation on Windows Server® 2008. AD FS is an identity solution that provides streamlined access to internal and external browser-based clients for one or more Internet-based applications that are protected. This is possible even when the user accounts and applications are located across a variety of networks or organizations.

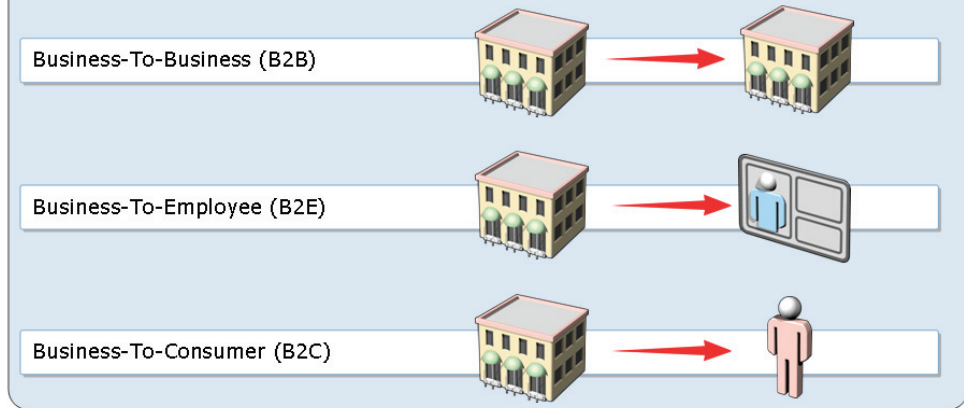


For more information, see:

- What's New in AD FS in Windows Server® 2008
- AD FS

Identity Federation Scenarios

Identity federation allows secure and efficient communication and collaboration in the following three scenarios:



Key Points

You can use AD FS to share securely the information on user identity over federation trusts. You can use a combination of various AD FS server roles to federate identities to meet the needs of your organization.

The following table describes various business scenarios, such as business-to-business (B2B), business-to-employee (B2E), and business-to-consumer (B2C).

Scenario	Description
B2B	<p>You can use AD FS in your organization to work alongside trusted partners, suppliers, and contractors. Federation trust helps organizations to work more efficiently without having to manage identities across various organizations.</p> <p>Identity federation provides a single logon that allows users to use their corporate credentials to sign in without exposing the</p>

Scenario	Description
	credentials to business partners.
B2E	<p>You can use AD FS to provide resources over the Internet to employees who are out of office. In addition, you can provide access to business applications on a perimeter network for users inside your organization. For example, you may integrate various internal systems to create information portals to provide consolidated information to users.</p> <p>AD FS can also be used to provide secure access to applications when you facilitate single sign-on access for the users.</p>
B2C	<p>You can use AD FS to provide resources over the Internet to individual users who are not employees and who may not have user accounts in any forest of the partner organization. In this scenario, you can create user accounts for customers in AD DS or AD LDS, and then implement a single authentication to access multiple applications.</p>



For more information, see **Federation scenarios**.

Discussion: Identity Federation Business Requirements

- What business requirements would lead to the deployment of an identity federation solution?

Key Points

Administrators can use AD FS to control user-access to resources, both within the organization and at partner organizations. You must identify the appropriate business requirements and map them to one of the supported deployment scenarios.

Users can use AD FS for Web-based, single-sign-on (SSO) authentication that supports B2B scenarios. In addition, AD FS can be designed for Federated Web SSO with Forest Trust to support B2E scenarios. You can also use AD FS for Web SSO to support customer access to applications in B2C scenarios.

Question: Identify the business requirements that can lead to the deployment of an identity federation solution.



For more information, see **What's New in AD FS in Windows Server® 2008**.

MCT USE ONLY. STUDENT USE PROHIBITED

What Is a Federation Trust?

A federation trust relationship provides efficient communication between organizations.

- **Federation trust:** This is the embodiment of a partnership between two organizations
- **Account partner:** This stores and manages user accounts in Active Directory® store or AD LDS
- **Resource partner:** This hosts the Web servers that host Web-based applications

Key Points

A federation trust is a business agreement between two organizations. This trust can be established when two partner organizations deploy at least one AD FS federation server. In addition, these partners must configure their Federation Service settings appropriately. Federated B2B partnerships identify business partners as one of the following types of organization.

Organization Type	Description
Resource Organization	These organizations own and manage resources that can be accessed from the Internet. They can deploy AD FS servers and AD FS-enabled Web servers to manage access to protected resources for trusted partners. These partners include external third parties or other departments in the same organization.
Account Organization	These organizations own and manage user accounts. They deploy AD FS servers that authenticate local users. These servers also create security tokens that the federation servers in the

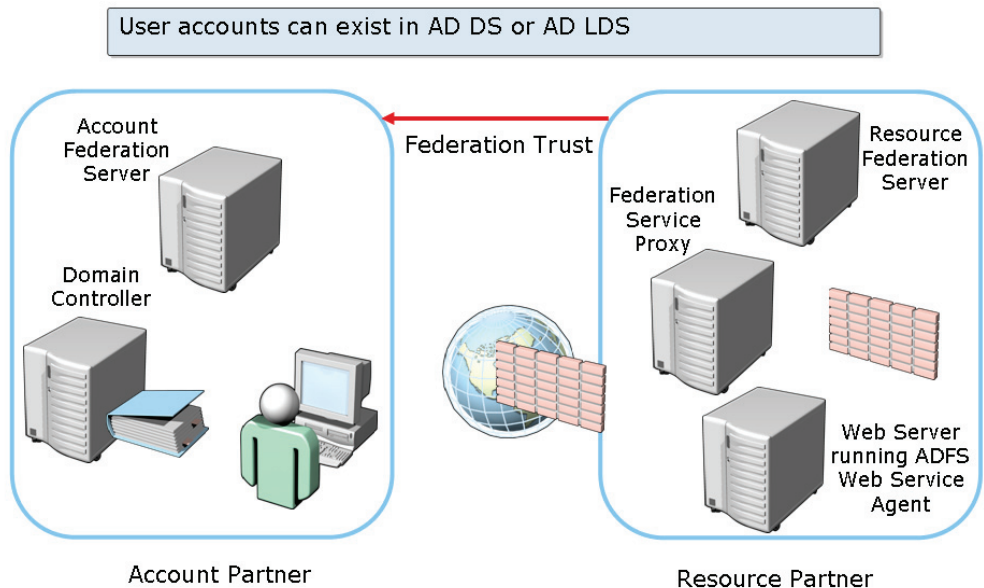
Organization Type	Description
	resource organization can use to decide on authorization.

After creating the federation trust, users in the account partner organization can send authentication requests by using the federation trust to the Web server in the resource partner organization. Federation trusts are not used in the Web SSO scenario.



For more information, see **Federation scenarios**.

AD FS Components



Key points

An AD FS solution consists of the following components:

- **Federation Trust.** This component is a part of the AD FS implementation when a business agreement or partnership is forged at an inter-organizational or intra-organizational setup. You can use AD FS to create a federation trust between two organizations for users to access resources across organizations or technical boundaries.
- **Account Partner.** This component in the federation trust hosts and manages user accounts of the trust. You can store user accounts in AD DS, Active Directory® Application Mode (ADAM), or AD LDS.
- **Resource Partner.** This component in the federation trust stores Web servers that host single or multiple Web-based applications. The resource partner trusts the account partner to authenticate users and provide security.

- **Federation Service (Server).** The Federation Service server functions as a security token service. In addition, this service routes authentication requests from external user accounts in partner organizations and clients on the Internet. All implementations of AD FS require at least one Federation Service to be installed.
- **Federation Service Proxy.** This component is usually deployed in a perimeter network. This deployment helps protect a federation server at the account partner level or at the resource partner level, or both. You can implement a proxy of the federation server to avoid direct exposure of the federation servers to the Internet.
- **AD FS Web Agents.** AD FS Web agents provide a connection between a Web-based application and the Federation Service. You can implement an AD FS Web agent as an Internet Server Application Programming Interface (ISAPI) extension in Internet Information Services (IIS) that either allows or denies access to two types of Web applications. The two types of Web applications are:
 - **Claims-aware applications.** These applications are written or modified to identify the way to use AD FS claims.
 - **Windows®-based token-enabled applications.** These applications, also known as legacy applications, are not coded to support claims. Instead, these applications can decide on authorization based on security identifiers (SIDs) and access control lists (ACLs).



For more information, see **Federation scenarios**.

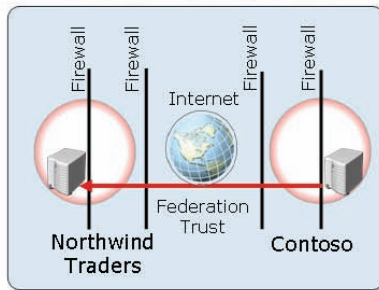
Lesson 2

AD FS Deployment Scenarios

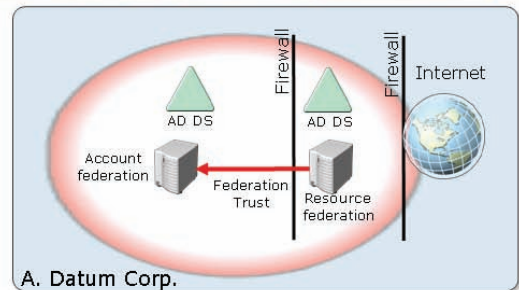
- AD FS Deployment Options
- How ADFS Traffic Flows in a B2B Federation Scenario
- How ADFS Traffic Flows in a B2E Federation Scenario
- How ADFS Traffic Flows in a B2C Federation Scenario
- AD FS Deployment Considerations

Deployment of AD FS includes working on various deployment scenarios including B2B, B2E, and B2C federation scenarios. The key aspect is to identify how AD FS traffic flows in each federation scenario and conclude on various deployment considerations of AD FS.

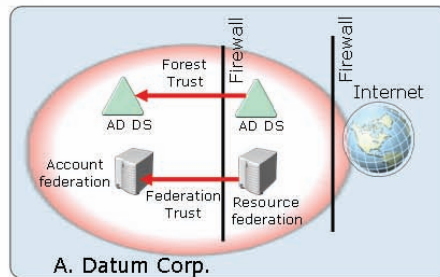
AD FS Deployment Options



Federated Web SSO



Web SSO



Federated Web SSO with Forest Trust

Key points

The success of the AD FS design depends on correct identification of the AD FS deployment goals. Once you have determined the goals related to deployment, you can map those goals to a specific AD FS design. There are three primary AD FS designs. However, you can also create a hybrid or custom AD FS design to meet the needs of the organization. You can use any combination of the AD FS deployment goals to create these designs.

The deployment can be mapped to the following options:

- **Federated Web SSO.** In this option, it may be two organizations or the security realms in a single organization that will provide access to applications across organizations.
- **Federated Web SSO with Forest Trust.** In this option, although an organization uses multiple forests to manage user accounts, it still uses AD FS to provide the SSO feature.

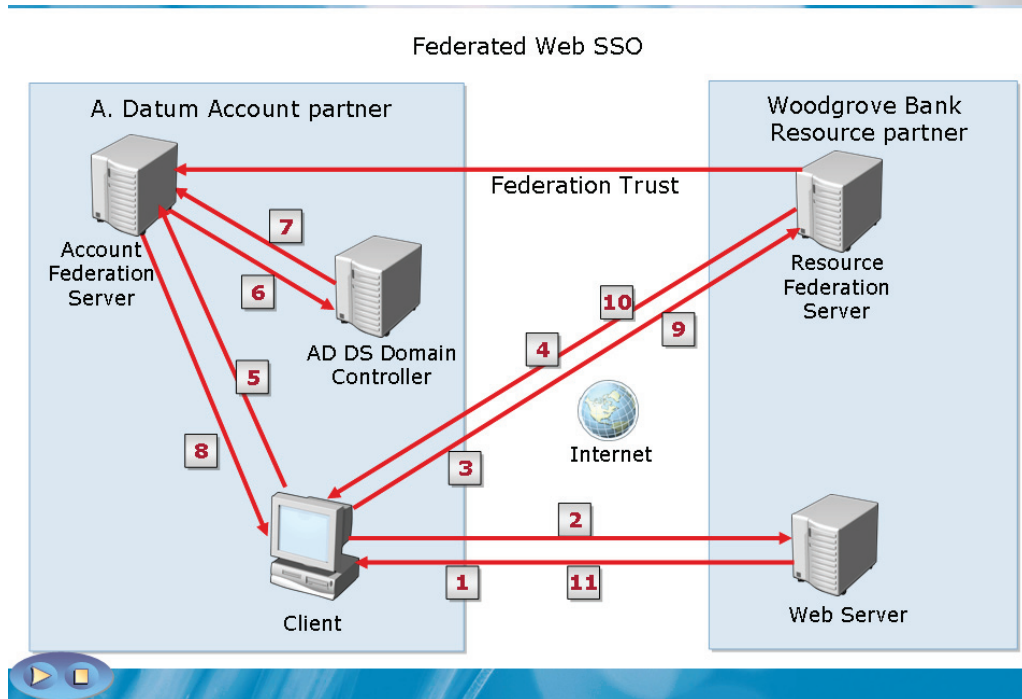
- **Web SSO.** In this option, a single organization deploys one or more Web applications that the users can access within an organization or in between organizations. With the help of AD FS, users can access these applications after a single authentication.



For more information, see:

- **Federation scenarios**
- **What's New in AD FS in Windows Server® 2008**

How ADFS Traffic Flows in a B2B Federation Scenario



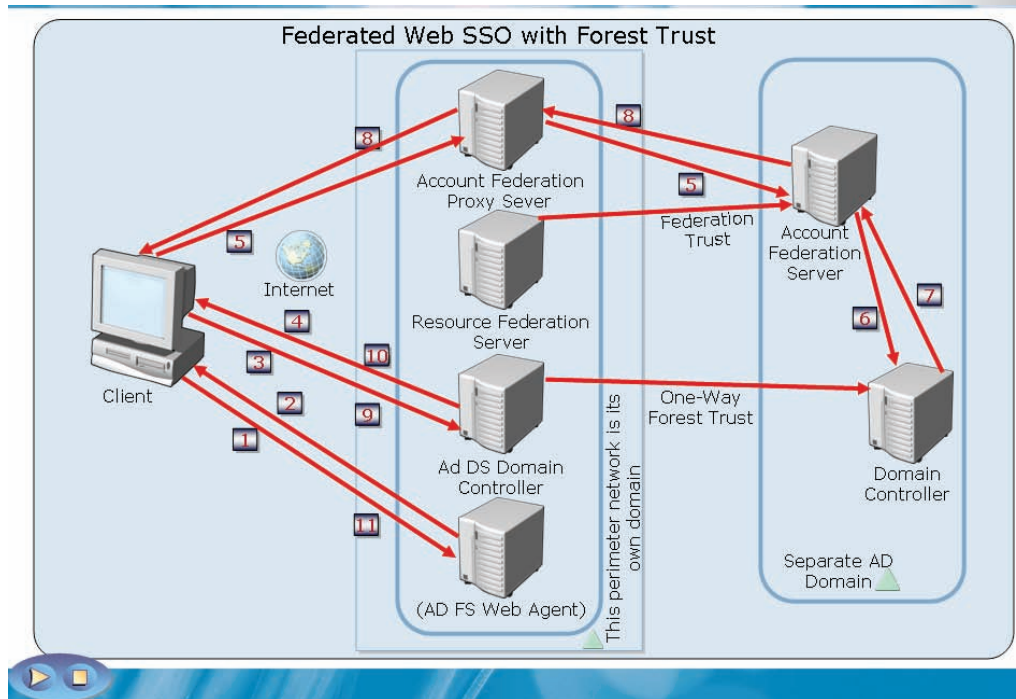
Key points

You can deploy AD FS to support B2B scenarios and collaboration across business units with independent forests. This type of deployment helps an organization to create a relationship like the federation trust for users in one organization (account partner) to access Web-based applications in another organization (resource partner). The following steps illustrate an AD FS traffic flow in B2B:

1. A user at a datum makes a request over Hypertext Transfer Protocol Secure (HTTPS). This request is for accessing an application that runs on the Web server at Woodgrove Bank.
2. The AD FS Web Agent intercepts the request and checks from the Web server to see if the client has presented a cookie to legitimize the request.
3. The client sends an HTTPS request to the federation server of the resource partner to determine the location of the account for that user. This process is known as the home realm discovery.

4. The client is redirected to the federation server of the account partner of a datum.
5. The client furnishes an HTTPS request to the Federation Service of the account partner.
6. AD DS uses Windows® integrated authentication to authenticate the user. The user can also be authenticated when he or she provides credentials when prompted by the federation server.
7. AD DS authenticates the user and returns a success message to the federation server.
8. The client receives an authentication cookie with the claims data placed in a digitally signed security token. Further, there is a redirection back to the Federation Service of the resource partner.
9. The client sends the security token to the Federation Service of the resource partner for validation of the security token.
10. The federation server creates, signs, and issues a new token to the client, after the successful validation of the security token.
11. The Web agent receives the request and validates the signed tokens. If successful, the agent issues a cookie and forwards the request to the Web service process.

How ADFS Traffic Flows in a B2E Federation Scenario



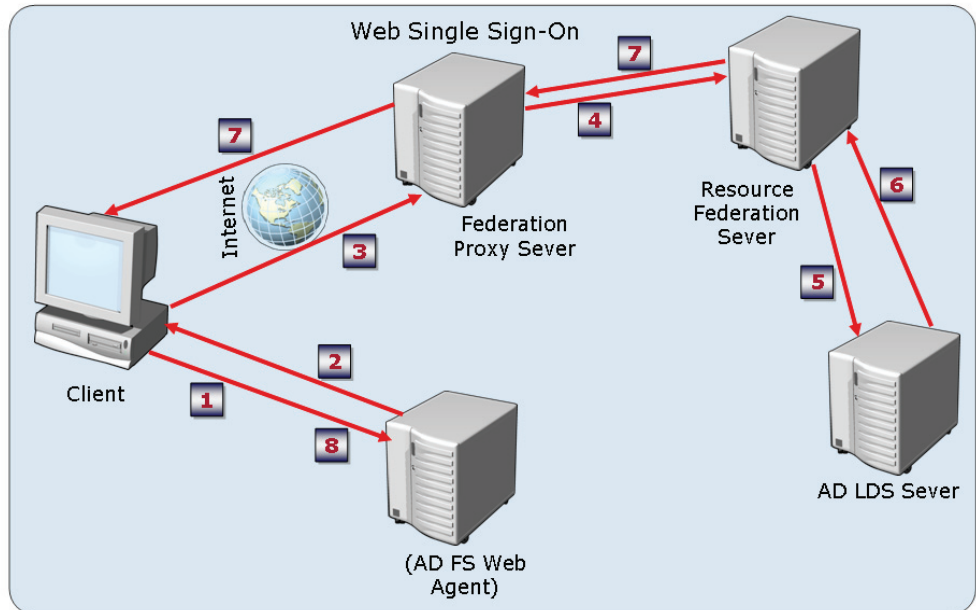
Key Points

The following steps illustrate the AD FS traffic flow in a B2E federation scenario:

1. An employee of Woodgrove Bank is traveling and uses a Web browser to make a request over HTTPS for accessing an application that runs on the Web server in the perimeter network.
2. The AD FS Web Agent intercepts the request and checks from the Web server to see if the client has presented a cookie to legitimize the request. If the client does not have the required cookie, the AD FS Web agent redirects the client to the federation server of the resource.
3. The client sends an HTTPS request to the federation server of the resource.
4. The resource federation server redirects the client to the proxy server of the account federation.

5. The proxy server of the account federation requests the user credentials, and then passes the request to the account federation server.
6. The account federation server forwards the authentication request to the AD DS domain controller.
7. If Active Directory® authenticates the user, it sends the success message back to the account federation server along with other information about the user stored in the directory—attributes and group memberships for generating the user's claims.
8. If the authentication is successful, the authentication and other information is wrapped up in a claim and passed back to the client by using the proxy, with a redirect message that tells the client to present the security token to the resource Federation Service.
9. The Web browser presents the security token to the resource federation server. The resource federation server builds the security and AD FS authentication tokens for the Web application.
10. The resource federation server provides the tokens to the Web browser and redirects the client to connect to the AD FS Web application.
11. The Web agent receives the request and the AD FS authentication cookie. The application is Windows NT® token-based and not a claims-aware application. Therefore, the application must build a copy of the Windows NT® token from the security token. The application then uses this Windows NT® token to impersonate the user account and provide the appropriate level of access.

How ADFS Traffic Flows in a B2C Federation Scenario



Key Points

An organization can provide resources across the Internet to individual users who are not employees of the organization or may not have partner user accounts. The organization first creates user accounts for those customers in AD LDS. It authenticates them once and then allows access to multiple applications.

The following list illustrates AD FS traffic flow in a B2C federation scenario:

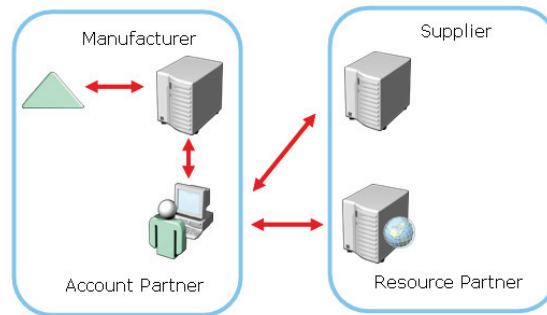
1. A customer of Woodgrove Bank uses a Web browser to create a request over HTTPS to access an application that runs on the Web server on the perimeter network at Woodgrove Bank.
2. The AD FS Web agent intercepts the request and checks whether the client computer has an AD FS authentication cookie that allows access to the application. If the client does not have this cookie, the client request is refused and the client is redirected to the proxy server of the federation.

3. The client sends an HTTPS request to the proxy server of the federation. The client is redirected to the authentication page of federation proxy server and is asked to fill the logon details.
4. The federation proxy server accepts the logon details, and the request is passed to the Federation Service of the resource.
5. The resource federation server goes directly to a local account store called the AD LDS to request authentication for the user.
6. AD LDS checks the authentication of the user. The resource federation server retrieves attributes from AD LDS by LDAP. It then builds the security and the AD FS authentication tokens for the AD FS-enabled Web server application.
7. The authentication information and other information is placed in a claim and passed back to the client via the proxy by using a redirect message, which informs the client to present the security token to the original URL.
8. The AD FS Web agent receives the request, validates the signed tokens, and if successful, issues another AD FS authentication cookie. Further, it forwards the request to the Web service process, which provides access to the application based on the claims.

AD FS Deployment Considerations

Consider the following when planning an AD FS solution:

- AD FS scenario to be deployed
- Certificate management
- Directory store requirements
- Application type



Key Points

- Consider the following points when you design the AD FS deployment:
- **Deployment of AD FS scenario.** In this consideration, the scenario that you deploy will determine the subsequent requirements for your AD FS solution. For example, if you provide collaboration between two organizations, you will deploy the Federated Web SSO scenario. On the other hand, if you provide access to a Web-based application, to your employee or customer, you can deploy either Web SSO or Federated Web SSO alongside the forest trust scenario.
- **Certificate management.** In this consideration, you must determine whether you will use a third-party organization for server certificates or deploy Microsoft® Certificate Services. You can use certificates to sign token and use SSL or TLS. You can also deploy self-signed certificates for the Federation Service. Self-signed certificates do not require a CA. You must configure these certificates explicitly in certain locations on the server as trusted certificates.

With self-signed certificates, it is difficult to establish an infrastructure to manage the life cycle and trust of certificates, and to renew and revoke certificates.

- **Directory store requirements.** In this consideration, you must determine the location for user accounts to be stored. The corresponding storage location would include AD DS and AD LDS. You can also decide to implement a separate directory store from your internal environment.
- **Application type.** In this consideration, based on the type of application to be deployed with AD FS, you must determine whether a forest trust is required between the directory stores that host the account and the resource federation servers. For example, a token-based application may require specific configurations, whereas a claims-aware application may not require them.

Lesson 3

Deploying AD FS

- AD FS System Requirements
- AD FS Prerequisites
- AD FS Certificate Requirements
- How To Install the AD FS Server Role
- Federation Service Configuration Tasks
- What Is an AD FS Trust Policy?
- Configuring AD FS Web Agent

To deploy AD FS, you must know about AD FS system requirements, prerequisites, and certificate requirements. You will be taken through the steps to install the AD FS server role. You will also be introduced you to the federation service configuration tasks and the concepts of AD FS Trust Policy. In addition, you must identify AD FS Web Agent configuration.

AD FS System Requirements

AD FS requirements for the Federation Service, Federation Service Proxy and FD FS Web Agent Roles:

- One of the following:
 - Windows Server® 2003 R2 Enterprise Edition
 - Windows Server® 2003 D2 Datacenter Edition
 - Windows Server® 2008 Enterprise
 - Windows Server® 2008 Datacenter
- Internet Information Services (IIS)
- Microsoft® ASP.NET 2.0
- Microsoft® .NET Framework 2.0
- A Web site with Transport Layer Security/Secure Sockets Layer (TLS/SSL) configured

Key Points

The key requirements for deploying an AD FS system are:

- **Hardware Requirements.**

Hardware Requirement	Minimum Requirement	Recommended Requirement
Central Processing Unit (CPU) speed	133 megahertz (MHz)	550 MHz
Random Access Memory (RAM)	128 megabytes (MB)	256 MB
Disk space	10 MB	100 MB

- **Software Requirements.**

Server Hosting the Federation Service Role Service	Server Hosting the Federation Service Proxy Role Service	Server Hosting the AD FS Web Agent Role Service
Windows Server® 2008 Enterprise or Windows Server® 2008 Datacenter	Windows Server® 2008 Enterprise or Windows Server® 2008 Datacenter	Windows Server® 2008 Standard, Windows Server® 2008 Enterprise, or Windows Server® 2008 Datacenter
IIS	IIS	IIS
Microsoft® ASP.NET 2.0	Microsoft® ASP.NET 2.0	Microsoft® ASP.NET 2.0
Microsoft® .NET Framework 2.0	Microsoft® .NET Framework 2.0	Microsoft® .NET Framework 2.0
A default Web site that is configured with Transport Layer Security / Secure Sockets Layer (TLS/SSL)	A default Web site that is configured with TLS/SSL	A Web agent that has configured at least one Web site in IIS with TLS/SSL so that federated users can access Web-based applications that are hosted on the Web server.

- **Browser Requirements.** You can use current Web browser with JScript® activated as an AD FS client program.
- **Cookies.** You must configure client browsers to accept authentication cookies that AD FS creates. These are stored on client computers to provide SSO functionality.

