

# Forefront Identity Manager 2010 Implementation Foundation Training

## Introduction

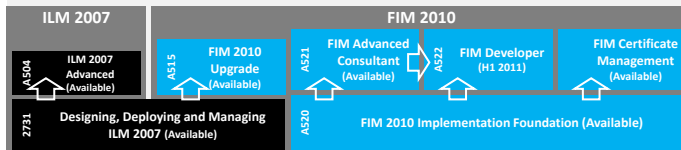
This course is for students who have no previous FIM or ILM 2007 experience. It makes use of presentation, discussion, demonstration, and a lot of hands-on exercises to introduce and explain the features and capabilities of FIM, and the solution scenarios it addresses. It is equivalent to Microsoft's course '50382'.

It is available as an instructor-led or online course.

## Audience and Pre-requisites

This four day class-room based course (reference number A520) is intended for Systems Engineers, Developers, Architects and Project Leaders who need to gain a good understanding of how FIM 2010 can be applied to managing identity information across a number of directories or databases. Typically they would follow on with a more advanced course - for more detail see the OCG FIM 2010 Training Roadmap on our website.

This course is also suitable for those people who simply want to review the technology in some depth. All students will have a sound understanding of the purpose and some experience of the workings of Active Directory (AD), Exchange and SQL Server.



## At Course Completion

At the end of the course the student 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 AD 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 MPRs

## Microsoft Certified Professional Exams

No MCP exam currently exists for this course.

## Student Materials

The student kit includes a workbook and other necessary materials for this class.

## Course Outline

### Module 1: Introducing Forefront Identity Manager 2010

This module involves a tour of many of the built-in features of FIM through the “user experience”, in which the student becomes familiar with the interface, the high level architecture, and the business needs FIM addresses. At this point you see the “finished article” – the rest of the course is spent understanding how this works, and building the “finished article” from a raw installation. The lab is a walkthrough of creating a new user and managing groups and credentials for that user – as well as the experience of that new user.

### Module 2: The Synchronization Service Manager

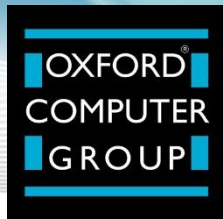
In this module we introduce the FIM Synchronization Service Manager and explain its features through scenarios that do not use the FIM Portal. We introduce the main tools (Metaverse Designer, Operations Tool, Joiner etc.), and we cover basic configuration of a Management Agent along with run profiles, verifying results, simple Metaverse search. During the lab, a new Management Agent is created for a simple HR system.

### Module 3: More About Synchronization

Here we look at various types of Management Agent (MA), including LDAP and file-based sources, with the particular emphasis on Inbound and Outbound Synchronization. We cover in detail: filters, join and projection rules, connectors and disconnectors, provisioning, deprovisioning, different kinds of attribute flow etc. In the lab, two more Management Agents are created, and a simple data driven scenario for managing a directory is established (ADLDS).

### Module 4: The FIM Service and Portal

We then examine the FIM Service and application database, introducing key concepts such as sets, workflows and policies, and how permissions are granted. Next we look at how the FIM Service integrates with the FIM Synchronization Service, and how data flows between them. The labs build a FIM MA and flows our HR data from the Synchronization Service to the portal, and portal data to the Synchronization Service.



# Forefront Identity Manager 2010 Implementation Foundation Training

## Module 5: Managing Synchronization from the Portal

In this module we cover the concept of declarative Synchronization Rules, and how they compare with the “Classic” Rules so far considered. We go on to consider how and where to use Synchronization Rules, Workflows and Management Policy Rules, including more complex attribute flows. We examine the special considerations when managing Active Directory user accounts. The labs provide experience of use of Synchronization Rules, and configure FIM so that users are automatically created (provisioned) into AD, renamed, and removed (deprovisioned) as necessary.

## Module 6: Credential Management

Primarily this module is about passwords. We address the essentials of Certificate Management (this is a large subject that has a course of its own) and then proceed to cover self-service password reset and password synchronization in detail. The labs cover all aspects of password management in FIM (with the exception of writing custom password management workflows and extensions).

## Module 7: Group Management

This module covers the management of distribution and security groups – including the relationship between groups in AD and other systems. More work is done on sync rules, workflows and MPRs. We also cover the configuration of workflow approvals.

The labs build on our scenario to include the management of various types of groups in AD.

Email: [info@oxfordcomputergroup.com](mailto:info@oxfordcomputergroup.com)  
 Web: [www.oxfordcomputergroup.com](http://www.oxfordcomputergroup.com)

US: Bellevue, WA | New York, NY  
 Tel: +1 877 862 1617

UK: Oxford  
 Tel: +44 (0)8456 584425

DE: Munich  
 Tel: +49 8122 892089-0

BeNeLux: The Hague | Brussels | Antwerp  
 Tel: +31 (0)70 36 21 627

## Module 8: Other Considerations

In this module we draw together the threads of what is perhaps the most important feature of the FIM Service – Management Policy Rules: the different types, different uses, how they are processed and how to troubleshoot them.

We then look at some operational considerations, including the management of run cycles using scripts, and also backup, restore and disaster recovery.

Five labs cover additional features of MPRs and also provide experience in the operational matters. The last of these labs puts the finishing touches on what has – perhaps surprisingly – turned out to be quite a thorough proof-of-concept system.



Oxford Computer Group (OCG) is an IT service company that specializes in Identity and Security with a particular focus on Identity and Access Management (IAM) and Information Protection. With 600+ enterprise projects completed and more than 6000 people trained on Microsoft identity and security technologies we have a wealth of expertise, solution components and training courses to offer. Operating from offices in the US, UK, BeNeLux and Germany, OCG is a Microsoft Gold Partner with Identity and Security Solutions, and Learning Solutions competencies. We understand identity and security – benefit from our experience and capability

Copyright © Oxford Computer Group 2011



**2011 PARTNER OF THE YEAR**  
 Identity and Security  
 Finalist