



May 31 – June 2, Oslo Spektrum
10th anniversary

John Craddock

Lifting the covers on Azure AD Authentication and Conditional Access

@john_Craddock johncra@xtseminars.co.uk

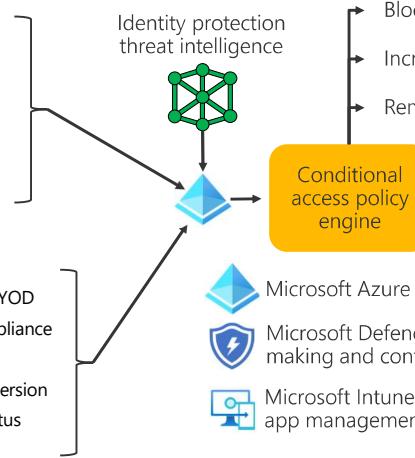


Conditional access in action

Users

- Groups/Role
- Location
- Application
- Sign-in risk
- User Risk

Identity protection threat intelligence



Block

→ Increase assurance

→ Remediate



Cloud SaaS
apps



On-premises
& web apps

Devices

- Managed or BYOD
- Health & compliance
- Device risk
- Type and OS version
- Encryption status



Microsoft Azure AD authenticates access to apps



Microsoft Defender products to enhance decision making and control access to apps



Microsoft Intune for device compliance and Mobile app management

3

Conditional access with John Craddock © XTSeminars Ltd 2022

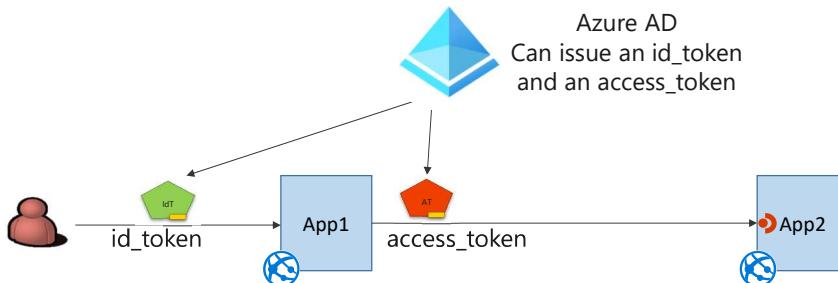
When is CA evaluated?

- ✖ Whenever an authentication request is made for
 - ✖ A SAML token
 - ✖ Id_token
 - ✖ Access_token
- ✖ The request can be made during sign in or proving authentication through the use of a
 - ✖ Session token (cookie)
 - ✖ Code which is exchanged for an access token
 - ✖ Refresh token
 - ✖ Refresh token lifetimes default to approximately 1hr

4

Conditional access with John Craddock © XTSeminars Ltd 2022

OpenID Connect & OAuth 2.0



- ✗ The **id_token** proves the user is authenticated to App1
- ✗ The **access_token** proves App1 is authorized for access to App2

5

Conditional access with John Craddock © XTSeminars Ltd 2022

Refresh token



- ✗ With the **access_token**, a **refresh token** may also be returned by Azure AD
 - ✗ An access token cannot be revoked, consequently the lifetime of the token is normally short
 - ✗ Azure AD sets this to approx one-hour
 - ✗ The client can obtain a new access token (and **id_token**) using the refresh token, this allows
 - ✗ The client to interact with the resource server even if the user is offline
 - ✗ The refresh token can be revoked and the AS will refuse to issue a new **access_token**
- ✗ Every time a refresh token is used, Azure AD re-evaluates conditional access