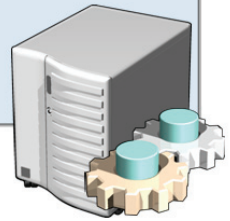


For more information, see **AD FS Role**.

AD FS Prerequisites

Network services critical to a successful AD FS deployment include:

- Active Directory® or AD LDS
- Domain Name System (DNS)
- Certificates



Key Points

To deploy AD FS successfully, several infrastructure components are required. You must configure the network infrastructure by using other prerequisites such as account store, name resolution, and certificates.

- **TCP/IP network connectivity.** You must configure a TCP/IP network connectivity between the:
 - Client
 - Domain controller
 - Computers that host the Federation Service
 - Proxy Federation Service, when used
 - AD FS Web Agent

- **Active Directory® or AD LDS.** AD FS requires at least one account store that is used to authenticate users and extract security claims for the users. Therefore, you must store accounts in Active Directory® or AD LDS.
- **Domain Name System (DNS).** DNS is required for user-friendly names to help users connect to computers and other resources on Internet Protocol (IP) networks.
- **Certificates.** Certificates are required to authenticate account and resource partners.

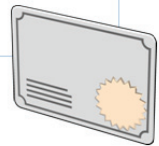


For more information, see **AD FS Role**.

AD FS Certificate Requirements

Certificates can be issued by a trusted Certification Authority. You can also use a self-signed certificate.

Role	Certificates Required
Federation Server	<ul style="list-style-type: none"> • Token-signing Certificate • Verification Certificate • SSL server authentication certificate
Federation Server Proxy	<ul style="list-style-type: none"> • SSL client authentication certificate • SSL server authentication certificate
ADFS Web Agent	<ul style="list-style-type: none"> • SSL server authentication certificate



Key Points

AD FS needs various certificates. These certificates will help to make communication secure and facilitate user authentications between Internet clients and federation servers. Each federation server needs to have a certificate to authorize a server called the server authentication certificate and one to sign all the security tokens called the token-signing certificate. Additionally, the AD FS trust policy requires an associated certificate, known as a verification certificate. A verification certificate is the public key portion of a token-signing certificate.

Federation servers need to have the following certificates:

- **Token-signing certificate.** A token-signing certificate is created to sign all security tokens produced by a federation server digitally.
- **Verification certificate.** A verification certificate is created to verify the validity of the federation server that has sent a security token. A verification certificate is also used to verify if the security token has been modified.

- **SSL server authentication certificate.** SSL server authentication certificate is created to make Web services traffic secure for communication with Web clients or the proxy federation server.

The certificates used with AD FS have the following sources:

- Internal certification authority (CA) or external CA
- Third-party CA
- Self-signed certificates



For more information, see **AD FS Role**.

Demonstration: How To Install the AD FS Server Role

- To install the AD FS server role
- To install the Federation Service role service

Key Points

The instructor will provide a demonstration to show how you can install the AD FS server role.

Questions:

- What are the available AD FS role services?
- Which are the two role services that cannot be installed on the same computer?
- What services are required to install the AD FS server role?



For more information, see **What's New in AD FS in Windows Server® 2008**.

Federation Service Configuration Tasks

Use the AD FS console to configure:

- Account Partners
- Resource Partners
- Trust Policy
- Account Stores
- ADFS-protected Applications
- Organization Claims

Key Points

- Specifying the Trust policy file to be used in AD FS communications
- Viewing and selecting the token-signing certificate used to sign security tokens
- Specifying Web pages associated with the Federation Service
- Setting debugging and logging to help troubleshoot the Federation Service
- Controlling anonymous access to organization claims

What Is an ADFS Trust Policy?

An AD FS trust policy consists of the configuration information that is associated with your Federation service.

Properties that can be configured include the following:

- Federation Service URI
- Federation Service endpoint URL
- Trust policy display name
- Verification certificates and federation server proxy certificates
- Event log level
- Advanced settings

Key Points

An AD FS trust policy defines the parameters that identify partners, certificates, account stores, claims, and other various properties. You need to configure a trust policy on both the account and the resource partners.

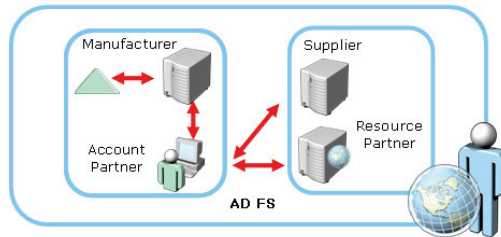
To create a federated partnership between two organizations, you need to define the trust policy on each of the AD FS servers. The trust policy will also include the public key of each federation server's verification certificates.

A default trust policy file is created when you install the AD FS sever role and is stored as an .xml file format.

Configuring AD FS Web Agent

Configuration options for AD FS Web Agent include:

- Federation Service URL
- Cookie path
- Cookie domain
- Return URL



Key Points

To configure the AD FS Web Agent for supporting Windows NT[®] token-based applications, you need to perform the following tasks:

- Specify whether the AD FS Web Agent for Windows NT[®] token-based applications is enabled.
- Provide a path to the location where the AD FS Web Agent stores the cookie for Windows NT[®] token-based application resources.
- Provide the domain name for which the cookie is valid.
- Specify the URL to which the AD FS Web Agent must direct the client after authentication.



For claims-aware applications, you still need to install the AD FS Web Agent; however, all configuration parameters take place in the Web.config file associated with the application.

Lesson 4

Implementing AD FS Claims

- What Are AD FS Claims?
- What Are Identity Claims?
- What Are Group and Custom Claims?
- What Is Incoming Claim Mapping?
- What Is Outgoing Claim Mapping?
- How To Configure AD FS Claim Mapping

To implement AD FS claims, you need to identify the key aspects of AD FS claims and identity claims. You should know the difference between group and custom claims. You should also identify the concept of incoming and outgoing claim mappings. Further, you need to know the steps to configure AD FS claim mapping.

What are AD FS Claims?

AD FS Claims:

- A statement made about a user that is understood by both the partners in an AD FS federation scenario.

The Federation Service supports following Claims:

- Identity Claims
- Group Claims
- Custom Claims



Key Points

Claims are statements that contain information about the user, such as a name, identity, privilege, or capability. Security tokens that authorize access to applications include claims. Claims originate from either an account store or an account partner.

AD FS supports the following types of claims:

- **Identity claim.** This claim includes User Principal Names (UPNs), e-mail addresses, or common names.
- **Group claim.** This claim indicates a membership in a security group. This claim can also indicate a role that is assigned to a user.
- **Custom claim.** This claim contains custom information about a user. For example, a custom claim might contain the employee ID number of a user.

AD FS provides the following grouping of claims:

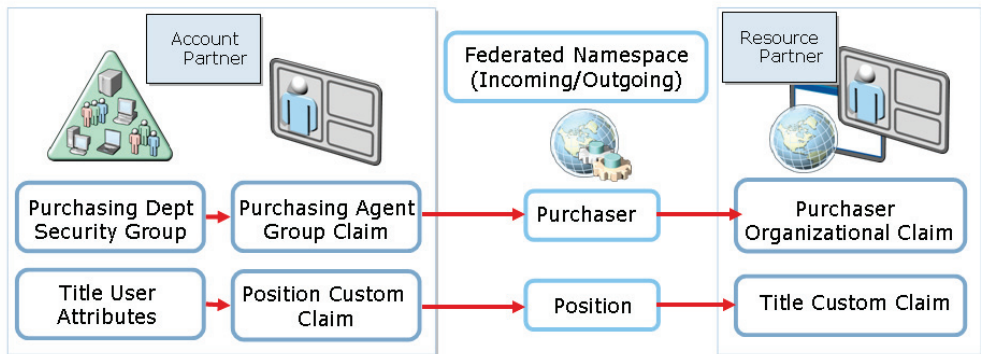
- **Organization claims.** This group is the normalized set of claims in an organization. You can perform internal Federation Service actions on the organization claims set.
- **Incoming claims.** This group consists of claims that a specific resource partner receives from the account partner organization.
- **Outgoing claims.** This group consists of claims that the account partner sends to a specific resource partner.



For more information, see **Federation scenarios**.

What Are Group and Custom Claims?

- Group claims contain group membership information.
- Custom claims contain information about a user.



Key Points

Group claims indicate membership information on a particular group or role.

You can define individual claims that have the group type, Group claims. For example, you can define the following set of group claims:

- Managers
- Executives
- Purchasing Agents

To populate and map claims, you can use each group claim as a separate administration unit.

Custom claims provide information about a user in the form of name-value pairs. For example, a custom claim may specify a user's employee ID attribute.



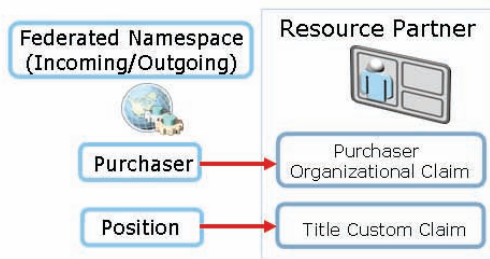
For more information, see **Federation scenarios**.

What Is Incoming Claim Mapping?

- Incoming Claim Mapping maps claims sent from the account partner to claims used by the resource partner.

The two types of outgoing claim mappings are:

- Incoming Group Claim Mapping
- Incoming Custom Claim Mapping



Key Points

Incoming claim mapping converts claims sent by an account partner into claims used by the resource partner. The resource partner then uses these claims for authorization. This process provides interoperability between different security mechanisms.

For example, an account partner sends a security token for a user to the resource partner. The security token contains a group claim, SalesReps, for the user. The resource partner cannot provide authorization decisions based on the account user's membership in the SalesReps group. Therefore, you use an incoming group claim mapping to map the SalesReps group claim in the account Federation Service to the organization group claim in the resource Federation Service. The organizational group claim is named Purchasers. The resource partner provides access to the local security group that is mapped by the Purchasers claim.



For more information, see:

- **Understanding Organizational Group Claims**
- **Federation scenarios**

What Is Outgoing Claim Mapping?

- Outgoing claim mapping modifies an account partner's organization claim to match a common attribute as agreed with the resource partner.

The two types of outgoing claim mappings are:

- Outgoing group claim mapping
- Outgoing custom claim mapping



Key Points

In the account Federation Service, you must map an organization claim, such as a group or custom claim, to an outgoing claim. The resource Federation Service receives the outgoing claim when a user in the account organization requests access to a resource.

The resource federation server receives the outgoing claim as an incoming claim. This incoming claim is configured to map to a local organization claim. The resource Federation Service uses the local organization claim to provide authorization decisions.



For more information, see:

- [Understanding Organizational Group Claims](#)
- [Federation scenarios](#)

Demonstration: How To Configure AD FS Claim Mapping

- To configure Organizational claims
- To configure Group and Custom claims
- To configure outgoing and incoming claim mapping

Key Points

The instructor will provide a demonstration to show how you can configure AD FS claim mapping.

Questions:

- What are claims?
- What is claim mapping?
- Why do you need to define identical claims for both AD FS partners?



For more information, see:

- **Understanding Organizational Group Claims**

- Federation scenarios

Lab 5A: Configuring the Federated Web SSO with Forest Trust Scenario

- Exercise 1: Installing the AD FS Server Role
- Exercise 2: Configuring Certificate Requirements
- Exercise 3: Configuring the AD FS Web Agent
- Exercise 4: Configuring the Web Server application on 6426A-CHI-DC1
- Exercise 5: Configuring the Forest Trust and the Federated Trust Policies
- Exercise 6: Configuring the Federation Service Within the Internal Network
- Exercise 7: Configuring the Federation Service Within the Extranet
- Exercise 8: Testing the AD FS Implementation

Logon information

Virtual machine	6426A-NYC-DC1	6426A-CHI-DC1	6426A-NYC-CL1
User name	Administrator	Administrator	William
Domain	woodgrovebank.com	WDextranet.net	woodgrovebank.com
Password	Pa\$\$wOrd	Pa\$\$wOrd	Pa\$\$wOrd

Estimated time: 75 minutes

Objectives

After completing the lab, you will be able to:

- Install the AD FS server role
- Configure certificate requirements
- Configure the AD FS web agent
- Configure the Web server application on the 6426A-NYC-EXNET1 virtual computer
- Configure the forest trust and the federated trust policies
- Configure the federation service within the internal network
- Configuring the federation service within the extranet

- Test the AD FS implementation

Scenario

Woodgrove Bank is a large multinational corporation having office locations across five countries. The organization is currently running Windows Server® 2003, but is planning to implement Windows Server® 2008.

Consolidation Requirements:

As the corporate server technology specialist, it is your duty to install and configure Windows Server® 2008 computers in the organization.

Woodgrove Bank is evaluating the use of Active Directory® Federation Services (AD FS) to provide secure access to an application located in the company's perimeter network. To do so, you must perform the following consolidation activities:

- Configure the perimeter network with its own domain named Northwindtraders.com.
- Provide an application within the perimeter network that is a Windows® token-based application along with a Forest Trust relationship with the internal Active Directory® domain.
- Implement the AD FS components to provide secure access to the application.

Exercise 1: Installing the AD FS Server Role

In this exercise, you will use the available virtual machine environment. Before you begin the exercise, you must:

1. Start the 6426A-NYC-DC1 virtual computer and log on by using the user name **woodgrovebank/Administrator** and the password **Pa\$\$w0rd**.
2. Start the 6426A-CHI-DC1 virtual computer and log on by using the user name **Northwindtrader/Administrator** and the password **Pa\$\$w0rd**.

The main tasks of this exercise are as follows:

1. Install the AD FS server role on the 6426A-NYC-DC1 virtual computer.
2. Install the AD FS server role on the 6426A-CHI-DC1 virtual computer.

► Task 1: To install the AD FS server role on the 6426A-NYC-DC1 virtual computer

- Use Server Manager to install the **Active Directory® Federation Services** server role. Use the following options:
- Role Service: Federation Service
- Install a self signed certificate for Secure Socket Layer (SSL) Encryption
- Install a self-signed certificate for token-signing.
- Accept all other default settings.

► Task 2: To install the AD FS server role on the 6426A-CHI-DC1 virtual computer

- Use Server Manager to install the **Active Directory® Federation Services** server role. Use the following options:
- Role Service: Federation Service
- Install a self signed certificate for SSL Encryption
- Install a self signed certificate for token-signing.
- Web Server (IIS): In addition to all default settings, also select **ASP**.

- Accept all other default settings.

Exercise 2: Configuring Certificate Requirements

The main tasks of this exercise are as follows:

1. Configure the SSL certificate for the 6426A-NYC-DC1 virtual computer.
2. Configure the SSL certificate for the 6426A-CHI-DC1 virtual computer.

▶ **Task 1: To configure the SSL certificate for the 6426A-NYC-DC1 virtual computer**

- Use a **Certificates MMC** focused on the Computer account to copy and paste the **nyc-dc1.woodgrovebank.com** certificate and the **Federation Server NYC-DC1** certificate to the **Trusted Root Certification Authorities** node.

▶ **Task 2: To configure the SSL certificate for the 6426A-CHI-DC1 virtual computer**

- Use a **Certificates MMC** focused on the Computer account to copy and paste the **CHI-DC1.NorthWindTraders.com** certificate and the **Federation Server CHI-DC1** certificate to the **Trusted Root Certification Authorities** node.

Exercise 3: Installing the AD FS Web Agent

The main tasks of this exercise are as follows:

1. Install the AD FS Web Agent to support Windows® Token-based applications on the 6426A-CHI-DC1 virtual computer.
2. Ensure that the SSL certificate is bound to the default Web Site on the 6426A-CHI-DC1 virtual computer.

► **Task 1: To install the AD FS Web Agent to support Windows® Token-based applications on the 6426A-CHI-DC1 virtual computer**

- On the 6426A-CHI-DC1 virtual computer, use **Server Manager** to add the **Windows® Token-based Agent Role Service** with the following options:
- Set **Federation Server** to the **6426A-CHI-DC1 virtual computer.Northwindtraders.com**.
- Restart the 6426A-CHI-DC1 virtual computer.
- Log on as **Administrator** by using the password **Pa\$\$w0rd**.

► **Task 2: To ensure that the SSL certificate is bound to the Default Web Site on the 6426A-CHI-DC1 virtual computer**

- On the 6426A-CHI-DC1 virtual computer, use **Internet Information Services (IIS) Manager** to verify the SSL bind between the **6426A-CHI-DC1 virtual computerNorthwindtraders.com** certificate to the default Web Site (port 443).
- Enforce the use of SSL on the **Default Web Site**.

Exercise 4: Configuring the Web Server application on the 6426A-CHI-DC1 virtual computer

The main task of this exercise is to:

1. Configure the Token-based application.
2. Configure the AD FS Web Agent.

► Task 1: To configure the Token-based application

- Use **Internet Information Services (IIS) Manager to Add Application**.
- Set **Alias** to **tokenapp**.
- Select **Classic .NET AppPool** and set the folder path to **C:\inetpub\wwwroot\tokenapp**. (Create a new folder called tokenapp)
- Copy the content of **\\NYC-DC1\d\$\Labfiles\Mod5\tokenapp** to **C:\inetpub\wwwroot\tokenapp**.
- Move the **blog.txt** file from the **tokenapp** folder to C:\.

► Task 2: To configure the AD FS Web Agent

- Use **Internet Information Services (IIS) Manager**, click **CHI-DC1** and then locate **Federation Service URL**.
- In the **Federation Service URL**, ensure that the following URL is entered:
https://CHI-DC1.NorthwindTraders.com/adfs/fs/federationsservice.asmx
- In the Console pane, expand **Default Web Site** and then click **tokenapp**
- In the Details pane open **Authentication** and enable **AD FS Windows Token-Based Agent Authentication**.
- Click **Edit** and set **Return URL** to the following: **https://CHI-DC1.NorthwindTraders.com/tokenapp/**

Exercise 5: Configuring the Forest Trust and the Federated Trust Policies

The main tasks of this exercise are as follows:

1. Configure a forest trust between the intranet and the extranet forest.
 2. Configure and export the trust policy on the 6426A-CHI-DC1 virtual computer.
 3. Configure and export the trust policy on the 6426A-NYC-DC1 virtual computer.
- **Task 1: To configure a forest trust between the intranet and the extranet forest**
- On the 6426A-NYC-DC1 virtual computer, use **Active Directory Domains and Trusts** to configure a one way incoming forest trust between **woodgrovebank.com** and **Northwindtraders.com**.
 - Set **Name** to **NorthwindTraders.com**.
 - Set **Sides of Trust** to **Both this domain and the specified domain**.
 - Use the username **Administrator** and the password **Pa\$\$w0rd**.
 - Set **Authentication Level** to **Forest-wide authentication**.
- **Task 2: To configure and export the trust policy on the 6426A-CHI-DC1 virtual computer**
- On the 6426A-CHI-DC1 virtual computer, use **Active Directory Federation Services** to export the **Trust Policy**.
 - Set **File** to **C:\CHIPolicy.xml**.
 - Open the **Run** command prompt box and browse to **\\NYC-DC1\c\$**.
 - Copy **C:\CHIPolicy.xml** from the **6426A-CHI-DC1 virtual computer** to **C:** on **NYC-DC1**.

- ▶ **Task 3: To configure and export the trust policy on the 6426A-NYC-DC1 virtual computer**
 - On the 6426A-NYC-DC1 virtual computer, use **Active Directory Federation Services** to export the **Trust Policy**.
 - Set **File** to **C:\WoodgrovePolicy.xml**.

Exercise 6: Configuring the Federation Service Within the Internal Network

The main tasks of this exercise are as follows:

1. Create the TokenApp organization claim.
2. Add the Woodgrovebank.com Active Directory account store.
3. Add Northwindtraders.com as a resource partner to Woodgrovebanks' Federation Service
4. Create an outgoing group claim mapping from the TokenApp organization claim to the TokenAppMapping outgoing claim

► Task 1: To create the TokenApp organization claim

- On the 6426A-NYC-DC1 virtual computer, use **Active Directory Federation Services (AD FS)** to create a new **Organization Claim**.
- Set **Claim name** to **TokenApp** and ensure **Group claim** is selected.

► Task 2: To add the Woodgrovebank.com Active Directory® account store

- On the 6426A-NYC-DC1 virtual computer, use **Active Directory Federation Services (AD FS)** to add new **Account Store**.
- Select **Active Directory Domain Services (AD DS)** and enable it.

► Task 3: To add Northwindtraders.com as a resource partner to Woodgrovebanks' Federation Service

- Use **Active Directory Federation Services (AD FS)** to add configure **NorthwindTraders.com** as a resource partner by using the following parameters:
- Policy file to import: **Yes**
- Path: **C:\CHIPolicy.xml**
- Resource Partner Details: **Defaults**
- Federation Scenario: **Federated Web SSO with Forest Trust**

- Resource Partner Identity Claims: **Defaults**
 - Select UPN Suffixes: **Pass all UPN suffixes through unchanged**
 - Enabled: **Yes**
- ▶ **Task 4: To create an outgoing group claim mapping from the TokenApp organization claim to the TokenAppMapping outgoing claim**
- On the 6426A-NYC-DC1 virtual computer, use **Active Directory Federation Services** to create an **Outgoing Group Claim Mapping**.
 - Set the name to **TokenApp** for **Organizational group claims** in the **Create a New Outgoing Group Claim Mapping** box.
 - Use **TokenAppMapping** for **Outgoing group claim name** box.

Exercise 7: Configuring the Federation Service within the Extranet

The main tasks of this exercise are as follows:

1. Open the Active Directory® Federation Services console and add the Northwindtraders.com Active Directory® account store on the 6426A-DCI-CHI virtual computer.
2. Create the WGAApp organization claim and map it to the WGAAppUser security group.
3. Add Woodgrovebank.com as an account partner.
4. Create an incoming group claim mapping from the TokenAppMapping claim to the WGAApp organizational group claim.
5. Add the token-based application to the Federation Service deployed in the extranet.

► **Task 1: To open the Active Directory® Federation Services console and add the Northwindtraders.com Active Directory® account store on the 6426A- CHI-DC1 virtual computer**

- On the 6426A-CHI-DC1 virtual computer, use **Active Directory Federation Services (AD FS)** to add new **Account Store**.
- Select the **Active Directory Domain Services (AD DS)** check box and enable it.

► **Task 2: To create the WGAApp organization claim and map it to the WGAAppUser security group**

- On the 6426A-CHI-DC1 virtual computer, use **Active Directory Federation Services (ADFS)** to create a new **Organization Claim**.
- Set claim name to **WGAApp** and ensure the **Group claim** check box is selected.
- On the **Resource Group** tab, select the check box next to **Map this claim to the following resource group**.
- Click the ... button and then type **WGAAppUser** in the text box.

- ▶ **Task 3: To add Woodgrovebank.com as an account partner**
 - Use **Active Directory Federation Services** to add **Woodgrovebank.com** as an account partner by using the following parameters:
 - Policy file to import: **Yes**
 - Path: **\\NYC-DC1\C\$\WoodgrovePolicy**
 - Account Partner Details: **Defaults**
 - Account Partner Verification Certificate: **Use the verification certificate in the import policy file**
 - Federation Scenario: **Federated Web SSO with Forest Trust**
 - Federated Web SSO with Forest Trust: **All AD DS domains and forests**
 - Account Partner Identity Claims: **Defaults**
 - Select UPN Suffixes: **All UPN suffixes**
 - Enabled: **Yes**

- ▶ **Task 4: To create an incoming group claim mapping from the TokenAppMapping claim to the WGAApp organizational group claim**
 - On the 6426A-CHI-DC1 virtual computer, use **Active Directory Federation Services (AD FS)** to create an Incoming Group Claim Mapping.
 - In the **Create a New Incoming Group Claim Mapping** box, under **Incoming group claim name**, type **TokenAppMapping**. Use **WGAApp** as the organizational group claim.

- ▶ **Task 5: To add the token-based application to the Federation Service deployed in the extranet**
 - Use **Active Directory Federation Services (AD FS)** to configure a new application by using the following parameters:
 - Application Type: **Windows NT® token-based application**
 - Display name: **Token Based App**
 - Application URL: **https://CHI-DC1.NorthwindTraders.com/tokenapp/**
 - Accepted Identity Claim: **UPN**

- Enabled: **Yes**
- In the Details pane, right-click **WGApp**, and then click **Enable**.

Exercise 8: Testing the AD FS implementation

For this exercise, you will use the available virtual machine environment. Before you begin the exercise, you must:

- Start the 6426A-NYC-CL1 virtual computer.
- Log on to the 6426A-NYC-CL1 virtual computer by using the user name **woodgrovebank\William** and the password **Pa\$\$w0rd**.

The main tasks of this exercise are as follows:

1. Configure browser settings to trust the woodgrovebank federation server.
2. Access the application from the 6426A-NYC-CL1 virtual computer.

► Task 1: To configure browser settings to trust the woodgrovebank federation server

- On the 6426A-NYC-CL1 virtual computer, in the Internet Explorer window, on the **Tools** menu, click **Internet Options**.
- On the **Security** tab, point to Local Intranet, click **Advanced**, and add **https://nyc-dc1.woodgrovebank.com**
- On the **Security** tab, point to Local Intranet, click **Advanced**, and add **https://CHI-DC1.NorthwindTraders.com**
- On the **Security** tab, clear the check box next to **Enable Protected Mode**. Click **OK** and then close the browser.

► Task 2: To access the application from the 6426A-NYC-CL1 virtual computer

- On the 6426A-NYC-CL1 virtual computer, open a browser window, and then install the required certificates on the client by doing the following:
 - Go to **https://nyc-dc1.woodgrovebank.com**
 - The browser displays a "Certificate Error: Navigation Blocked" error message that notifies you that the incoming certificate was not issued by a trusted certification authority. This error is expected behavior when you deploy AD FS servers with self-signed certificates.

- Click the **Continue to this website (not recommended)** link.
- In the address bar, click **Certificate Error**, and then click **View certificates**.
- In the **Certificate** dialog box, click **Install Certificate**.
- On the **Welcome to the Certificate Import Wizard** page, click **Next**.
- On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Browse**.
- In the **Select Certificate Store** dialog box, highlight **Trusted Root Certification Authorities**, click **OK**, and then click **Next**.
- On the **Completing the Certificate Import Wizard** page, click **Finish**.
- On the **Security Warning** dialog box, click **Yes**.
- Click **OK** twice.
- Repeat the above steps for **https://CHI-DC1.NorthwindTraders.com** to install required certificates into the Trusted Root Certification Authorities certificate store.
- Go to **https://CHI-DC1.NorthwindTraders.com/tokenapp**. When you are prompted for your home realm, click **NYC-DC1.WoodgroveBank.com**, and then click **Submit**.
- At this point the Sample Application appears in the browser.



