2021

Conditional Access demystified whitepaper

WHITEPAPER ON IMPLEMENTING CONDITIONAL ACCESS

KENNETH VAN SURKSUM | WWW.VANSURKSUM.COM | INSIGHT24

VERSION 1.2 | FEBRUARY, 2021

Table of contents

About: Kenneth van Surksum

Kenneth van Surksum works as a modern workplace consultant at Insight24 and is specialized in building modern workplace solutions on top of Microsoft 365. Kenneth also works with public and private cloud solutions based on Azure and System Center.

Kenneth is co-founder of the Windows Management User Group Netherlands (WMUG_NL) which was recently rebranded to the Workplace Ninja User Group Netherlands and organizes (virtual) community meetings on a regular basis.

Kenneth loves to speak about technical topics related to his daily work. Kenneth is Microsoft Certified Trainer (MCT) and has multiple certifications, he has received the MVP and VMware vExpert award multiple times.

A special thanks to Peter Daalmans for reviewing the content.

Changelog:

Name & Version	Released	Comment
Conditional Access demystified-v1.0.pdf	August 2019	Initial version based on my series of blogposts on this topic
Conditional Access demystified-v1.1.pdf	May 2020	Updated cheatsheet, implementation workflow, documentation spreadsheet,
Conditional Access demystified-v1.2.pdf	February 2021	Big update, going from 30 to 77 pages including updated reference sheets. Describing some more scenario's and providing a set of default conditional access policies for anyone to use as a starting point.

If you have any suggestions or feedback, please reach out to me via:

Email: kenneth@vansurksum.com
Twitter: @kennethvs
LinkedIn: https://www.linkedin.com/in/kennethvansurksum/

1 Introduction

In July 2016 Microsoft made Conditional Access generally available as a feature of Azure Active Directory (AzureAD). Since that time, I had a love and hate relationship with this functionality of Azure AD. Mainly because it is difficult to test scenario's and some changes can have a really high impact. I even experienced being locked out of accessing the Azure portal during one of my tests.

1.1 Why this whitepaper?

There is already some good documentation from Microsoft and many blogposts by fellow bloggers detailing Conditional Access scenarios, but not really a one-stop shopping overview. With this whitepaper I hope to achieve this.

The paper combines several blogposts I wrote on this subject, where needed I will make references to those blogposts. I did my best to provide some structure in this paper, but it might be that you recognize that it exists of multiple blogposts tied together. I will do my upper best to correct that in future versions of this paper.

I will try to describe everything that I find important and lessons learned while implementing Conditional Access in my own tenants and at customers. I will not go into much detail on creating individual Conditional Access policies, since that is both well documented by Microsoft and described by well-known bloggers on this subject like Peter van der Woude, Per Larsen, Alex Fields, Daniel Chronlund, Peter Daalmans, among others.

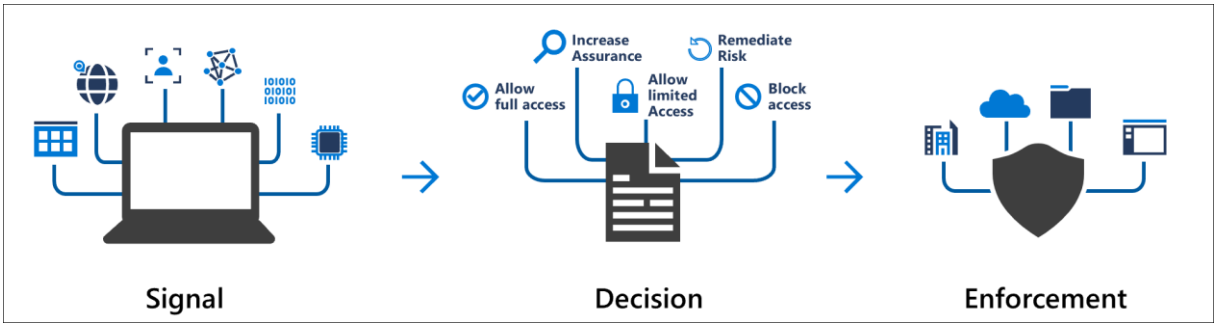
Microsoft is continuously adding functionality to Conditional Access, first functionality is added in a preview from which can be recognized by the (preview) tag in the name of the feature or Conditional Access policy and later it will eventually be released. The best way to keep up to date is by monitoring the Azure Updates webpage, where available, in preview and in development features of Azure Active Directory are shared.

