Course 50403B:

# Implementing Active Directory Rights Management Services with Exchange and SharePoint

**Course Details**

Course Outline

Module 1: Why Rights Management?

This module provides an overview of Microsoft Active Directory Rights Management Services (AD RMS). The overview describes how the product works, the business reasons for using AD RMS, and the technology that you use to deploy an AD RMS environment.

Lessons

- A Bit of History
- Business Reasons for AD RMS
- What AD RMS Does
- AD RMS Usage Scenarios
- AD RMS Technology Overview
- AD RMS in Windows Server 2008 R2 and Windows 7

Lab : AD RMS Demonstration

- User experience protecting Microsoft Office–based documents.

After completing this module, students will be able to:

- Understand how RMS technology has evolved on the Windows platform.
- Explain the business reasons for using AD RMS.
- Explain the features AD RMS provides.
- Identify the advantages and limitations inherent in AD RMS.
- Describe how AD RMS works with public key technology.
- Describe how AD RMS works.
- Describe the new AD RMS features in Windows Server 2008 and Windows Vista.

Module 2: AD RMS Architecture

This module covers the basic architecture and concepts of the Microsoft Active Directory Rights Management Services product. Most of the concepts that are introduced in this module will be covered in more detail in other modules later in the course.

Lessons

- AD RMS Components Overview
- AD RMS Bootstrapping Process
- AD RMS Publishing and Licensing Process
- AD RMS Service Connection Point (SCP)
- AD RMS Topology
- AD RMS Components Details

After completing this module, students will be able to:

- Describe Public Key Infrastructure (PKI) technology.
- Explain how AD RMS can be used to address challenges inherent in PKI.
- Describe how AD RMS works.
- Identify the major components of AD RMS.
- Describe the types of licenses used in the AD RMS process.
- Describe the client-side software and applications required for AD RMS.
- Identify the AD RMS enhancements in Windows Server 2008 and Windows 7.

### Module 3: AD RMS Installation and Provisioning

In this module, the student will learn about network infrastructure, hardware, and software requirements for installing AD RMS. The student will learn the procedure for deploying AD RMS servers, as well as the permissions required for the accounts that are used in the deployment and management of AD RMS.

Lessons

- AD RMS Requirements
- AD RMS Prerequisites
- Installing and Provisioning AD RMS
- AD RMS Server Installation Best Practices
- Migrating RMS to AD RMS

Lab : Creating the AD RMS Service Account

- Create an AD RMS Service Account

Lab : Installing and Provisioning AD RMS

- Install and provision AD RMS

After completing this module, students will be able to:

- Identify the AD RMS server hardware and software requirements.
- Install a database server.
- Identify best practices for installing an AD RMS server.
- Install and provision an AD RMS server.
- Configure the AD RMS service connection point.
- Migrate RMS to AD RMS.

### Module 4: Information Rights Management on Desktop Applications

This module begins by describing the AD RMS client software, its requirements, and how to deploy it. Next, the module identifies the Information Rights Management (IRM) components on client machines and the bootstrapping process the AD RMS client performs for each user. The module then discusses how IRM is provided in Microsoft Office products, the XPS format, Window Mobile 6.0, and read-only access in Windows Internet Explorer. The module ends with a discussion of how registry keys interact with AD RMS.

#### Lessons

- Operating System Versions and AD RMS Clients
- Microsoft Office IRM
- XPS IRM
- Windows Mobile 6.0 IRM
- RM Add-on for Internet Explorer and Rights-Managed HTML (RMH)
- Office Viewers and AD RMS
- IRM Client Registry Settings

#### Lab : Protecting and Consuming AD RMS Protected Documents

- Protect and Consume AD RMS Protected Documents

#### Lab : Creating and Consuming AD RMS Content Using Microsoft Outlook 2007

- Create and Consume AD RMS Content Using Microsoft Outlook 2007

#### Lab : Protecting and Consuming Content Using XPS

- Protect and Consume Content Using XPS

#### Lab : Consuming Content Using the Rights Management Add-on for Internet Explorer

- Consume Content Using the Rights Management Add-on for Internet Explorer

### Lab : Using Active Directory Security Groups

- Using Active Directory Security Groups

After completing this module, students will be able to:

- Describe the AD RMS client software and its requirements.
- Deploy the Windows RMS client software in legacy clients.
- Identify the AD RMS components that are installed on client machines.
- Explain the AD RMS client bootstrapping process.
- Explain how IRM works in Microsoft Office products.
- Describe how the XPS format uses IRM and how XPS can be used in conjunction with Microsoft Office applications.
- Explain how the Rights Management Add-on for Internet Explorer enables users to view restricted files.
- Describe how to set registry keys that are related to AD RMS.