Note: If you have problems accessing the application, try running `iisreset` or restarting the 6426A-CHI-DC1 virtual computer. Then, try to access the application again.



After completing this exercise, turn off all virtual computers and discard undo disks.

Lab Review: Configuring 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 export the trust policy
- Created the TokenApp organization claim
- Added the Woodgrovebank.com Active Directory® account store
- Added Northwindtraders.com as a resource partner to Woodgrovebanks' Federation Service
- Created an outgoing group claim mapping from the TokenApp organization claim to the TokenAppMapping outgoing claim
- Started the Active Directory® Federation Services console and added the Northwindtraders.com Active Directory® account store
- Create the WGApp organization claim and mapped it to the WGAppUser security group
- Added Woodgrovebank.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 woodgrovebank federation server
- Accessed the application

Lab Resources

There are no additional lab resources for this lab.

Lab 5B: Configuring AD FS by Using Federated Web SSO Scenario

- Exercise 1: Installing the AD FS Server Role
- Exercise 2: Configuring Certificate Requirements
- Exercise 3: Configuring the AD FS Web Agent
- Exercise 4: Configuring the Web Server application on the 6426A-CHI-DC1 virtual computer
- Exercise 5: Configuring the Federation Trust Policies
- Exercise 6: Configuring the Account Partner Federation Service
- Exercise 7: Configuring the Resource Partner Federation Service
- Exercise 8: Testing the AD FS implementation

Logon information

Virtual machine	6426A-NYC-DC1 and 6426A-CHI-DC1
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 75 minutes

Objectives

After completing the lab, you will be able to:

- Install the AD FS Server Role
- Configure certificate requirements
- Configure the AD FS web agent
- Configure the web server application on the 6426A-VAN-DC1 virtual computer
- Configure the federation trust policies
- Configure the Account Partner federation service
- Configure the Resource Partner federation service
- Testing the AD FS implementation

Scenario

Woodgrove Bank is a large multinational corporation with office locations located in 5 different countries. The organization is currently running Windows Server® 2003 but is planning to implement Windows Server® 2008. The organization has formed a strategic partnership with Northwind Traders. To enhance collaboration between the organizations, they have agreed to implement an Active Directory® Federation Service (AD FS) infrastructure that will provide access for Woodgrove Bank users to an ordering application running on a Web server at Northwind Traders.

Consolidation Requirements:

As the corporate server technology specialist, you have to install and configure Windows Server® 2008 computers in the organization. To do so, you must perform the following consolidation activity:

- Deploy the AD FS components at both Woodgrove Bank and at Northwind Traders to enable access to the ordering application.

Exercise 1: Installing the AD FS Server Role

In this exercise, you will use the available virtual machine environment. Before you begin the exercise, you must:

1. Start the 6426A-NYC-DC1 virtual computer, and log on by using the user name **woodgrovebank/Administrator** and the password **Pa\$\$w0rd**.
2. Start the 6426A-CHI-DC1 virtual computer, and log on by using the user name **Northwindtrader/Administrator** and the password **Pa\$\$w0rd**.

The main task for this exercise is as follows:

1. Install the AD FS Server Role.
- **Task 1: To install the AD FS Server Role on the 6426A-NYC-DC1 and the 6426A-CHI-DC1 virtual computers**
1. Use Server Manager to install the AD FS server role on both the 6426A-NYC-DC1 and the 6426A-CHI-DC1 virtual computers.
 2. Use the following options:
 - Role Service: Federation Service
 - Self-signed certificates for Secure Socket Layer (SSL) encryption and the Token-Signing Certificate.
 - Default path and name for the trust policy.

Exercise 2: Configuring Certificate Requirements

The main tasks of this exercise are as follows:

1. Export the server authentication certificate to a file.
2. Import the server authentication certificate into the Trusted Root Certification Authorities folder.

► **Task 1: To export the CHI-DC1 server authentication certificate to a file**

1. On the 6426A-CHI-DC1 virtual computer, use IIS Manager to export the **CHI-DC1.NorthwindTraders.com** certificate to C:\CHI-DC1.pfx.
2. Use the password **Pa\$\$w0rd**.

► **Task 2: To import the server authentication certificate for CHI-DC1 into the Trusted Root Certification Authorities folder**

1. On the 6426A-CHI-DC1 virtual computer, use the **Certificates MMC** to import the **CHI-DC1.NorthwindTraders.com** certificate from C:\CHI-DC1.pfx into the local Trusted Root Certification Authorities folder.
2. Use the password **Pa\$\$w0rd**.

Exercise 3: Configuring the AD FS Web Agent

The main tasks of this exercise are as follows:

1. Install the AD FS Web Agent to support claims-aware applications on the 6426A-CHI-DC1 virtual computer.
2. Ensure that the SSL certificate is bound to the Default Web site on the 6426A-CHI-DC1 virtual computer.

► **Task 1: To install the AD FS Web Agent to support claims-aware applications on the 6426A-CHI-DC1 virtual computer**

1. On the 6426A-CHI-DC1 virtual computer, use Server Manager to add the AD FS claims-aware Agent Role Service.

► **Task 2: To ensure that the SSL certificate is bound to the Default Web site on the 6426A-CHI-DC1 virtual computer**

1. On the 6426A-CHI-DC1 virtual computer, use IIS Manager to bind **CHI-DC1.NorthwindTraders.com** certificate to the default Web site.
2. Enforce the use of SSL on the default Web Site.

Exercise 4: Configuring the Web Server application on the 6426A-CHI-DC1 virtual computer

The main tasks of this exercise are as follows:

1. Configure the claims-aware application.
2. Configure Authorization Manager to support the ordering application.

► Task 1: To configure the claims-aware application

1. On the 6426A-CHI-DC1 virtual computer, in the Internet Information Services Manager console, in the Console tree, right-click **Default Web Site**, and then click **Add Application**.
2. Set **Alias** to **ordering**.
3. Click **Select**, click **Classic .NET AppPool** and specify the folder path as **C:\inetpub\wwwroot\ordering**.
4. Copy the content of \\NYC-DC1\d\$\Labfiles\Mod5\ordering to **C:\inetpub\wwwroot\ordering**.
5. Edit **C:\inetpub\wwwroot\ordering\Web.config** and replace all instances of <ServerName> with **CHI-DC1.NorthwindTraders.com**.
6. Save and close the **Web.config** file.



Note: There are three instances of <ServerName> with **CHI-DC1.Northwindtraders.com**.

► Task 2: To configure Authorization Manager to support the ordering application

1. Open a blank MMC console and add the Authorization Manager snap-in.
2. Right-click **Authorization Manager**, and click **Open Authorization Store**.
3. In the **Open Authorization Store** box, under **Store name**, type **C:\inetpub\wwwroot\ordering\AzStore.xml**, and then click **OK**.
4. Close the MMC console and do not save changes to the console settings.



Note: The ordering claims-aware application uses Authorization Manager or AzMan to authorize actions. The application contains a set of operations that are mapped into tasks that are then assigned roles. Groups that come in through claims are mapped into corresponding roles in AzMan. After the AzMan context has been populated with roles, authorization decisions can be made against this context.

Exercise 5: Configuring the Federation Trust Policies

The main tasks of this exercise are as follows:

1. Configure and export the Trust Policy on the 6426A-CHI-DC1 virtual computer.
2. Configure and export the trust policy on the 6426A-NYC-DC1 virtual computer.

► Task 1: To configure and export the Trust Policy on the 6426A-CHI-DC1 virtual computer

1. On the 6426A-CHI-DC1 virtual computer, use Active Directory® Federation Services to edit and export the Trust Policy.
 - Set Federation Service URI to **urn:federation:NorthwindTraders**.
 - Change display name to **NorthwindTraders.com**.
 - Right-click **Trust Policy** and click **Export Basic Partner Policy**.

Claim type	Woodgrove Bank. (Account)		Federated namespace (outgoing/incoming)	Northwind Traders (Resource)	
	Active Directory®	Account organization claims		Resource organization claims	Enabled in application
Group	Purchasing Admins	Purchasing Administrator	Administrator	Administrator	Yes
	Purchasing Dept	Purchasing Agent	Purchaser	Purchaser	Yes
	Authenticated Users	Woodgrovebank	Woodgrovebank	Platinum, Gold, or Silver	Yes
Custom	Title	Position	Position	Title	Yes
	DisplayName	DisplayName	DisplayName	DisplayName	Yes

E	Identity	UPN	UPN	UPN	UPN	Yes
---	----------	-----	-----	-----	-----	-----

port the policy to C:\NWTraders.xml.

► **Task 2: To configure and export the Trust Policy on the 6426A-NYC-DC1 virtual computer**

1. Use Active Directory® Federation Services to edit and export the Trust Policy.
 - Set Federation Service URI to **urn:federation:Woodgrovebank**.
 - Change display name to **Woodgrovebank.com**.
 - Right-click **Trust Policy** and then click **Export Basic Partner Policy**.
 - Export the policy to C:\ **Woodgrovebank.xml**.

Exercise 6: Configuring the Account Partner Federation Service

In this exercise, you will configure the Federation Service located on the account partner as described in the following table.

The main tasks of this exercise are as follows:

1. Open the AD FS console window on the 6426A-NYC-DC1 virtual computer.
2. Create the Account custom organization claims.
3. Add the Woodgrovebank.com Active Directory® account store.
4. Create Group and Custom claim extractions from Active Directory®.
5. Add Northwindtraders.com as a resource partner to Woodgrovebanks' Federation Service.
6. Create the outgoing group claim mappings.
7. Create the outgoing custom claim mappings.

► **Task 1: To create the account group organization claims on the 6426A-NYC-DC1 virtual computer by using the AD FS console**

1. Use Active Directory® Federation Services to create a new **Organization Claim**.

2. Specify Claim name as **Purchasing Administrator** and ensure Group claim is selected.
 3. Repeat steps 1 through 2 for **Purchasing Agent** and **Woodgrovebank**.
- ▶ **Task 2: To create the Account custom organization claims**
1. On the 6426A-NYC-DC1 virtual computer, use Active Directory® Federation Services to create a new **Organization Claim**.
 2. Specify Claim name as **Position** and ensure that **Custom claim** is selected.
 3. Repeat steps 1 through 2 for DisplayName.
- ▶ **Task 3: To add the Woodgrovebank.com Active Directory® account store**
1. On the 6426A-NYC-DC1 virtual computer, use **Active Directory Federation Services** to add new **Account Store**.
 2. Select **Active Directory Domain Services** and enable it.
- ▶ **Task 4: To create Group and Custom claim extractions from Active Directory®**
1. On the 6426A-NYC-DC1 virtual computer, use **Active Directory® Federation Services** to expand **Account Stores**.
 2. Create new **Group Claim Extraction**.
 3. On the **Create a New Group Claim Extraction**, click **Add**. In the **Select Users or Group** box, type **Purchasing Admins**, and then click **OK**.
 4. Ensure that **Purchasing Administrator** is displayed under **Map to this Organization claim**, and then click **OK**.
 5. Repeat steps 2 through 4 for the following mappings:
 1. **Purchasing Dept - Purchasing Agent**
 2. **Authenticated Users - Woodgrovebank**
 6. Create new **Custom Claim Extraction**.
 7. On the **Create a New Custom Claim Extraction**, type **Title**.
 8. Ensure that **Position** is displayed under **Map** to this Organization claim, and then click **OK**.
 9. Repeat steps 6 through 8 for the following mappings:

1. **DisplayName - DisplayName**

► **Task 5: To add Northwindtraders.com as a resource partner to Woodgrovebanks' Federation Service**

1. On the 6426A-NYC-DC1 virtual computer, in the AD FS console, expand **Partner Organizations**, and then click **Resource Partners**. Configure Northwindtraders.com as a resource partner by using the following parameters:
 1. Policy file to import: **Yes**
 2. Path: **\\CHI-DC1\c\$\nwtraders.xml**
 3. Resource Partner Details: **Defaults**
 4. Federation Scenario: **Federated Web SSO**
 5. Resource Partner Identity Claims: **Defaults**
 6. Select UPN Suffixes: **Pass all UPN suffixes through unchanged**
 7. Select E-mail Suffix: **Pass all E-mail suffixes through unchanged**
 8. Enabled: **Yes**

► **Task 6: To create outgoing group claim mappings**

1. On the 6426A-NYC-DC1 virtual computer, use Active Directory® Federation Services to expand Resource Partners and create new Outgoing Group Claim Mapping.
2. In the **Create a New Outgoing Group Claim Mapping** box, under Organization group claims, select **Purchasing Administrator**.
3. In the **Outgoing group claim name** box, type **Administrator**, and then click **OK**.
4. Repeat steps 1 through 3 for the following mappings:
 1. **Purchasing Agent - Purchaser**
 2. **Woodgrovebank - Woodgrovebank**

► **Task 7: To create outgoing custom claim mappings**

1. Use Active Directory® Federation Services to create an Outgoing Custom Claim Mapping.
2. In the **Create a New Outgoing Custom Claim Mapping** box, under Organization group claims, select **Position**.

3. Under **Outgoing custom claim name** box, type **Position**, and then click **OK**.
4. Repeat steps 1 through 3 for the following mapping:
 1. **DisplayName - DisplayName**

Exercise 7: Configuring the Resource Partner Federation Service

In this exercise, you will configure the Federation Service located on the resource partner as described in the table.

Claim type	Woodgrove Bank. (Account)		Federated namespace (outgoing/incoming)	Northwind Traders (Resource)	
	Active Directory®	Account organization claims		Resource organization claims	Enabled in application
Group	Purchasing Admins	Purchasing Administrator	Administrator	Administrator	Yes
	Purchasing Dept	Purchasing Agent	Purchaser	Purchaser	Yes
	Authenticated Users	Woodgrovebank	Woodgrovebank	Platinum, Gold, or Silver	Yes
Custom	Title	Position	Position	Title	Yes
	DisplayName	DisplayName	DisplayName	DisplayName	Yes
Identity	UPN	UPN	UPN	UPN	Yes

The main tasks for this exercise are as follows:

1. Create the Resource group organization claims on the 6426A-CHI-DC1 virtual computer by using the AD FS console.
2. Create the Resource custom organization claims.
3. Add Woodgrovebank as an account partner.
4. Create the incoming group claim mappings.
5. Create the incoming custom claim mappings.
6. Add the claims-aware application to AD FS.
7. Enable each of the group and custom claims for the ordering application.

- ▶ **Task 1: To create the Resource group organization claims on the 6426A-CHI-DC1 virtual computer by using the AD FS console**
 1. On the 6426A-CHI-DC1 virtual computer, use Active Directory® Federation Services to create an Organization Claim.
 2. In the **Create a New Organization claim** box, under Claim name, type **Administrator**.
 3. Ensure that **Group claim** is selected, and then click **OK**.
 4. Repeat steps 1 through 3 by using the following claim names: Purchaser, Platinum, Gold, and Silver.

- ▶ **Task 2: To create the Resource custom organization claims**
 1. On the 6426A-CHI-DC1 virtual computer, use Active Directory® Federation Services to create an Organization Claim.
 2. In the **Create a New Organization claim** box, under Claim name, type **Title**.
 3. Ensure that **Custom claim** is selected, and then click **OK**.
 4. Repeat steps 1 through 3 for the claim **DisplayName**.

- ▶ **Task 3: To add Woodgrovebank as an account partner**
 1. On the 6426A-CHI-DC1 virtual computer, use Active Directory® Federation Services to configure woodgrovebank.com as an account partner by using the following parameters:
 1. Policy file to import: **Yes**
 2. Path: `\\nyc-dc1\c$\woodgrovebank.xml`
 3. Account Partner Details: **Defaults**
 4. Account Partner Verification Certificate: **Use the verification certificate in the import policy file**
 5. Federation Scenario: **Federated Web SSO**
 6. Resource Partner Identity Claims: **Defaults**
 7. Accepted UPN Suffixes: **Woodgrovebank.com**
 8. Accepted E-mail Suffixes: **Woodgrovebank.com**
 9. Enabled: **Yes**

- ▶ **Task 4: To create the incoming group claim mappings**
 1. On the 6426A-CHI-DC1 virtual computer, use Active Directory® Federation Services to create an Incoming Group Claim Mapping.
 2. In the **Create a New Incoming Group Claim Mapping** box, under Organization group claim, select **Administrator**.
 3. Under **Incoming group claim name** box, type **Administrator**, and then click **OK**.
 4. Repeat steps 1 through 3 for the following mapping:
 1. **Purchaser - Purchaser**
 2. **Woodgrovebank - Gold**

- ▶ **Task 5: To create the incoming custom claim mappings**
 1. On the 6426A-CHI-DC1 virtual computer, use Active Directory® Federation Services to create an Incoming Custom Claim Mapping.
 2. In the **Create a New Incoming Custom Claim Mapping** box, under Organization custom claim, select **Title**.
 3. Under **Incoming custom claim name** box, type **Position**, and then click **OK**.
 4. Repeat steps 1 through 3 for the following mapping:
 1. **DisplayName - DisplayName**

- ▶ **Task 6: To add the claims-aware application to AD FS**
 1. On the 6426A-CHI-DC1 virtual computer, use Active Directory® Federation Services to create a new Application.
 2. Select the **Claims-aware application** check box, and set the display name to **Ordering.s**
 3. Under Application URL type **https://CHI-DC1.NorthwindTraders.com/ordering/simpleapp.aspx**.
 4. On the **Application Identity Claim** page, select **User principal name** (UPN).
 5. Ensure that **Enable this application** check box is selected.

- ▶ **Task 7: To enable each of the group and custom claims for the ordering application**
 1. Under the **Applications** node, click **Ordering**, and enable the following organizational claims:

1. Administrator
2. DisplayName
3. Gold
4. Platinum
5. Purchaser
6. Silver
7. Title

Exercise 8: Testing the AD FS implementation

In this exercise, you will configure test the AD FS implementation.

The main tasks of this exercise are as follows:

1. Configure browser settings to trust the woodgrovebank federation server.
2. Install client certificates for the 6426A-NYC-CL1 virtual computer.
3. Access the ordering application.

► Task 1: To configure browser settings to trust the Woodgrovebank federation server

1. Start the 6426A-NYC-CL1 virtual computer, and log on as woodgrovebank\William by using the password **Pa\$\$wOrd**.
2. Start **Internet Explorer**.
3. On the **Tools** menu, click **Internet Options**.
4. On the **Security** tab, click **Local intranet >Advanced**, and then add **https://nyc-dc1.woodgrovebank.com**, and **https://CHI-DC1.NorthwindTraders.com**.
5. On the **Security** tab, clear the **Enable Protected Mode** check box.
6. Click **OK**, and then close the browser.

► Task 2: To install client certificates for the 6426A-NYC-CL1 virtual computer

1. On the 6426A-NYC-CL1 virtual computer, open a browser window, and then install the required certificates on the client by doing the following:
 1. Go to **https://nyc-dc1.woodgrovebank.com/**.
 2. The browser displays a "**Certificate Error: Navigation Blocked**" error message that notifies you that the incoming certificate was not issued by a trusted CA. This error is expected behavior when you deploy AD FS servers with self-signed certificates.
 3. Click the **Continue to this website (not recommended)** link.
 4. In the address bar, click **Certificate Error**, and then click **View certificates**.

5. In the **Certificate** dialog box, click **Install Certificate**.
6. On the **Welcome to the Certificate Import Wizard** page, click **Next**.
7. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Browse**.
8. In the **Select Certificate Store** dialog box, highlight **Trusted Root Certification Authorities**, click **OK**, and then click **Next**.
9. On the **Completing the Certificate Import Wizard** page, click **Finish**.
10. On the **Security Warning** dialog box, click **Yes**.
11. Click **OK** twice.
12. Repeat steps 1 through 10 using <https://CHI-DC1.NorthwindTraders.com> to install required certificates into the Trusted Root Certification Authorities certificate store.
13. Close the Web browser.



▶ **Task 3: To access the ordering application**

1. On the 6426A-NYC-CL1 virtual computer, open a browser window and go to <https://CHI-DC1.NorthwindTraders.com/ordering/simpleapp.aspx>.
2. Close Internet Explorer, and then click **OK**.
3. On the **Northwind Traders ordering application** page, click **Place order**.



Note: The application is using the identity claim to recognize William as a unique user. However, William does not obtain access rights to any functionality because he has not yet been added to the purchasing-related groups within Active Directory® at the account partner. Therefore, he does not present the Purchaser or Administrator claims needed by the ordering application.

4. Close Internet Explorer, and log off the 6426A-NYC-CL1 virtual computer.
5. Switch to the 6426A-NYC-CL1 virtual computer, open **Active Directory Users and Computers**, and then add William to the Purchasing Dept security group. (Found in the Miami BranchManagers OU)

6. Log back on to the 6426A-NYC-CL1 virtual computer as William, open Internet Explorer and attempt to access **https://CHI-DC1.NorthwindTraders.com/ordering/simpleapp.aspx**.
7. Click **Place Order**.
8. Repeat steps 5 through 7 and place William in the Purchasing Admins security group.
9. Test access to the application and verify permissions.



Note: You can also modify the Woodgrovebank incoming group claim on the 6426A-CHI-DC1 virtual computer. You can change the level of discount based upon the Platinum, Silver, or Gold mappings.



After completing this exercise, turn off all virtual computers and discard undo disks.

Lab Review: Configuring AD FS by Using 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 Woodgrovebank.com Active Directory® account store
- Created Group and Custom claim extractions from Active Directory®
- Added Northwindtraders.com as a resource partner to Woodgrovebanks' 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 Woodgrovebank 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 Woodgrovebank federation server
- Installed client certificates
- Accessed the ordering application

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

Module 6

Configuring AD RMS

Contents:

Lesson 1: Overview of AD RMS	6-3
Lesson 2: Installing and Configuring AD RMS Server Components	6-18
Lesson 3: Administering AD RMS	6-33
Lesson 4: Implementing AD RMS Trust Policies	6-44
Lab 6: Configuring AD RMS	6-54

Module Overview

- Overview of AD RMS
- Installing and Configuring AD RMS Server Components
- Administering AD RMS
- Implementing AD RMS Trust Policies

Configuring Active Directory® Rights Management System (AD RMS) requires the knowledge of AD RMS and the installation and configuration of AD RMS server components. Further, the knowledge of AD RMS administration and implementation of AD RMS trust policies, aids in configuring that particular instance of AD RMS in alignment with the particular business objectives from such a deployment.

Lesson 1

Overview of AD RMS

- How Access Management Is Enforced by Using AD RMS
- Usage Scenarios of AD RMS
- Comparing Technologies Used to Protect Information
- Identifying AD RMS Components
- AD RMS Certificates and Licenses
- Overview of AD RMS Workflow
- How Files Are Protected by Using AD RMS

You can protect information by using AD RMS. Usage scenarios of AD RMS include e-mail message protection, rights enforcement, and Internet content protection. You can compare the Secure / Multipurpose Internet Mail Extensions (S/MIME), Access™ Control Lists (ACLs), Encrypting File System (EFS), and Active Directory® Rights Management System (AD RMS) technologies to select the most appropriate technology to protect information in your business scenario.

You should also be able to identify the server and client components to work with the AD RMS infrastructure. AD RMS issues several licenses and certificates that the AD RMS-enabled client applications use to manage rights-protected content.

How Access Management Is Enforced by Using AD RMS

AD RMS enforces access management by :

- Establishing trusted participants within the AD RMS system
- Assigning persistent usage rights and conditions on how a trusted participant can use protected information
- Encrypting information and allowing access to users that have the required components and rights to open and view the information

Types of information that can be protected includes:

- Sensitive documents such as plans, proposals, reports
- E-mail messages
- Content stored in AD RMS-aware intranet services

Key Points

AD RMS is a Windows Server® 2008 rights management technology that helps secure digital assets, such as, documents, emails, and other content.

AD RMS uses policy rules to determine whether the recipient can access or share data. It also defines how the recipient can use such data. In addition, AD RMS determines the time period for which the recipient can use the data. Further, it provides persistent enforcement of information access policies. You can use the policies to manage access to information that needs to be secured.

An AD RMS solution requires the following components:

- An AD RMS server

- An AD RMS-enabled client that runs an AD RMS-enabled browser such as, Internet Explorer® or a program, such as, Microsoft Word®, or Microsoft PowerPoint® in Microsoft Office 2007



For more information, see AD RMS.

Usage Scenarios for AD RMS

Usage Scenario	Application	Features
Secure Confidential Files	Microsoft® Office: <ul style="list-style-type: none"> • Word® • Excel® • PowerPoint® 	<ul style="list-style-type: none"> • Set rights (View, Change, Print) • Set validity period
Do-Not-Forward/Print E-Mail Message	Microsoft® Office Outlook®: <ul style="list-style-type: none"> • Microsoft® Exchange Server 2007 Service Pack (SP1) 	<ul style="list-style-type: none"> • Help protect sensitive e-mail messages from being sent to the Internet • Help protect confidential e-mail messages from being taken outside the company • Help protect Rights Management Services (RMS) preclicensing agent
Help Safeguard Intranet Content	<ul style="list-style-type: none"> • Microsoft® Office SharePoint® Services 	<ul style="list-style-type: none"> • Help safeguard intranet content by restricting access to View, Change, and Print
Identity Federation Support	<ul style="list-style-type: none"> • All RMS-enabled application • Active Directory® Federation Services (AD FS) 	<ul style="list-style-type: none"> • Help safeguard data across AD FS trusts

Key Points

AD RMS is an information-protection technology that AD RMS-enabled applications use to secure digital information from unauthorized access. You can also use AD RMS to provide persistent protection to digital information. AD RMS is a flexible technology that allows developers to create applications to work with AD RMS.

You can use AD RMS to:

- **Protect e-mail messages.** You can restrict users from forwarding e-mail or set an expiry date on the e-mail messages.
- **Enforce file rights.** You can restrict users from modifying or printing confidential files.
- **Protect intranet content.** You can integrate AD RMS infrastructure with Microsoft® Office SharePoint® Server 2007 to secure documents on a

SharePoint®-based intranet site. You can then permit only authorized users to access the data on the intranet site.



