

MOC 50382 B Implementing Forefront Identity Manager 2010

Course Summary

Description

This course introduces and explains the features and capabilities of Microsoft Forefront Identity Manager 2010 (FIM), and provides an overview of the solution scenarios that FIM addresses. The course format includes presentation, discussion, demonstration, and many hands-on exercises. It is intended for students who have no previous Forefront Identity Manager 2010 or Microsoft Identity Lifecycle Manager 2007 (ILM) experience.

Objectives

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

- Understand FIM concepts and components.
- Identify appropriate FIM scenarios.
- Manage users, groups, and passwords using FIM.
- Synchronize identity data across systems, such as Active Directory and HR.
- Understand the issues involved in loading data (initial load, backup, and disaster recovery).
- Configure security for different levels of user.
- Manage password self-service reset and synchronization.
- Automate run cycles.
- Handle sets, simple workflows, and management policy rules (MPRs).

Topics

- Introducing Forefront Identity Manager 2010
- The Synchronization Service Manager
- More about Synchronization
- The FIM Service and Portal
- Managing Synchronization from the Portal
- Managing Credentials with FIM
- Group Management
- Other Considerations

Audience

This course is intended for Systems Engineers, Developers, Architects, and Project Leaders who need to gain a good understanding of how Forefront Identity Manager 2010 can be applied to manage identity information across a number of directories or databases. It is also suitable for those who simply want to review the technology in some depth.

Prerequisites

Before attending this course, students must have:

- A sound understanding of the purpose and some experience of the workings of Active Directory.
- A sound understanding of the purpose and some experience of the workings of Microsoft Exchange Server.
- A sound understanding of the purpose and some experience of the workings of Microsoft SQL Server.

Duration

Four days

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 50382 B Implementing Forefront Identity Manager 2010

Course Outline

I. Introducing Forefront Identity Manager 2010

This module is a tour of many of the built-in features of FIM focusing on the user experience. The student will explore the FIM interface, the high level architecture of FIM, and the business needs that FIM addresses. In this module, the student will examine FIM in its installed and configured state, whereas the rest of the course will be spent understanding how FIM works, and building the fully configured FIM from a raw installation. The lab explores creating a new user, managing groups and credentials for that user, and the experience of that new user.

- A. Lesson 1: Introducing FIM
- B. Lesson 2: Synchronization Concepts
- C. Lesson 3: Other FIM Concepts

Lab: The FIM Experience

- Exercise 1: Log on and examine the environment
- Exercise 2: Add some new users and examine group memberships
- Exercise 3: Examine how groups are managed
- Exercise 4: The user experience

After completing this module, students will be able to:

- Understand what an identity management system is for, and how FIM meets these requirements.
- Operate FIM as a user, while understanding the high level functionality.

II. The Synchronization Service Manager

This module introduces the FIM Synchronization Service Manager and explains its features through scenarios that do not use the FIM Portal. It introduces the main tools (such as Metaverse Designer, Operations Tool, and Joiner), and covers the basic configuration of a Management Agent along with run profiles, results verification, and simple Metaverse search. During the lab, students will create a new Management Agent for a simple HR system.

- A. Lesson 1: The Synchronization Service

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

- B. Lesson 2: The Synchronization Service Manager: The Management Agents Tool
- C. Lesson 3: Synchronization Service Manager: Other Tools

Lab: Importing and Synchronizing Data

- Exercise 1: Connect to an HR data source and import identity data
- Exercise 2: Examine the metaverse
- Exercise 3: Importing changes

After completing this module, students will be able to:

- Understand the purpose, architecture, and functionality of the Synchronization Service.
- Understand the purpose of the Synchronization Service Manager.
- Create a simple SQL Server management agent, import identity data, and manage it.

III. More about Synchronization

This module looks at various types of Management Agent (MA), including LDAP and file-based sources. It covers concepts such as schema discovery, filters, join and projection rules, connectors and disconnectors, joining, provisioning, deprovisioning, and different kinds of attribute flow. In the lab, students create two more Management Agents, and establish a simple data-driven scenario for managing a directory (AD LDS).

- A. Lesson 1: Inbound Synchronization
- B. Lesson 2: Outbound Synchronization

Lab: Joining Data from Another MA

- Exercise 1: Creating and configuring the MA
- Exercise 2: Importing, synchronizing, and joining data
- Exercise 3: Breadcrumbs and testing

Lab: Provisioning AD LDS

- Exercise 1: Creating an AD LDS MA
- Exercise 2: Provisioning AD LDS

MOC 50382 B Implementing Forefront Identity Manager 2010

Course Outline (cont'd)

After completing this module, students will be able to:

- Understand the Synchronization Service at a more detailed level.
- Configure inbound and outbound synchronization for different types of MA.
- Apply "classic" rules to simple identity synchronization requirements.

