John Craddock

Lifting the covers on Azure AD Authentication and Conditional Access

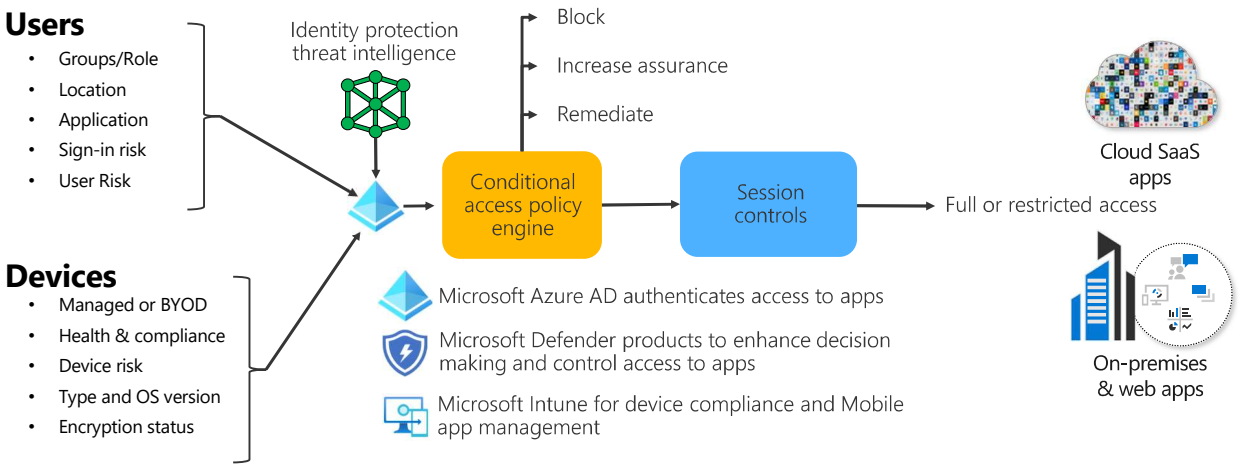
@john_Craddock johncra@xtseminars.co.uk

XTSeminars

nic X edition

XTSeminars

Conditional access in action



nicX edition

XTSeminars

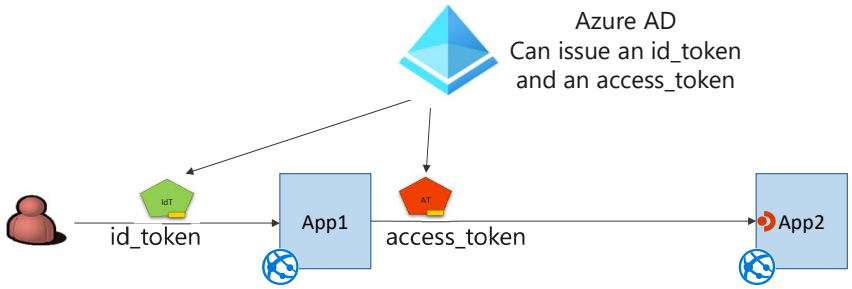
When is CA evaluated?

- Whenever and 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

nicX edition

XTSeminars

OpenID Connect & OAuth 2.0

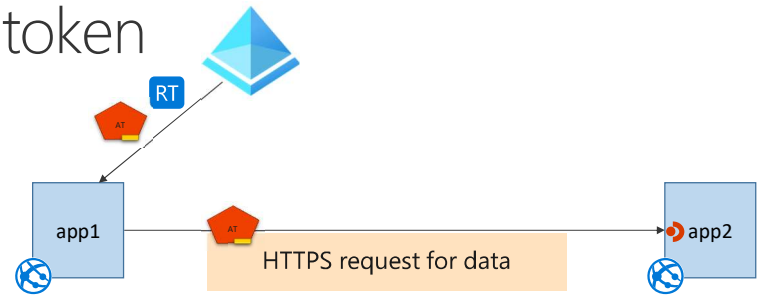


- The id_token proves the user is authenticated to App1
- The access_token proves App1 is authorized for access to App2