For more information, see:

- [AD RMS](#)
- [AD RMS Overview](#)

Comparing Technologies Used to Protect Information

Feature	AD RMS	Secure/Multipurpose Internet Mail Extension (S/MIME) Signing	S/MIME Encryption	Access control lists (ACLs)	Encrypting File Systems (EFS)
Attests to the identity of the publisher	✓	✓		✓	
Differentiates permissions by a user	✓		✓	✓	✓
Prevents unauthorized viewing	✓				
Encrypts protected content	✓		✓		✓
Offers content expiration	✓				
Controls content reading	✓			✓ *	
Modifying, or printing by user	✓			✓	
Extends protection beyond initial publication	✓	✓	✓		✓ *

* With some limitations

Key Points

For an organization, you might need to secure e-mail messages that are sent through the firewall. In addition, you might need to secure documents so that only users with specific permissions can view or print the documents. To implement such security and data protection, you can use the following technologies:

- **S/MIME.** This technology provides public key encryption and support for digital signatures to MIME. However, you cannot use S/MIME to secure documents other than e-mail. S/MIME also cannot control usage rights such as the ability to restrict copying or printing protected information.
- **ACLs.** This technology protects files and folders from unauthorized access. ACLs, however, require the NT file system (NTFS) file system. If you remove a file with ACL permissions from the container in which the permissions are set, the permission restrictions for the file are no longer valid.

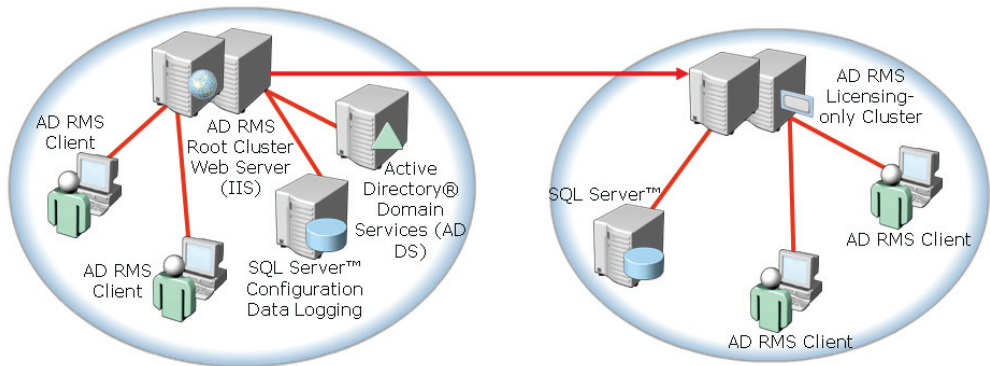
- **EFS.** This technology secures files by using symmetric key encryption along with public key technology. EFS encryption supports moving and renaming of data only on NTFS volumes. If you copy or move the encrypted file or folder to a hard drive formatted with a file system other than NTFS, the file or folder is decrypted.
- **AD RMS.** This technology safeguards digital information from unauthorized usage, online and offline, and inside and outside the firewall. AD RMS is not a technology you can use to replace S/MIME, ACL, or EFS. AD RMS only enhances the security strategy of an organization. AD RMS protects information through persistent usage policies, which remain with the information, no matter where it is moved. After you add AD RMS protection to a digital file, the protection remains with the file. By default, only the content owner can remove the protection from the file. The owner can also grant other users permissions to view, copy, or print the file.



For more information, see:

- [AD RMS](#)
- [AD RMS Overview](#)

Identifying AD RMS Components



Key Points

The AD RMS infrastructure includes several server and client components. The following table describes various AD RMS components.

AD RMS Components	Description
AD RMS Cluster	<p>AD RMS clusters are of two types: root cluster and license cluster.</p> <p>Root cluster. This is the first server that you install in an AD RMS installation. The root cluster manages licensing and certification requests for the Active Directory® Domain Services (AD DS) domain in which it is installed. The cluster can consist of a single server or a group of servers.</p> <p>Licensing-only cluster. You use this cluster in distributed environments such as departments that might require various policies.</p>

AD RMS Components	Description
Web Services	The Web Server Internet Information Services (IIS) server role provides several Web-related server roles and features for the AD RMS server role.
Active Directory® Domain Services (AD DS)	The AD RMS server must be a member of an Active Directory® domain. AD DS hosts the Service Connection Point (SCP). Intranet clients use SCPs to automatically discover the URL for the AD RMS cluster.
Database Services	AD RMS uses a database such as SQL Server™ to store configuration information, user and server keys, and logging information. In a smaller environment, you can configure AD RMS to use the internal database provided by Windows Server® 2008.
AD RMS Client	AD RMS client contains several components to secure and communicate with the RMS server cluster. An RMS server cluster is also known as a lockbox. Windows Vista® and Windows Server® 2008 both include the client components. Windows® XP, Windows® 2000, and Windows Server® 2003 require an add-on that is available at the Microsoft® Download Center.
AD RMS-Aware Applications	Users must use applications that provide AD RMS features.



For more information, see [RMS Technology Components](#).

AD RMS Certificates and Licenses

Server Licensor Certificate

Gets created when the AD RMS server role is installed and configured on the first server of an AD RMS Root Cluster

Machine Certificate

Identifies a trusted computer and contains the unique public key for that machine, on a per user per computer basis

Rights Account Certificate

Names a trusted user identity by using the e-mail address or SID of the user on a per user basis

Client Licensor Certificate

Names a trusted user that is authorized to publish RMS-protected information without requiring connectivity to an RMS server. This naming is based on per user on a computer

Publishing License

Sets the policy for acquiring a used license for rights-protected information

Use License

Grants an authorized user with valid RAC rights to consume rights-protected information based on policy established in the publishing license



Key Points

AD RMS issues several licenses and certificates that the AD RMS-enabled client applications use to manage rights-protected content. Server and client components use eXtensible rights Markup language (XrML)-based certificates and licenses to ensure trusted connections and to protect content. Certificates and licenses are certificate chains that begin at the root certificate and continue through the leaf certificate. Examples of certificates and licenses are end-user licenses and rights account certificates (RACs). Certificates and licenses are connected in a hierarchy. AD RMS clients follow a chain from a certificate or license up to a trusted key pair.

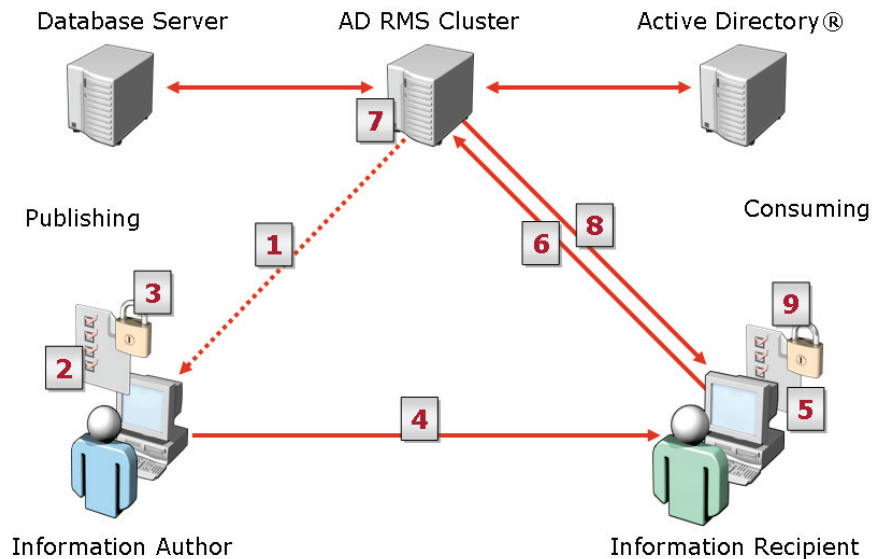
The licenses and certificates that AD RMS provides include:

- **Machine certificate.** This certificate is attached to the lockbox and contains the public key of the computer. The computer uses the certificate to form a trusted connection. The root of trust signs the machine certificate.
- **RAC.** This certificate attaches the machine certificate to an issuance license, end-user license, and other license. Each user on the computer has an RAC

that contains the public key and private key of the user. The public key of the user is available in plaintext. The public key of the machine certificate encrypts the private key of the user.

- **Client licensor certificate.** This certificate allows an application to sign an issuance license without contacting a licensing server.
- **Publishing license.** This license identifies usage rights and conditions assigned to data. This license specifies the authorized users who can view the information. In addition, the publishing license specifies how to use and share the information.
- **Use license.** The AD RMS server validates the recipient who attempts to retrieve the protected data. The AD RMS server then issues a use license for the recipient. The use license contains the usage rights and conditions specified in the publishing license.

Overview of AD RMS Workflow



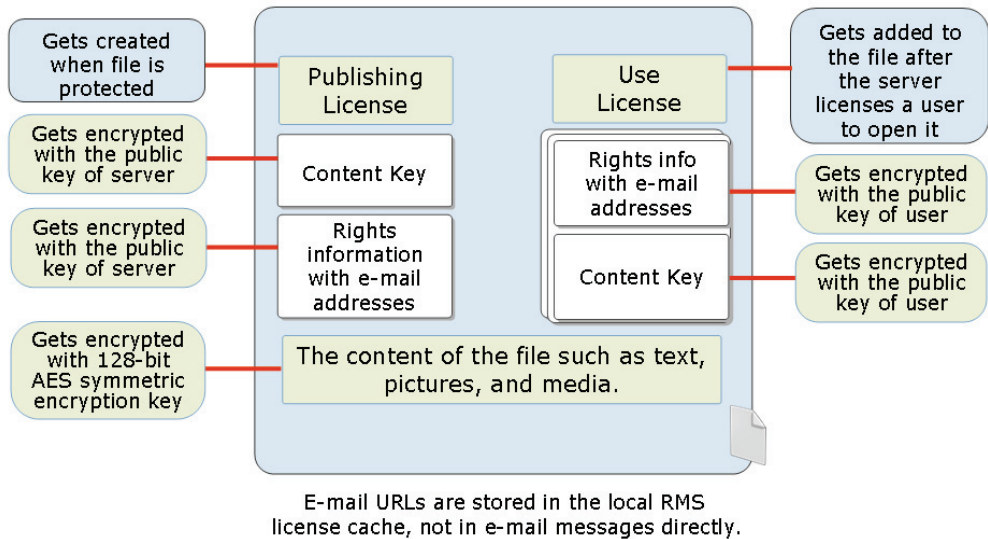
Key Points

The following sequence demonstrates the AD RMS workflow:

1. When the author initially secures the information, the AD RMS cluster provides an RAC and Client Licensor Certificate (CLC). This step establishes the author's AD RMS credentials. The author can also publish secured information offline.
2. The author can create a file and specify usage rights and conditions for it, by using an AD RMS-enabled application. A publishing license containing the usage policies is then generated.
3. The application encrypts the file with a symmetric key, which is encrypted by the public key of the AD RMS cluster. The key is inserted into the publishing license and the publishing license is bound to the file.
4. The author distributes the file.

5. A recipient receives a secured file through a regular distribution channel and opens it by using an AD RMS-enabled application. If the recipient does not have an RAC on the current computer, an RAC is issued from the AD RMS cluster.
6. The application requests a use license. This request is sent to the AD RMS cluster that issued the publishing license for the secured information.
7. The AD RMS cluster confirms that the recipient is authorized, checks that the recipient is a named user, and creates a use license. The server decrypts the symmetric key by using the private key of the server, re-encrypts the symmetric key by using the public key of the recipient, and then adds the encrypted symmetric key to the use license.
8. After the confirmation is complete, the licensing server returns the use license to the client computer of the recipient.
9. After receiving the use license, the application verifies the license and the account certificate of the recipient. This helps determine whether any certificate, in either chain of trust, requires a revocation list. If required, the application checks for a local copy of the revocation list that has not expired. If required, it retrieves a current copy of the revocation list. The application then applies any relevant revocation conditions in the current context. If the revocation conditions allow access to the file, the application renders the data. Users can then apply their granted rights.

How Files Are Protected by Using AD RMS



Key Points

An AD RMS-enabled application encrypts document contents by using a generated symmetric key. This key and the corresponding rights information are then sent to the AD RMS server for the verification of user and recipient information. After successful verification, the content key and rights information is encrypted by using the public key of the AD RMS and returned to the user.

AD RMS supports offline publishing for any content key and rights information encrypted by using a CLC. This certificate contains the public key of the AD RMS server. Microsoft® Office 2007 Professional Plus utilizes offline publishing by using AD RMS.


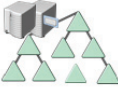

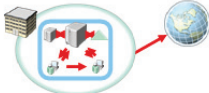
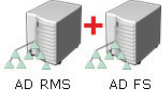
Lesson 2

Installing and Configuring AD RMS Server Components

- AD RMS Deployment Scenarios
- Preinstallation Considerations
- AD RMS System Requirements
- How to Install the First Server of an AD RMS Cluster
- What Is a Service Connection Point?
- Implementing an AD RMS Client
- Configuring Client Service Discovery

The installation and configuration of AD RMS requires the knowledge of AD RMS deployment scenarios and preinstallation considerations. In addition, you should also have the knowledge of the AD RMS system requirements, installation of the first server of an AD RMS cluster, and service connection points. Finally, you must also know about AD RMS client implementation, and configuration of client service discovery.

AD RMS Deployment Scenarios

	<ul style="list-style-type: none"> • Deploying AD RMS in a single Forest
	<ul style="list-style-type: none"> • Deploying an AD RMS Licensing-Only cluster
	<ul style="list-style-type: none"> • Deploying AD RMS in a Multi-Forest environment
	<ul style="list-style-type: none"> • Deploying AD RMS in an Extranet
	<ul style="list-style-type: none"> • Deploying AD RMS with AD FS

Key Points

The standard topology for AD RMS consists of one or more physical servers that make up the AD RMS root installation or cluster. The combination of one or more AD RMS servers to a root cluster increases the availability and redundancy of the deployment.

The information on how to deploy AD RMS in various scenarios is as follows:

- **AD RMS in a single forest.** This scenario can contain a single server or have multiple servers in a single AD RMS cluster. This helps provide fault tolerance and high availability.
- **AD RMS licensing-only cluster.** This scenario is used to distribute licensing services. Unlike the root cluster, which provides all AD RMS services, servers in a licensing-only cluster provide only licensing and publishing services. Licensing-only clusters are optional and are deployed to manage specific licensing requirements. These requirements include:

- The support of exclusive rights-management requirements of a department
- The support of rights management for external business partners as part of an extranet that requires a strong separation and resource tracking for specific business partners
- The removal of root cluster licensing tasks
- **AD RMS in a multi forest environment.** This scenario requires the use of AD RMS root clusters. AD RMS trust policies must be configured so that certificates and licenses generated by other AD RMS clusters can be trusted.
- **AD RMS in an extranet.** This scenario is an extension of an AD RMS cluster to the Internet. In this scenario, users can consume rights-protected content if not connected to the internal network. This deployment supports the collaboration of partners or customers that need to exchange protected content through file transfer, e-mail messages, or Web sites.
- **AD RMS by using AD FS.** This scenario is an optional service role that allows federated identities consume rights-protected content by using Active Directory® Federation Services (AD FS).



For more information, see [Deploying AD RMS in an Extranet Step-by-Step Guide](#).

Preinstallation Considerations

Consider the following points before deploying AD RMS:

- Install AD RMS on a member server in the same domain as the user accounts that will participate in AD RMS.
- Determine whether to use an external database or the internal database provided by Windows Server® 2008.
- Create a specific AD RMS service account with standard user permissions.
- Make the account used to install AD RMS, as the member of the Enterprise Admins group or equivalent, if the service connection point is to be registered during installation.
- Create a DNS alias (CNAME) record for the AD RMS cluster URL, and a CNAME record for the computer hosting the configuration database.
- Obtain an Secure Socket Layer (SSL) certificate from a trusted Certification Authority, if secure communication to and from the AD RMS cluster is required.

Key Points

Pre-installation requirements and recommendations include the following:

- AD RMS can be installed on a domain controller. However, the service account must be a Domain Admins group member. This introduces security considerations for having additional accounts be administrators of the entire domain.
- Windows® Internal Database can install only on a single-server AD RMS cluster because this type of database does not support remote connections. The Windows® Internal Database with AD RMS can only be used in test environments.
- If you use an external database for AD RMS, you must have rights to create databases in SQL Server™.
- The user account that you use to install the AD RMS server must differ from your AD RMS service account.

AD RMS System Requirements

Hardware Requirements	
Required	Recommended
<ul style="list-style-type: none"> • One Pentium 4 processor (3Ghz or higher) • 512 MB RAM • 40 GB free disk space 	<ul style="list-style-type: none"> • Two Pentium 4 processors (3Ghz or higher) • 1024 MB RAM • 80 GB free disk space
Software Requirements	
Software	Requirement
Operating System	<ul style="list-style-type: none"> • Windows Server® 2008
File System	<ul style="list-style-type: none"> • NTFS file system is recommended
Messaging	<ul style="list-style-type: none"> • Message Queuing
Web Services	<ul style="list-style-type: none"> • Internet Information Services (IIS) • ASP.NET must be enabled
Active Directory® or AD DS	<ul style="list-style-type: none"> • AD RMS must be installed in an Active Directory® domain. The domain controllers should run Windows Server® 2000 with Service Pack 3, Windows Server® 2003, or Windows Server® 2008. • All users and groups who use AD RMS to acquire licenses and publish content must have an e-mail address configured in Active Directory®
Database Server	<ul style="list-style-type: none"> • Microsoft® SQL Server™ 2005 or equivalent, and stored procedures

Key Points

In addition to the hardware and software requirements, you need to know a few key aspects.

The AD RMS service account is a Windows® account that is used to host the AD RMS service. The account is also used to communicate with other services on the server and the network. This service account is granted permission to resources that are required for AD RMS.

The client requirements for an AD RMS service account are as follows:

- You must install AD RMS client software to configure an AD RMS service account.
- You also must setup an AD RMS-enabled browser or application to configure an AD RMS Service account.
- You can configure a domain account for use as an AD RMS service account.

- In addition, you must setup a mail-enabled user account in AD DS.



For more information, see:

- 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
- Pre-installation Information for AD RMS

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

- To use DNS to configure a CNAME for the AD RMS cluster
- To use Server Manager to install the AD RMS server role

Key Points

The instructor will provide a demonstration to show how you can install the first server of an AD RMS cluster.

Questions:

1. What tool would you use to install the AD RMS server role?
2. What are the various server roles that are required for the installation of the AD RMS server role?
3. Identify the servers that can be included in an AD RMS cluster if Windows® Internal Database is used.

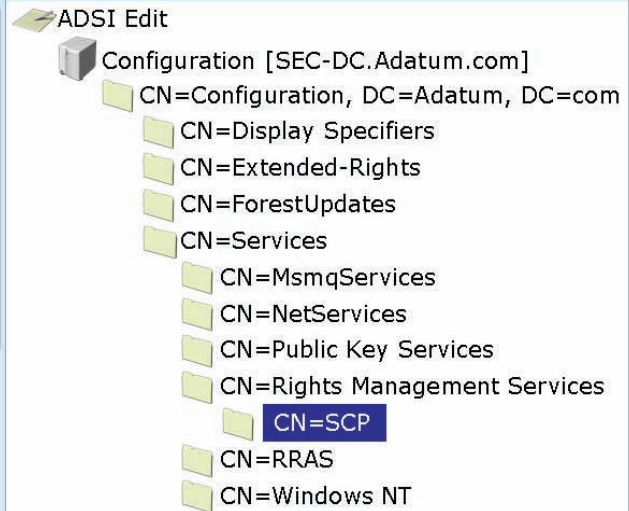


For more information, see [Pre-installation Information for AD RMS](#).

What Is a Service Connection Point?

A service connection point:

- Provides automatic discovery of the AD RMS cluster URL
- Contains only one SCP per Active Directory® forest
- Requires AD RMS management console to be registered or removed
- Requires ADSI Edit to be viewed and modified



Key Points

SCPs are objects that are created and used by services that are published explicitly by AD DS.

You can create AD RMS SCP in the Services container of the AD DS Configuration partition. This SCP provides the certification URL that directs you to the AD RMS cluster in the forest. The AD RMS-enabled clients use the AD RMS cluster to obtain a rights-account certificate.

During AD RMS server installation, you can register AD RMS services as SCPs in AD DS. These SCPs allow clients to locate the AD RMS servers. You can change SCPs by using the AD RMS console and a user account that is a member of the Enterprise Administrators group, or an equivalent. An example of a root cluster URL is https://rms.woodgrovebank.com:443/_wmcs/certification



For more information, see [AD RMS Help File: Register a Service Connection Point](#).

Implementing an AD RMS Client



The AD RMS client creates and manages the machine certificate and lockbox.



The AD RMS client works with AD RMS-compatible applications such as the 2007 Office System.



The AD RMS client is integrated with the Windows Vista® and Windows Server® 2008 operating systems.



The AD RMS client is downloaded from the Microsoft® Download center for earlier versions of Windows®.



The AD RMS client is deployed manually or automated using Active Directory® Group Policy.

Key Points

The following methods can be used to implement the AD RMS client:

- By default, Windows Vista® includes the AD RMS client. For other client operating systems, you need to install the AD RMS client.
- You can download the AD RMS client from the Microsoft® Download Center. This AD RMS client can work on earlier versions of client operating systems than Windows Vista® and Windows Server® 2008.
- The AD RMS client installation is simple and requires little interaction from the system administrator who is administering the client computers.
- You can use the AD RMS client to implement the Systems Management Server or System Center Configuration Manager 2007.
- To create rights protected content, you need an AD RMS-enabled browser such as Internet Explorer®, or an AD RMS-enabled application such as Microsoft® Office 2007.

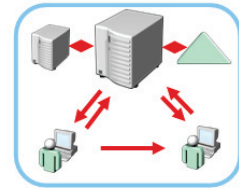


For more information, see [Pre-installation Information for AD RMS](#).

Configuring Client Service Discovery

AD RMS clients discover the AD RMS cluster using the following methods:

- AD DS service connection point
- AD RMS client registry override
 - HKEY_LOCAL_MACHINE\Software\Microsoft\MSDRM\ServiceLocation
 - Activation (syntax: `http(s):// <cluster>/_wmcs/ certification`)
 - EnterprisePublishing (syntax: `http(s):// <cluster> /_wmcs /certification`)



Key Points

AD RMS client service discovery is the method of discovering an AD RMS cluster by using the AD RMS client. The following are ways in which this can be discovered:

- **SCP automatic service discovery.** In this method, the client queries AD DS for SCP of the AD RMS cluster. This is a recommended way of deploying an AD RMS environment, because for automatic service discovery, no additional AD RMS client configuration is required.
- **AD RMS client registry overrides keys.** In this method, complex AD RMS deployment topologies are configured for client service discovery. This is because complex deployments require more specific control of the AD RMS client. The client registry override keys are the following:
 - **Activation.** In this method, the default AD RMS certification service that is configured in the SCP gets overridden.

- **Enterprise Publishing.** In this method, the default AD RMS licensing service gets overridden.
- **Discovery via the CLC.** In this method, when the rights-protected content is published, both the certification and licensing URLs are added to CLC. Client will retrieve the certification and licensing URLs from the client licensor certificate if other discovery methods are unavailable



For more information, see [Pre-installation Information for AD RMS](#).

Lesson 3

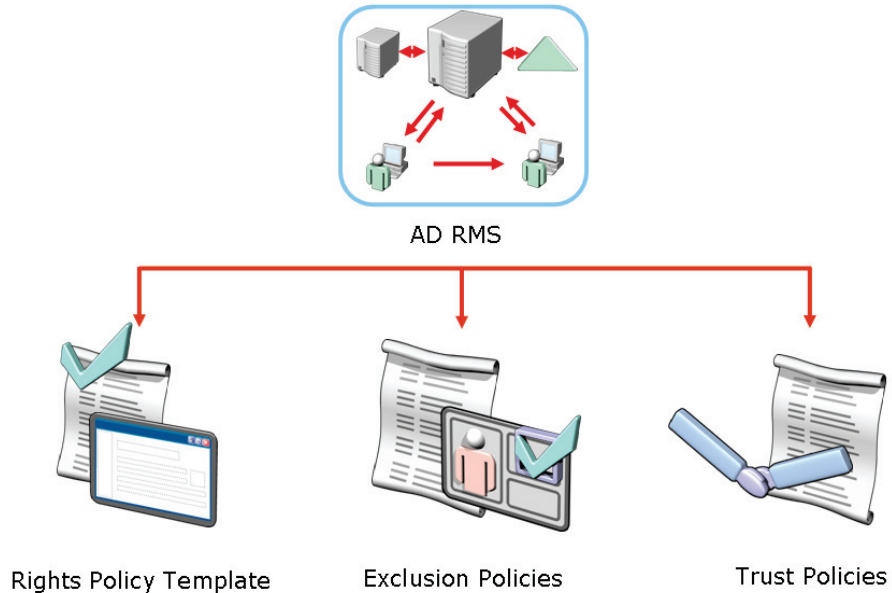
Administering AD RMS

- AD RMS Administration Tasks
- What Is a Rights Policy Template?
- How To Create a Rights Policy Template
- Providing Rights Policy Templates for Offline Use
- What Are Exclusion Policies?

AD RMS combines the features of RMS in Windows Server® 2003, developer tools, and industry security technologies. These tools and technologies include encryption, certificates, and authentication that help organizations create reliable information protection solutions.

Administering AD RMS requires the knowledge of AD RMS administration tasks, rights policy templates, their creation and provision for offline usage, and exclusion policies.

AD RMS Administration Tasks



Key Points

The important tool to administer AD RMS features is the Active Directory® Rights Management Services console. Following are the common administration tasks:

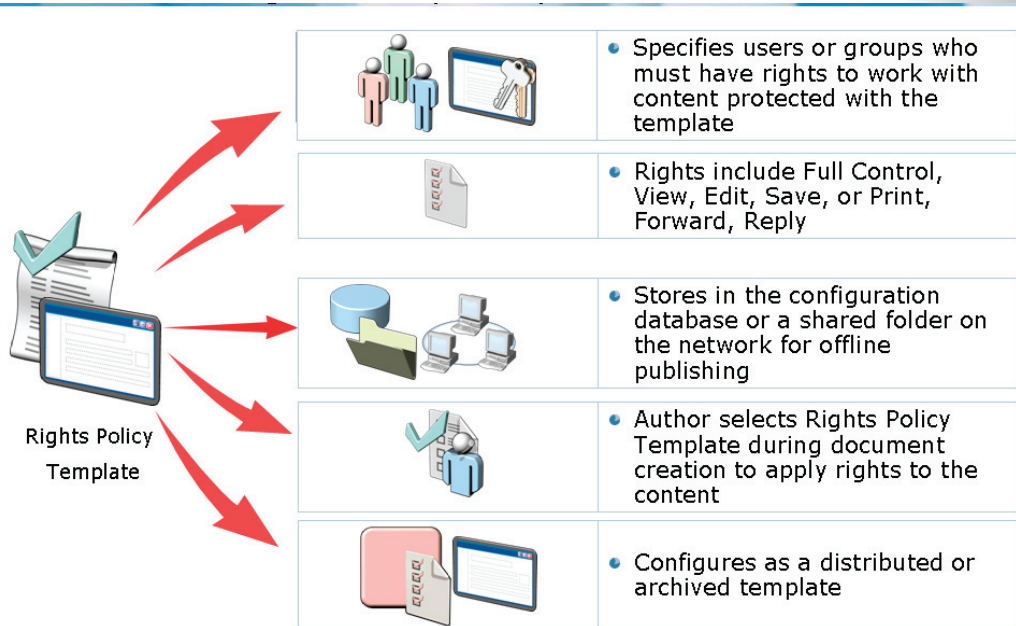
- Manage the Exclusion Policies so that you can deny certain entities the capability to acquire certificate and license requests.
- Establish Trust Policies so that you can activate a trust relationship between your AD RMS cluster and an AD RMS cluster in another domain. It is also possible to activate such relationships with a cluster that is part of a different organization.
- Configure Rights Policy Templates used to control the rights that a user or group has on a particular piece of rights-protected content.
- Administer certificates and licenses used by AD RMS

- Manage the AD RMS databases and configuration, logging, and directory services information stored for use by AD RMS
- Configure accounts used for the operation and maintenance of an AD RMS cluster



For more information, see [Pre-installation Information for AD RMS](#).

