XTSeminars

A John Craddock 5-day Hands-on Masterclass: Implementing and troubleshooting authentication and authorisation protocols

As we move into a world of digital transformation where resources are ubiquitously distributed, authentication and authorisation become the primary mechanisms to protect valuable resources. No longer are our environments constrain within our network boundaries, we need to stretch out and embrace disparate systems. These systems may include both providers and consumers of identity.

The key to success is through the efficacious implementation of the appropriate authentication and authorisation protocols to support our ecosystems. Only through a deep understanding of the protocols involved will you be able to validate and troubleshoot your systems.

Come on this 5-day masterclass and learn how to work with and troubleshoot:

- HTTPS
- WS-Federation
- SAML-P
- OpenID Connect
- OAuth 2.0
- REST API access
- Windows Kerberos authentication and Kerberos Constrained Delegation

The class provides you with a thorough grounding in the different protocols and shows you how to configure, test and troubleshoot. Applications/resources are running on IIS, and although the primary identity provider is Azure AD, you learn how to integrate with other identity providers.

Working with a range of troubleshooting tools including Fiddler, Wireshark, Postman and browser development tools you hone your troubleshooting skills.

If you want to resolve issues quickly, this masterclass is a must. All too often we have seen issues take days to fix whereas with the correct tools and techniques it could have been resolved in minutes. After this class, you are in an exemplary position to dramatically reduce resolution times.

Overlap with the John Craddock Identity masterclass

This class uses Azure AD and an on-premises AD as the primary sources of Identity; there is a small amount of overlap with the identity masterclass when you configure Azure AD and Azure AD Connect. This class only gives a sparse explanation of the management aspects of Azure AD focusing on configuring and troubleshooting authentication and authorisation for resource access.

If you have not attended the masterclass, please make sure you are familiar with Azure AD concepts and terminology before attending this class. The class is for experienced administrators.

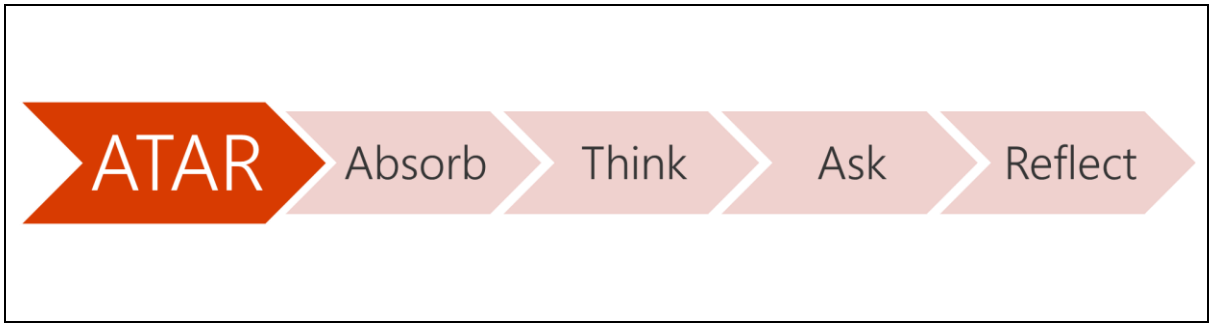
Pre-requisites

You should have hands-on system administrator's skills, which include knowing how to:

- Create and manage users, groups, OUs and group policies in on-premises AD
- Perform basic server/DC troubleshooting (for example check if a service is running, and restart it)
- Add a DNS record
- Add an URL to a browser's Intranet zone
- Create and manage users and groups in Azure AD
- Register OpenID Connect and OAuth 2.0 applications in Azure AD
- Run Azure AD PowerShell commands
- Perform basic network and protocol tracing using Wireshark and Fiddler

More details

Creating a deep-dive course is always challenging. The challenge is throwing people in at the deep end, but no so deep that they drown! The course introduces all concepts in a fairly terse and fact-packed basis before diving deep. For some of you, the intros are a revision and consolidation exercise, for others, the intros may reveal new concepts. The key to making the masterclass work for you is ATAR.