nicX edition

XTSeminars

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

nicX edition

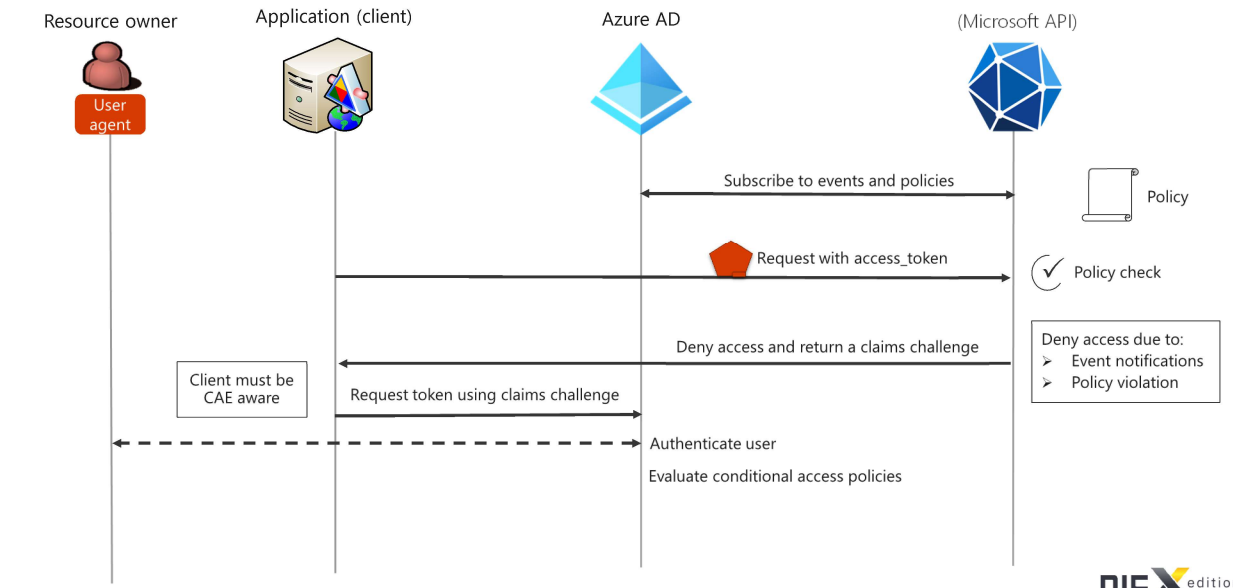
XTSeminars

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

XTSeminars

CAE



XTSeminars

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

XTSeminars

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)