What Is a Rights Policy Template?



Key Points

Rights policy templates are used to control the rights of users and groups to a particular piece of rights-protected content. They can include various conditions, such as specific recipients or AD DS groups. Some other conditions can be the period for which a use license for the content remains valid and the period for which after publication the content can be consumed.

Configuration database stores the Rights policy templates. Optionally, the linked clients can access the copy of all rights policy templates. They are stored in a specified shared folder. Users must have access to the template to be able to access rights-protected content. Most administrators prefer to place the template files on the local client computers so that they can be used for offline and online publishing of rights-protected content.

AD RMS-enabled clients running Windows Server® 2008 and Windows Vista® SP1 can use the template distribution pipeline to automatically update their rights policy templates. If a rights policy template has changed or is deleted, the client

will automatically detect these changes and update the local rights policy templates.

All versions of the RMS client prior to Windows Server® 2008 and Windows Vista® SP1, use the previous method for rights policy template distribution. They use Group Policy or Systems Management Server (SMS).



For more information, see [Pre-installation Information for AD RMS](#).

Demonstration: How To Create a Rights Policy Template

- To configure a distributed rights policy template
- To manage archived rights policy templates

Key Points

The instructor will provide a demonstration to show how you can create a rights policy template.

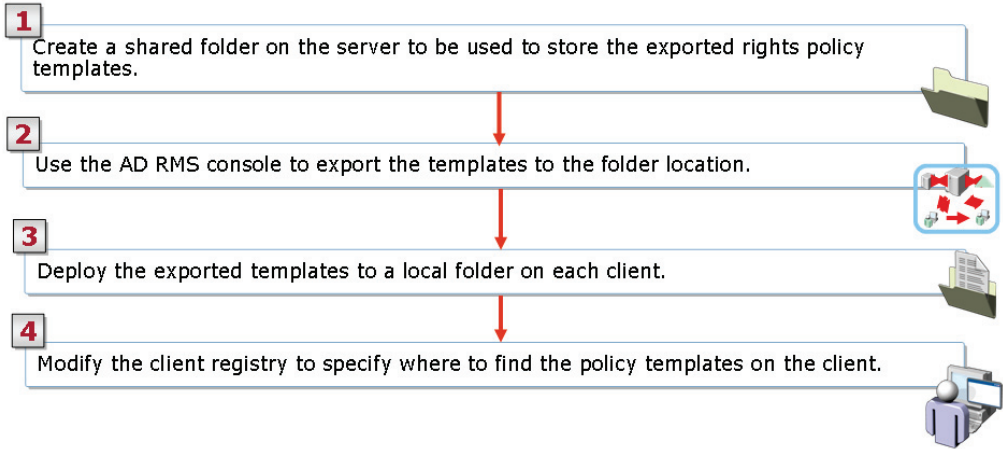
Questions:

1. What are rights policy templates?
2. What is the purpose of archiving rights policy templates?
3. 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?



For more information, see [Creating and Deploying AD RMS Rights Policy Templates Step-by-Step Guide](#).

Providing Rights Policy Templates for Offline Use



```
Example: For Office 2007
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\12.0\Common\DRM\AdminiTemplat
ePath
Type: REG_EXPAND_SZ
Recommended Value:
%allusersprofile%\Application Data\Microsoft\DRM\<templatefoldername>
```

Key Points

You can provide the rights policy templates for offline use by following the steps listed:

1. **Distributing rights policy templates.** You must distribute the rights policy templates to the computers that will use the templates. You must create a shared folder on the server for storing rights policy templates.
2. **Share settings in AD RMS console.** You must define the share settings in the AD RMS console.
3. **Locally deploying template files.** You must locally deploy template files on client computers. This helps users to access templates while their computers are not connected to the network. You must redeploy each template to client systems after it is modified. This avails users with the latest template version on their computers. AD RMS clients running on Windows Vista® with SP1 and Windows Server® 2008, automatically detect changes. Their system will update the rights policy templates while connected to the network.

4. **Locating templates.** You must have the template location determined by RMS-enabled applications. In addition, you must have an AD RMS client to locate templates in the following location from the registry key:
 HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\DRM\AdminTemplatePath or
 HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DRM\AdminTemplatePath

Finally, the client computers must access templates from the location specified in the registry key depending on the operating system used by them. The following table shows the registry keys for the various operating systems.

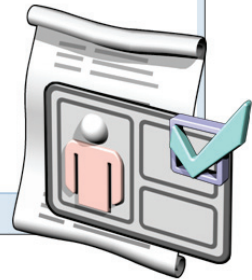
Operation System	Registry Key
Office 2003 and later versions	AdminTemplatePath registry key.
Microsoft® Office 2007	%userprofile%\AppData\Local\Microsoft\DRM\templates
Windows Server® 2008 and Windows Vista® client	%userprofile%\AppData\Local\Microsoft\DRM\templates
Windows® XP, Windows® 2000, and Windows Server® 2003	%appdata%\Microsoft\DRM\templates

What Are Exclusion Policies?

Prevent compromised principals from acquiring new use license; however, existing licenses associated with excluded principals are still valid.

Administrators can exclude following principles:

- User IDs
- Applications
- Lockbox versions
- Windows® versions



Key Points

AD RMS exclusion policies prevent specific principals from acquiring new licenses from a particular AD RMS server or cluster. Only new licensing requests are denied and any existing licenses that are associated with excluded principals are still valid.

Exclusion policies are very useful for disabling the rights of terminated users or preventing specific applications or users of unsupported Windows® operating systems from accessing the protected content.

The several types of exclusion policies are listed below:

- **By user.** User RAC can be excluded when you exclude its public key. This kind of exclusion policy is useful when a trusted user's AD RMS credentials are compromised.
- **By application.** You can also use licensing requests to verify against the version of an AD RMS-enabled application.

- **By Lockbox version.** You use Lockbox version to exclude previous versions of the client software. When requests of clients are using a version of the lockbox software that is earlier than the one specified, the requests are denied. In this case, the client computers will not be able to acquire rights account certificates or use licenses.
- **By Windows® version.** You use Windows® version to exclude users based on Windows® version to prevent used licenses. This includes used licenses on clients that are running older or unsupported versions of Windows®, such as Windows® 98 Second Edition or Windows® Millennium Edition.




For more information, see [Managing Exclusion Policy](#).

Lesson 4

Implementing AD RMS Trust Policies

- Methods of Defining Trust Policies
- Overview of Trusted User Domain Interaction
- Overview of Trusted Publishing Domain Interaction
- How To configure Trust Policies
- Deploying AD RMS with AD FS







Implementing AD RMS trust policies requires the knowledge of types of trust policies, and trusted user and publishing domain interaction. You should also know about configuration of trust policies and deployment of AD RMS by using AD FS.

Methods of Defining Trust Policies

Trust Policies help an AD RMS cluster to process licensing requests for content that are rights-protected by another AD RMS cluster.



Trust policies can be defined for the following:	
Trusted user domains	
Trusted publishing domains	
Windows Live™ ID	
Federated Trust	

Key Points

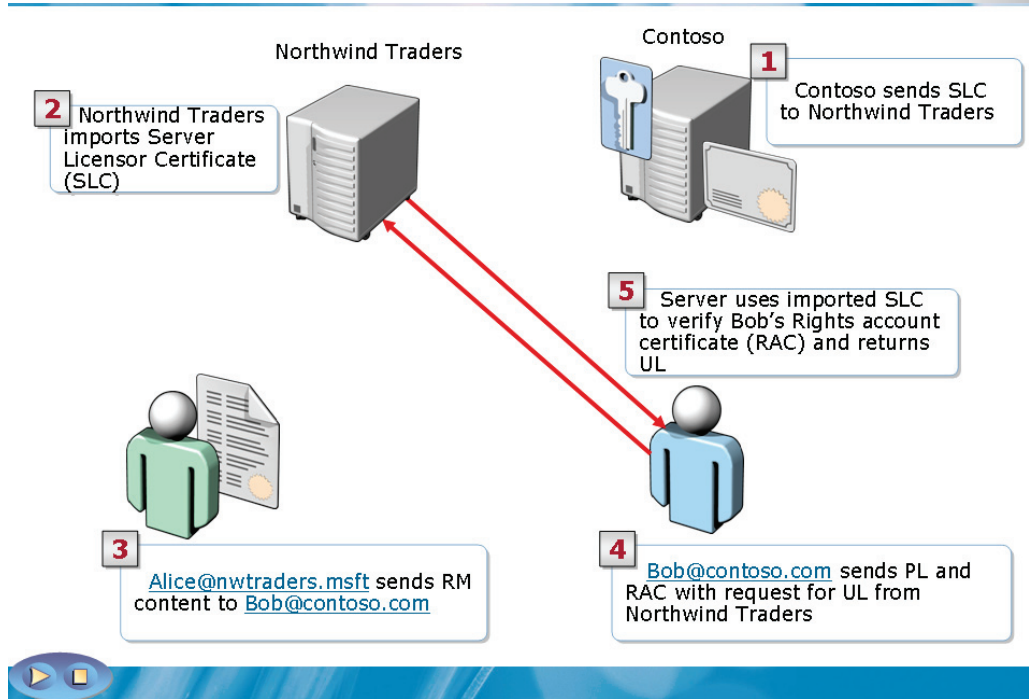
You can implement several trust hierarchies for an organization. A trust hierarchy contains an AD RMS cluster. An AD RMS root cluster issues RACs to users. By default, an AD RMS cluster does not service requests for a user with an RAC from an AD RMS root cluster in a different trust hierarchy. You can create trust policies so that the AD RMS system trusts and processes licensing requests from users or groups of a different AD DS forest.

You can use the following methods to define trust policies:

- Trusted user domains.** You can add a trusted user domain so that the AD RMS root cluster processes requests for client licensor certificates. A trusted user domain also allows the AD RMS root cluster to process licenses from users with RACs issued by a different AD RMS root cluster. You can add a trusted user domain by importing the server licensor certificate of the AD RMS cluster to trust.

- **Trusted publishing domains.** You can add a trusted publishing domain so that an AD RMS cluster can issue use licenses against publishing licenses from a different cluster. You can add a trusted publishing domain by importing the server licensor certificate and the private key of the server, to the trust.
- **Windows Live™ ID.** You can configure a trust with Windows Live™ ID so that an AD RMS user can send rights-protected content to a user who has a Windows Live™ ID. However, the Windows Live™ ID user will not be able to create content that is rights-protected by the AD RMS cluster.
- **Federated Trust.** You can establish a federated trust between two forests by using AD FS. Some AD DS forests might not have AD RMS installed. The users of these forests can use federated trust when they need to consume rights-protected content from another forest.

Overview of Trusted User Domain Interaction



Key Points

By default, AD RMS does not issue use licenses to users whose RACs were issued by a different user domain. To configure AD RMS to issue these use licenses, you must import the server licensor certificate of the required user domain. You must then add the imported certificate to the list of trusted user domains for AD RMS.

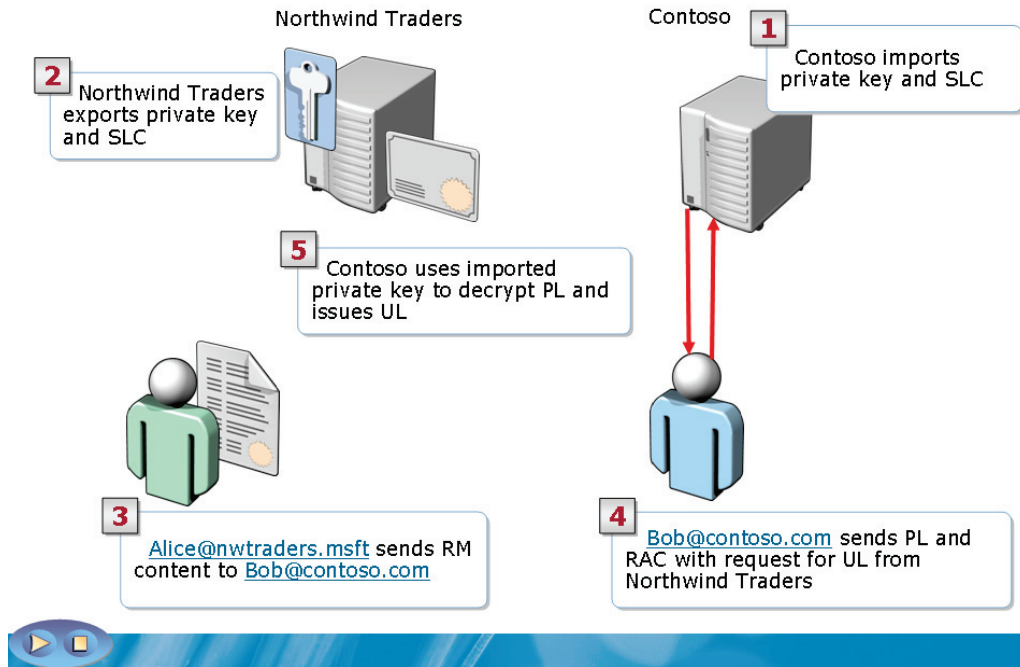
After you configure AD RMS, users with RACs that were issued by the trusted user domain can submit requests for use licenses to your AD RMS installation. AD RMS then processes these use licenses as requests from internal users.

Each organization has an associated AD RMS installation. After you configure trusted user domains, an organization can add the AD RMS installation of another organization to the list of trusted user domains. Users from both organizations can then work together on protected content. These users can also exchange the content through the Internet or an extranet.



For more information, see **Trusted User Domains**.

Overview of Trusted Publishing Domain Interaction



Key Points

By default, AD RMS servers do not issue use licenses against publishing licenses issued by an AD RMS server in a different cluster. However, you can configure an AD RMS cluster to trust the publishing licenses issued by a different AD RMS cluster. The AD RMS cluster can then implement a trusted publishing domain (TPD) to issue use licenses against publishing licenses.

For an organization, you might publish content by using AD RMS root clusters either in another organization or in a division in another forest. You must configure TPDs when you publish such content. By using a TPD, the AD RMS cluster that you implement can grant use licenses to users for the published content.

When you add a TPD, you implement a trust relationship between the AD RMS cluster that you install and the other root cluster. For the trust relationship, you

import the server licensor certificate (SLC) of the other cluster. You can configure any number of TPDs for an AD RMS cluster.



For more information, see [Trusted User Domains](#).

Demonstration: How To configure Trust Policies

- To export a trusted user domain certificate
- To import a trusted user domain certificate
- To configure trusted publishing domains

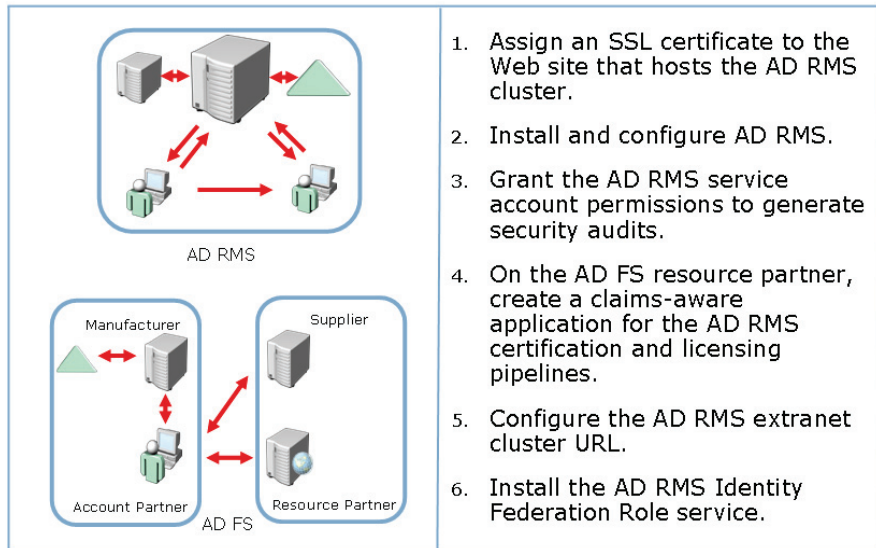
Key Points

The instructor will provide a demonstration to show how you can configure trust policies.

Questions:

1. What is the purpose of setting up trusted publishing domains?
2. What is the format in which trusted publishing domain certificates are created?
3. What is the purpose of setting up trusted user domains?

Deploying AD RMS with AD FS



Key Points

AD RMS depends upon AD DS to authenticate a user attempting to access rights-protected content. If the user is authorized to access the rights protected document, authentication is given to the user.

- Identity federation support in AD RMS enables business organizations to control existing federated relationships. It also helps the business organizations to collaborate with partners outside their enterprise boundaries. Thus, they can share access rights protected content between the organizations.
- An organization where AD RMS is deployed can establish a federation relationship with another organization that has not deployed AD RMS. This establishment of federation relationship is done by sharing access to the organization's rights-protected content where AD RMS is not deployed, without having to establish a separate trust.

- You can authenticate external users attempting to access an organization's protected content, by using AD FS. AD RMS policies are enforced after these external users are authenticated. AD RMS will then automatically provide the external user with appropriate content licenses to work with an organization's protected content.
- Federated AD RMS in Windows Server® 2008 is fully compatible with existing Office SharePoint® Server 2007 deployments and fully supports down-level AD RMS clients. AD RMS can use federation servers that are running either Windows Server® 2003 R2 Enterprise Edition or Windows Server® 2008 Enterprise. To configure clients for federation support in AD RMS, you need to assign the AD FS home realm for AD RMS in the client's registry.



For more information, see:

- [Using Identity Federation with AD RMS Step-by-Step Guide](#)
- [AD RMS Role](#)

Lab 6: Configuring AD RMS

- Exercise 1: Installing the AD RMS Server Role
 - Exercise 2: Managing AD RMS rights policy templates
 - Exercise 3: Configuring Trust Policies
 - Exercise 4: Testing AD RMS functionality
- Logon information

Virtual machine	6426A-NYC-DC1 6426A-NYC-SVR1 6426A-NYC-CL1
User name	Administrator
Domain	woodgrovebank
Password	Pa\$\$w0rd

Estimated time: 60 minutes

Objectives:

After completing the lab, you will be able to:

- Install the AD RMS server role
- Manage AD RMS rights policy template
- Configure trust policies
- Test AD RMS functionality

Scenario

Woodgrove Bank is a multinational corporation with offices in several countries. The bank management has been concerned about the lack of security measures to protect their confidential data. As the enterprise administrator, you have been exploring options to enhance data security. You have decided to pilot an Active Directory® Rights Management Services (AD RMS) solution to implement rights-

protection technology for lines of business that require persistent protection for data, such as sensitive e-mails and corporate financial statements.

Woodgrove Bank has also recently acquired Contoso Ltd., which also uses AD RMS to protect their data. The Contoso administrators have provided the required import files and details to facilitate the necessary trust between both AD RMS infrastructures. You need to ensure that authorized users in both organizations can author and view the content.

Consolidation Requirements:

As an enterprise administrator, you must design the AD RMS infrastructure for Woodgrove Bank. For the pilot project, you have to perform the following consolidation activities:

- Create a Rights Policy Template for the Woodgrove Bank network users. The template will automatically apply centrally defined usage rights to help protect sensitive corporate information.

Exercise 1: Installing the AD RMS Server Role

In this exercise, you will use the available virtual machine environment. Before you begin the exercise, you must:

1. Start the 6426A-NYC-DC1 virtual computer and log on using the user name **woodgrovebank/Administrator** and the password **Pa\$\$w0rd**.
2. Start the 6426A-NYC-SVR1 virtual computer and log on using the user name **woodgrovebank/Administrator** and the password **Pa\$\$w0rd**.
3. Start the 6426A-NYC-CL1 virtual computer (Do not log on at this time).

The main task for this exercise is as follows:

1. Install and configure AD RMS.

► Task 1: To install and configure AD RMS

1. On the 6426A-NYC-SVR1 virtual computer, use the Server Manager to install the AD RMS server role with the following options:
 - Add the Required Role Services when prompted.
 - Create a new AD RMS cluster
 - Select the **Windows Internal Database**.
 - Specify the service account by using the user name **woodgrovebank\ADRMSService** and the password **Pa\$\$w0rd**.
 - Use the AD RMS centrally managed key storage by using a Cluster Key password of **Pa\$\$w0rd**.
 - For the Cluster Address, specify **http://rms.woodgrovebank.com**, and then select **unencrypted connection (http://)**.
 - For the Server Licensor Certificate name, type **Woodgrove Bank RMS**.
 - Configure the AD RMS service connection point to register during installation.

Exercise 2: Managing AD RMS Rights Policy Templates

The main tasks for this exercise are as follows:

1. Manage AD RMS rights policy templates.
2. Configure AD RMS Rights Policy Template Distribution for Windows Vista® SP1 clients.
3. Use Group Policy Management Console to distribute the AD RMS Rights Policy Template to clients prior to Windows Vista® SP1.

► Task 1: To manage AD RMS templates

1. Log on to the 6426A-NYC-SVR1 virtual machine by using the user name **woodgrovebank\Administrator** and the password **Pa\$\$w0rd**.
2. Enable export of the rights policy templates and specify the export location as **\\NYC-DC1\Templates**.
3. Create a **Distributed rights policy template** with the following information:
 - Name: Confidential Projects
 - Description: Woodgrove Bank IT Department
 - Expiry duration: 14 days
 - Permissions:
 - ITAdmins@woodgrovebank.com: Edit permissions
 - Everyone else: View permissions

► Task 2: To configure AD RMS Rights Policy Template Distribution for Windows Vista® SP1 clients

1. Log on to the 6426A-NYC-CL1 virtual computer by using the user name **woodgrovebank\Betsy**, and the password **Pa\$\$w0rd**.
2. Start the Computer Management console as the Administrator with the password of Pa\$\$w0rd. Expand **Task Scheduler** and browse to **Active Directory Rights Management Services Client**.

3. Enable the **AD RMS Rights Policy Template Management (Automated)** task and then Run the task.
4. Start the Registry Editor by using regedit.exe. In the **Registry Editor**, expand the **HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common** key.
5. Create a new registry key under **Common** called **DRM**.
6. Under **DRM**, create a new expandable string value and name it **AdminTemplatePath**.
5. Specify the value data for the **AdminTemplatePath** key as **%LocalAppData%\Microsoft\DRM\Templates**.
6. Close the Registry Editor, and then log off the 6426A-NYC-CL1 virtual computer.

► **Task 3: To use Group Policy Management Console to distribute the AD RMS Rights Policy Template to clients prior to Windows Vista® SP1**

1. On the 6426A-NYC-DC1 virtual computer, open the **Group Policy Management** console.
2. Edit the **Default Domain Policy** Group Policy Object.
2. Add the **\\NYC-DC1\Templates\Office12.adm** template to the Administrative Templates node.
3. In the **Group Policy Management Editor**, browse to **User Configuration\Policies\Administrative Templates\Classic Administrative templates (ADM)\Microsoft Office 2007 System\Manage Restricted Permissions**.
4. Enable the **Specify Permission Policy Path** option.
5. In the **Enter path to policy templates for content permission** box, type **\\NYC-DC1\Templates** and then click **OK**.

Exercise 3: Configuring Trust Policies

The main tasks for this exercise are as follows:

1. To export the Trusted User Domains policy.
2. To export the Trusted Publishing Domains policy.
3. To import the Trusted User Domain policy from the Contoso domain.
4. To import the Trusted Publishing Domains policy from the Contoso domain.

► Task 1: To export the Trusted User Domains policy

1. On the 6426A-NYC-SVR1 virtual computer, use **Active Directory Rights Management Services** to export the **woodgrovebank.com** Trusted User Domain.
2. Save the output as `c:\woodgrovebank.bin`.

► Task 2: To export the Trusted Publishing Domains policy

1. On the 6426A-NYC-SVR1 virtual computer use **Active Directory Rights Management Services** to export the **woodgrovebank.com** Trusted Publishing Domain.
2. Save the output as `c:\woodgrovebank.xml`.

► Task 3: To import the Trusted User Domain policy from the Contoso domain

1. On the 6426A-NYC-SVR1 virtual computer, use **Active Directory Rights Management Services** to import the **Contoso** Trusted User Domain.
2. Import the file from `\\NYC-DC1\d$\Labfiles\Mod6\contoso.bin`.
3. Configure the Display name as **Contoso Domain**.

- ▶ **Task 4: To import the Trusted Publishing Domains policy from the Contoso domain**
 1. On the 6426A-NYC-SVR1 virtual computer, use **Active Directory Rights Management Services** to import the **Contoso** Trusted Publishing Domain.
 2. Import the file from \\NYC-DC1\d\$\Labfiles\Mod6\contoso.xml.
 3. In the **Display name** box, type **Contoso RMS**, and then type **Pa\$\$w0rd** as the password.

Exercise 4: Testing AD RMS Functionality

The main tasks for this exercise are as follows:

1. Create a rights-protected document.
2. Start the 6426A-NYC-CL1 virtual computer and log on as an unauthorized user.
3. Start the 6426A-NYC-CL1 virtual computer and log on as an authorized recipient.

► Task 1: To create a rights-protected document

1. Log on to the 6426A-NYC-CL1 virtual computer by using the user name **woodgrovebank\Betsy** and the password **Pa\$\$w0rd**.
2. Start Microsoft® Office Word 2007.
3. Create a protected document using the **Confidential Projects** rights policy template.
4. In the document body, type **This is a protected document**.
5. Save the document as **\\NYC-DC1\Templates\Protected.docx**.
6. Close Microsoft® Office Word® 2007, and then log off.