If you need more explanation about any of the topics, your job is to ask. Please remember there is no such thing as a silly question, only silly answers.

Hands-on

This hands-on masterclass does what it says on the tin, "Hands-On"; there are over 25 hands-on labs to strengthen and augment your learning. Through the hands-on, you consolidate your knowledge and discover a variety of troubleshooting tools and techniques.

The hands-on environment provides a perfect environment for troubleshooting, all the labs are running in the cloud, and you have access to the environment for two months after the class. We also give you a build document that shows you how to build the labs in your own VMs and supply you with all the masterclass websites and scripts.

Sharing and discussions

Enhance your troubleshooting ninja skills through sharing the tips and trips that you have learned either during or outside the class. Most of the hands-on exercises are augmented with a tip and trips guide and a quiz which becomes a discussion point in which attendees can share their experiences and expertise. Sharing is a pot of gold.

Read what attendees are saying about the course

- Brilliant course, excellent instructor
- Very good course. Good drill down on troubleshooting using the tools, going through valid responses/request and errors with possible solutions
- Excellent course speaker. Deep digging troubleshooting :)
- The topics were very relevant and were extremely well explained.
- The slides were brilliant, and John Craddock is one of the very best speakers/course trainers I have experienced. He has tremendous knowledge and ability to convey it to the audience in whatever he is presenting.

Day 1

The day starts with an introduction to identity and authentication/authorization protocol. Even if you switch to federated protocols, inevitably some applications are using Windows Authentication. To integrate those apps requires Kerberos authentication. In this first day, you configure and troubleshoot Kerberos for a variety of situations. Some of the scenarios are decidedly tricky, challenging you with cross-forest scenarios even if you don't have requirements for Kerberos in your environment, the tools and techniques that you learn work across all protocols.

Hands-on include:

- Getting started with the lab environment
- Investigating Windows authentication
- Baseline captures with Wireshark
- Troubleshooting with Wireshark

Day 2

Day two continues with the examination of Kerberos delegation including constrained delegation and protocol transition which is used by the Azure AD application proxy. Once you have completed the Kerberos challenges, you create an Azure AD tenant and install Azure AD Connect to synchronise identities from on-premises to the cloud. Using your Kerberos knowledge, you investigate seamless SSO while using password hash synchronization.

Hands-on include:

- Investigating Kerberos delegation
- Configuring constrained delegation
- Investigating protocol transition
- Creating an Azure AD
- Installing and configuring Azure AD Connect
- Validating Seamless SSO

Day 3

Day 3 starts with publishing and troubleshooting your windows auth apps through the Azure AD Application Proxy. You then progress to investigating the protocols used by the proxy to authenticate users and extend that knowledge to configure and troubleshoot Open ID Connect and OAuth2.0 applications using the Azure AD V1 endpoints

Hands-on include:

- Publishing and troubleshooting a Windows auth app
- Tracing Azure AD Proxy authentication
- Installing, configuring and troubleshooting an OpenID Connect / OAuth 2.0 app
- Remotely tracing back-channel traffic
- Testing token validation with Fiddler breakpoints
- Testing and troubleshooting with Postman
- Investigating consent with the V1 endpoints

Day 4

Microsoft introduced new behaviours for Open ID Connect and OAuth 2.0 with the Azure AD V2 endpoints. Discover how to publish V2 apps and work with V2 dynamic consent. After completing the session on the V2 endpoints, we shift gear, and you learn how to support applications using forms authentication in your Azure AD SSO environment.

Hands-on include:

- Deploying an app that uses the V2 endpoints
- Investigating consent with the V2 endpoints
- Publishing an OpenID Connect / OAuth 2.0 app through the proxy
- Installing & publishing a forms auth app with SSO

Day 5

In this final day, you install, configure and troubleshoot applications using WS-Federation and SAML protocols. The masterclass concludes with examining the options for sharing apps with users who are external to your organization.

Hands-on include:

- Installing, configuring and troubleshooting a WS-Federation app
- Installing, configuring and troubleshooting a SAML app
- B2B federation with Google
- B2B access Windows auth applications

Precise day-to-day timings are subject to change