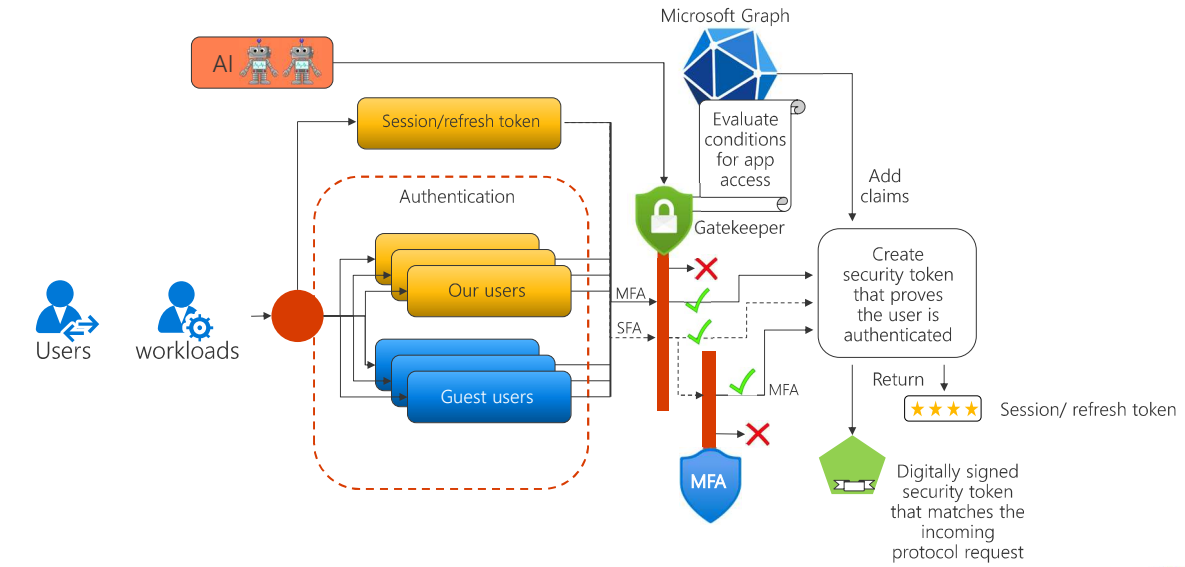
CAE disabled

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)

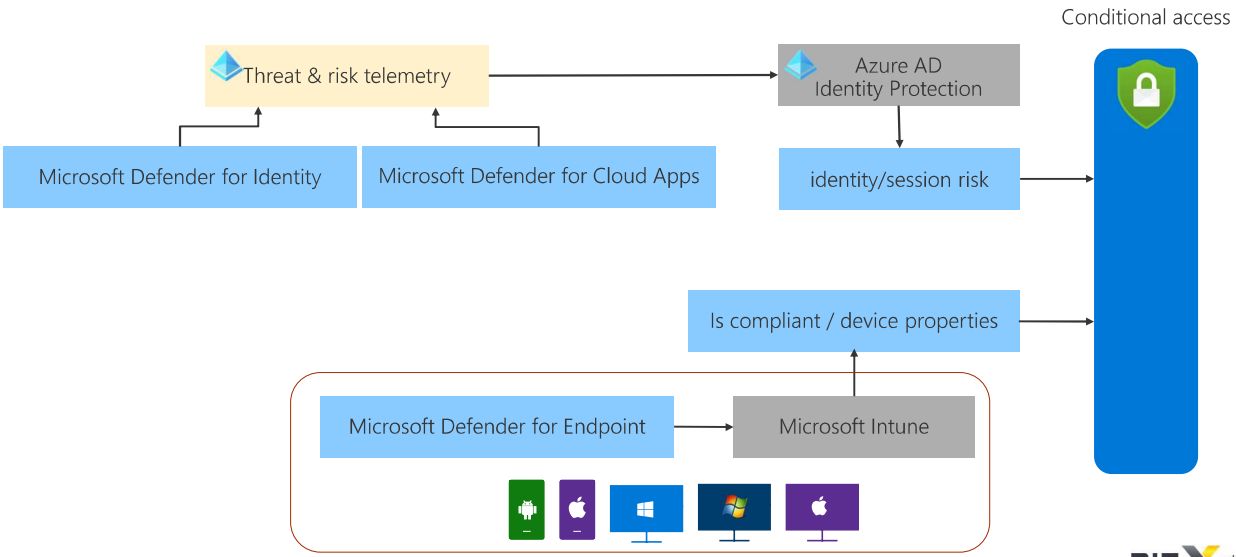
CAE enabled

- 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

Conditional access



Adding signals to enhance CA decisions



Defining CA policies

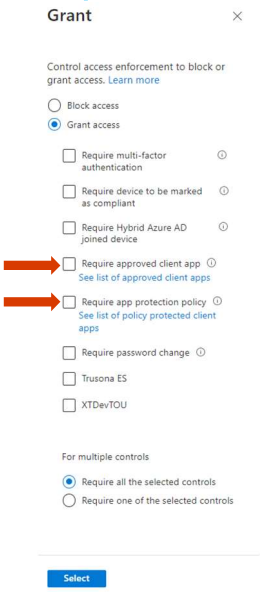
If principal X want's to access resource Y and conditions A-G are met, the policy applies

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

Alternatively block access

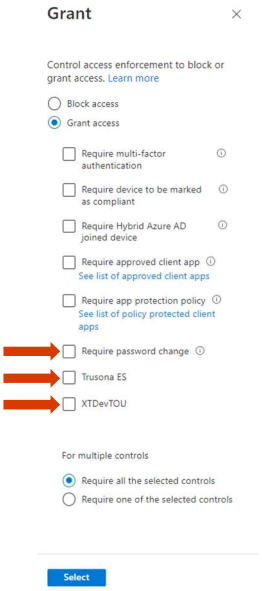
If access is granted, enforce the required session controls