► Task 2: To start the 6426A-NYC-CL1 virtual computer and log on as a Standard user

1. Log on to the 6426A-NYC-CL1 virtual computer by using the user name **woodgrovebank\aaroon** and the password **Pa\$\$w0rd**. Note that Arron is not a member of the ITAdmins group and should only have view access to the document.
2. Start Microsoft® Office Word® 2007
3. Open the **\\NYC-DC1\Templates\protected.docx** document.
4. Verify the permissions that are allowed for the document.
5. Close Microsoft® Office Word® 2007, and then log off.

► **Task 3: To start the 6426A-NYC-CL1 virtual computer and log on as an authorized recipient**

1. Log on to 6426A-NYC-CL1 virtual computer by using the user name **woodgrovebank\Axel** and the password **Pa\$\$w0rd**. Note that Axel is a member of the IT Admins group and should have Editing access to the document.
2. Start Microsoft® Office Word® 2007
3. Open the \\NYC-DC1\Templates\protected.docx document.
4. Verify the permissions that are allowed for the document.
5. Type **Accessed successfully by Axel** in a new line.
6. Save the document.
7. Close Microsoft® Office Word® 2007, and then log off.



After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review: Configuring AD RMS

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 Domains 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 6426A-NYC-CL1 virtual computer and log on as a Standard user
- Started the 6426A-NYC-CL1 virtual computer and log on as an authorized recipient

Lab Resources

There are no additional lab resources for this lab.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

Module 7

Maintaining Access Management Solutions

Contents:

Lesson 1: Supporting AD CS	7-4
Lesson 2: Maintaining AD LDS	7-16
Lesson 3: Maintaining AD FS	7-27
Lesson 4: Maintaining AD RMS	7-36
Lab 7: Maintaining Access Management Solutions	7-44

Module Overview

- Supporting AD CS
- Maintaining AD LDS
- Maintaining AD FS
- Maintaining AD RMS

It has become vital for business organizations to provide strong authentication, and manage multiple authentication methods. You must do this because vital information can be exposed to end-users. The right identity and access management solutions can greatly enhance the user's experience by helping them to manage their online identities. This is because the users will no longer be required to manage multiple passwords.

After you configure Identity and Access (IDA) solutions, you must also know how to maintain IDA solutions. IDA maintenance involves providing support for Active Directory® Certificate Services (AD CS). It also requires maintenance of Active Directory® Lightweight Directory Services (AD LDS). To maintain access solutions you must provide long-term support for AD LDS. You must also know how to use the Active Directory® Right Management Services (AD RMS) console to manage AD RMS.

Lesson 1

Supporting AD CS

- Common AD CS Maintenance Tasks
- Configuration of Role-Based Administration for Managing and Maintaining AD CS
- Tools Used to Maintain AD CS
- Configuration of CA Event Auditing
- How To Configure CA Event Auditing
- Methods of Backing Up and Restoring a CA

To provide AD CS support to maintain IDA solutions you must be able to identify common AD CS maintenance tasks. To support AD CS you must configure role-based administration to manage AD CS. You must be able to identify tools such as Server Manager, Certification Authority snap-in, Enterprise PKI snap-in, Certificate Templates snap-in, and Certutil.exe to maintain AD CS. In addition, you must audit CA event by using the Certification Authority snap-in. Moreover, you must be familiar with methods to back up and restore a CA.

Common AD CS Maintenance Tasks



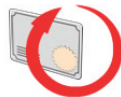
Managing role-based administration



Configuring and monitoring CA event auditing



Monitoring system services



Renewing CA certificate



Backing up and restoring the CA

Key Points

After you have set up the CA environment, your next challenge is to maintain and monitor the CA environment. The following table describes the most common AD CS Maintenance Tasks.

AD CS Maintenance Task	Task Description
Manage role-based administration	You have to assign the CA roles to the CA administrators. Each CA role has to be assigned with a unique set of tasks.
Configure CA event auditing	You have to audit all the events related to the management of a CA.
Examine system services	You have to examine system services to ensure that the CA servers are available to process certificate requests.

AD CS Maintenance Task	Task Description
Review pending certificate requests	You have to decide if the request for a certificate should be considered or not.
Renew CA certificates	You have to take necessary steps to renew CA certificates before expiry.
Back up and restore the CA	You have to take the necessary steps to shield a CA against any kind of data loss.
Revoke certificates	You have to revoke certificates when the certificates are compromised or no longer valid for an intended purpose.
Publish certificate templates	You have to publish new and remove old certificate templates.
Publish certificate revocation lists (CRLs)	You have to inform your clients if they can trust a certificate or not



For more information see, **AD CS CRL Publishing**.

Configuration of Role-Based Administration for Managing and Maintaining AD CS

Role and Group	Security Permission	Description
CA Administrator	Manage CA	Allows configuring and maintaining of CA. This CA role includes the ability to assign other CA roles and renew a CA certificate.
Certificate Manager	Issue and Manage Certificates	Allows approving of certificate enrollment and revocation requests. This is a CA role, also called as CA officer.
Backup Operator	<ul style="list-style-type: none"> • Back up file and directories • Restore file and directories 	Allows performing of system backup and recovery. Backup is an operating system feature.
Auditor	Manage auditing and security log	Allows configuring, viewing, and maintaining of audit logs. This is an operating system feature and an operating system role.
Enrollees	<ul style="list-style-type: none"> • Read • Enroll 	Allows requesting of certificates from a CA. This is not a CA role. Enrollees are authorized clients for this purpose.

Key Points

Role-based administration helps manage certification authority (CA) administrators into separate, predefined roles. A CA administrator can use the specific security settings of each role to assign roles to users.

For example, a user with the Manage CA permission can perform certain CA tasks that a user with the Issue and Manage Certificates permission cannot perform. A CA administrator can assign multiple roles to a user.

The following table describes the roles, users, and groups that you can use to implement role-based administration and the associated security permissions.

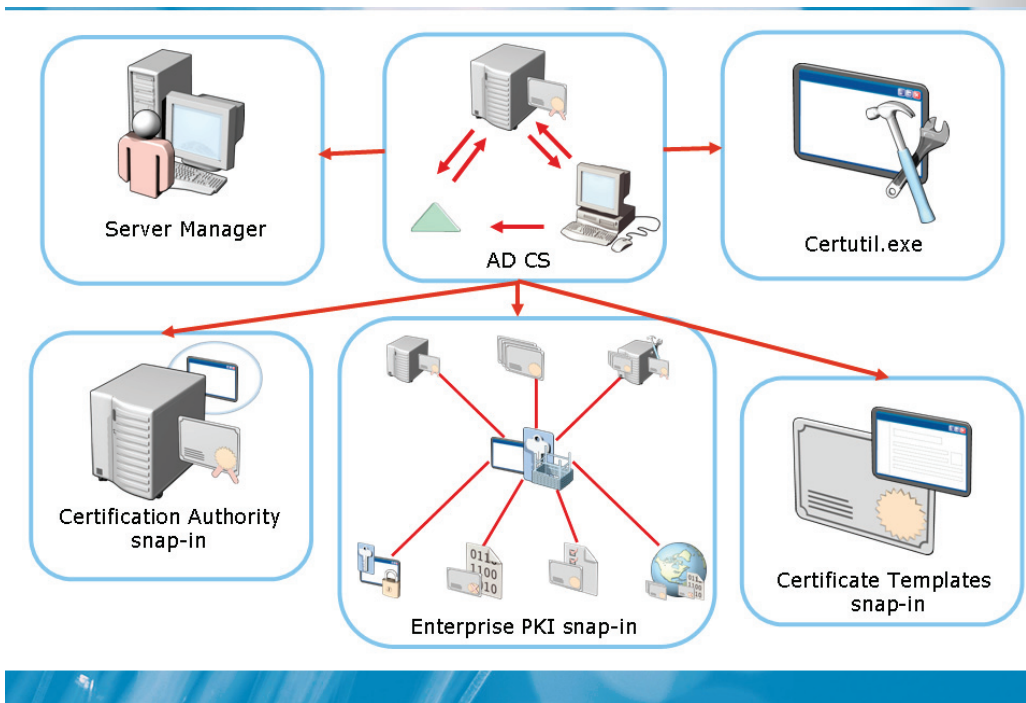
Roles and groups	Description of associated security permission
CA administrator	CA administrator configures and maintains the CA. In addition, a CA administrator can assign the CA administrator and CA manager roles and to renew the CA certificates.

Roles and groups	Description of associated security permission
Certificate manager	Certificate manager approves certificate enrollment and revocation requests. The certificate manager is also known as the CA officer. The Certification Authority snap-in helps assign CA roles.
Backup operator	<ul style="list-style-type: none"> Backup operator performs system backup and recovery. The backup operator is assigned the permission to backup and restore associated files and directories.
Auditor	Auditor helps configure, view, and maintain audit trials. Auditing is an operating system feature and so an auditor is an operating system role. Auditors are assigned the permission to manage auditing and security log.
Enrollees	Enrollees request certificates from a CA. Enrollees are not CA roles they are authorized clients. They are assigned the Read and Enroll permissions.



For more information, see **Restore AD LDS Instance Data**.

Tools Used to Maintain AD CS



Key Points

The following table describes a few tools used to maintain AD CS:

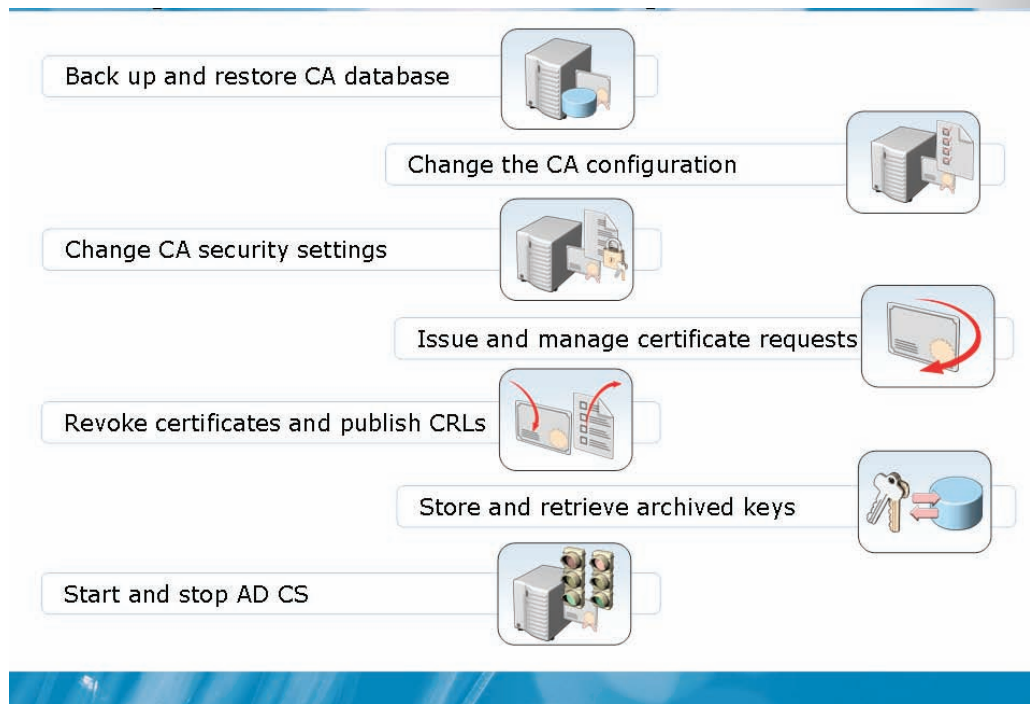
Tool	Description
Server Manager	Server Manager is a tool that helps set up the components of AD CS. You can use the Server Manager tool, to set up the following AD CS components: <ul style="list-style-type: none"> • CAs • Web enrollment • Online Responder • Network Device Enrollment Service
Certification Authority snap-in (Certsrv.msc)	Certsrv.msc is a tool that helps manage multiple CAs. You can use this tool to perform the following administrative tasks:

Tool	Description
	<ul style="list-style-type: none"> • Start and stop the CA • Back up and restore the CA • Renew certificates • Configure security permissions and delegating administrative control for the CA • Revoke certificates
Enterprise PKI snap-in (PKIView)	PKIView is a tool that provides the status of the network's PKI environment. You can use this tool to view multiple CAs and their current health state. The current health state can include the validity or accessibility of authority information access (AIA) locations and certificate revocation list (CRL) distribution points.
Certificate Templates snap-in	The Certificate Templates snap-in helps manage certificate templates that define the format and content of a certificate.
Certutil.exe	<p>Certutil.exe is a command-line program installed as part of AD CS. You can use Certutil.exe tool to perform the following tasks:</p> <ul style="list-style-type: none"> • Extract and show CA configuration information • Configure Certificate Services • Back up and restore CA components • Verify certificates, key pairs, and certificate chains



For more information, see **Certificate Services Technical Reference**.

Configuration of CA Event Auditing



Key Points

As an administrator, you can audit the following management and activity events of the CA:

- Back up and restore the CA database
- Change the CA configuration
- Change CA security settings
- Send out and manage certificate requests
- Revoke certificates and CRLs
- Store and retrieve archived keys
- Start and stop AD CS

A CA administrator or a CA auditor can use the Certification Authority snap-in to facilitate CA auditing. If the CA has been configured to enforce role-based administration, CA auditing can be enabled.

Prior to auditing events, you need to configure the computer to audit the access of item. You can view and manage audit policy options in local or domain Group Policy along the path:

Computer Configuration\Windows Settings\Security Settings\Local Policies



For more information, see **CA Help File**.

Demonstration: How To Configure CA Event Auditing

- To configure the CA for auditing of object access
- To configure CA event auditing

Key Points

The instructor will provide a demonstration to show how you can configure CA event auditing.

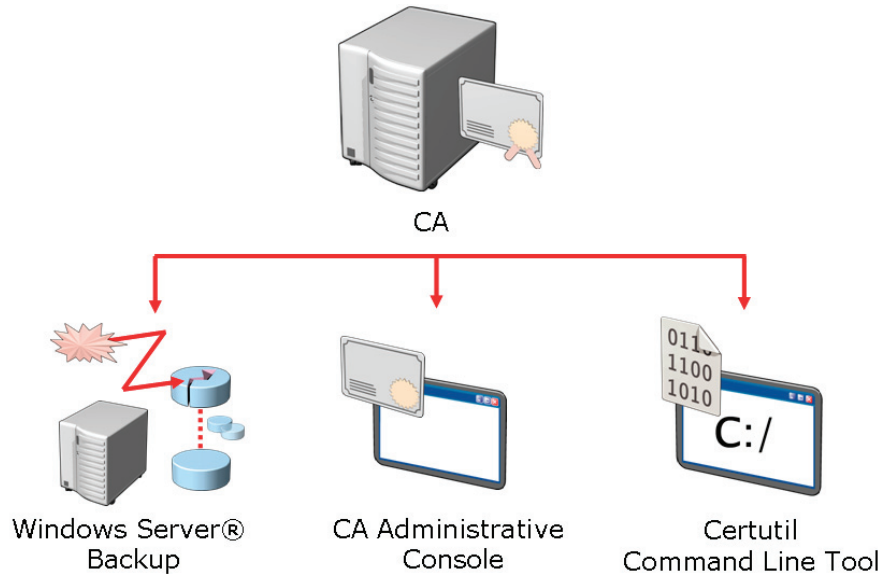
Questions:

1. How do you activate object access auditing?
2. Where is the audit events logged?
3. How do you activate CA event auditing?



For more information, see **CA Auditing**.

Methods of Backing Up and Restoring a CA



Key Points

You can back up a Certification Authority (CA) without backing up the entire server. You can use the Backup snap-in to back up and restore the CA and the server simultaneously. To restore a CA without restoring the server on which it is installed, you can use the Certification Authority snap-in or the Certutil command-line tool. The Certification Authority snap-in and the Certutil command-line tool can restore a CA from a backup copy. You can also use these tools to back up only the CA components. However, you should manually restore the IIS metabase and registry settings.

You can use Windows Server® Backup to back up the CA and all its components. Windows Server® Backup backs up all the components, which include the IIS metabase and any Certificate Services registry settings.

You must be a CA administrator or a member of the Backup Operators group, or equivalent, to perform backup and restore procedures.



For More Information, see the Certification Authority help file for:

- **Back Up a Certification Authority**
- **Restore a CA from a Backup Copy**

Lesson 2

Maintaining AD LDS

- AD LDS Maintenance Tasks
- Backing Up AD LDS
- Restoration of Data to an AD LDS Instance
- Performing an Authoritative Restore of Data on an AD LDS Instance
- How To Back Up and Restore AD LDS Instances

To manage IDA solutions, you should maintain AD LDS. To do so, you also need to back up AD LDS. You must be able to restore data to an AD LDS instance, which already exists or belongs to a configuration set. Use Windows® Backup to perform an authoritative restore of AD LDS data. You must be familiar with the steps to backup and restore Ad LDS instance.

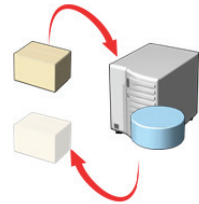
AD LDS Maintenance Tasks

AD LDS Maintenance Tasks include :

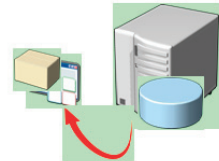
Monitoring system events and services



Backing up and restoring AD LDS instances



Performing an authoritative restore of directory objects



Key Points

To maintain AD LDS, you need to:

- Start, stop, and restart an AD LDS instance
- Perform back up and authoritative restores of AD LDS data
- Move the AD LDS data files
- Change the AD LDS service account and port numbers
- Administer containers and objects
- Extend AD LDS schema
- Copy a schema from AD DS
- Import an AD DS schema into AD LDS
- Manage directory data between all sites in an AD LDS configuration set

- Manage object permissions
- Synchronize AD LDS and AD DS
- Import and export data to or from AD LDS



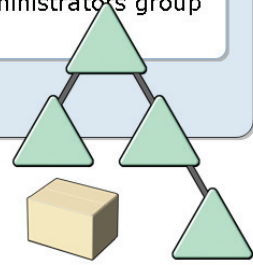
For more information, see:

- **Practice Using AD LDS Administration Tools**
- **AD LDS**

Backing Up AD LDS

Consider the following when backing up AD LDS:

- By default each instance stores **Adamntds.dit** and associated log files in `%Program Files%\Microsoft ADAM\instancename\data`.
- You can use Windows Server® Backup or any compatible third party backup utility to backup AD LDS.
- You should ensure that the instance is started before backing up its AD LDS folder.
- You should ensure that you are a member of the Administrators group or equivalent.



Key Points

You should back up AD LDS data and log files regularly, to ensure data availability. You can use Windows Server® Backup or any other backup program to perform the back up. By default, each AD LDS instance stores its database file and the associated log files in an instance-specific folder. The default location for this folder is `%ProgramFiles%\Microsoft ADAM\instancename`, where *instancename* refers to the AD LDS instance name. You should include these files in the regular backup schedule of the organization.



When you back up an instance, ensure that the instance is running.



For more information, see:

- [Restore AD LDS Instance Data](#)

- **Back up AD LDS Instance Data**, in the Active Directory® Lightweight Directory Services help file

Restoration of Data to an AD LDS Instance

Consider the following when restoring data to an existing AD LDS instance:

- Stop the AD LDS instance for which the data will be restored.
- Use the backup program to restore the instance and overwrite existing files.
- Restart the AD LDS instance.

Consider the following when data to a new AD LDS instance that does not belong to a configuration set:

- Create a new instance specifying the same settings used during the original AD LDS installation, without creating an application partition.
- Stop the newly created AD LDS instance.
- Use the backup program to restore the instance and overwrite existing files.
- Restart the AD LDS instance.

Key Points

Consider the following key aspects when restoring data to an AD LDS instance:

- You should check if the instance:
 - Already exists
 - Belongs to a configuration set
- You should stop the instance if you want to restore it.
- You should move or delete the existing database and log files from the AD LDS instance before the restore operation.
-



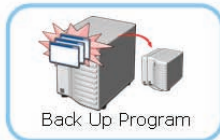
For more information, see:

- **Restore AD LDS Instance Data**
- **Restore AD LDS Instance Data**, in the Active Directory® Lightweight Directory Services help file

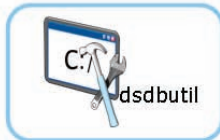
Performing an Authoritative Restore of Data on an AD LDS Instance



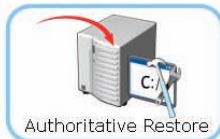
- Stop the running AD LDS instance for which the data is restored.



- Use the backup program to restore the instance and overwrite existing files.



- Activate the instance by using dsdbutil, at a command prompt.



- Use dsdbutil to perform an authoritative restore using one of the following commands:
 - restore database
 - restore object dn
 - restore subtree dn

Key Points

You can force the AD LDS data that is restored to override authoritatively the existing data in the configuration set. The following steps help perform an authoritative restore of AD LDS data on an AD LDS instance that is a part of a configuration set.

1. Stop the AD LDS instance for which data is restored.
2. Use Windows® Backup and follow the steps in the Recovery Wizard to:
 - Specify the location of the source backup data.
 - Identify the specific backup from which you want to recover the instance data.
3. Select the folder that contains the instance data files.
4. Replace existing files by recovered files.

5. Close Windows® Backup after the completion of restore.
6. Use the dsdbutil tool to perform the authoritative restore.



For more information, see:

- **Restore AD LDS Instance Data**
- **Restore AD LDS Instance Data**, in the Active Directory® Lightweight Directory Services help file

Demonstration: How To Back Up and Restore AD LDS Instances

- To back up a volume that contains an AD LDS instance by using Windows Server® Backup
- To restore an existing AD LDS instance

Key Points

The instructor will provide a demonstration to show how you can back up and restore AD LDS instances.

Questions:

1. What is the built-in tool that you can use to back up and restore AD LDS instances?
2. Which is the default location of AD LDS instance files?
3. Will you choose to stop or run the AD LDS instance, during the backup and restore process?



For more information, see **Restore AD LDS Instance Data Generation**.

MCT USE ONLY. STUDENT USE PROHIBITED



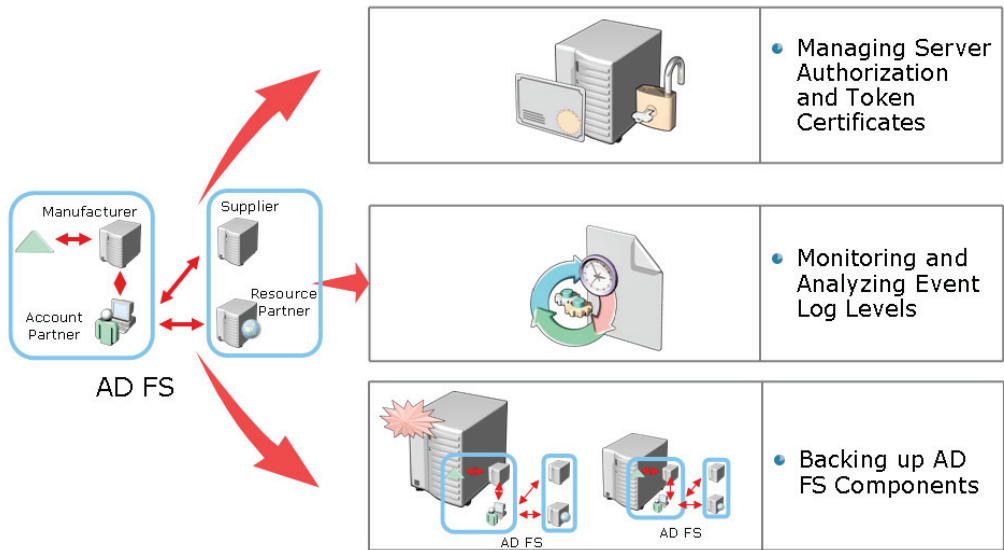
Lesson 3

Maintaining AD FS

- AD FS Maintenance Tasks
- Monitoring AD FS Events
- How To Monitor AD FS Events
- Backing Up AD FS Components

Maintenance of IDA solution requires providing long-term support for AD FS. You can provide support for AD FS by maintaining a few Ad FS tasks such as Renewing and importing certificates, Managing resource groups, and Resolving DNS names. You must also be familiar with AD FS events and the steps to monitor AD FS events. In addition, you can provide AD FS support by backing up AD FS components to maintain an AD FS state snapshot.

AD FS Maintenance Tasks



Key Points

When you need to the maintenance tasks for AD FS, you need to:

- Monitor and maintain AD DS and AD LDS to ensure account store availability.
- Manage resource groups of the resource partner organization if you use Windows® token-based applications.
- Resolve DNS names to ensure that the server and clients can locate resources.
- Ensure network connectivity for the server and clients.
- Maintain and monitor forest trusts that AD FS deployment relies on.
- Back up and restore AD FS components.

In addition, you need to:

- **Renew and import certificates.** When you renew and import certificates you need to manage the server authorization and token certificates.
- **Add new applications.** When you need to add new applications, you need to install and configure the applications by using the AD FS Web server. You can add new applications if Windows® Token-based or claims-aware applications are made available.
- **Maintain the health and performance of Web servers.** When you maintain the health and performance of Web servers, you also need to monitor and analyze event logs. These Web servers host the AD FS Web server role, federation servers, and federation server proxies.

Monitoring AD FS Events

AD FS Trust Policy Event Log levels can be configured to provide the following information:	
Error	Records events logged by significant problems, to the event log
Warning	Records insignificant events that may cause future problems to the event log
Informational	Records informational logged events; such as token validations, or claim mappings
Success Audit	Records a security audit for every successful authentication or changed trust policy to this Federation Service
Failure Audit	Records a security audit for every unsuccessful change to trust policy for this Federation Service
Detailed Success	Records a detailed security audit for successful authentications
Detailed Failure	Records a detailed security audit for failed authentications

Key Points

Some AD FS events are logged in the Event Viewer by default. You can configure event logging on federation servers, federation server proxies, and Web servers. AD FS events are logged in the Application event log and the Security event log.

AD FS Federation Service events are logged in the Application event log by servers that run the Federation Service role. These events provide information about the components of the local organization. In addition, the events provide information on components of the partner organizations covered by the trust policy.

Federation servers log AD FS Federation Service events in the Application and Security event logs. On a federation server proxy, events in the Application log contain additional information about errors related to the contact with the Federation Service. In addition, if you use a federation server proxy, the Federation Service events contain information about the proxy certificates that are used.