6

Conditional access with John Craddock © XTSeminars Ltd 2022

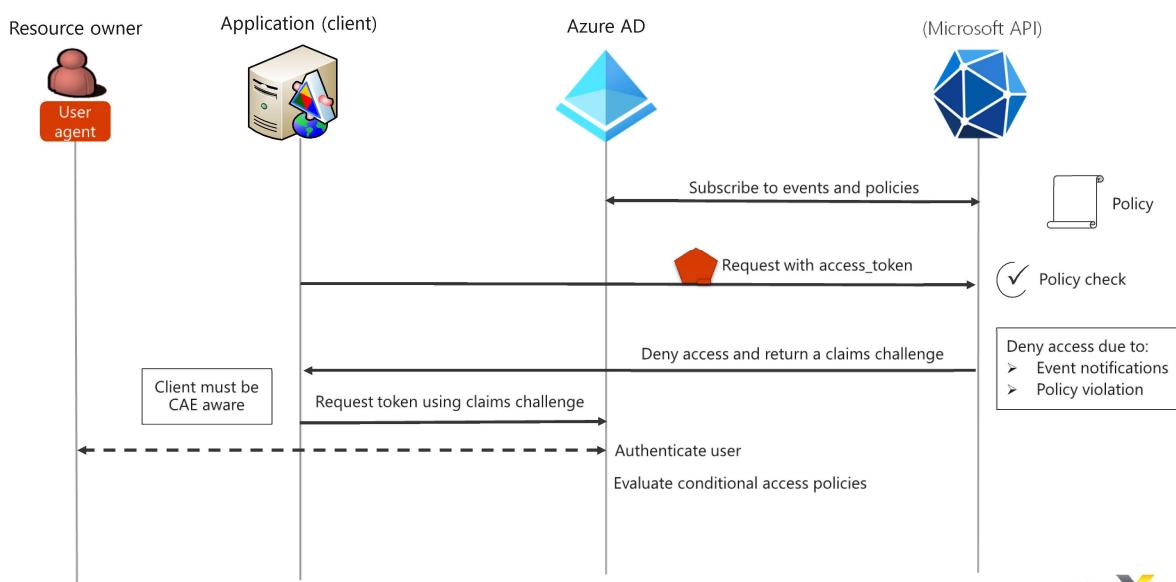
Continuous Access Evaluation

- ✖ Microsoft proprietary implementation of the core of the Continuous Access Evaluation Protocol (CAEP)
- ✖ CAEP is a work in progress by the OpenID Shared Signals and Events Working Group

7

Conditional access with John Craddock © XTSeminars Ltd 2022

CAE



8

Conditional access with John Craddock © XTSeminars Ltd 2022

Microsoft CAE

- ✖ Initially focused on Exchange, Teams and SharePoint online
- ✖ Critical events (current)
 - ✖ User account deleted/disabled
 - ✖ Password changed/reset
 - ✖ MFA enabled for user
 - ✖ Refresh tokens revoked
 - ✖ Azure AD Identity Protection detects elevated user risk
- ✖ CA policy (current)
 - ✖ Network location change
- ✖ See Microsoft documentation for current level of support for resources, clients and functionality

9

Conditional access with John Craddock © XTSeminars Ltd 2022

Outlook client access_token

iat	Sat Nov 28 2020 16:16:46 GMT+0000 (Greenwich Mean Time)
nbf	Sat Nov 28 2020 16:16:46 GMT+0000 (Greenwich Mean Time)
exp	Sat Nov 28 2020 17:21:46 GMT+0000 (Greenwich Mean Time)

CAE disabled

iat	Sat Nov 28 2020 19:05:30 GMT+0000 (Greenwich Mean Time)
nbf	Sat Nov 28 2020 19:05:30 GMT+0000 (Greenwich Mean Time)
exp	Sun Nov 29 2020 20:18:09 GMT+0000 (Greenwich Mean Time)

