



To register or for more information call our office **(208) 898-9036** or email [register@leapfoxlearning.com](mailto:register@leapfoxlearning.com)

**Microsoft**

## MS— 50412 Implementing Active Directory Federation Services for Windows Server 2008

### Duration:

Traditional Instructor Led Learning -4.00 Day(s)

### Software Assurance Vouchers Accepted



### About this Course

This four-day instructor-led course provides students with the knowledge and skills to install and configure Active Directory Federation Services 2.0 (AD FS). The course focuses on terminology, user interfaces, and common configuration scenarios for AD FS. Students will learn how to design AD FS environments and supporting technology such as a Public Key Infrastructure. Students will also learn how to design AD FS for security and high availability.

### Audience Profile

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.

### At Course Completion

After completing this course, students will be able to:

- Define key concepts and terminology relating to Active Directory Federation Services 2.0.
- Install and configure Windows prerequisites 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.

### Prerequisites

Before attending this course, students must have:

- Basic understanding of networking.
- Intermediate understanding of network operating systems.
- An awareness of security best practices.
- Basic knowledge of server hardware.
- Some experience creating objects in Active Directory.
- Foundation course (6424) or equivalent knowledge.
- Basic concepts of backup and recovery in a Windows Server Environment.

## 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.

#### Lessons

- Introducing the Identity Metasystem
- Existing Solutions for Managing Identities
- The Benefits of Claims-based Identity
- The Evolution of AD FS
- Use Cases for AD FS
- AD FS and Claims-based Terminology

#### Lab : Familiarizing Yourself with the Lab Environment

- Accessing Servers Using Hyper-V
- Accessing Servers Using Remote Desktop

After completing this module, students will be able to:

- Discuss and describe the Seven Laws of Identity, and how they pertain to managing identities for users and applications.
- Examine existing solutions for managing identities.
- Describe the benefits of the Claims-based Identity model.
- Discuss the evolution of Active Directory Federation Services (AD FS).
- Describe common use cases for AD FS.
- Discuss common terminology used when working with AD FS and Claims-based Identity.

### Module 2: AD FS Prerequisites

This module explains how to configure Windows prerequisites 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.

#### Lessons

- Windows Prerequisites
- Introducing Directory Services
- Active Directory and Active Directory Lightweight Directory Services
- Web Services, Standards, and Interoperability
- Internet Information Services

#### Lab : Installing Windows Prerequisites for AD FS 2.0

- Configuring DNS Forwarders
- Configure a Sample WIF Application

After completing this module, students will be able to:

- Identify the key Windows components required for AD FS.
- Describe the key characteristics of a Directory Service.
- Describe the role Active Directory and AD LDS perform in an AD FS deployment.

- Describe what is meant by the terms Web Services, WS-\*, and Security Assertion Markup Language (SAML).
- Recognize the role of IIS in a successful AD FS deployment.

### **Module 3: Public Key Infrastructure (PKI)**

This module explains how to install and configure the Public Key Infrastructure (PKI) requirements necessary to deploy AD FS 2.0.

#### Lessons

- Introducing the Public Key Infrastructure
- PKI Basics
- Introduction to Cryptography
- PKI Design
- Installing and Configuring Certificate Services

#### Lab : Installing and Configuring a Public Key Infrastructure (PKI)

- Installing and Configuring an Enterprise Root CA in the A. Datum Active Directory
- Configure an SSL Certificate for the Web Server
- Import Certificates in the Necessary Locations

After completing this module, students will be able to:

- Describe the concepts of a Public Key Infrastructure (PKI).
- Define and discuss the basics of PKI.
- Describe symmetric key and public key cryptography.
- Discuss options for PKI design.
- Describe the steps needed to install and configure Certificate Services.