## Module 5: Rights Policy Templates

This module provides an introduction to rights policy templates and the concepts related to protecting and consuming content that is protected by templates. These templates are used to standardize security policies and protect information according to the latest policy.

### Lessons

- Introduction to Rights Policy Templates
- Creating Rights Policy Templates
- Protecting Content Using Templates
- Consuming Content Protected by Templates
- Managing Rights Policy Templates
- Template Distribution Strategy

### Lab : Creating and Using a Rights Policy Template

- Create and Use a Rights Policy Template

### Lab : Modifying Existing Templates

- Modify Existing Templates

### Lab : Distribute a Rights Policy Template

- Distribute a Rights Policy Template

After completing this module, students will be able to:

- Describe the features offered in rights policy templates.
- Identify template distribution features in AD RMS.
- Describe the processes for protecting and consuming content protected by rights policy templates.
- Define rights policy templates.
- Assign users and groups to rights policy templates.
- Specify expiration policies in rights policy templates.
- Explain how to retire and back up rights policy templates.

### Module 6: Information Rights Management on Server Applications

In this module, students will see how AD RMS integrates with server-side applications, which use AD RMS to automatically protect and license content. This module covers the following server products:
- Microsoft Office SharePoint Server (MOSS) 2007
- Microsoft Exchange Server 2010
- AD RMS Bulk Protection Tool + FCI

#### Lessons

- Microsoft Office SharePoint Server 2007 IRM
- Email Protection in Exchange Server
- New AD RMS Features in Exchange Server 2010

#### Lab : Integrating AD RMS and Microsoft SharePoint Server 2007

- Enabling MOSS IRM
- Configuring MOSS IRM on Document Libraries
- Consuming Content using MOSS IRM

#### Lab : Integrating AD RMS and Exchange Server 2010

- Using OWA without Microsoft Exchange IRM integration
- Configuring Microsoft Exchange Server 2010 and AD RMS integration
- Implementing and validating Microsoft Exchange Server 2010 and AD RMS integration

#### Lab : Integrating AD RMS with Bulk Protection Tool

- Use Bulk Protection Tool to decrypt protected content
- Use Bulk Protection Tool to Protect content using AD RMS Templates

#### Lab : Protect information Automatically Integrating AD RMS with FCI and Bulk Protection Tool

- Setup environment for FCI and AD RMS bulk protection
- Create classification property and rules for Contoso documents
- Create file management tasks to restrict access to low and high business impact information
- Verify FCI and AD RMS bulk protection functionality

After completing this module, students will be able to:

- MOSS IRM
- Describe how MOSS works with AD RMS to protect documents stored in MOSS document libraries.
- Identify MOSS functionality.
- Describe MOSS's logical and physical architecture.
- Describe how IRM works with MOSS to provide information protection.
- Exchange Server 2010
- Explain the new features provided in Exchange Server2010 around AD RMS.
- AD RMS Bulk Protection Tool + FCI
- Describe how AD RMS Bulk Protection Tool can be used.
- Describe how FCI can be used.

### Module 7: Administering AD RMS

This module introduces some of the elements of the AD RMS Management Console. It discusses exclusion policies that can be defined by an administrator, provides an overview of revocation, and discusses the Super Users group and how it can be used to recover content. The module also introduces the new AD RMS reporting capabilities.

#### Lessons

- The AD RMS Administration Console
- New AD RMS Administration Roles
- Rights Account Certificate Policies
- Exclusion Policies
- Revocation
- The Super Users Group

#### Lab : AD RMS Role Separation

- Review the AD RMS Role Separation Security Options

#### Lab : Configuring Exclusion Policies

- Excluding Internal User Accounts

### Lab : Configuring the Super Users Group

- Create AD RMS-protected content by using Microsoft Office Excel 2007
- Enabling and Testing the Super Users Group

### Lab : AD RMS Reports

- Review the AD RMS Reports options

### Lab : GPO/Registry Override Settings

- Configure GPO and Registry Override Settings

After completing this module, students will be able to:

- Explain the advantages of the administrative console.
- Describe the new administrative roles in AD RMS.
- Describe the types of trust offered in AD RMS.
- Describe the types of exclusion policies provided in AD RMS.
- Explain how revocation is used in AD RMS.
- Describe the Super Users group and its characteristics.
- Describe the reports provided in AD RMS

## Module 8: Managing Trust

This module discusses the trust architecture in AD RMS, the types of trusts that are available, and how trusted user domains operate.