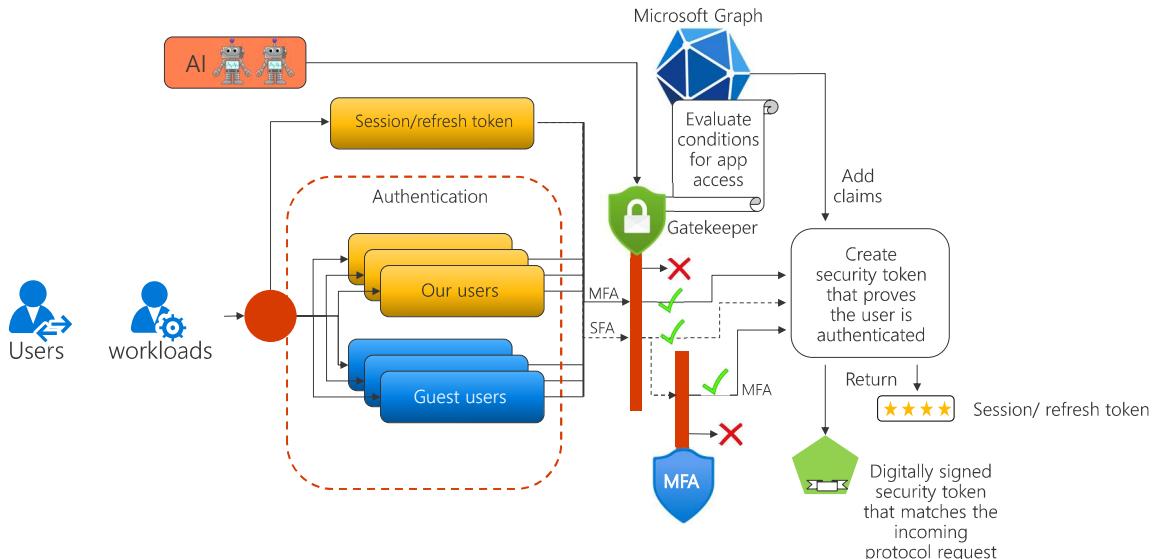
CAE enabled

- ✖ For CAE sessions the access_token lifetime can increase up to 28 hours
- ✖ The revocation of access is now event and policy driven
 - ✖ Revocation no longer relies on the attempted renewal of the access_token using a refresh token

10

Conditional access with John Craddock © XTSeminars Ltd 2022

Conditional access

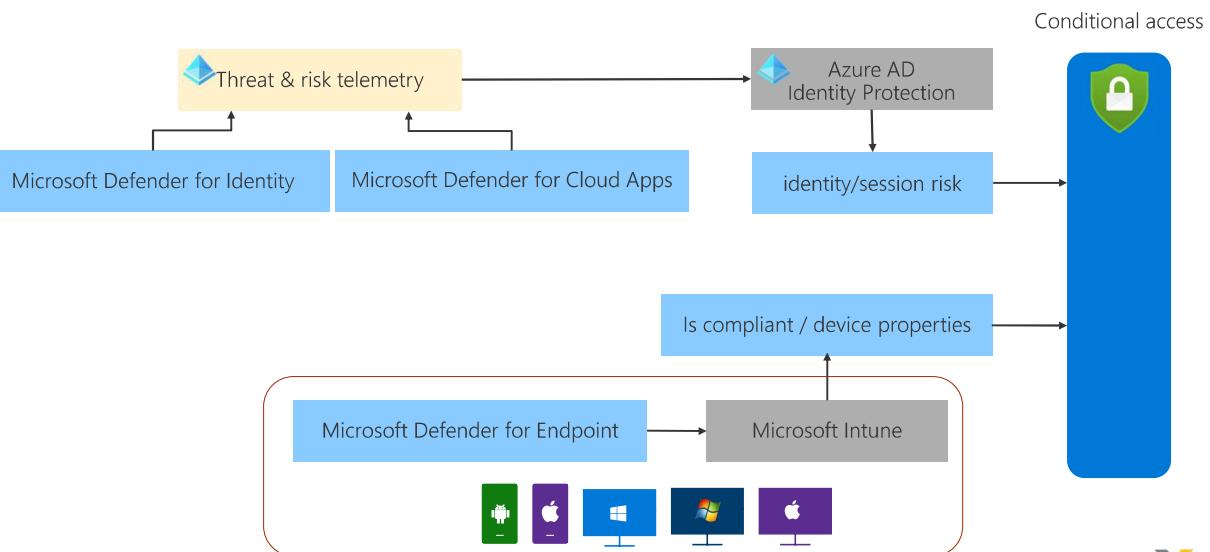


11

Conditional access with John Craddock © XTSeminars Ltd 2022

NIC X edition

Adding signals to enhance CA decisions



12

Conditional access with John Craddock © XTSeminars Ltd 2022

NIC X edition

Defining CA policies

If **principal X** want's to access **resource Y** and **conditions A-G** are met, the policy applies