2 What is Conditional Access?

Organizations are moving services which they traditionally hosted in their on-premises environment to the cloud. Because of this traditional network security in the form of Firewalls and other equipment no longer offers full protection when it comes to protecting company data.

Identity has become the new perimeter and is becoming the new attack surface for bad actors. So besides protecting our traditional assets which are either hosted on-premises or within an IaaS environment we also must protect the identity. Azure AD Conditional Access is one of the available methods to protect your identity.

Microsoft describes Conditional Access as following: "*With Conditional Access, you can implement automated access control decisions for accessing your cloud apps that are based on conditions.*" and "*Conditional Access policies are enforced **after** the first-factor authentication has been completed. Therefore, Conditional Access is not intended as a first line defense for scenarios like denial-of-service (DoS) attacks, but can utilize signals from these events (e.g. the sign-in risk level, location of the request, and so on) to determine access.*"



The way I see it, the best way to explain what Conditional Access does, is by making the comparison to a firewall. A firewall determines what traffic can access your resources, under what circumstances and Conditional Access sort of does the same. Conditional Access describes under what circumstances users can access (by acquiring an Access Token) your cloud data or applications. Keep in mind though that Conditional Access polices are enforced **after** the first authentication has taken place.

With cloud applications in Azure AD, Microsoft references to applications which use Azure Active Directory (Azure AD) for authentication (and sometimes also for authorization). Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. So, if you access a SaaS based application through Azure AD you can use Conditional Access as your "access firewall". Microsoft's SaaS offerings like Office 365, Dynamics, the Azure Portal all use Azure AD as its authentication and authorization mechanism.

This also means that if you can access the SaaS application in some other way, you can bypass Conditional Access making the solution less effective. For example, you store only the credentials of the application in Azure AD, allowing you to use SSO to login to the applications and making use of Conditional Access, but when accessing the SaaS application directly you can also provide your userid and password, which allows you to bypass the Conditional Access policies. So, it is important that you modify the SaaS identity provider to only allow Azure Active Directory signins, and not accept local logins anymore (except for maybe a breakglass account in case of emergency).

If you have SaaS apps which have a federation with your ADFS infrastructure, you can use claim rules in ADFS which provide similar functionality as Conditional Access, if you want to make use of Conditional Access you need to modify the federation to use Azure AD instead of ADFS.

2.1 Licensing

Conditional Access is a feature which is part of an Azure AD Premium P1 and P2 license which you can buy individually or is part of a suite license like Enterprise Mobility and Security (EM+S) E3/E5 or Microsoft 365 E3/E5, and recently announced Conditional Access is now also included as part of Microsoft 365 Business Premium licensing as well, since that license includes Azure AD Premium P1.

Some of the Conditional Access settings require that you have licensed other products, for example in order to use the sign-in risk condition you need to have Azure AD Identity Protection licensed. (Part of Azure AD premium P2). In order integrate Conditional Access with Microsoft Cloud App Security (MCAS), you must have MCAS licensed as well.

Keep in mind, that you can apply Conditional Access policies to users which are not licensed for Azure AD Premium P1 and P2, since assigning Azure AD Premium P1/P2 to any user in the Azure AD puts the whole Azure AD in that modus. Even though this technically works, you are in conflict with the licensing terms. Microsoft states that ***if you use/benefit from a specific service within Azure, you must be licensed for it***.

Therefore, I advise to use group-based licensing and make sure that these groups are used for conditional access configuration as well.