### Lessons

- Introduction to Trust Policies
- Trusted User Domains
- Trusted Publishing Domains
- AD RMS and Active Directory Federation Services
- Windows Live ID Trust
- Trust Scenarios
- General Infrastructure Requirements and Product Capabilities

### Lab : Configuring Trusted User Domains

- Export and import the TUD certificate
- Verifying AD RMS Functionality

### Lab : Configuring a Trusted Publishing Domain

- Remove the TUD Trust Relationship with Adatum
- Bootstrap and Protecting Information Before the Merge
- Exporting and Importing the Private Key from the Trusted Publishing Domain
- Verifying the Functionality of a Trusted Publishing Domain

### Lab : Configuring AD FS Trust and user experience

- Reset Existing AD RMS Trust
- Configure AD RMS Support for AD FS
- Adding SPN entries
- Configure AD RMS Applications for Federation
- Configure the AD FS Client
- Verify AD RMS and Federation Functionality

After completing this module, students will be able to:

- Describe the core trust architecture in AD RMS.
- Describe Trusted User Domains and how they work.
- Explain when Trusted Publishing Domains are used and how they work.
- Describe the Active Directory Federation Service and how it works with AD RMS.
- Describe Windows Live ID and how it works.

## Module 9: Extranet Considerations

This module discusses the extranet and how you can use it with AD RMS to provide access to protected content. The module provides reasons for establishing extranet access to AD RMS, and offers examples and scenarios. The module also discusses the use of a firewall, like Microsoft Internet Security and Acceleration Server (ISA Server), to address security with AD RMS.

### Lessons

- Extranet Access to AD RMS
- Extranet Access to AD RMS Pipelines
- Extranet Client Considerations
- AD RMS and Firewall Options
- Extranet Scenarios

### Lab : Configure AD RMS Pipelines

- Configure AD RMS Pipelines

### Lab : Configure Forefront TMG to Publish AD RMS

- Configure Forefront TMG to Publish AD RMS

### Lab : Verify the AD RMS functionality from an Internet Client

- Verify the AD RMS Functionality from an Internet Client

### Lab : OWA Consumption

- OWA Consumption

After completing this module, students will be able to:

- Explain why an organization might need to establish extranet access to AD RMS.
- Identify extranet-specific details to consider when you are establishing AD RMS access.
- Describe scenarios in which extranet access to AD RMS would be useful.
- Explain how a firewall works when you are using AD RMS in a perimeter network instead of an intranet.
- Explain how to use TMG to increase security when publishing AD RMS.

## Module 10: Deploying and Maintaining AD RMS Infrastructure

This module covers some of the key concepts to deploy and maintain the AD RMS service. Keep in mind that after key documents are protected, AD RMS becomes a very critical service in the organization.

### Lessons

- AD RMS General Performance Guidelines
- Adding a Server to a Cluster
- Managing Clusters
- AD RMS Disaster Recovery

### Lab : Installing AD RMS Root Certification cluster additional nodes

- Installing Network Load Balancing
- Configuring the AD RMS cluster for High Availability
- Checking the service functionality – tasks
- Decommissioning an AD RMS infrastructure

After completing this module, students will be able to:

- Understand AD RMS General Performance Guidelines
- Add a server to a cluster
- Manage clusters

- Understand AD RMS Disaster Recovery Strategies

### Module 11: Troubleshooting AD RMS

This module focuses on common issues in AD RMS and the tools available to help troubleshoot them. We examine in detail each of the common AD RMS support issues and the steps you can take to troubleshoot them. At the end of the module, we provide a list of additional resources for troubleshooting issues in AD RMS.

Lessons

- Troubleshooting Core Infrastructure
- Troubleshooting Product Installation
- Troubleshooting Product Usage
- Diagnostic Tools
- Additional Tools

After completing this module, students will be able to:

- Identify the main groups of tools available for troubleshooting AD RMS.
- Enable tracing on the AD RMS server and client.
- Explain how to access and use DebugView to monitor debugging output.
- Identify the types of reports that can be generated in AD RMS.
- Identify the most common issues in AD RMS and how to address them.
- Identify some of the resources available for additional troubleshooting information.