Requirements L-Q



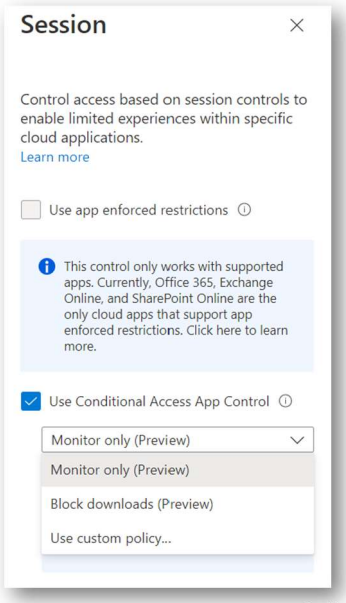
- (1) Only allows access to a cloud app from an approved client app
  - Apps support Intune app protection policy
  - Device must be registered in Azure AD
    - iOS and Android are supported devices and require a broker app
      - Microsoft Authenticator for iOS
      - Microsoft Authenticator or Microsoft 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

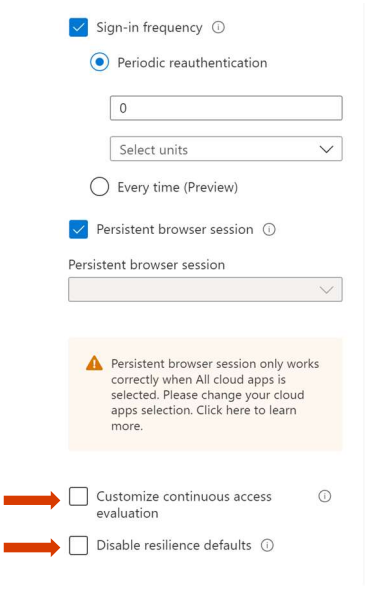
Requirements L-Q (continued)



- 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 depreciated
- XTDevTOU is a terms of use agreement

