

## **MOC 50403 B Implementing Active Directory Rights Management Services with Exchange and SharePoint**

### **Course Summary**

#### **Description**

This four-day instructor-led course provides students with the knowledge and skills to deploy Microsoft Active Directory Rights Management Services (AD RMS), and to understand the role AD RMS plays in a wider infrastructure and how it interacts with other Microsoft technologies.

#### **Objectives**

**At the end of this course, students will be able to:**

- Understand AD RMS architecture, and the role the product plays as part of a wider infrastructure.
- Understand the AD RMS interaction model with other Microsoft technologies.
- Install and provision AD RMS and understand installation pre requisites and best practices.
- Understand how several other Microsoft technologies use AD RMS to protect documents and email messages.
- Understand how to use AD RMS on server applications such as Microsoft Office SharePoint Server and Microsoft Exchange Server.
- Create, manage, and distribute rights policy templates as AD RMS administrators.
- Understand the different trust relationships that can extend AD RMS protection beyond your infrastructure.
- Troubleshoot common issues in the core infrastructure, product installation, and product usage.

#### **Topics**

- Why Rights Management?
- AD RMS Architecture
- AD RMS Installation and Provisioning
- Information Rights Management on Desktop Applications
- Rights Policy Templates
- Information Rights Management on Server Applications
- Administering AD RMS
- Managing Trust
- Extranet Considerations
- Deploying and Maintaining AD RMS Infrastructure
- Troubleshooting AD RMS

#### **Audience**

This course is intended for experienced systems administrators who have working experience and background knowledge of Windows Server 2008, and basic understanding of Active Directory, IIS, Microsoft SQL Server, and Microsoft Exchange Server technologies. Basic knowledge of DNS, general networking, and PKI principles is also helpful.

#### **Prerequisites**

Before attending this course, students must have:

- Working experience and background knowledge of Windows Server 2008.
- Basic understanding of Active Directory, IIS, Microsoft SQL Server, and Microsoft Exchange Server technologies.
- Basic knowledge of DNS, general networking, and PKI principles is also suggested.

#### **Duration**

Four days



## **MOC 50403 B Implementing Active Directory Rights Management Services with Exchange and SharePoint**

### **Course Outline**

#### **I. 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

- A. A Bit of History
- B. Business Reasons for AD RMS
- C. What AD RMS Does
- D. AD RMS Usage Scenarios
- E. AD RMS Technology Overview
- F. AD RMS in Windows Server 2008 R2 and Windows 7

Lab: AD RMS Demonstration

- User experience protecting Microsoft Office–based documents.

#### **II. 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

- A. AD RMS Components Overview
- B. AD RMS Bootstrapping Process
- C. AD RMS Publishing and Licensing Process
- D. AD RMS Service Connection Point (SCP)
- E. AD RMS Topology
- F. AD RMS Components Details

#### **III. 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.

- A. AD RMS Requirements
- B. AD RMS Prerequisites
- C. Installing and Provisioning AD RMS
- D. AD RMS Server Installation Best Practices
- E. 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

#### **IV. 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, Windows 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.

- A. Operating System Versions and AD RMS Clients
- B. Microsoft Office IRM
- C. XPS IRM
- D. Windows Mobile 6.0 IRM
- E. RM Add-on for Internet Explorer and Rights-Managed HTML (RMH)
- F. Office Viewers and AD RMS
- G. 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

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically



## **MOC 50403 B Implementing Active Directory Rights Management Services with Exchange and SharePoint**

### **Course Outline (cont'd)**

#### **V. 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.

- A. Introduction to Rights Policy Templates
- B. Creating Rights Policy Templates
- C. Protecting Content Using Templates
- D. Consuming Content Protected by Templates
- E. Managing Rights Policy Templates
- F. 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

#### **VI. 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

- A. Microsoft Office SharePoint Server 2007 IRM
- B. Email Protection in Exchange Server
- C. 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

#### **VII. 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.

- A. The AD RMS Administration Console
- B. New AD RMS Administration Roles
- C. Rights Account Certificate Policies
- D. Exclusion Policies
- E. Revocation
- F. 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

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically



## **MOC 50403 B Implementing Active Directory Rights Management Services with Exchange and SharePoint**

### **Course Outline (cont'd)**

- 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

#### **VIII. Managing Trust**

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

- A. Introduction to Trust Policies
- B. Trusted User Domains
- C. Trusted Publishing Domains
- D. AD RMS and Active Directory Federation Services
- E. Windows Live ID Trust
- F. Trust Scenarios
- G. 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 Datum
- 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

#### **IX. 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

- A. Extranet Access to AD RMS
- B. Extranet Access to AD RMS Pipelines
- C. Extranet Client Considerations
- D. AD RMS and Firewall Options
- E. 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

#### **X. 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.

- A. AD RMS General Performance Guidelines
- B. Adding a Server to a Cluster
- C. Managing Clusters
- D. 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

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

*"Charting the Course ...*



*... to Your Success!"*

## **MOC 50403 B Implementing Active Directory Rights Management Services with Exchange and SharePoint**

### **Course Outline (cont'd)**

#### **XI. 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.

- A. Troubleshooting Core Infrastructure
- B. Troubleshooting Product Installation
- C. Troubleshooting Product Usage
- D. Diagnostic Tools
- E. Additional Tools

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

PT8941\_MOC50403BIMPLEMENTINGACTIVEDIRECTORY.DOC