Security:
Modern authentication and authorization

WorkshopPLUS

Duration: 3 Days | **Focus Area:** Security and Compliance | **Level**: 300

Building applications operating in the internet environment requires understanding of options available for performing authentication and authorization. These options include, both a variety of protocols such as OAuth2 and WS-Federation, as well as tools and toolkits such as Azure AD, AD FS and MSAL or OWIN.

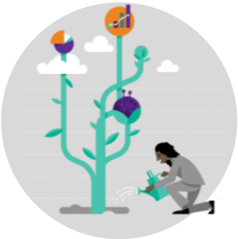
The purpose of this three-day WorkshopPLUS is to train architects and developers, to develop applications requiring cloud-appropriate authentication and authorization technology.

The WorkshopPLUS covers both common architectural patterns, industry standard protocols and tools used to implement these. The tools and infrastructure aspects of the course are focused on Microsoft technology. This WorkshopPLUS presents level 300 content targeting technical roles involved in building software such as architects and developers to help them understand the new approach based on standard protocols such as OAuth2, OpenID Connect, JWT and SAML.

OUTCOMES

Skills

You will get an understanding of how access control, authentication and authorization changes when applications and/or users use the internet.



Best Practices

You will learn how to use Microsoft infrastructure, Azure AD (corporate or B2C), AD FS and development tools to secure your applications using industry protocols such as OAuth2 or SAML.

Way Forward

Recommendations and guidance on how to apply the knowledge acquired to resolve real problems at the workplace

PREREQUISITES

Participants that have existing development skills will receive the most value from this course.

Recommended Qualifications

- Experience with Visual Studio
- Basic knowledge of C# to understand the source code shown on demos and to complete the labs

Hardware Requirements

- An Intel Core-i5-based PC
- 4 GB RAM
- 128 GB HDD
- Windows 8.1 or later
- Visual Studio 2017 (Free Community edition or higher)
- Office 2013 SP1 Professional Plus
- Internet access with at least 1 Mbps bandwidth per student
- PDF Reader

AGENDA

Duration: 3 days

START

DAY 1

Introduction: identity architecture and protocols
OAuth2 and OpenID Connect

DAY 2

If Open Workshop: Enterprise focus only:
Introduction to Azure AD
Securing REST APIs with API Management

If Closed Workshop:
Choice on either Enterprise or Consumer focus:
Consumer focus:
Introduction to AAD B2C Using Identity Experience Framework (IEF)
B2C UI customization

DAY3

Claims-based applications
ADAL/MSAL toolkits
OWIN protocol handlers

End

SYLLABUS

Introduction:

- An overview of authentication and authorization issues in internet-based applications and the purpose of various protocols (e.g. OpenID Connect, OAuth2, SAML) and Microsoft tools used to support them (Azure AD, AD FS, Windows Application Proxy, OWIN and ADAL toolkits)

OAuth2 and OpenID Connect:

- This modules delves into the details of these two protocols. It reviews the various flows defined by OAuth2 and how they apply to common application topologies. It also describes their security threat models.

Introduction to Azure AD:

- Discusses the purpose and main features of the Azure AD, including an overview of its B2E, B2B and B2C functionality, user management, application configuration and use of Graph API.

Securing REST APIs with API Management:

- Looks at features of the Azure API Management gateway that provides an additional level of security, particularly in terms of access control to your REST APIs, e.g. token pre-validation, throttling, authentication scheme conversion.

Azure AD B2C:

- Introduces the Azure AD tenant type specifically designed for consumer and citizen identities, including support for social and custom identities.
- Overview of Identity Experience and UI customization

Developing Applications:

- This module focuses on hands-on use of knowledge acquired in the previous modules to implement a set of related applications using OAuth2 protocols, Graph API and various other features of Azure AD (e.g. application roles).

ADAL/MSAL toolkits:

- Review of APIs used to obtain OAuth2 and OIDC tokens from Azure AD, ADFS and/or federated providers (gmail, FB, etc.).

OWIN protocol handlers:

- Review of toolkits used to initiate passive protocols in web applications and handle (validate/augment) received security tokens.

NEXT STEPS: If you are interested in a WorkshopPLUS – Security: Modern Authentication and Authorization for your organization, contact your Microsoft Account Representative.