Session controls





XTSeminars

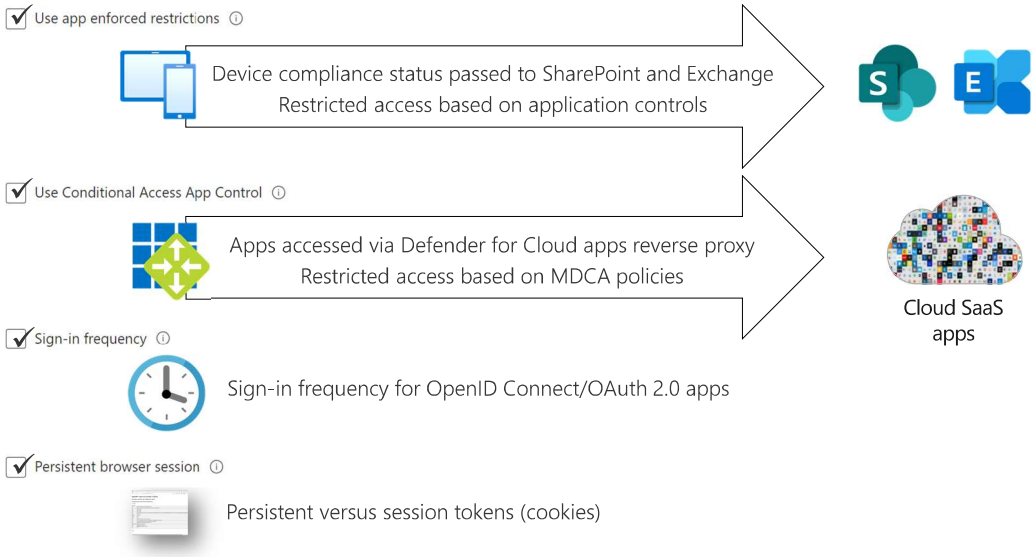
Resilience setting

- 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

NIC edition

XTSeminars

Enhancing session controls

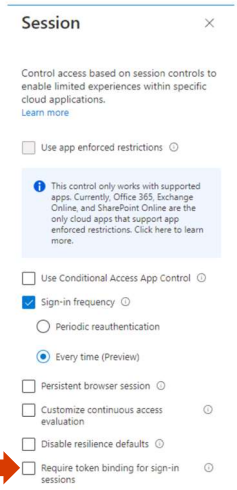


NIC edition

CA is a key component of Zero Trust

A work in progress

Sometimes things are give away



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

Naming Policies

XTSeminars

SN	Resource	Requirements	for	Principal	When	Conditions

- 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..

nic X edition

Demo...

