

Active Directory Federation Services: Deployment, Administration, and Troubleshooting



WorkshopPLUS

Target Audience:

This WorkshopPLUS is targeted at architects, developers and IT administrators.

Attendees must possess knowledge of the following:

- *Active Directory Domain Services*
- *XML Document and Schema*
- *HTTP Protocol/Troubleshooting*
- *SQL Server/Active Directory Lightweight Directory Services (AD LDS)*

Overview

This three-day Active Directory Federation Services: Deployment, Administration, and Troubleshooting WorkshopPLUS is designed to help customers address the significant changes to identity and managing access to resources that have developed thanks to Web Service (WS-*) standards and interoperability. It is difficult to make a suitable choice with so many alternatives. This often results in poor selection, and imposes limitation on authentication and authorization for how the applications will be accessed in future. This WorkshopPLUS puts concepts of claims-based authentication and authorization into action, and helps organizations to deploy AD FS.

Key Features and Benefits

This WorkshopPLUS will give attendees the knowledge to understand the requirements and approaches involved in implementing federated authentication, and will enable them to deploy and troubleshoot AD FS. The WorkshopPLUS covers the AD FS 3.0 in Windows Server 2012 R2.

Technical Highlights

After attending this WorkshopPLUS, students will be able to:

- Understand claims-based identity and authentication.
- Plan and deploy AD FS server in an enterprise.
- Configure claims-based application.
- Troubleshoot AD FS issues.

Syllabus

Hosted Requirements:

Participants will require a computer with the following configuration:

- **Operating system:**
Windows 7
- **Hard Disk:** *50 GB free drive space*
- **Peripherals:** *USB port*
- **Network:** *10 Mbps or faster network adapter*
- **Application Software:**
At least an evaluation copy of Microsoft Office 2010 Professional and a PDF reader

Participants also need a Microsoft account to connect to the virtual environment. The classroom must be networked with access to the Internet and at least total Internet bandwidth of 2 Mbps. TCP port 443 must be open. We highly recommend a wired network in the classroom.

IT Requirements:

Participants will require a computer with the following configuration:

- **Operating system:**
Windows Server 2012 R2 Hyper-V Role or Windows 8.1 with Client Hyper-V
- **Memory:** *16 GB of RAM*
- **Hard disk:** *40 GB of available hard disk space*

This Workshop *PLUS* runs for three full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

Module 1: Introduction to Claims-Based Authentication: This module provides an overview of Claims Based authentication, AD FS Planning and Deployment and how to install AD FS, use a managed service account, install the AD FS Proxy, and setup federation trust with other organization.

Module 2: SSO, Claims and Tokens: This module discusses Single Sign-On (SSO) for intranet application and federated access. This will also cover Kerberos Device and User Claims and different AD FS token types.

Module 3: Workplace Join: This module presents new features introduced in AD FS 3.0 such as workplace join, work folders, Web Application Proxy (WAP) and publishing non-claims aware application with AD FS.

Module 4: Authentication Policies and Multi-Factor

Authentication: This module covers Web Single Sign-On (WebSSO) from domain join and workplace join with different authentication types, password reset/notification/soft account lock out.

Module 5: Advanced Concepts: This module focuses on the advanced AD FS topic like attribute store, IdP-initiated Single Sign-On, home realm discovery, and customizing the look and feel of AD FS UI and webpages.

Module 6: Troubleshooting: This module provides troubleshooting steps to identify issues related to SSO, authentication prompts, certificates, workplace joins.