2.2 Security defaults

If you are not licensed to use Azure AD Conditional Access, you can enable Security Defaults on your Azure AD tenant.

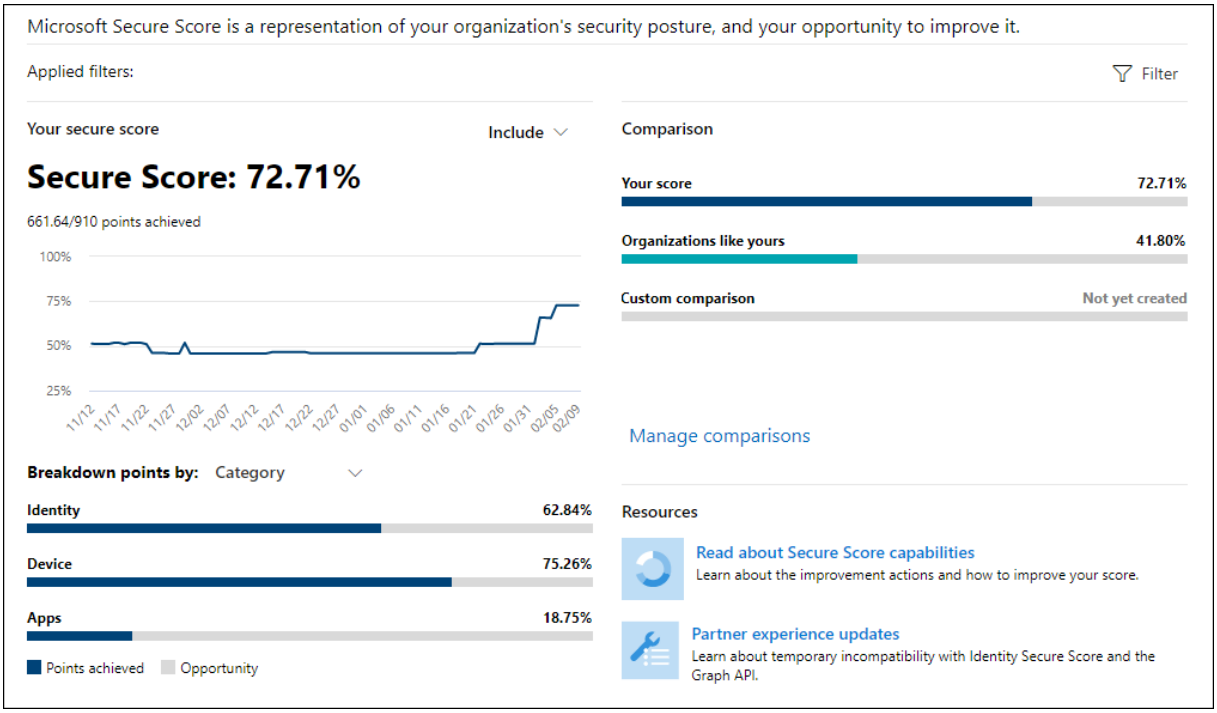
Microsoft explains the security defaults as following: "*Security defaults provide secure default settings that we manage on behalf of organizations to keep customers safe until they are ready to manage their own identity security story*." For now when the security defaults are enabled the following security settings are enforced:

1. Requiring all users and admins to register for MFA.
2. Challenging users with MFA – mostly when they show up on a new device or app, but more often for critical roles and tasks.
3. Disabling authentication from legacy authentication clients, which can't do MFA.

Since security defaults are enabled for newly created tenants by default, they will provide a good security baseline for new customers, which is actually good news since many customers are still not using any form of MFA and have the "old" default option (which is nothing at all) enabled.

2.3 Secure score

Implementing Conditional Access policies can help with receiving points in Secure Score (https://securescore.microsoft.com/). Secure Score provides a numerical summary of your security posture based on system configurations, user behavior and other security related measurements.