You can log events for Windows® NT token-based applications on a Web server that runs the AD FS Web Agent. You can also set event logging for claims-aware applications in the Web.config file of the applications.



For more information, see **Configuring ADFS Servers for Troubleshooting**.

Demonstration: How To Monitor AD FS Events

- To enable trust policy logging
- To use Server Manager to view events and service summary data

Key Points

The instructor will provide a demonstration to show how you can monitor AD FS events.

Questions:

1. What are the prerequisites for AD FS to log errors?
2. Where can you change the default levels of the AD FS event log?
3. How can you activate AD FS debugging?



For more information, see **Configuring event logging on a federation server**.

Backing Up AD FS Components

Components to Back Up by running AD FS Component on Server Files	
Component	Files to Back Up
Federation Service	<ul style="list-style-type: none"> • TrustPolicy.xml file • Web.config and other files under %systemdrive%\E\ADFS\... • System state • Custom transform module (.dll) and related files, if any
Federation Service Proxy	<ul style="list-style-type: none"> • Web.config and other files under %systemdrive%\ADFS\... • System state
AD FS Web Agent	<ul style="list-style-type: none"> • %systemdrive%\ADFS\... • System state

Key Points

You can back up AD FS components to maintain a snapshot of an AD FS state. Back up is critical to ensure the recovery options if you lose data or hardware components fail.

You can use the Windows® Backup tool to create a backup for AD FS components on federation servers, federation server proxies, and Web servers that run the AD FS Web Agent.

The following table describes the components that you must back up on servers that run AD FS components.

AD FS Component	Components to back up
Federation Service	<ul style="list-style-type: none"> • TrustPolicy.xml • Web.config and other files located in %systemdrive%\ADFS

AD FS Component	Components to back up
	<ul style="list-style-type: none"> • System state • Custom transform module (.dll) and other related files
Federation Service Proxy	<ul style="list-style-type: none"> • Web.config and other files under %systemdrive%\ADFS • System state
AD FS Web Agent	<ul style="list-style-type: none"> • %systemdrive%\ADFS • System state

For claims-aware applications, AD FS settings are located in the Web.config file. For Windows® NT token-based applications, AD FS settings are located in the IIS metabase files. You may also regularly back up certificates that are used by AD FS components.



For more information, see **Back up AD FS components on a federation server, federation server proxy, or Web server.**

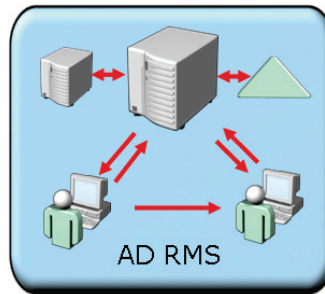
Lesson 4

Maintaining AD RMS

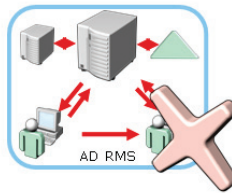
- AD RMS Maintenance Tasks
- How To Verify AD RMS Logging
- Viewing AD RMS Reports
- Decommissioning AD RMS

To maintain IDA solutions, you must preserve AD RMS. You can preserve AD RMS by maintaining AD RMS tasks by using the AD RMS console. In addition, you must be familiar with the steps to verify AD RSM logging. You must also be able to generate reports by using AD RMS. Moreover, you must identify the reasons to remove AD RMS.

AD RMS Maintenance Tasks



Viewing AD RMS Reports



Decommissioning AD RMS



Managing AD RMS log information

Key Points

You can use the AD RMS console to manage AD RMS. When you manage AD RMS, you need to:

- Enable exclusion policies.
- Establish trust policies.
- Manage the following AD RMS databases:
 - Configuration database
 - Logging database
 - Directory Services database
- Configure and distribute rights policy templates
- Change the AD RMS service account
- Register or change the service connection point (SCP)

- Change the cluster key password.
- View AD RMS reports.
- Configure AD RMS logging.
- Maintain the health and performance of AD RMS servers.
- Configure and maintain user accounts in the following AD DS and AD RMS administrative groups:
 - AD RMS Enterprise Administrators
 - AD RMS Auditors
 - AD RMS Template Administrators
 - AD RMS super user group
 -

In addition, you also need to:

- Ensure that you can use AD DS to authenticate users, resolve group memberships, and store AD RMS SCPs.
- Ensure that clients and servers can use the DNS functionality and name resolution to locate resources by name.
- Ensure network connectivity.

Demonstration: How to Verify AD RMS Logging

- To verify default enabling
- To verify the configuration of the server node Properties box
- To verify:
 - Requestor identification
 - Time of making
 - Source IP address
 - RMS server identification that handled the request
 - Success of request




Key Points

The instructor will provide a demonstration to show how you can verify AD RMS logging.

Questions:

1. Identify the types of databases used by AD RMS.
2. What is the role of the logging database?
3. Name the tool that you can use to administer logging for the AD RMS cluster.

Viewing AD RMS Reports

 <p>Statistics Report</p>	<p>Lists the number of total accounts, domain accounts, and federated identities certified, or granted a rights account certificate (RAC), by the AD RMS root cluster.</p>
 <p>System Health</p>	<p>Provides information about the overall health of the AD RMS cluster by using a wizard. The System Health report has two views:</p> <ul style="list-style-type: none"> • Request Type Summary • Request Performance Summary
 <p>Troubleshooting Reports</p>	<p>Assists you in troubleshooting issues with AD RMS licenses by using a wizard.</p>

Key Points

You can use AD RMS to generate reports that provide information about troubleshooting issues with AD RMS licenses. You can also use AD RMS to generate reports about domain accounts and the overall health of the AD RMS cluster.

The following table lists the reports that AD RMS can generate.

Reports	Description
Statistics reports	This report provides information about the number of total accounts, domain accounts, and federated identities that the AD RMS root cluster certifies, or grants a rights account certificate.
Health reports	This report uses a wizard to provide information about the overall health of

Reports	Description
	the AD RMS cluster. The system health report has two views: <ul style="list-style-type: none">• Request Type Summary• Request Performance Summary
Troubleshooting reports	This report uses a wizard to provide information about troubleshooting issues with AD RMS licenses.

You must install the Microsoft® Report Viewer to access the system health and troubleshooting reports.



For more information, see **Microsoft® Report Viewer Redistributable 2005**.

Decommissioning AD RMS

Steps to decommission AD RMS:

- 1 Encourage creative thinking among team members.
- 2 Ensure that you have all the information.
- 3 Manage discussions about the validity of a threat.
- 4 Include specialized network penetration testers.
- 5 Apply caution when it involves conflict of interests.
- 6 Consider technology-specific threats.



Key Points

Before you remove the AD RMS role from a server, you should back up AD RMS databases that are used by the server.

After you back up the databases, you need to decommission AD RMS before you uninstall the server role. When you decommission the AD RMS, the AD RMS cluster provides a key. This key decrypts the rights-protected content that the AD RMS cluster had previously published.

After you enable decommissioning, the AD RMS management console displays the information page of Decommissioning server in the results pane. The console then does not support further AD RMS administration.

The requirements for removing an AD RMS server depend on the role of the server and topology of the AD RMS installation. The common scenarios in which you can remove the AD RMS server role are when you:

- **Remove a server from a cluster.** In this scenario, you must first decommission and uninstall AD RMS on the server that you want to retire. You must then remove the server from the load-balancing rotation.
- **Retire a stand-alone server.** In this scenario, you need to first decommission and uninstall the existing AD RMS server. You must then disconnect the server from the network, immediately install and provision AD RMS on the replacement server.
- **Replace an AD RMS installation with an existing AD RMS installation.** In this scenario, you need to first export the trusted user domain (TUD) and trusted publishing domain (TPD) from the AD RMS cluster that you want to retire. You must then import the TUD and TPD into the active AD RMS cluster.



For more information, see **Removing an AD RMS Cluster**.

Lab 7: Maintaining Access Management Solutions

- Exercise 1: Configuring CA Event Logging
- Exercise 2: Implementing role-based administration in AD CS
- Exercise 3: Backing up a CA
- Exercise 4: Reconfiguring AD RMS cluster settings
- Exercise 5: Generating AD RMS Reports
- Exercise 6: Configuring AD RMS logging

Logon information

Virtual machine	6426A-NYC-DC1-B
User name	Administrator
Password	Pa\$\$w0rd
Domain name	woodgrovebank.com

Estimated time: 60 minutes

Objectives

After completing the lab, you will be able to:

- Configure CA event logging
- Implement role-based administration in AD CS
- Back up a CA
- Reconfigure AD RMS cluster settings
- Generate AD RMS reports
- Configure AD RMS logging

Scenario

Woodgrove Bank is a large multinational corporation with office locations located in 5 many countries. At present, the organization is currently running Windows Server® 2003. It is also implementing Windows Server® 2008, which is at an initial stage.

Consolidation Requirements:

As the corporate server technology specialist, it is your role to monitor and maintain Windows Server® 2008 computers in the organization. Woodgrove Bank has recently implemented an Enterprise Certificate Authority (CA).

As an administrator responsible for designing AD CS infrastructure, you want to ensure the overall health of your PKI infrastructure. To do so, you must perform the following consolidation activities:

- Distribute CA management roles across different individuals in the organization.
- Audit events relating to the management and activities of the CA.
- Ensure that CA can be restored in the event of a disaster by implementing a CA backup strategy.
- Change the AD RMS cluster key password and AD RMS service account settings. This is because you have just taken the support of the bank's Active Directory® Rights Management Services (AD RMS) infrastructure. The previous administrator left the organization and you have been asked to ensure systems' security.
- Change the AD RMS cluster key password and AD RMS service account settings.
- Control the size of the message queue related to AD RMS logging. This is because the amount of free disk space on the AD RMS server is limited.
- Generate System Health reports to get information on the AD RMS system's health.

Exercise 1: Configuring CA Event Auditing

In this exercise, you will use the available virtual computer environment. Before you begin the exercise, you must:

1. Start the 6426A-NYC-DC1-B virtual computer, and log on by using the user name **woodgrovebank/Administrator**, and the password **Pa\$\$w0rd**.

The main tasks for this exercise are as follows:

1. Use Enterprise PKI to view the health of the CA.
2. Enable the auditing of object access.
3. Enable CA auditing.

► **Task 1: To use Enterprise PKI to view the health of the CA**

1. On the 6426A-NYC-DC1-B virtual computer, use the Server Manager to install the **Certification Authority Web Enrollment** role service.
2. On the 6426A-NYC-DC1-B virtual computer, start the **Enterprise PKI** tool.
3. In the Enterprise PKI console, view each object under the Name column, and ensure that there are no warning icons next to these objects.



If the use of Secure Socket Layer (SSL) is enforced on the Default Web site, you will see errors next to the Authority Information Access™ (AIA) Location #2, DeltaCRL Location #2, and CDP Location #2 because by default these locations are configured to use HTTP. Clear the "**Require SSL on the Default Web site**" check box in the IIS snap-in and refresh the view in Enterprise PKI snap-in.

► **Task 2: To enable auditing of object access**

1. On the 6426A-NYC-DC1-B virtual computer, modify the **Default Domain Controller Policy** to enable **Audit object access** auditing for **Success** and **Failure** events.
2. Open a command prompt window and run **gpupdate /force**.

► **Task 3: To enable CA auditing**

1. Use the **Certification Authority** snap-in to enable **Auditing** of all CA events.
2. Restart the **AD CS** service

Exercise 2: Implementing role-based administration in AD CS

In this exercise, you will implement role-based administration.

The main tasks for this exercise are as follows:

1. Delegate role specific permissions

► Task 1: To delegate role specific permissions

1. Configure certification authority administrators.
 1. On the 6426A-NYC-DC1-B virtual computer, use the **Certification Authority** console to modify the **Security** settings.
 2. Grant **woodgrovebank\CA Admins** the **Manage CA** permissions.
2. Configure certificate managers.
 1. On the 6426A-NYC-DC1-B virtual computer, use the **Certification Authority** console to modify the **Security** settings.
 2. Grant **woodgrovebank\CA Managers** the **Issue and Manage certificates** permissions.
3. Configure CA auditors
 1. On the 6426A-NYC-DC1-B virtual computer, edit **Default Domain Controller Policy** to change **User Rights Assignments**.
 2. Define the **Manage auditing and security log** policy settings.
 3. Add **CA Auditors**, and then click **OK**.
 -
4. To add CA backup operators
 1. On the 6426A-NYC-DC1-B virtual computer, edit the **Default Domain Controller Policy** to change **User Rights Assignments**.
 2. Define the **Backup files and directories**, and the **Restore files and directories** policy settings.
 3. Add **CA Backup Operators**, and then click **OK**.
 4. In the Command prompt window, type **gpupdate /force**.

► **Task 2: To enable CA auditing**

1. Use the Certification Authority console to enable Auditing of all CA events.
2. Restart the **AD CS** service.

Exercise 3: Backing up a CA

In this exercise, you will schedule a task to backup a CA on a daily basis.

The main tasks for this exercise are as follows:

1. Schedule a task to perform CA backup.

► Task 1: To schedule a task to perform CA backup

1. On the 6426A-NYC-DC1-B virtual computer, use **Task Scheduler** to create a new task with the following parameters:
 1. Name: **CA Backup**.
 2. User account to run the task: **woodgrovebank\Backup**.
 3. User password: **Pas\$\$w0rd**
 4. Options:
 1. **Run whether user is logged on or not**.
 2. **Run with highest privileges**.
 5. Trigger: **Daily** (set the time to run within 5 minutes from now).
 6. Action:
 1. Program/script: **certutil**.
 2. Add arguments (optional): **-backup -p Pa\$\$w0rd c:\backup**.
 7. Wait for the task to start and complete the backup.
 8. Confirm that the backup has completed successfully by viewing the content of the **c:\backup** folder, and checking the task status.
 9. Log off from the 6426A-NYC-DC1-B virtual computer.

Exercise 4: Reconfiguring AD RMS cluster settings

In this exercise, you will reconfigure AD RMS cluster key password and the service account password.

The main tasks for this exercise are as follows:

1. Log on to 6426A-NYC-DC1-B virtual computer.
2. Reset the AD RMS Cluster Key Password.
3. Reset the AD RMS Service Account.
4. Change the AD RMS Service Account.

► Task 1: To log on to the 6426A-NYC-DC1-B virtual computer

1. Log on to the 6426A-NYC-DC1-B virtual computer as **woodgrovebank/Administrator**, by using the password **Pa\$\$w0rd**.

► Task 2: To reset the AD RMS Cluster Key Password

1. On the 6426A-NYC-DC1-B virtual computer, use the **AD RMS** console window to change the cluster key password to **Pa\$\$w0rd**.

► Task 3: To reset the AD RMS Service Account

1. On the 6426A-NYC-DC1-B virtual computer, use the **Active Directory Users and Computers** window, to locate the service account named **admsservice**, and reset the password to **Pa\$\$w0rd1**.

► Task 4: To change the AD RMS Service Account

1. On the 6426A-NYC-DC1-B virtual computer, use the **AD RMS** console window, to change the **woodgrovebank\admsservice** service account password, to **Pa\$\$w0rd1**.

Exercise 5: Generating AD RMS Reports

In this exercise, you will generate AD RMS reports.

The main tasks for this exercise are as follows:

1. Install Microsoft® Report Viewer.
2. View AD RMS System Health reports.
3. View AD RMS Statistics reports.

► Task 1: To install Microsoft® Report Viewer

1. On the 6426A-NYC-DC1-B virtual computer, browse to and double-click **c:\ReportViewer.exe** to install Microsoft® Report Viewer.
2. Follow the wizard steps to complete the setup.

► Task 2: To view AD RMS System Health reports

1. On the 6426A-NYC-DC1-B virtual computer, use the **AD RMS** console window to select **System Health** reports.
2. In the Actions pane, click **View Report**.
3. Specify the query start and end dates when prompted and click **Finish**.



No report will be visible since this is a newly installed server.

► Task 3: To view AD RMS Statistics reports

1. On the 6426A-NYC-DC1-B virtual computer, use the AD RMS console window to select **Statistics Reports**.
2. View the statistics in the main window.
3. Close the **AD RMS** console window.
4. Log off the 6426A-NYC-DC1-B virtual computer.

Exercise 6: Configuring AD RMS logging

In this exercise, you will configure AD RMS event and message logging.

The main tasks for this exercise are as follows:

1. Log on to the 6426A-NYC-DC1-B virtual computer.
2. Enable logging for the cluster.
3. Limit disk space usage for message queuing.

► Task 1: Log on to the 6426A-NYC-DC1-B virtual computer

1. Log on to the 6426A-NYC-DC1-B virtual computer as **woodgrovebank/Administrator** using the password, **Pa\$\$w0rd**.

► Task 2: Enable logging for the cluster

1. On the 6426A-NYC-DC1-B virtual computer, use the **AD RMS** console window to enable logging.

► Task 3: Limit disk space usage for message queuing

1. On the 6426A-NYC-DC1-B virtual computer, use **Server Manager** to access Private Queues.
2. Expand Features, expand Message Queuing, expand Private queues, and then set the **Limit message storage (KB)** to **1 024 000**.
3. Log off the 6426A-NYC-DC1-B virtual computer.



Message Queuing stores all queued messages up to the limit of the free storage space. If all of the available disk space is used, the AD RMS server will not be able to service any client requests.



After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review: Configuring AD CS

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

Lab Resources

There are no additional lab resources for this lab.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

Module 8


Troubleshooting IDA Solutions

Contents:

Lesson 1: Troubleshooting AD CS	8-3
Lesson 2: Troubleshooting AD LDS	8-19
Lesson 3: Resolving AD FS Issues	8-28
Lesson 4: Solving AD RMS Issues	8-37
Lab 8: Troubleshooting IDA Solutions	8-42

Module Overview

- Troubleshooting AD CS
- Troubleshooting AD LDS
- Resolution of AD FS Issues
- Solving AD RMS Problems



After configuring Identity and Access (IDA) solutions, you should be able to identify ways to troubleshoot IDA solutions.

To troubleshoot IDA solutions you must be able to troubleshoot Active Directory® Certificate Services (AD CS) and Active Directory® Lightweight Directory Services (AD LDS). In addition, you must know how to resolve Active Directory® Federation Services (AD FS) issues. You should also be able to solve Active Directory® Rights Management Solution (AD RMS) problems.

Lesson 1

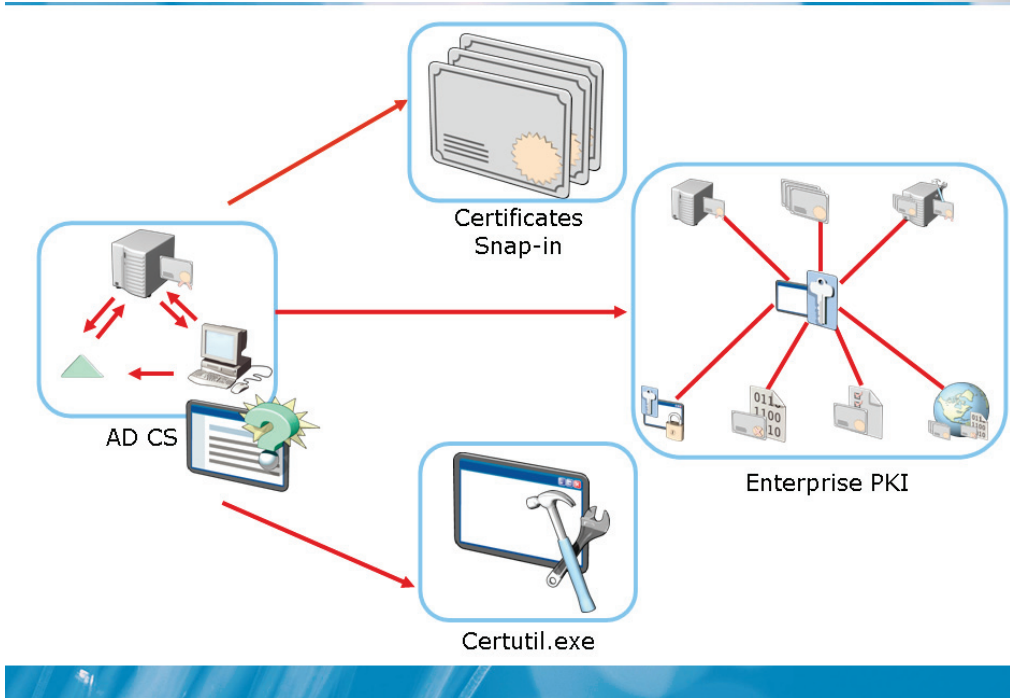
Troubleshooting AD CS

- Tools Used to Troubleshoot AD CS
- What Is Enterprise PKI?
- How To Use Enterprise PKI to Troubleshoot AD CS
- Common AD CS Issues
- Troubleshooting Web Enrollment Errors
- Troubleshooting Client Autoenrollment
- Troubleshooting Certificate Validation Errors

You can troubleshoot AD CS by using tools such as, Certificates snap-in, Enterprise PKI, Certification Authority snap-in, Certutil.exe, and Certificate Templates snap-in. You should know what is Enterprise Public Key Infrastructure (PKI). Further, you need to know how to troubleshoot AD CS by using Enterprise PKI. You should also be able to identify common AD CS issues. Further, to troubleshoot AD CS, you should be able to troubleshoot errors related to Web Enrollment, client Autoenrollment, and Certificate validation.

AD CS includes Certification Authorities (CAs), Online Responders, Network Device Enrollment Service (NDES), and related client services that support the issuance and management of digital x.509 certificates used in a variety of applications.

Tools Used to Troubleshoot AD CS



Key Points

The prime administrative tasks are to monitor and troubleshoot the error conditions of all CAs in a PKI.

A few of the tools that you can use to accomplish these tasks are listed here:

- **Certificates snap-in.** This snap-in is used to view and manage certificate stores for a computer, user, or service
- **Enterprise PKI.** This PKI is used to monitor multiple CAs, Certificate Revocation Lists (CRLs), and authority information access (AIA) locations, and manage AD CS objects that are published to AD DS.
- **Certification Authority snap-in.** This snap-in can be used to administer a CA, and revoke and enroll a certificate.

- **Certutil.exe.** This command line tool can be used to display CA configuration information, configure Certificate Services, back up and restore CA components, verify certificates, key pairs, and certificate chains.
- **Certificate Templates snap-in.** This snap-in is used to analyze and provide critical information to manage the certificate templates in a domain.



For more information, see **CA** help file.

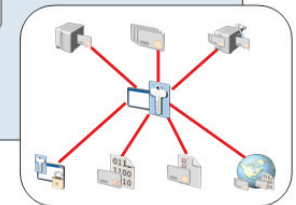
What Is Enterprise PKI?

Enterprise PKI:

- Indicates the validity and accessibility of authority information access (AIA) locations and certificate revocation list (CRL) distribution points

Reports various status levels such as:

- **OK.** The CA certificate or CRL at the referenced URL is valid.
- **Expiring.** The CA certificate or CRL at the referenced URL is close to the expiration date.
- **Expired.** The CA certificate or CRL at the referenced URL is expired.
- **Unable to download.** The CA certificate or CRL cannot be downloaded from the referenced URL.



Key Points

Enterprise PKI is a Microsoft Management Console (MMC) snap-in that is included in the Windows Server® 2008 operating system. Enterprise PKI was originally a part of the Microsoft Windows Server® 2003 Resource Kit and called the PKI Health tool. It provides a view of the status of the PKI environment. It also allows the viewing of multiple CAs and their current health state.

- Enterprise PKI can be used to check and manage:
- Multiple CAs
- CRLs
- AIA locations
- AD CS objects that are published to AD DS

You must use the following diagnostic and troubleshooting tools to address the listed issues:

- **Error on the server hosting CA.** When a warning or serious error is indicated on a server hosting a CA or Online Responder, you must look for additional information on that computer. You should examine the events logged in the Event Viewer on that computer to acquire additional information. This will help you to diagnose and rectify the problem.
- **CA-related issues.** When you face problems such as connecting to a current CRL, you must use the Certification Authority snap-in to rectify the problem.
- **Online Responder-related issues.** When you correct revocation configuration problems, you must use the Online Responder snap-in to perform tasks.
- **Expiry of CA certificates.** When Enterprise PKI indicates that one or more CA certificates are about to expire, you must use the Certificates snap-in to reissue or renew these certificates.



For more information, see Troubleshoot AD CS.

Demonstration: How To Use Enterprise PKI to Troubleshoot AD CS

- To view CA, AIA, CDP, and CRL status by using Enterprise PKI



Key Points

The instructor will provide a demonstration to show how you can use Enterprise PKI to troubleshoot AD CS.

Questions:

1. Can you use the Enterprise PKI snap-in to monitor multiple CAs?
2. Can you use the Enterprise PKI snap-in to resolve the issues?
3. List the information available in the Enterprise PKI snap-in.



For more information, see [Troubleshoot AD CS](#).

Common AD CS Issues

Common AD CS troubleshooting issues are:

Web enrollment errors



Client autoenrollment problems



Certificate validation errors



Key Points

The common AD CS issues you may encounter include the following:

- **Client autoenrollment issues.** This issue occurs when clients do not automatically enroll for certificates after autoenrollment is configured. It may be caused by Group Policy information, which is not replicated or wrongly configured.
- **Unavailable enterprise CA option.** This issue occurs when a user who is not a member of the Enterprise Admins or Domain Admins group installs CA, the CA might not be installed as an enterprise CA. In this case, the enterprise CA option is unavailable and information about the CA cannot be published to AD DS.
- **Error in access of CA Web pages.** This error occurs while accessing the CA Web pages. In this case, you should check to ensure that the user is a member of the Administrators or Power Users group on the client computer.

- **Enrollment agent restrictions.** This restriction occurs when an enrollment agent is not able to enroll on behalf of a user for a specific certificate template. This may occur because of the restrictions that may have been configured on the enrollment agent.
- **Certificate validation errors.** This error occurs when a new version 2 or version 3 certificate templates cannot be added to a CA. This happens when a CA is installed on a server that runs Windows Server® 2008 Standard.



For more information, see [Troubleshoot AD CS](#).

Troubleshooting Web Enrollment Errors

Problem	Solution
<p>Web pages on enterprise CAs don't generate certificates</p> <p>or</p> <p>Web pages on enterprise CAs generate invalid certificates</p>	<p>Web pages on an enterprise CA require user authentication. If the pages are set to allow anonymous connections, then the CA will either fail to generate certificates or will generate invalid certificates.</p>
<p>Web pages of Certificate Authority generate error during access</p>	<p>Log on as a user who is a member of the Administrators or Power Users group, to access the Web enrollment pages and download the latest version of the software. Check whether the Web pages have execute script permissions in IIS.</p>



Key Points

Certificate Services includes several CA Web pages that users can access to submit basic and advanced certificate requests. By default, these pages are located at <https://servername/certsrv>, where server name is the name of the server hosting the Web pages.