CA walk through

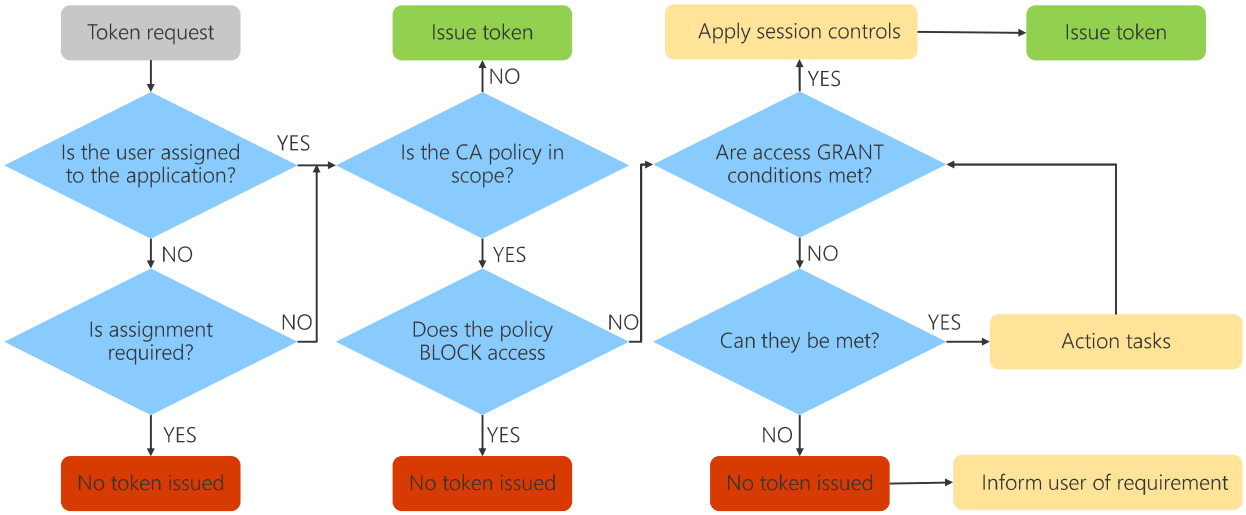
XTSeminars

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

XTSeminars

Policy evaluation



XTSeminars

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

XTSeminars

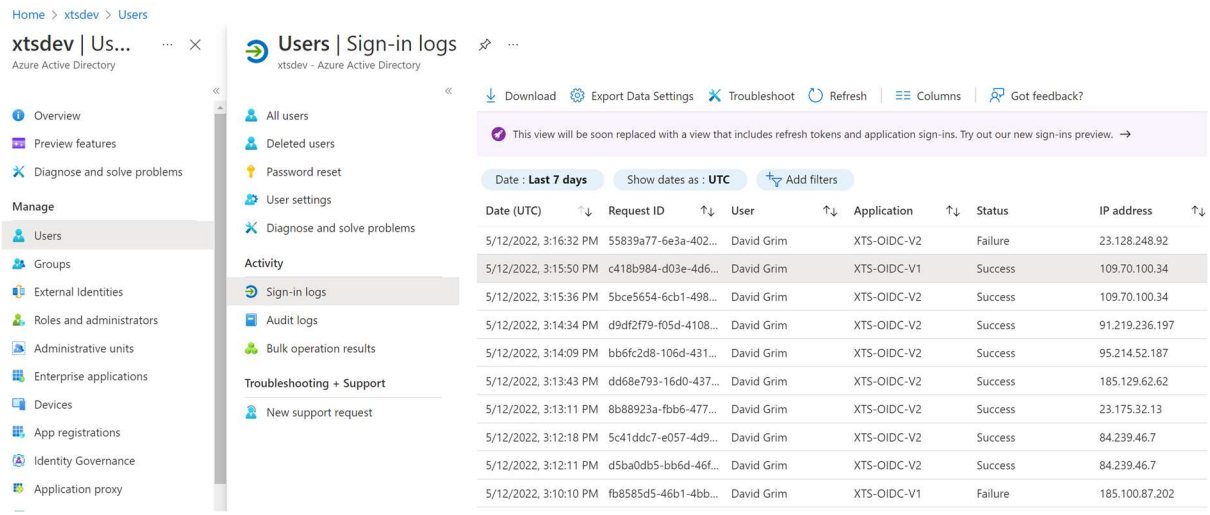
Structuring policies

- Many different ways of structuring policies
  - Resource focussed – only access resource with a know 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
  - Admins
  - Developers
  - Externals
  - Guests
  - Guest Admins
  - Service account
  - Workload identities
- A policy can be created to block access to all apps for accounts that have not be classified

Rolling-out conditional access policies

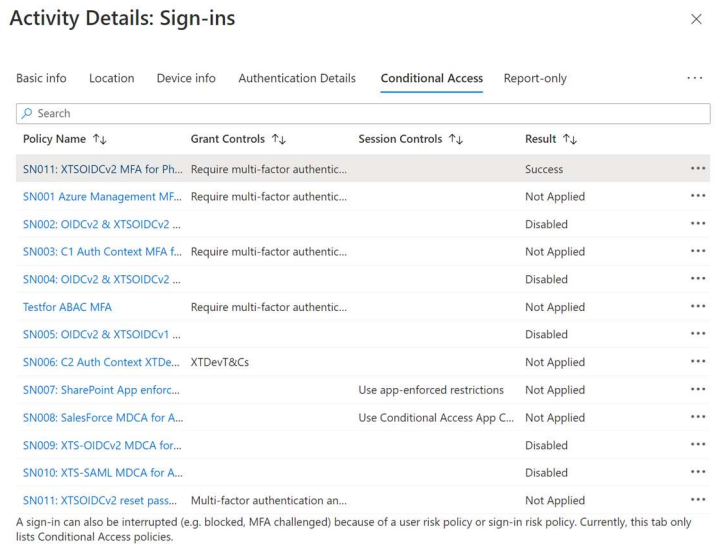
- Initially test using report-only mode
  - Check positive and negative scenarios
- Notify/educate appropriate users before deploying
- Automate the management of policies
  - Can be managed with PowerShell
- Consider a ring-based approach when deploying