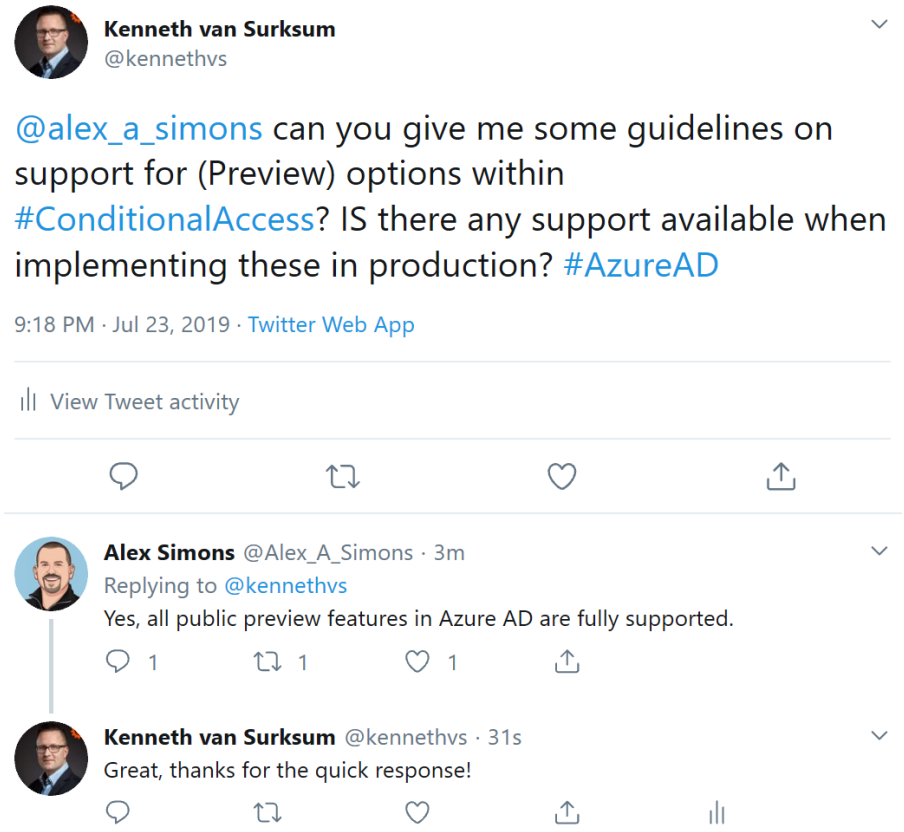


More information: Microsoft Secure Score - https://docs.microsoft.com/en-us/office365/securitycompliance/microsoft-secure-score

Conditional access provides functionality, which is part of a secure identity infrastructure, more actions than just implementing conditional access are needed. See this article for more information on the steps needed to secure your identity infrastructure: **Five steps to securing your identity infrastructure** - https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

2.4 What's up with the preview label?

Sometimes you will see the label "Preview" added to certain Conditional Access functionality. which made me wonder if enabling these policies is supported in production environment. I reached out to Alex Simons, who is Corporate Vice President PM for Microsoft's Identity Division, providing the following answer. "Yes, all public preview features in Azure AD are fully supported"