If the policy applies, allow access provided, **requirements L-Q** are satisfied

Alternatively block access



If access is granted, enforce the required session controls

Requirements L-Q

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access Grant access

Require multi-factor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

→ Require approved client app [See list of approved client apps](#)

→ Require app protection policy [See list of policy protected client apps](#)

Require password change

Trusona ES

XTDevTOU

For multiple controls

Require all the selected controls Require one of the selected controls

- ✖(1) Only allows access to a cloud app from an approved client app
- ✖ Apps support Intune app protection policy
- ✖ Device must be registered in Azure AD
 - ✖ iOS and Android are supported devices and require a broker app
 - ✖ Microsoft Authenticator for iOS
 - ✖ Microsoft Authenticator or Microsoft Company Portal for Android
- ✖(2) Requires an app protection policy to be enabled on the client
- ✖ For a list of apps see
 - ✖ <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant#require-app-protection-policy>

Requirements L-Q (continued)

Grant

Control access enforcement to block or grant access. Learn more

- Block access
- Grant access
- Require multi-factor authentication
- Require device to be marked as compliant
- Require Hybrid Azure AD joined device
- Require approved client app
 - See list of approved client apps
- Require app protection policy
 - See list of policy protected client apps

- Require password change
- Trusona ES
- XTDevTOU

For multiple controls

- Require all the selected controls
- Require one of the selected controls

Select

✗Require password change

✗Only triggered by user-risk

✗Requires MFA

✗Set for All cloud apps

✗User must have previously registered for MFA & SSPR

✗Trusona ES is a custom control

✗This will probably be deprecated

✗XTDevTOU is a terms of use agreement

15

Conditional access with John Craddock © XTSeminars Ltd 2022

Session controls

Session

Control access based on session controls to enable limited experiences within specific cloud applications.

[Learn more](#) Use app enforced restrictions

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

 Use Conditional Access App Control

- Monitor only (Preview)
- Monitor only (Preview)
- Block downloads (Preview)
- Use custom policy...

 Sign-in frequency Periodic reauthentication

Select units

 Every time (Preview) Persistent browser session

Persistent browser session

⚠ Persistent browser session only works correctly when All cloud apps is selected. Please change your cloud apps selection. Click here to learn more.