### **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.

#### Lessons

- The Federation Server Role
- Claims Types, Endpoints, and Attribute Stores
- AD FS Security
- The Federation Server Proxy Role
- Administering AD FS
- Windows Identity Foundation

#### Lab : Installing AD FS Server

- Installing AD FS on ADATUM-DC1
- Installing AD FS on CONTOSO-DC1

After completing this module, students will be able to:

- Describe the role of the federation server in an AD FS 2.0 installation.

- Understand the importance of claims, claim types, endpoints, and attribute stores for a successful AD FS implementation.
- Discuss best practices for securing an AD FS implementation, including the role of Public Key Infrastructure (PKI) certificates in securing the authentication and communication process.
- Describe the role of the Federation Server Proxy.
- Describe the methods available to administer an AD FS server.
- Understand the role of the Windows Identity Foundation (WIF) in creating claims-based applications.

### **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.

#### Lessons

- Preparing for AD FS in a Single Organization
- AD FS Within a Single Organization
- Understanding Claims and Claim Types
- Claim Rules and Claim Rule Templates
- Creating Claim Rules from Templates
- Configuring AD FS in a Single Organization

#### Lab : Configuring Claims-based Authentication in a Single Organization

- Prepare CONTOSO-DC1 with Certificates and Claim Rules
- Configure the Sample WIF SDK Application Using FedUtil.exe
- Configure a Relying Party Trust to the WIF SDK Sample Application
- Configuring Claims-aware Access to SharePoint 2010

After completing this module, students will be able to:

- Define the certificate requirements for AD FS in a single organization.
- Discuss PKI certificate management for AD FS.

### **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.

#### Lessons

- Deploying AD FS in a Federated Environment
- Configuring a Claims Provider Trust
- Understanding Home Realm Discovery
- Managing Claims Across Organizations

#### Lab : Configuring Claims-based Authentication in a Business-to-Business Federation

- Configure the WIF Sample Application for B2B Federated WebSSO
- Configure SharePoint 2010 for Federated WebSSO Access

After completing this module, students will be able to:

- Deploy AD FS 2.0 in a business-to-business federation.
- Configure an AD FS Claims Provider Trust.
- Describe and configure the Home Realm Discovery process.
- Manage AD FS Claims and Federation Trust relationships across organizations.

### **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, and how to configure AD FS 2.0 to achieve interoperability with SAML 2.0-compatible products and applications.

#### Lessons

- Implementing the Federation Server Proxy
- Planning for High Availability
- Additional AD FS Configuration Scenarios
- AD FS 2.0 and SAML Interoperability

#### Lab : Advanced AD FS Deployment Scenarios

- Install and Configure the AD FS Proxy
- Install and Configure an AD LDS Attribute Store

After completing this module, students will be able to:

- Configure the AD FS 2.0 server in the Federation Server Proxy role.
- Configure AD FS 2.0 for redundancy and high availability.
- Deploy AD FS 2.0 to provide interoperability with SAML 2.0-compliant federation partners.

### **Module 8: The AD FS Claims Rule Language**

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

#### Lessons

- Reviewing the Claims Pipeline and Claims Engine
- Introducing the Claims Rule Language

#### Lab : The AD FS Claims Rule Language

- Create Rules Using the Claim Rule Language
- Query an AD FS Attribute Store

After completing this module, students will be able to:

- Describe the AD FS 2.0 Claims Pipeline and Claims Engine processes.
- Create and configure custom claim rules using the AD FS 2.0 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.

## Lessons

- Configuring Auditing for AD FS
- AD FS Troubleshooting
- Tracing AD FS Traffic

## Lab : AD FS Troubleshooting

- View AD FS Troubleshooting Information
- View AD FS Web Browser Traffic

After completing this module, students will be able to:

- Configure troubleshooting and security auditing for AD FS 2.0.
- Use built-in Windows tools to troubleshoot AD FS components and prerequisites.
- Trace AD FS Web traffic for troubleshooting and configuration purposes.

To register or for more information call our office **(208) 898-9036** or email [register@leapfoxlearning.com](mailto:register@leapfoxlearning.com)