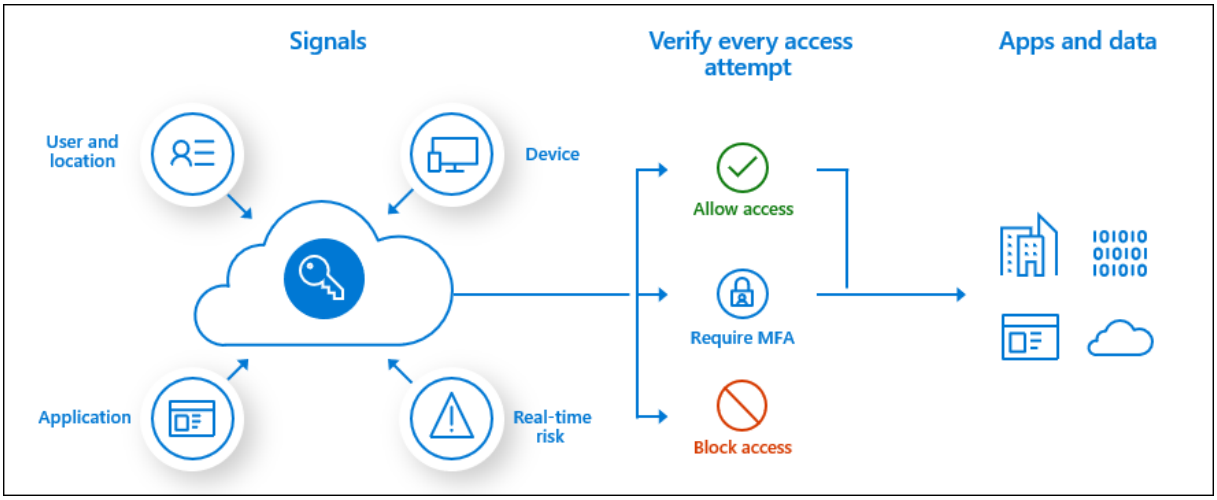
2.5 Legacy authentication

When using Basic/Legacy Authentication application sends a username and password with every request to Exchange Online which either forwards the credentials towards Azure AD or a federated authentication provider like Active Directory Federation Services (ADFS). The problem with Basic/Legacy authentication is that it is vulnerable to brute force or password spray attacks. When legacy authentication is used, it's also possible to bypass Conditional Access.

Modern Authentication is based on OAuth 2.0 and the Active Directory Authentication Library (ADAL) providing token-based authentication. OAuth 2.0 in this case is the protocol being used, and ADAL is used to authenticate against Azure AD.

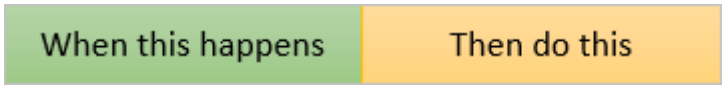
At current time, Microsoft postponed their plans to disable legacy authentication for Exchange Online. Main reason currently is timing due to the pandemic. That does not mean that the urge to get rid of legacy authentication has disappeared, and I therefore advise to move away from legacy authentication soon. I've written an extensive article on how to that which you can read here: Microsoft is going to disable basic/legacy authentication for Exchange Online. What does that actually mean and does that impact me?

3 How does Conditional Access work?



Microsoft explains Conditional Access in the following way.

Conditional Access consists of access scenario's called Conditional Access policies. An Conditional Access policy follows the following pattern:



"When this happens" defines the reason for triggering your policy. This reason is characterized by a group of conditions that have been satisfied. With "**Then do this**" you define how users can access your cloud apps.

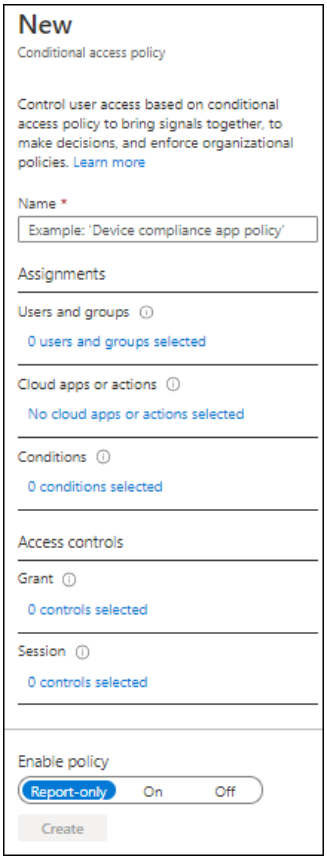
Technically this is translated to Conditions (When this happens) and Access controls (Then do this)

Microsoft provides some examples on their website for the most commonly used Conditional Access policies, which you can use for reference. The following Conditional Access policies have been described:

