

Active Directory Federation Services 2.0

Introduction

This course is intended for Windows IT professionals who want to become Active Directory Federation Services (AD FS) enterprise administrators and move into the role of designing AD FS environments. It is equivalent to Microsoft's course 50412.

This course is only available in an instructor-led format.

Audience and Pre-requisites

This four day course provides students with the knowledge and skills to install and configure AD FS 2.0. It focuses on terminology, user interfaces, and common configuration scenarios for AD FS 2.0. Students learn how to design AD FS environments and supporting technology such as a Public Key Infrastructure. Students also learn how to design AD FS for security and high availability.

At Course Completion

At the end of the course the student will be able to:

- Define key concepts and terminology relating to Active Directory Federation Services 2.0
- Install and configure Windows pre-requisites for AD FS 2.0
- Install and configure Public Key Infrastructure (PKI) for AD FS 2.0
- Deploy AD FS 2.0 to provide claims-aware authentication in a single organization
- Configure AD FS 2.0 to provide claims-aware authentication in a business-to-business federation
- Design and deploy advanced AD FS 2.0 scenarios, including providing for high availability and SAML interoperability
- Use the AD FS 2.0 claims rule language to create custom claim rules
- Troubleshoot AD FS 2.0

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 Claims-Based Identity

This module explains how to recognize AD FS terminology and common use cases for AD FS 2.0. In the lab you become acquainted with the Virtual PC environment and initial configuration of the machines.

Module 2: AD FS Pre-requisites

This module explains how to configure Windows pre-requisites for AD FS 2.0, including Windows Server and Internet Information Services (IIS). This module also explains how AD FS 2.0 utilizes Web services to achieve interoperability. In the lab you perform several tasks relating to DNS name resolution, and configure a sample IIS application for use in later labs.

Module 3: Public Key Infrastructure (PKI)

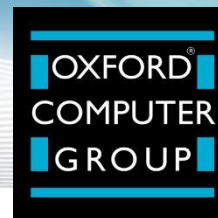
This module explains how to install and configure the PKI requirements necessary to deploy AD FS 2.0. In the lab you configure a private PKI infrastructure for two separate organizations, in order to facilitate the creation of an AD FS federation trust later.

Module 4: AD FS 2.0 Components

This module explains how to install and configure the Windows Identity Foundation (WIF), and how to install the AD FS 2.0 service in the federation server role. In the lab you install and configure the AD FS 2.0 server software, and verify that the installation completed successfully.

Module 5: Claims-Based Authentication in a Single Organization

This module explains how to design and deploy AD FS 2.0 to provide claims-based authentication within a single organization. In the lab you configure AD FS to provide claims-aware authentication in a single organization.



Active Directory Federation Services 2.0

Module 6: Claims-Based Authentication in a Business-to-Business Federation

This module explains how to design and deploy AD FS 2.0 to provide claims-based authentication in a business-to-business federation scenario. In the lab you configure the trust and claim rules for claims-based authentication in a business-to-business federation.

Module 7: Advanced AD FS Deployment Scenarios

This module explains how to deploy an AD FS server as a Federation Server Proxy. It also explains how to design an AD FS deployment to create a high-availability configuration, as well as how to configure AD FS 2.0 to achieve interoperability with SAML 2.0-compatible products and applications. In the lab you install and configure the Federation Server Proxy role, and add an AD LDS attribute store to an AD FS 2.0 server.

Module 8: The AD FS Claim Rule Language

This module explains how to configure custom AD FS claim rules using the AD FS 2.0 claim rule language. The lab covers creating custom AD FS claim rules using the claim rule language.

Module 9: AD FS Troubleshooting

This module explains how to audit, troubleshoot, and trace AD FS 2.0 components and claims-aware applications, at both the server and client level. In the lab you perform various tasks related to troubleshooting AD FS 2.0 and its dependent components.

Email: info@oxfordcomputergroup.com

Web: 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



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