- Customize continuous access evaluation

- Disable resilience defaults

16

Conditional access with John Craddock © XTSeminars Ltd 2022

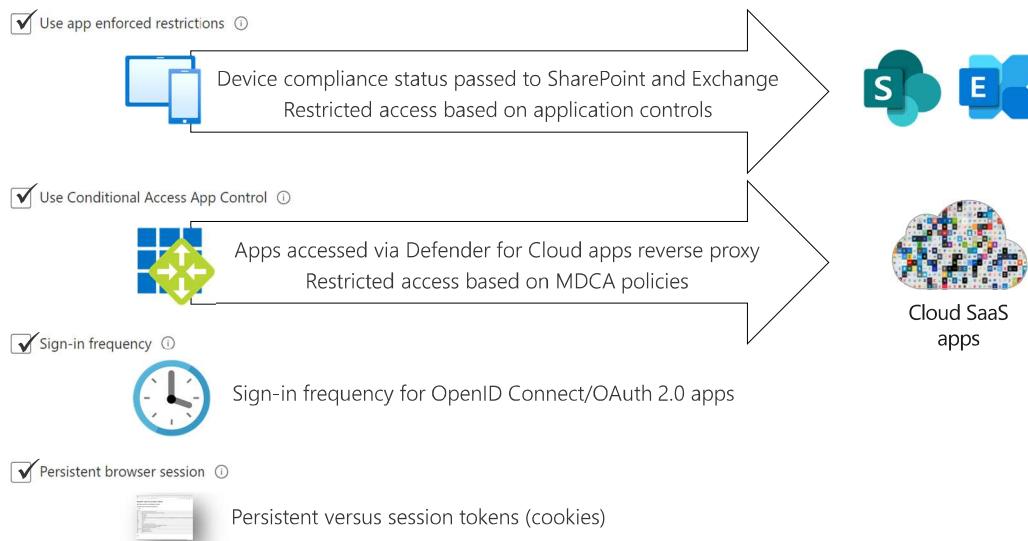
Resilience setting

- ✖ During an outage of the Azure AD primary authentication service
 - ✖ The backup authentication service can issue access tokens for existing sessions
 - ✖ CA will not be able to evaluate real-time data
 - ✖ Sign-in risk
 - ✖ User risk
 - ✖ Group Membership
 - ✖ Role Membership
 - ✖ Country location
- ✖ For CA policies, resilience is enable by default
 - ✖ Disable it, if you don't want a token to be reissued unless real-time data can be evaluated
 - ✖ Only disable the resilience setting for key users, this avoids reducing resilience for all user

17

Conditional access with John Craddock © XTSeminars Ltd 2022

Enhancing session controls



18

Conditional access with John Craddock © XTSeminars Ltd 2022

CA is a key component of Zero Trust



A work in progress

Sometimes things are give away



Session

Control access based on session controls to enable limited experiences within specific cloud applications.

[Learn more](#)

Use app enforced restrictions

! This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

Use Conditional Access App Control

Sign-in frequency

Periodic reauthentication

Every time (Preview)

Persistent browser session

Customize continuous access evaluation

Disable resilience defaults

Require token binding for sign-in sessions

19

Conditional access with John Craddock © XTSeminars Ltd 2022



Before you start



- ✖ Carefully define what you want to achieve
 - ✖ Who should be allowed or blocked from a particular resource
 - ✖ What conditions (signals) should be true/false to allow/block access
 - ✖ User risk, sign-in risk, location, device, etc
 - ✖ What requirements should be met before granting access
 - ✖ MFA, Hybrid Azure AD joined, terms of use (TOU), etc
 - ✖ When access is granted what session controls should be enforced
 - ✖ Browser session persistence, sign-in frequency, etc

20

Conditional access with John Craddock © XTSeminars Ltd 2022



Naming Policies



- ✗ Name your policies so that they make sense
 - ✗ Add a sequence number for easy reference
- ✗ SN001-v1: O365, require MFA, for all users, when on external networks
- ✗ You could also use sequence numbers to categorise your policies
 - ✗ Base, identity, data, compliance etc..

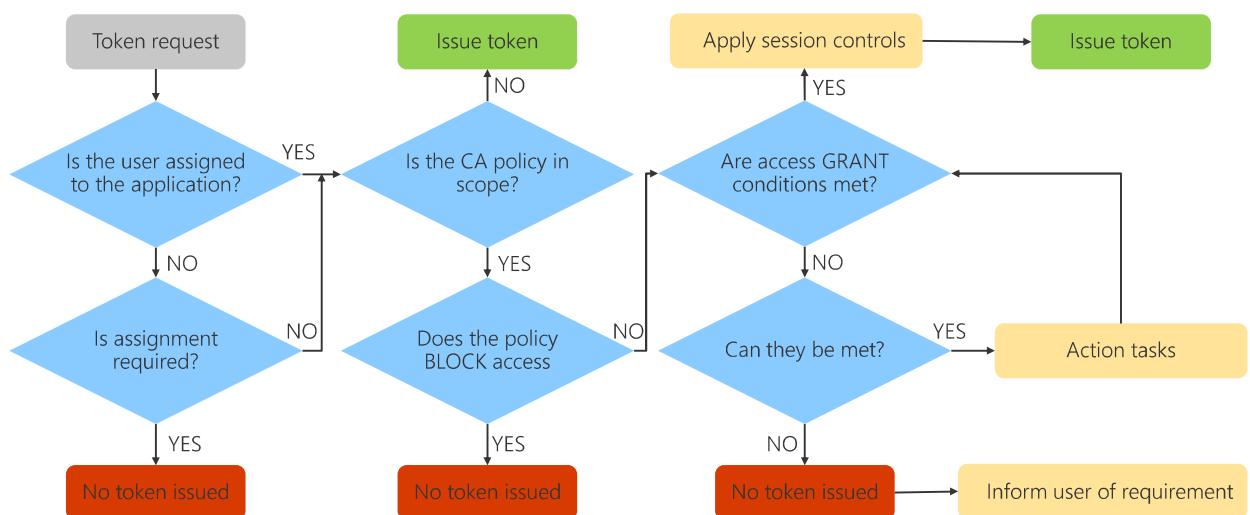
Demo...