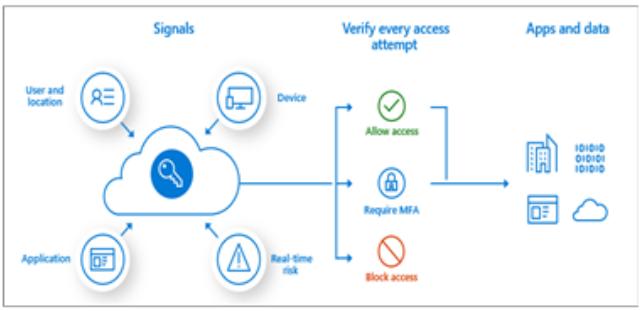
1. Block Legacy Authentication
2. Require MFA for administrators
3. Require MFA for Azure Management
4. Require MFA for all users
5. Sign-in risk-based Conditional Access
6. User risk-based Conditional Access
7. Secure security info registration
8. Block access by location
9. Require compliant devices
10. Block access

3.1 Custom Conditional Access policies

Besides some of the common policies, customers can also create their own "custom" Conditional Access policies, the figure shows how a new Conditional Access policy are grouped into sections. The Conditions (When this happens) are grouped as assignments, and Access controls (Then do this) are grouped as Access controls.



The Microsoft description covers Conditional Access from a high-level overview, practically Conditional Access is a little more complex as explained in the following flowchart or cheat sheet. You can download this cheat sheet as PDF from the following location: Conditional Access Workflow – v1.2.pdf

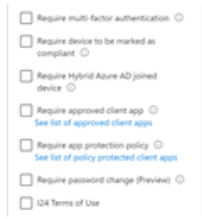


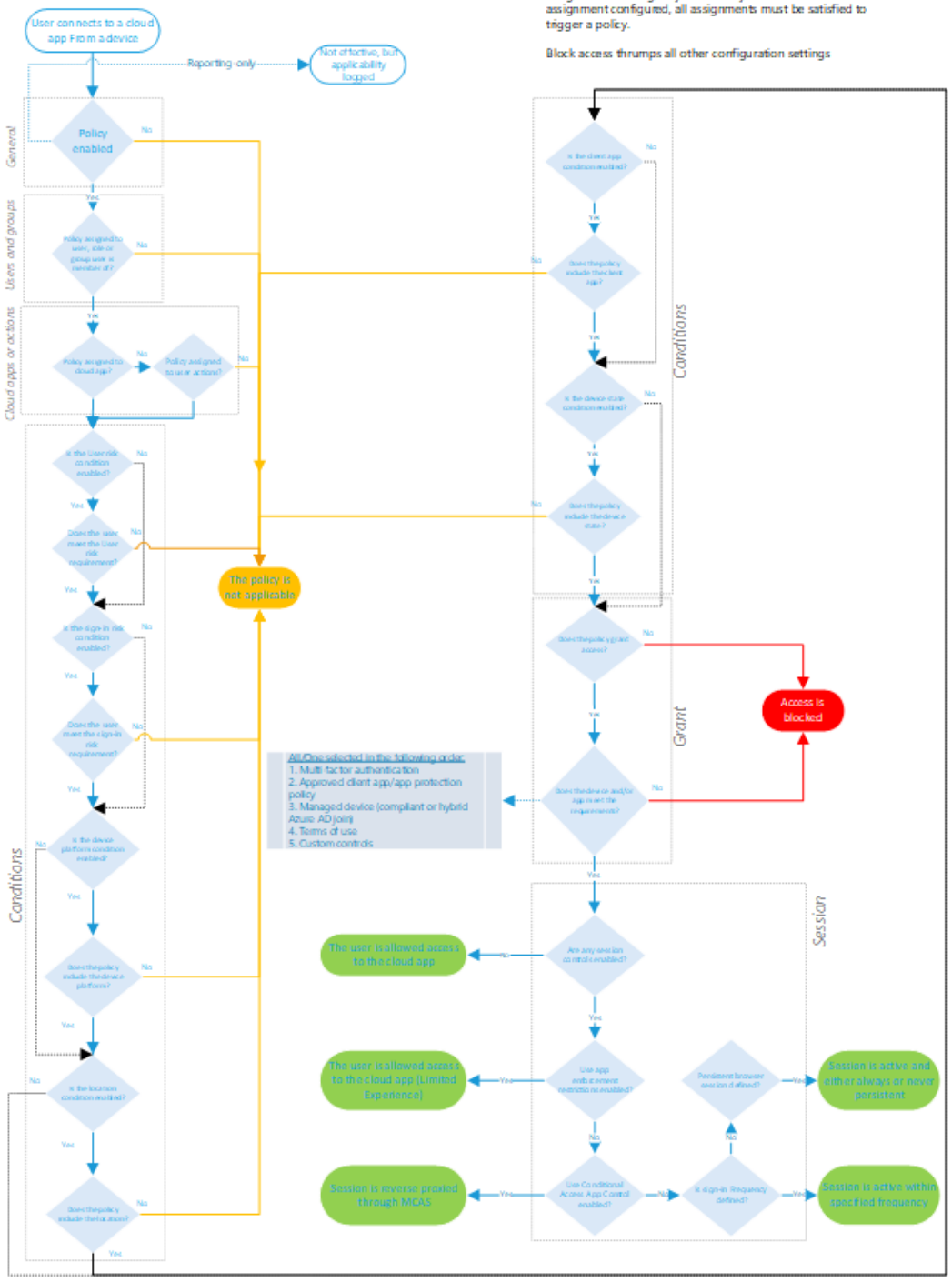
Rules:
All policies are enforced in two phases:
In the first phase, all policies are evaluated and all access controls that aren't satisfied are collected.
In the second phase, you are prompted to satisfy the requirements you haven't met.
If one of the policies blocks access, you are blocked and not prompted to satisfy other policy controls. If none of the policies blocks you, you are prompted to satisfy either one or all selected policy controls in the following order. (see picture on the right)

