

Installing and Configuring an Active Directory Federation Services Solution (ADFS)

■ Introduction

This four day instructor-led course is designed for IT professionals who need to develop a thorough understanding of the way in which federation can be used to resolve typical inter-security realm resource access problems. The business drivers for federation are first explored before installing and configuring Microsoft Active Directory Federation Services (ADFS) as a solution. Delegates will learn how to choose the right ADFS deployment option for specific business needs and then go on to configure the trust policy appropriately, along with the organization claims, account stores, applications and partner organizations.

■ Audience

This course is intended for the IT Professionals - Systems Engineers or architects who need to gain a good, basic understanding of where to use federation, and the opportunities and challenges of implementing ADFS in a variety of configurations. They will have good experience of Active Directory, Windows operating systems, along with a general awareness of the need for certificate-based security mechanisms.

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

- Understand basic ADFS concepts.
- Prepare for an ADFS deployment.
- Understand key principles of PKI technology.
- Explain how ADFS is used in B2B and B2C scenarios.
- Deploy ADFS using the federated WebSSO with forest trust option.
- Deploy ADFS using ADAM and WebSSO.
- Understand when and how to use AzMan.
- Understand common troubleshooting strategies with ADFS.
- Understand concepts of interoperability with ADFS.

■ Prerequisites

Before attending this course, students must have familiarity with the following technologies and concepts:

- Basic understanding of networking.
- Intermediate understanding of network operating systems.
- An awareness of security best practices.
- Basic knowledge of server hardware.
- A+ or equivalent knowledge
- Some experience creating objects in Active Directory.
- Foundation course (6424A) or equivalent knowledge.

■ Microsoft Certified Professional Exams

No MCP exam currently exists for this course.

■ Student Materials

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

■ ADFS Course Outline

Module 1: Introducing Federation

- The business challenge (how users typically access resources in their own security realm)
- The Challenge of Inter-Organization Collaboration
 - Adding accounts alongside existing users (B2B)
 - Separate directories (usually B2C)
 - Separate directories with sync (B2B and B2E)
 - Shared central directory (like Passport, or a core retailer)
- What is ADFS? (key benefits and components)
- ADFS Traffic Flow
 - B2B • B2E • B2C
- Technologies required for federation
- Identity Management – the basis for federation

Module 2: Preparing for ADFS

- Hardware and software requirements for ADFS
- The Internet Information Services (IIS) 6.0 platform
- Information Data Stores
 - What is Active Directory?
 - What is Active Directory Application Mode (ADAM)?
- Directory Services and ADFS

Module 3: Introduction to Public Key Infrastructure

- Certificate Requirements for ADFS
- What is a PKI?
 - Key Components of a PKI • PKI Tools
- Encryption and Digital Signatures
- Certification Authority Hierarchies
- Designing a CA Hierarchy

Module 4: Introducing ADFS

- Federation and business scenarios
- ADFS deployment options
 - ADFS WebSSO • ADFS using Federated WebSSO
 - ADFS using Federated WebSSO with Forest Trust – B2E
- Understanding the roles of ADFS components
 - The role of the Account Partner
 - The role of the Resource Partner
 - The role of the Federation Service Proxy (FSP)
 - The role of the ADFS Web Agents
- What are ADFS claims and how are they used?
 - Identity claims • Group claims • Custom claims
- Claim transformations
- ADFS Cookies and how they are used
- ADFS authentication and SSO
- ADFS and authorization
- Certificate requirements for ADFS
 - Federation Trust and PKI
 - SSL Certificates • Token Signing Certificates
 - Client Authentication Certificates
 - Managing Certificates in ADFS
- Traffic flow in a typical B2B Federated WebSSO
- Traffic flow in a typical B2E WebSSO
- Traffic flow in a typical B2B federated WebSSO and B2E WebSSO

Module 5: Deploying ADFS in a B2B Scenario using the Federated WebSSO Configuration

- Installing the ADFS Components
- Configuring the ADFS Trust Policy
- Configuring Account partners and Resource partners
- Configuring the ADFS web agent redirect URL
- Configuring ADFS for NT token-based applications

Module 6: Deploying ADFS using Federated WebSSO with a Forest Trust

- Windows trusts and collaboration
- ADFS and Widows trusts
- Configuring an account partner to use a forest trust
- Configuring a resource partner to use a forest trust

Module 7: Deploying ADFS in a B2C Scenario using ADAM and WebSSO

- The Federation Service Proxy in a B2C scenario
- Preparing to deploy an FSP
- Implementing an FSP
- Configuring group claims extractions with ADAM
- Multiple authentication stores and the home realm discovery process