The following issues may be related to Web enrollment:

- You must set the appropriate permissions on the certificate templates based on the requested certificate.
- You must confirm that script execution permissions are activated on the %systemroot%/System32/Certsrv folder on the Web server to prevent errors that may arise when you access the certification authority for Web pages.
- You must modify the certificate enrollment Web site to require SSL for HTTPS transport, for Windows Vista®-based client computers or Windows Server®

2008-based client computers to use Windows Server® 2008 certificate enrollment Web pages.

- For Windows Vista®-based client computers or Windows Server® 2008-based client computers to use Windows Server® 2008 certificate enrollment Web pages, you must modify the certificate enrollment Web site to require Secure Socket Layer (SSL) for Secure Hypertext Transfer Protocol (HTTPS) transport.
- You must ensure that the user is a member of the Administrators or Power Users group on the local computer for client computers that are prior to Windows Server® 2008 and Windows Vista® to install the Xenroll ActiveX® control software.
- You must check if the users have added the Web site to the list of trusted sites in the Internet Explorer® to access the Web server for a CA for the first time.



For more information, see [Troubleshoot AD CS](#).

Troubleshooting Client Autoenrollment

Problem	Solution
<p>Clients do not enroll for certificates automatically after autoenrollment is configured.</p>	<ul style="list-style-type: none"> • Wait for Group Policy to complete replication. • Alternatively, use the Gpupdate command to force replication to occur. • Ensure that the user is a member of a group that has enroll permissions on the certificate template being used.



Key Points

AD CS can distribute some types of certificates without any manual interaction by the client or without the client knowing that enrollment is occurring. To enroll clients automatically for certificates in a domain environment, you need to configure a certificate template with Autoenroll permissions. You also need to define an autoenrollment group policy for a particular domain.

One of the most common issues that you may face while troubleshooting autoenrollment is client servers not being able to enroll automatically for certificates. This happens because the group policy information used for autoenrollment is not being replicated to the client computers. By default, Group policy information can take up to two hours to replicate to all computers. However, you can apply Group Policy immediately by using the Gpupdate command-line tool.

To configure autoenrollment permissions you need to ensure that the user is a member of a group having enrolled permissions on the certificate template that is being used. In case a computer is removed, the certificates that were autoenrolled from a previous forest will not be removed. However, in case the machine is a domain controller the certificates sent from the previous forest will be removed. You may need to delete old certificates once a machine joins a new domain or forest in case users have certificates that are required for secure network communications.

By default, autoenrollment logs errors, failures, and successful enrollments in the Application event log, on the client computer. To audit events, you need to configure the audit policy. You can view and manage audit policy options in the local or domain Group Policy under the following path:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy



For more information, see [Troubleshoot AD CS](#).

Troubleshooting Certificate Validation Errors

Problem	Solution
Validation errors occur when users access resources by using certificates.	Use Enterprise PKI to verify that the AIA and CDP locations and certificates are valid.



Key Points


All certificates have a validity period. After the validity period expires, the certificate is no longer considered as an acceptable credential. Client computers may not be able to connect to resources that require certificates, if any certificate validation problems occur. AD CS startup may stop if there are problems of availability, validity, and chain validation for the CA certificate.

As an IT administrator, you need to use Enterprise PKI to verify that the AIA and CRL distribution point (CDP) locations and certificates are valid. In addition, you need to use Certification Authority snap-in to install the new certificates.

Lesson 2

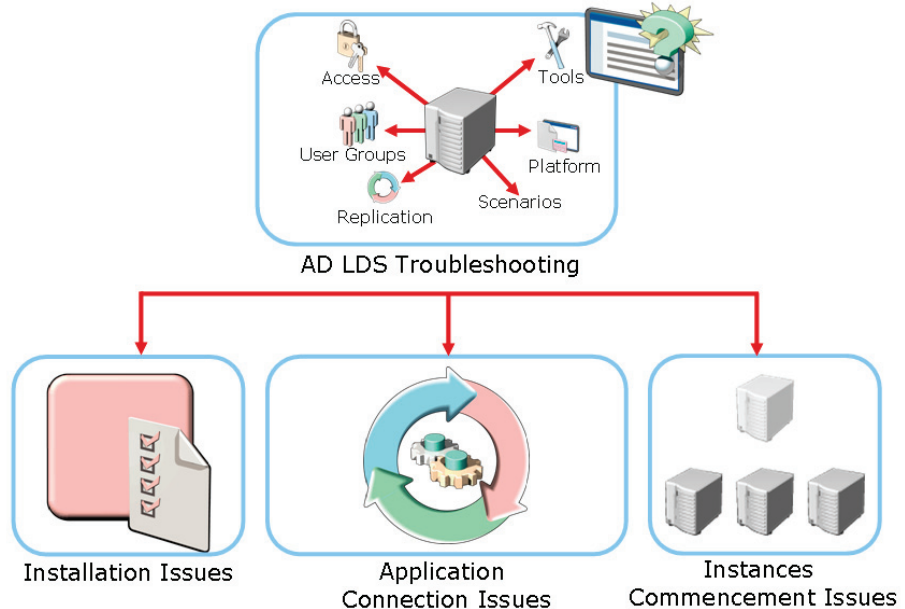
Troubleshooting AD LDS

- Common Issues of AD LDS
- Installation Issues of AD LDS Instances
- Application Connection Issues of AD LDS
- Initiating Issues of Instances



To troubleshoot IDA solutions must be able to troubleshoot AD LDS. To troubleshoot AD LDS you must be able to identify AD LDS common issues. You should be able to install AD LDS instances. You must be able to identify AD LDS application connection issues. Further, you must be must know how to initiate issues with instances.

Common Issues of AD LDS



Key Points

The most common AD LDS issues are communication failures, replication failures, and service startup failures.

The following issues describe common AD LDS failures:

- You must register configuration changes to an AD LDS instance in the internal database of that instance and the databases of any configured replication partners. If the local instance cannot receive any updates from its replication partners, you must replicate changes made to the local instance to its partners. Changes that require the update of replication partners include the host name modification, and changes to the network communication port, and the service account.
- You must ensure that the communication port numbers specified for the AD LDS instance is correct to avoid related connectivity problems.

- You must ensure that certificates are present on the server and clients to establish SSL connections.
- You must ensure that the credentials are valid and the service account has Run as a service permission to avoid logon failures of a service account. Because AD LDS instance startup failures may be related to logon failures of a service account.



For more information, see [ADAM troubleshooting and frequently asked questions \(FAQs\)](#).

Installation Issues of AD LDS Instances

Problem:

The installation or removal of an AD LDS instance fails to complete successfully.

Solution:

- If no screen message appears and setup fails to complete successfully, view the setup log at:
`%windir%\Debug\adamsetup.log`
- If no screen message appears and Instance removal fails to complete successfully, view the uninstall log at:
`%windir%\Debug\adamuninstall.log`



In some situations, the installation or removal of an AD LDS instance fails to complete successfully.

If an error occurs in the Active Directory® Application Mode (ADAM) setup wizard before completion of the ADAM Setup Wizard page, you should review the error message that describes the cause of the problem.

Situation	Location of the Error Message
Setup of AD LDS instance fails	log at %windir%\Debug\adamsetup.log
Removal of AD LDS fails	%windir%\Debug\adamuninstall.log

You will find information that can help you troubleshoot the cause of the AD LDS setup failure in these log files.

You will be prompted to restart the computer after removing AD LDS. Restart the computer to complete the future installations of AD LDS successfully.



For more information see, **ADAM troubleshooting and frequently asked questions (FAQs)**.

Application Connection Issues of AD LDS

Problem:

A directory-enabled application cannot find the AD LDS instance.

Solution:

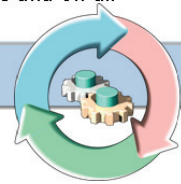
- Refer to the correct communication port number when specifying an AD LDS instance. The communication port number is 389 or 636.

Problem:

A user is not able to connect to an AD LDS instance.

Solution:

- Install certificates on the computer running the AD LDS instance and on all client computers, to enable SSL connections.



Key Points

Incorrect communication port numbers specified for the AD LDS instance always lead to connectivity problems. You should ensure that the same port is used by all AD LDS instances in the configuration set.

You need certificates on the server and clients to establish SSL connections.

To secure an SSL communication, you must ensure that the AD LDS server and all clients import the root CA certificate into the trusted root CAs store.

When you install or import a certificate from a trusted CA to the computer that runs AD LDS, you should store the certificate in the personal store of AD LDS service.

You need to run Ldp.exe and then connect to with an SSL option enabled on the computer that runs the AD LDS instance.



For more information see, **ADAM troubleshooting and frequently asked questions (FAQs)**.

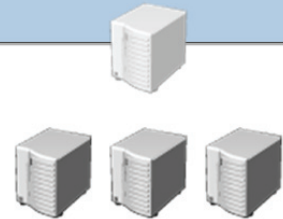
Initiating Issues of Instances

Problem:

An AD LDS instance will not start.

Solution:

- Ensure that the service is running. If the service account that is specified for ADAM is a workstation or a domain user account, make sure that the account possesses the Run as a service right.



Key Points

You may encounter the following issues when using the Certification Authority snap-in or CAs.

Issue	Cause
A client is not able to enroll automatically for certificates after autoenrollment is configured.	CA is configured inappropriately or not yet replicated Group Policy information
A CA could not be installed as an enterprise CA.	User is not a member of the Enterprise Admins or Domain Admins group who installs a CA on the client computer.

Issue	Cause
An error message appears when a client accesses the CA Web pages.	User is not a member of the Administrators or Power Users group on the client computer.
An enrollment agent cannot enroll on behalf of a user for a specific certificate template.	Restrictions on the enrollment agent are configured.
New version 2 or version 3 certificate templates cannot be added to a CA.	CA is installed on a server that runs Windows Server® 2008 Standard.



For more information, see [Troubleshoot AD CS](#).

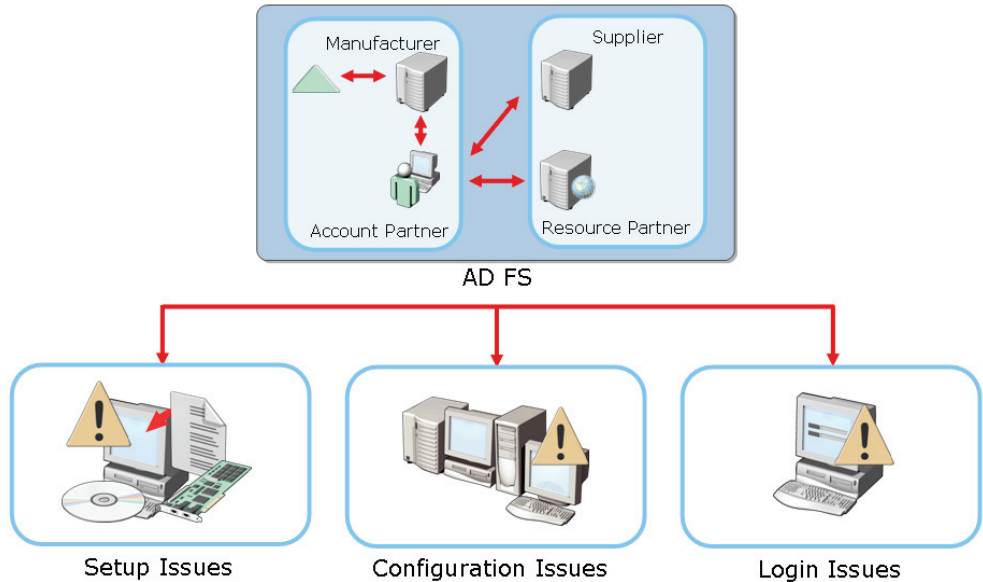
Lesson 3

Resolving AD FS Issues

- Common Issues of AD FS
- Setup Issues of AD FS
- Configuration Issues of AD FS
- Enabling Debug Logging with AD FS

To troubleshoot IDA solution, you must be able to resolve AD FS issues. To troubleshoot AD FS issues, you must be able to identify common AD FS issues. Further, you must also know AD FS setup issues. To solve AD FS problems, you must be able to identify AD FS configuration issues. You also require enabling of AD FS debug log.

Common Issues of AD FS



Key Points

When you troubleshoot an AD FS issue, it is important to trace the point of failure within the AD FS system.

You need to troubleshoot the following common types of AD FS issues:

- **Setup issues.** These issues include errors related to the Internet Explorer®, or incorrect configuration of virtual directory.
- **Configuration issues.** These issues include certificate problems and return Uniform Resource Locators (URLs) in the application Web.config file that are incorrectly configured. These return URLs must match the application URL specified in the trust policy. In addition, configuration issues can also include server errors and validation errors.
- **Logging issues.** These issues are related to logging inactivated or incorrect logging.

- **Connectivity issues.** These issues include connectivity problem from the AD FS client to the Web site on the AD FS Web server. You can troubleshoot this issue by verifying the connection.

Setup Issues of AD FS

Problem	Solution
I receive an Internet Explorer® error page with the message "This page cannot be displayed," "Cannot find server," or "DNS Error."	<ul style="list-style-type: none"> Verify that all federation servers and AD FS-enabled Web servers have a server authentication certificate issued to the default Web site.
When I try to connect to the application, I get an Internet Explorer® error page with the message "This page cannot be found" or "HTTP Error 404 – File or directory not found."	<ul style="list-style-type: none"> Verify that the correct Federation Service host name was used during installation, if there is an external account partner Federation Service Proxy involved. Verify that the Federation Service URL in the IIS Manager snap-in (is configured correctly, if you are using a Windows NT® token-based application. Verify that the Web application is properly configured in IIS. Verify that the Web application URL is properly named in the Active Directory® Federation Services snap-in.
After setting up a Windows NT® token-based application, I attempt to connect to it but I am not prompted to choose a host realm and login credentials.	<ul style="list-style-type: none"> Verify that Microsoft® ASP.NET is installed on the AD FS-enabled Web server and in the Federation Service. Verify that the virtual directory of the Windows NT® token-based application is set up to use the Ifsext.dll Internet Server Application Programming Interface (ISAPI) extension.



Key Points

Certificates often cause an AD FS setup to fail. For example, clients might be prompted about certificates that cannot be trusted. To avoid errors about untrusted certificates, you need to configure the clients to trust the root authority of the certificate. In addition, error messages that indicate Domain Name System (DNS) or server errors might also appear.

The following table describes the error messages that occur during AD FS setup.

Error message	Conditions
<p>Consider the following error messages in Internet Explorer®:</p> <ul style="list-style-type: none"> This page cannot be displayed. Cannot find server DNS Error 	<p>These error messages occur when:</p> <ul style="list-style-type: none"> Federation servers do not have a server authentication certificate issued for the default Web site. AD FS-enabled Web servers do not have a server authentication certificate issued

Error message	Conditions
	<p>for the Web site that contains the application.</p> <ul style="list-style-type: none"> • You specify an incorrect Federation Service host name during the AD FS installation. • You incorrectly configure the Federation Service URL in the Internet Information Services (IIS) Manager snap-in for a Windows NT® token-based application.
<p>Consider the following error messages in Internet Explorer®:</p> <ul style="list-style-type: none"> • This page cannot be found. • HTTP Error 404 – File or directory not found 	<p>These error messages occur when:</p> <ul style="list-style-type: none"> • You incorrectly configure the Web application in IIS. • You incorrectly name the Web application URL in the AD FS snap-in. • You do not install Microsoft ASP.NET on the AD FS-enabled Web server and in the Federation Service.

For a Windows NT® token-based application that uses ASP, a 404 error might occur after you provide the required credentials. To resolve this error, you must verify that the ASPClassic handler in IIS is enabled and configured to handle *.asp pages. Further, you must ensure that you installed the ASP feature for IIS.

Configuration Issues of AD FS

Problem	Solution
I am receiving a server error	<ul style="list-style-type: none"> Ensure that the application has been added to the trust policy for the Federation Service.
Web pages on an enterprise CAs generate invalid certificates	<ul style="list-style-type: none"> Verify that the return URL is typed correctly in the application's Web.config file and that it matches the application URL that is specified in the trust policy of the Federation Service for a claims-aware application. Verify that the return URL is typed correctly in IIS and that it matches the application URL in the trust policy of the Federation Service For a Windows NT® token-based application.



Key Points










When you configure AD FS for an organization, server or validation error messages might appear. The following table describes the error messages that appear.

Error message	Conditions
The token request for the application with URL https://... cannot be fulfilled because the Uniform Resource Locator (URL) does not identify any known trusting application.	This server error message appears when the application URL cannot identify a known application. To resolve this error, you need to ensure that you add the application to the trust policy for the Federation Service.
Validation of view state media access control (MAC) failed. If this application is hosted by a Web farm or cluster, ensure that <machineKey> configuration	This validation error message appears when an unhandled exception occurs when you run a Web request. You should review the stack trace for more

Error message	Conditions
specifies the same validation key and validation algorithm.	information about the error and its origin in the code.

Further, you might configure an AD FS Windows NT® token-based application. This application might be authenticating as an anonymous user due to a mapping of an account to an AD user or group.

Enabling Debug Logging with AD FS

Issue	Description
 Error	Records events for significant problems to the debug log
 Warning	Records events, which are not necessarily significant but that may cause future problems, to the debug log
 Informational	Records informational events to the debug log
 Verbose	Records detailed information about events to the debug log
 Audit success	Records a security audit for every successful user authentication or trust policy change that is made to this Federation Service
 Audit failure	Records a security audit for every unsuccessful attempt to change the trust policy for this Federation Service
 Event log entries	Records all Active Directory® Federation Services (AD FS) events to the debug log
 Cookie	Records cookies to the debug log
 Log files directory	Provides a space to type or browse to the location of the log file



Key Points

You need to configure the AD FS system for troubleshooting before you can identify and solve AD FS problems. You can activate debug logging and then set levels so that the logs provide detailed feedback.

There are various types of issues to identify and record in the debug log, when you set debug levels. These issues include error, warning, informational, verbose, audit success, audit failure, event log entries, cookie, and log files directory.

In addition, you can view event logs that contain information for identifying problems. Event logging is available for both Windows NT® token-based applications and claims-aware applications.



For more information, see [ADFS Product Support Blog](#).

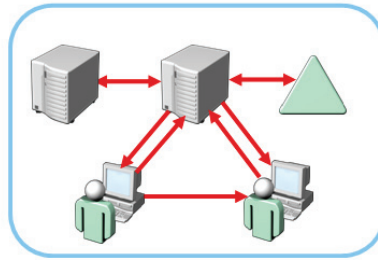
Lesson 4

Solving AD RMS Problems

- Common Issues of AD RMS
- Troubleshooting AD RMS Cluster Installation
- Troubleshooting AD RMS Cluster URL Availability
- Troubleshooting Service Connection Point Registration

While troubleshooting AD FS, you must be able to resolve AD RMS issues. You must also be able to troubleshoot the AD RMS cluster installation and URL availability. Further, you must also be able to identify how to troubleshoot service connection point (SCP).

Common Issues of AD RMS



AD RMS

Common issues related to AD RMS include:

- Cluster installation
- Cluster URL availability
- SCP configuration
- Federation Identity support installation

Key Points

You can use the troubleshooting reports in the AD RMS console to identify common AD RMS issues. To view these reports, you must install and use Microsoft Report Viewer.

Some AD RMS issues are related to:

- AD RMS installation
- Cluster URL configuration
- Federated Identity Support installation
- SCP registration in AD DS

In addition, operational issues can occur if the AD RMS service account password expires. AD RMS stops if the password expires.



For more information, see **AD RMS Web Services**.

Troubleshooting AD RMS Cluster Installation



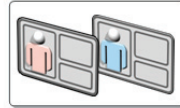
Verify that the user installing AD RMS is a member of the local administrators group.



Verify that the AD RMS administrator account has read, write, and delete access to the `_wcms` virtual directory in IIS.



Grant access to the AD RMS administrator account on the configuration database server.



Ensure that the AD RMS service account and the account used to install AD RMS are different.



Add the AD RMS service account to the Domain Administrator security group if installing the AD RMS cluster on a domain controller.

Key Points

You can use the Server Manager to install the AD RMS server role. However, the AD RMS installation might not be successful. Some of the causes for a failed AD RMS installation and their solution are as follows:

- **The AD RMS administrator account is not a member of the Administrators group.** Ensure that the user account you use to install AD RMS is a member of the local Administrators group on the AD RMS server.
- **AD RMS cluster versions do not match.** Ensure that the version installed on the server matches the AD RMS cluster version, and then reinstall the AD RMS server role when you join a server to an AD RMS cluster.

- **The public key in the server licenser CRL is not valid.** Ensure that the public key in the revocation list file of the server licenser certificate is valid, and then reinstall AD RMS.
- **ASP .NET or Web Server (IIS) role components cannot be installed.** Ensure that the requirements to install the required ASP .NET or Web Server (IIS) role components are met.
- **The service accounts do not match.** Ensure that the service account entered during the installation of AD RMS server role is the same as the service account used by the AD RMS cluster.
- **The configuration database is not installed.** Ensure that the AD RMS configuration database is available on the network. Ensure that the user account that you use to install AD RMS has permissions to create databases on the database server.
- **AD RMS server cannot be added to the cluster.** Ensure that the cluster type stored in the AD RMS configuration database is valid, and then reinstall the AD RMS role. A cluster must be either a certification cluster or a licensing cluster to be valid. The cluster type is stored in a configuration database created during the installation of AD RMS.

In addition, the following reasons might prevent an upgrade to AD RMS from a previous version of RMS:

- The RMS logging service does not exist.
- The AD RMS upgrade wizard cannot locate or modify the RMS web.config file.
- The AD RMS upgrade wizard cannot locate the RMS virtual directories.
- The RMS is installed on the computer but not provisioned.



For more information, see AD RMS Web Services.

Troubleshooting AD RMS Cluster URL Availability



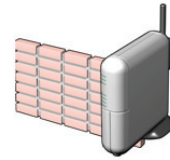
Cluster URL does not respond to HTTP(S) requests



Verify that DNS is configured and working correctly.



Ensure that all SSL certificates are valid and properly installed on all servers and clients.



Create AD RMS port exceptions such as TCP port 80 and TCP port 433 for Windows® Firewall.

Key Points

If the cluster URL that you specify in the AD RMS installation does not respond to an HTTP request, you must ensure that the AD RMS cluster is available on the network.

AD RMS uses Transmission Control Protocol (TCP) ports 80 and 443 to communicate with AD RMS-enabled clients and AD RMS servers in the cluster.

In addition, the firewall restricts these ports, and then AD RMS cannot communicate with these ports. The AD RMS cluster is then not available on the network. So, you might need to create AD RMS port exceptions for Windows Firewall. Further, you must ensure that you provide correct URL for the cluster.



For more information, see [AD RMS Web Services](#).

Troubleshooting Service Connection Point Registration

Failure to register the Service Connection Point.



Solution:

- Make sure to ensure that the user registering the service connection point (SCP) is a member of the AD RMS Enterprise Administrators and the Enterprise Admins security groups.
- Delete any existing SCP and create a new one.
- Verify that DNS is configured and working correctly.

Key Points

AD RMS clients use a SCP to automatically locate the AD RMS cluster.

If the AD RMS installation fails to register the SCP in AD DS, use the AD RMS console to register the SCP after the installation. When you configure an SCP, you must use an account that is a member of the Enterprise Admins group or has equivalent privileges.



For more information, see [AD RMS Service Connection Point Registration](#).

Lab 8: Troubleshooting Identity and Access Solutions

- Exercise 1: Identifying Tools and Troubleshooting Techniques of IDA Solutions

Estimated time: 20 minutes

Objectives

After completing the lab, you will be able to:

- Identify built-in IDA solutions tools
- Describe the troubleshooting steps to identify the possible causes

Scenario

Woodgrove Bank is a large multinational corporation having office locations around the world. The company has recently implemented Windows Server® 2008 and an Active Directory® Domain Services (AD DS) environment.

The organization has also deployed various identity and access (IDA) technologies, including Active Directory® Lightweight Directory Services (AD LDS), Active

Directory® Certificate Services (AD CS), Active Directory® Rights Management Services (AD RMS), and Active Directory® Federation Services (AD FS) to support their growing user population.

Consolidation Requirements:

As an enterprise administrator, you are responsible for maintaining and troubleshooting the environment. There are many built-in Windows Server® 2008 tools and utilities that will help you accomplish the task.

Several support cases registered by the Helpdesk personnel have been assigned to your team and lined up in queue. You need to investigate the possible causes of these issues, and identify the required tools to resolve them.

The cases assigned to your team include the following:

- You have recently deployed a Root Certificate Authority (AD CS) into your environment by using default installation options. One of the support teams has complained that they cannot request Web certificates from the Certificate Authority (CA) Web site.
- You have also deployed an AD RMS system just a month ago and users have been extremely satisfied with its performance and features. Users are now complaining that they cannot protect the content from an unauthorized access with the AD RMS solution.
- One of the corporate applications that required custom identity features was recently deployed along with AD LDS. You have been told that users are experiencing issues in connecting the AD LDS instance. The problem had crept in after a network upgrade project was implemented.
- Your organization has recently acquired another bank. AD FS Federated Web (Single Sign-On) SSO design was implemented in your bank to provide support to a claims-aware application. Users are complaining that they receive several error messages such as “The page cannot be displayed” and “Cannot find server” while connecting to the application by using Internet Explorer®.

Exercise 1: Identifying Tools and Troubleshooting Techniques of IDA Solutions

In this exercise, you will identify the tools and troubleshooting techniques of IDA solutions.

The main tasks for this exercise are as follows:

1. Identify built-in IDA Solutions tools.
2. Describe the troubleshooting steps to identify the possible causes for various issues.

► Task 1: To identify built-in IDA solutions tools

Question: Identify some of the Windows Server® 2008 built-in tools that can be used to troubleshoot each support case identified in the scenario.

► Task 2: To describe the troubleshooting steps to identify the possible causes

Question: Based on the scenario, and using the built-in tools available, describe the troubleshooting steps to be performed to identify the cause for each issue.

Lab Review: Troubleshooting Identity and Access Solutions

In this lab, you have:

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

Lab Resources

There are no additional lab resources for this lab.

6426A Evaluation

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

Please work with your training provider to access the course evaluation form.

Microsoft will keep your answers to this survey private and confidential and will use your responses to improve your future learning experience. Your open and honest feedback is valuable and appreciated.

MCT USE ONLY. STUDENT USE PROHIBITED