CA walk through

Demo takeaways

- ✖ Don't lock yourself out
 - ✖ Exclude appropriate admins and emergency access accounts
 - ✖ Exclude appropriate apps
- ✖ All the selected conditions must be true before a policy is enforced
 - ✖ If multiple choices exist for a particular condition
 - ✖ If any of the choices match the incoming signal the condition is treated as true
- ✖ Think about the use of block for all users/applications/devices in combination with excludes
 - ✖ Provide appropriate policies for the excluded entities

Policy evaluation



When multiple policies are in scope

✖ Phase 1

- ✖ All access controls that are within scope are collected

✖ Phase 2

- ✖ If one or more access controls are block, access is blocked and no further actions are taken
- ✖ If access is granted subject to certain requirements and those requirements have not been already satisfied
 - ✖ The user is prompted to comply, if possible

✖ Once access is granted the selected session controls are applied

✖ Keep controls separate to aid troubleshooting

25

Conditional access with John Craddock © XTSeminars Ltd 2022

Structuring policies

✖ Many different ways of structuring policies

- ✖ Resource focussed – only access resource with a known user and a compliant device
 - ✖ Now we have a problem. How do we allow access for guest users?

✖ Another approach is to categorise your users based on common access needs and design the appropriate policies

✖ Examples

- | | |
|--------------|-----------------------|
| ✖ Internals | ✖ Guests |
| ✖ Admins | ✖ Guest Admins |
| ✖ Developers | ✖ Service account |
| ✖ Externals | ✖ Workload identities |

✖ A policy can be created to block access to all apps for accounts that have not been classified

26

Conditional access with John Craddock © XTSeminars Ltd 2022

Rolling-out conditional access policies

- ✖ Initially test using report-only mode
 - ✖ Check positive and negative scenarios
- ✖ Notify/educate appropriate users before deploying
- ✖ Automate the management of policies
 - ✖ Can be managed with PowerShell
- ✖ Consider a ring-based approach when deploying

27

Conditional access with John Craddock © XTSeminars Ltd 2022

Troubleshoot with the sign-in logs

Home > xtsdev > Users

xtsdev - Azure Active Directory

- [Overview](#)
- [Preview features](#)
- [Diagnose and solve problems](#)
- Manage**
 - [Users](#)
 - [Groups](#)
 - [External identities](#)
 - [Roles and administrators](#)
 - [Administrative units](#)
 - [Enterprise applications](#)
 - [Devices](#)
 - [App registrations](#)
 - [Identity Governance](#)
 - [Application proxy](#)

Users | Sign-in logs

xtsdev - Azure Active Directory

Date (UTC)	Request ID	User	Application	Status	IP address
5/12/2022, 3:16:32 PM	55839a77-6e3a-402...	David Grim	XTS-OIDC-V2	Failure	23.128.248.92
5/12/2022, 3:15:50 PM	c418b984-d03e-4d6...	David Grim	XTS-OIDC-V1	Success	109.70.100.34
5/12/2022, 3:15:36 PM	5bce5654-6cb1-498...	David Grim	XTS-OIDC-V2	Success	109.70.100.34
5/12/2022, 3:14:34 PM	d9df2f79-f05d-4108...	David Grim	XTS-OIDC-V2	Success	91.219.236.197
5/12/2022, 3:14:09 PM	bb6fc2d8-106d-431...	David Grim	XTS-OIDC-V2	Success	95.214.52.187
5/12/2022, 3:13:43 PM	dd68e793-16d0-437...	David Grim	XTS-OIDC-V2	Success	185.129.62.62
5/12/2022, 3:13:11 PM	8b88923a-fb6b-477...	David Grim	XTS-OIDC-V2	Success	23.175.32.13
5/12/2022, 3:12:18 PM	5c41ddc7-e057-4d9...	David Grim	XTS-OIDC-V2	Success	84.239.46.7
5/12/2022, 3:12:11 PM	d5ba0db5-bb6d-46f...	David Grim	XTS-OIDC-V2	Success	84.239.46.7
5/12/2022, 3:10:10 PM	fb8585d5-46b1-4bb...	David Grim	XTS-OIDC-V1	Failure	185.100.87.202