Module 8: Using AzMan with ADFS

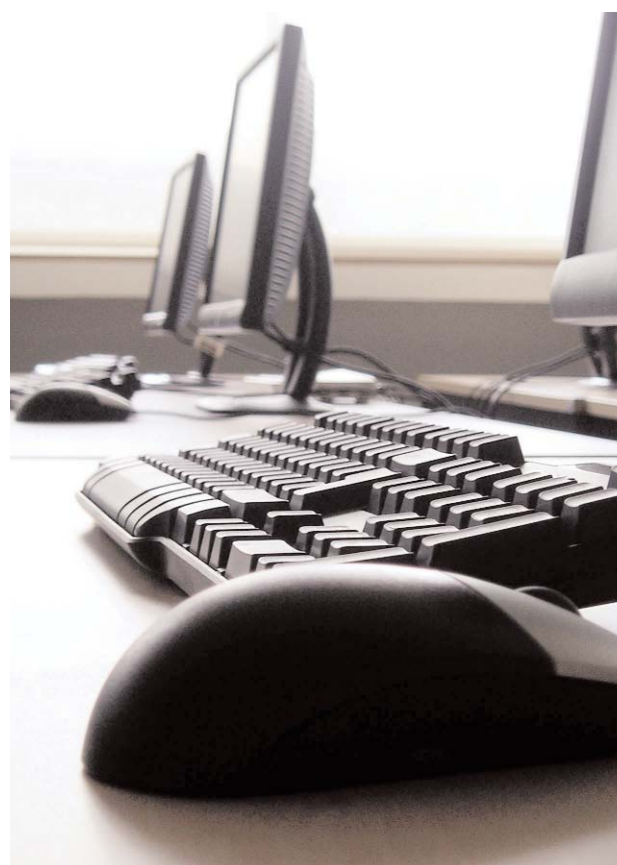
- Methods of authorization
- AzMan, ADFS and claims-aware applications
- AzMan profile stores and XML
- Creating an AzMan profile store in Active Directory
- Creating an AzMan profile store in ADAM
- Adding new AzMan applications
- Managing the AzMan components

Module 9: Troubleshooting ADFS

- Setup issues
- Configuration issues
- Directory service issues
- Troubleshooting tools
- Tracing HTTP traffic in a B2B Scenario using isHTTPHeaders
- Configuring auditing on the account and resource partner federation servers
- Configuring trace logging on the federation servers
- Configuring auditing on the ADFS web agent
- Configuring event logging on the federation service proxy

Module 10: ADFS and Interoperability

- The WS* Architecture
- What is WS-Federation?
- Interoperable federation solutions
- What is Shibboleth?
- Shibboleth traffic flow in a B2B deployment
- ADFS FS-A to Shibboleth SP
- Shibboleth IdP to ADFS FS-R



Microsoft
GOLD CERTIFIED
Partner

2008 ADVANCED INFRASTRUCTURE SOLUTIONS
PARTNER OF THE YEAR-WINNER
Active Directory

Microsoft
GOLD CERTIFIED
Partner

2008 SECURITY SOLUTIONS
PARTNER OF THE YEAR-FINALIST
Identity and Secure Access

Oxford Computer Group UK
Bignell Park Barns
Chesterton, Oxfordshire OX26 1TD UK

Tel: +44 (0)8456 584425
Fax: +44 (0)8456 584426
Email: info@oxfordcomputergroup.com
www.oxfordcomputergroup.com

Oxford Computer Group Deutschland
Winterlestr. 10b
D-85435 Erding, Deutschland

Tel: +49 8122 892089-0
Fax: +49 8122 892089-99
Email: info@oxfordcomputergroup.com
www.oxfordcomputergroup.de

Oxford Computer Group North America
111 Avenue C, Suite 104
Snohomish, WA 98290

Tel: +1 360 862 1617
Fax: +1 206 770 6193
Email: info@oxfordcomputergroup.com
www.oxfordcomputergroup.com

Oxford Computer Group Benelux
Hardwareweg 4, 3821BM Amersfoort
Nederland

Tel: +31 33 454 6950
Fax: +31 33 454 6666
Email: info@oxfordcomputergroup.com
www.oxfordcomputergroup.com

About Oxford Computer Group

Oxford Computer Group (OCG) is an IT service company that specializes in Identity & Access Management. With operations in North America, the UK, Benelux and Germany, OCG has an enviable repository of expertise, solution components and training courses. OCG has deployed 300+ enterprise-wide identity and access solutions and our instructors have trained over 3000 people on Microsoft IDA technologies. We understand identity and access management – benefit from our experience and capability.