IV. The FIM Service and Portal

This module introduces the FIM Synchronization Service Manager and explains its features through scenarios that do not use the FIM Portal. It introduces the main tools (such as Metaverse Designer, Operations Tool, and Joiner), and covers the basic configuration of a Management Agent along with run profiles, verifying results, and simple Metaverse search. During the lab, students create a new Management Agent for a simple HR system.

- A. Lesson 1: Introducing the Portal
- B. Lesson 2: Integrating the FIM Service and FIM Synchronization Service

Lab: Managing Users in the FIM Portal

- Exercise 1: Examining simple sets and MPRs
- Exercise 2: Create and modify a user

Lab: Creating the FIM MA and Synchronizing

- Exercise 1: Create the FIM MA
- Exercise 2: Synchronizing data

After completing this module, students will be able to:

- Understand the key FIM service concepts such as sets, workflows, and management policy rules.
- Navigate the FIM Service Portal, and use the portal's permission-granting system.
- Edit identity data in the FIM Portal.
- Integrate the FIM Service and the FIM Synchronization Service.

V. Managing Synchronization from the Portal

This module explores creation of an Active Directory MA, and configuration via the portal to manage mailbox-enabled users in AD. Aspects of this process include synchronization rules, workflows, and management policy rules, including complex attribute flows. In the labs, students configure FIM so that users are automatically created (provisioned) into AD, renamed, and removed (deprovisioned) as necessary.

- A. Lesson 1: Synchronization Rules
- B. Lesson 2: Outbound Synchronization Rules
- C. Lesson 3: Managing Users in Active Directory
- D. Lesson 4: More About Synchronization Rules

Lab: Inbound Synchronization Rules

- Exercise 1: Using a synchronization rule to manage the HR data MA

Lab: Synchronizing Active Directory Users

- Exercise 1: Provision users in Active Directory
- Exercise 2: Configure automatic OU provisioning and population based on DN

After completing this module, students will be able to:

- Understand inbound and outbound synchronization rules and how these relate to "classic" rules.
- Create and configure synchronization rules to manage identity data, including Active Directory (AD) Users.
- Control AD users including enable/disable and DN renames.

VI. Managing Credentials with FIM

This module primarily explores passwords. First, it addresses the essentials of Certificate Management, and then explores in detail the self-service password reset and password synchronization functions.

MOC 50382 B Implementing Forefront Identity Manager 2010

Course Outline (cont'd)

The two labs cover all aspects of password management in FIM (with the exception of writing custom password management workflows and extensions).

- A. Lesson 1: FIM Password Management
- B. Lesson 2: Password Self-service Reset
- C. Lesson 3: Synchronizing Passwords – PCNS
- D. Lesson 4: FIM Certificate Management

Lab: Password Self-service

- Exercise 1: Verify and modify the environment
- Exercise 2: Modify the configuration for password registration and reset
- Exercise 3: Testing password registration and reset
- Exercise 4: Configuring password reset lockout

Lab: Configuring PCNS

- Exercise 1: Configuring PCNS

After completing this module, students will be able to:

- Configure self-service password reset (and lockout) for chosen FIM Portal users.
- Configure password synchronization across systems.
- Identify where the use of Certificate Management might be appropriate.

VII. Group Management

This module covers the management of distribution and security groups, including the relationship between groups in Active Directory and other systems. Synchronization rules, workflows, and MPRs are explored further, along with the configuration of workflow approvals.

- A. Lesson 1: Groups and the Portal
- B. Lesson 2: Managing Groups in Active Directory

Lab: Managing Groups

- Exercise 1: Distribution groups

- Exercise 2: Provisioning distribution groups in Active Directory
- Exercise 3: Security groups
- Exercise 4: Provisioning security groups in Active Directory

After completing this module, students will be able to:

- Manage various types of groups in the FIM Portal, including self-service and member approval workflows.
- Configure FIM so that portal groups manage the corresponding AD groups.

VIII. Other Considerations

This module examines management policy rules (MPRs)—perhaps the most important feature of FIM. It explores the different types of management policy rules, their different uses, how they are processed, and how to troubleshoot them. Then it examines some operational considerations, such as the management of run cycles using scripts, and also covers backup, restore, and disaster recovery.

- A. Lesson 1: Managing MPRs
- B. Lesson 2: Operations

Lab: Portal Security

- Exercise 1: Configuring portal permissions

Lab: Examining Requests

- Exercise 1: Examine the requests concerning group membership changes

Lab: Backup, Restore, and Disaster Recovery

- Exercise 1: Perform a data reload
- Exercise 2: Backup
- Exercise 3: Restore

Lab: MA Run Scripts

- Exercise 1: Running MA run profiles with scripts

Lab: Finishing Touches

- Exercise 1: Finishing touches

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 50382 B Implementing Forefront Identity Manager 2010

Course Outline (cont'd)

After completing this module, students will be able to:

- Understand the various types of MPR, why they are used, and where they are used.
- Understand the nature of requests, and how requests can be managed and tracked.
- Configure a system for a regular cycle of Management Agent runs.
- Deal with simple backup and recovery scenarios.