28

Conditional access with John Craddock © XTSeminars Ltd 2022

Conditional access details

Activity Details: Sign-ins

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	...
<input type="text"/> Search						
Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓			...
SN011: XTSOIDCv2 MFA for Ph...	Require multi-factor authentic...		Success	...		
SN001 Azure Management MF...	Require multi-factor authentic...		Not Applied	...		
SN002: OIDCv2 & XTSOIDCv2 ...			Disabled	...		
SN003: C1 Auth Context MFA ...	Require multi-factor authentic...		Not Applied	...		
SN004: OIDCv2 & XTSOIDCv2 ...			Disabled	...		
Testfor ABAC MFA	Require multi-factor authentic...		Not Applied	...		
SN005: OIDCv2 & XTSOIDCv1 ...			Disabled	...		
SN006: C2 Auth Context XTD...	XTDevT&Cs		Not Applied	...		
SN007: SharePoint App enforc...		Use app-enforced restrictions	Not Applied	...		
SN008: SalesForce MDCA for A...		Use Conditional Access App C...	Not Applied	...		
SN009: XTS-OIDCv2 MDCA for ...			Disabled	...		
SN010: XTS-SAML MDCA for A...			Disabled	...		
SN011: XTSOIDCv2 reset pass...	Multi-factor authentication an...		Not Applied	...		

A sign-in can also be interrupted (e.g. blocked, MFA challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.

Conditional Access Policy details

↑ Previous	↓ Next
Policy: SN011: XTSOIDCv2 MFA for Phil when Medium risk	
Policy state: Enabled	
Result: Success	
Assignments	
User	David Grim Matched
Application	XTS-OIDC-V1 Matched
Conditions	
Sign-in risk	Matched
High	
Device platform	Windows 10 Not configured
Location	Wieden, AT 109.70.100.34 Not configured
Client app	Browser Not configured
Device	Unknown Not configured
User risk	Not configured
Access controls	
Grant Controls	Satisfied

29

Conditional access with John Craddock © XTSeminars Ltd 2022

Authentication Context

Authentication context

```
Claims={"id_token":{"acrs":{"essential":true,"value":"c1"}}}
OR
Claims={"access_token":{"acrs":{"essential":true,"value":"c1"}}}
```

- ✖ Authentication contexts can be set by an application

- ✖ Supported in SharePoint
- ✖ A custom app can make an authentication request and pass an Authentication context in the request string
 - ✖ In the example above "c1" identifies the CA Policy to enforce
 - ✖ You can create up to 25 authentication context definitions in the portal
 - ✖ Each context will be identified by a display name and an Id c1-c25

31

Conditional access with John Craddock © XTSeminars Ltd 2022

Manage an authentication context

Home > xtsdev > Security > Conditional Access

Conditional Access | Authentication context (F)
Azure Active Directory

- Policies
- Insights and reporting
- Diagnose and solve problems
- Manage**
 - Named locations
 - Custom controls (Preview)
 - Terms of use
 - VPN connectivity
 - Authentication context (Preview)**
 - Classic policies

« + New authentication context ⏪ Refresh

Get started **Authentication context (I)**

Manage authentication context to protect d

Name **Agree T&Cs**

Modify authentication context

Configure an authentication context that will be used to protect application data and actions. Use names and descriptions that can be understood by application administrators. [Learn more](#)

Name *

Agree T&Cs

Description

Add description for the authentication context

Publish to apps will make the authentication context available for apps to use. Publish once you finish configuring Conditional Access policy for the tag. [Learn more](#)

Publish to apps



ID

c1

32

Conditional access with John Craddock © XTSeminars Ltd 2022

CA Policy enforcement

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

CA Example 006 

Assignments

Users and groups 

0 users and groups selected

Cloud apps or actions 

1 authentication context included

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Authentication context (preview) 

Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security.