1. Multi-factor authentication
2. Approved client app/app protection policy
3. Managed device (compliant or hybrid Azure AD join)
4. Terms of use
5. Custom controls

External MFA providers and terms of use come next. All assignments are logically ANDed. If you have more than one assignment configured, all assignments must be satisfied to trigger a policy.

Block access thrumps all other configuration settings





Date: February 2021 | Version 1.2 | Author: Kenneth van Surksum | www.vansurksum.com

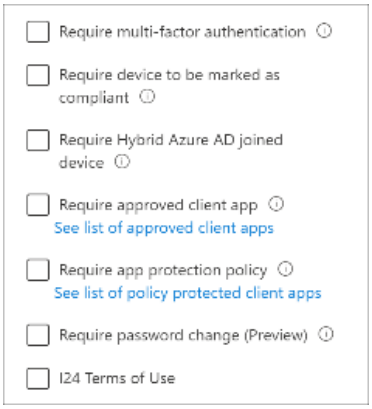
Based on the Conditional Access Workflow Cheat sheet, we can translate the conditional access to the following formula:

Conditional Access = Access to <provided> Clouds Apps except <provided> Cloud apps by <provided> users and/or <provided> roles and/or <provided> groups except <provided> users and/or <provided> groups using <provided> User Risk and/or <provided> Sign-in Risk and/or <provided> Device Platform except <provided> Device Platform from <provided> Location except <provided> Location using <provided> Client apps with <provided> device state, except <provided> device state Grants, Grants but <provided requirement must be fulfilled> or Blocks access and/or applies Session controls.

When multiple Conditional Access policies apply for a user when accessing a cloud app, **all the policies must grant access** before the user can access the cloud app.