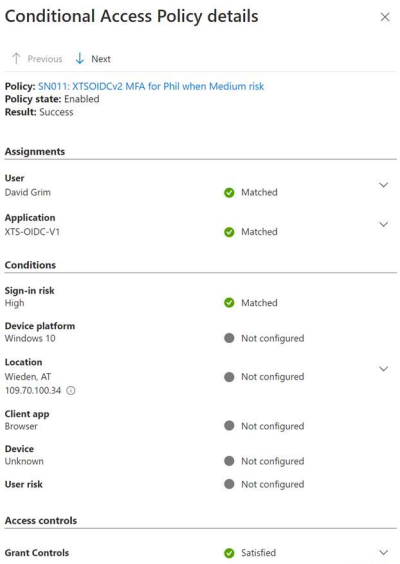
Troubleshoot with the sign-in logs



XTSeminars

Conditional access details





NIC X edition

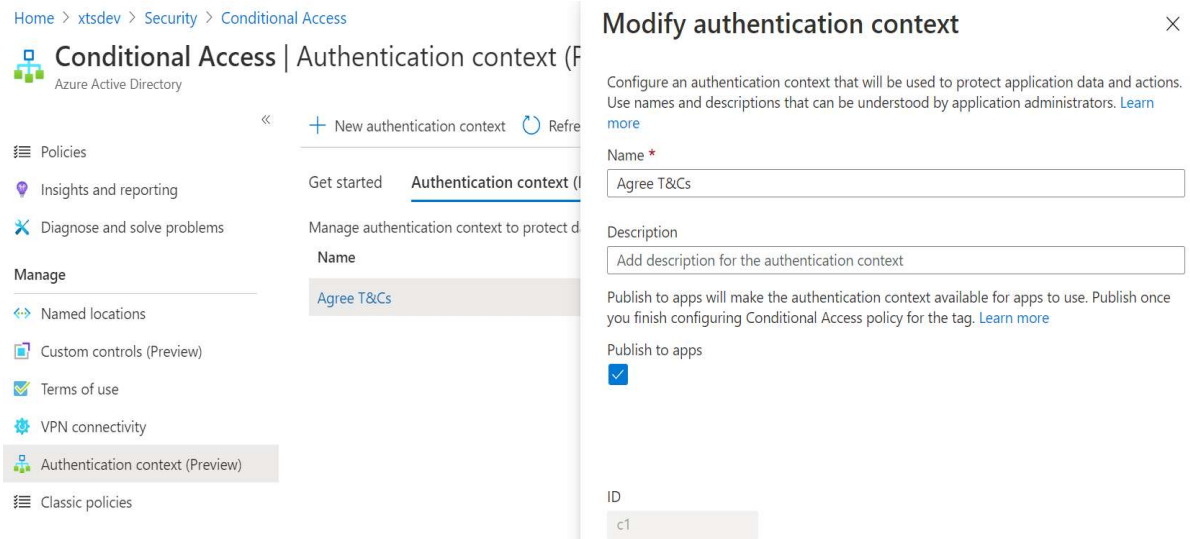
Authentication Context

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

Manage an authentication context



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

Setting an authentication context in SharePoint

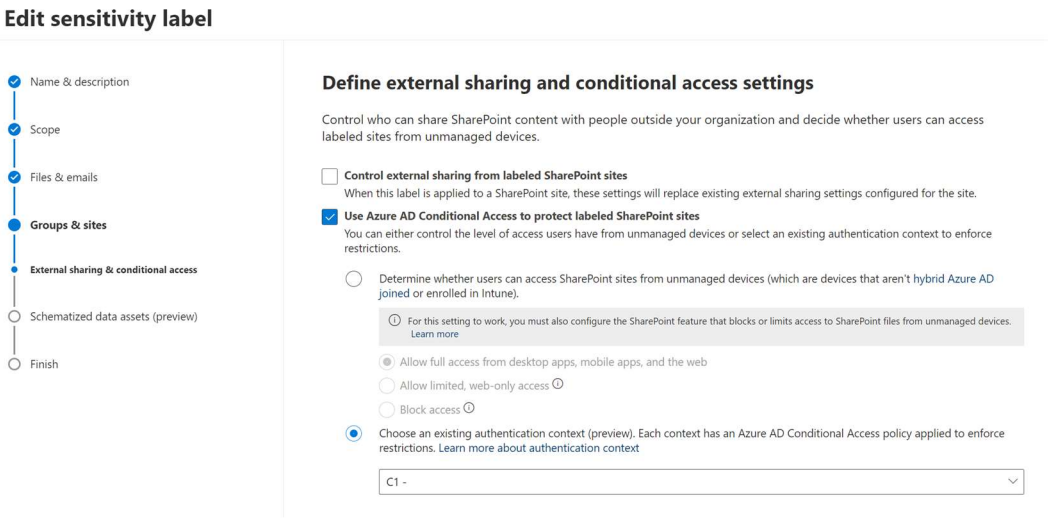
Edit sensitivity setting

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 trigger during site access
  - Requires sensitivity labels to be created and published via Purview (Compliance centre)

Creating a sensitivity label



Demo…

Authentication contexts

XTSeminars

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

nic edition

XTSeminars

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

nic edition

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