[Learn more](#)

Select the authentication contexts this policy will apply to

Agree T&Cs

 The policy is evaluated when the app makes an authentication context request with a value of C1

33

Conditional access with John Craddock © XTSeminars Ltd 2022

Setting an authentication context in SharePoint

Edit sensitivity setting

Select the sensitivity level you want to apply to this site. For more info about these labels, or to create a new one, go to the [Microsoft Purview portal](#). [Learn more](#)

- Block SharePoint
Block access to a SharePoint site
- C1 auth context
This will trigger a C1 auth context request
- C2 auth context
This will trigger a C2 auth context request
- None

 Authentication context can be triggered during site access

 Requires sensitivity labels to be created and published via Purview (Compliance centre)

34

Conditional access with John Craddock © XTSeminars Ltd 2022

Creating a sensitivity label

Edit sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- External sharing & conditional access
- Schematized data assets (preview)
- Finish

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Use Azure AD Conditional Access to protect labeled SharePoint sites
You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

- Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't hybrid Azure AD joined or enrolled in Intune).
 - For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices.
[Learn more](#)
 - Allow full access from desktop apps, mobile apps, and the web
 - Allow limited, web-only access
 - Block access
- Choose an existing authentication context (preview). Each context has an Azure AD Conditional Access policy applied to enforce restrictions. [Learn more about authentication context](#)

C1 -

35

Conditional access with John Craddock © XTSeminars Ltd 2022

nicX edition

Demo...

Authentication contexts

Take it step-by-step

- ✖ Start simply and layer on additional policies
 - ✖ Authentication
 - ✖ MFA for Admins, MFA for Users, Block legacy authentication
 - ✖ Devices
 - ✖ Require: compliant devices, Azure AD joined, approved apps for mobile access
 - ✖ Block unsupported devices
 - ✖ Stricter controls
 - ✖ Evaluate sign-in and user risk
 - ✖ Control sign-in frequency
 - ✖ Disable persistent cookies
 - ✖ Require, terms of use
 - ✖ Block MFA registrations from untrusted locations
 - ✖ Block access from foreign countries
 - ✖ Integrate with Microsoft Defender for Cloud App Security
 - ✖ Leverage signals from other Microsoft Defender products

37

Conditional access with John Craddock © XTSeminars Ltd 2022

My Identity Masterclass

June 13-17 CET - just a few seats left – BOOK TODAY

"Although working with Microsoft IAM and cloud solutions for over 10 years this course was very valuable to me. Gives an excellent overview of almost all IAM capabilities and really goes into detail on the protocols involved." Eddie, IAM Solution Architect

"The best prepared labs I've ever seen in any course!" Erik, IAM Specialist

"This training is exceptionally good! Course outline covers many different aspects but it does not prevent to go really deep in each aspect. John is an excellent teacher who can talk about complicated stuff in really simple terms." Przemyslaw, Devops Engineer

Full details here: <https://learn.xtseminars.co.uk>

38

Conditional access with John Craddock © XTSeminars Ltd 2022

Consulting services on request



**John
Craddock**
Identity and security
architect
XTSeminars Ltd

johncra@xtseminars.co.uk
@john_craddock

John has designed and implemented computing systems ranging from high-speed industrial controllers through to distributed IT systems with a focus on security and high-availability. A key player in many IT projects for industry leaders including Microsoft, the UK Government and multi-nationals that require optimized IT systems. A specialist in identity systems for the last 20 years with a particular focus on federated identities to provide authentication and authorization solutions that seamlessly transition across digital boundaries. Developed technical training courses that have been published worldwide, co-authored a highly successful book on Microsoft Active Directory Internals, presents regularly at major international conferences including TechEd, IT Forum and European summits. John can be engaged as a consultant or booked for speaking engagements through XTSeminars. www.xtseminars.co.uk