Some important rules are:

1. All policies are enforced in two phases:
    - In the first phase, all policies are evaluated and all access controls that are not satisfied are collected.
    - In the second phase, you are prompted to satisfy the requirements you have not met.
    - If one of the policies blocks access, you are blocked and not prompted to satisfy other policy controls. If none of the policies blocks you, you are prompted to satisfy other policy controls, for which you require ALL or ONE of the selected controls, depending on the chosen option under "For multiple controls." If ONE is selected, the following order is used while evaluating.
        - 1. Multi-factor authentication
        - 2. Approved client app/app protection policy
        - 3. Managed device (compliant or hybrid Azure AD join)
        - 4. Terms of use
        - 5. Custom controls



2. External MFA providers and terms of use come next. All assignments are logically ANDed. If you have more than one assignment configured, all assignments must be satisfied to trigger a policy.

3. Block access trumps all other configuration settings

A Conditional Access policy is built from the following components:

- General
- Assignments
- Access controls

The different components are further described in the following paragraphs.

3.2 Structure of a Conditional Access explained

In this section we are going to explain how a Conditional Access policy is setup, there are some general settings like name on whether the policy is turned on, in report-only mode or off. And we have the Assignments and Access controls.

3.2.1 General

The conditional access policy must have a unique name, use a name which gives an idea of what the policy is doing under what circumstances.

Microsoft recommends the following naming structure for your Conditional Access policies

Within the name the following information should appear.

- A Sequence Number
- The cloud app(s) it applies to
- The response
- Who it applies to?
- When it applies (if applicable)

My personal recommendation is to further extend this suggested naming convention and device the policies into categories and version them.

For sequence numbers I use categories with a 3 digit follow up number:

- CAPxxx = Conditional Access Prerequisite
- CAUxxx = Conditional Access User
- CADxxx = Conditional Access Device
- CALxxx = Conditional Access Location

And I also version the Conditional Access policy, allowing me to release new versions and test those on a few users first.

An example of my proposed naming convention would be:

CAD007-O365: Session set Sign-in Frequency for Apps for All users when Modern Auth Clients and Non-Compliant-v1.0

Policies can either be enabled (On), disabled (Off) or defined in Report-only mode which can help to determine whether the policy is working as supposed to. More on Report-only mode in chapter 5, Implementing Conditional Access.

3.2.2 Assignments

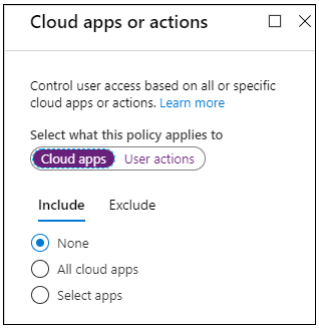
Assignments define the "When this happens" part of the Conditional Access rule and consists of the following conditions.

3.2.2.1 Users and Groups

In the users and groups condition you can specify for which users, Azure AD roles or groups the policy is applicable. You can either include and optionally exclude users, roles, and groups from the condition. It is also possible to include or exclude "guest and external users". Directory roles are especially interesting when using Azure Privileged Identity Management (PIM) where the Global Administrator role is assigned "temporarily" to a user instead of permanent. You can for example have a more restricting Conditional Access policy applied while the user has activated the Global Administrator rights.

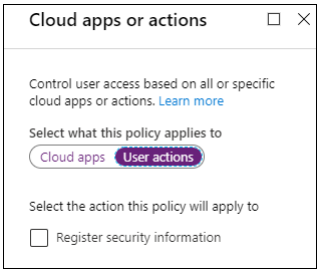
Make sure that when defining your users that you always exclude your break glass accounts, and create a unique group for each conditional access policy, using the sequence number in its name so that you can allow an exception on your policy. Having this flexibility will help you, especially during initial rollout or migration to a new set of Conditional Access policies.

3.2.2.2 Cloud apps or actions



Microsoft defines a cloud app as a website, service or “endpoint protected by Azure AD Application Proxy”. The supported cloud apps from Microsoft can be found in the following list: Microsoft cloud applications. Some of these cloud apps are Office 365, Office 365 Exchange Online, Office 365 SharePoint Online and Microsoft Azure Management (the Azure Portal). Besides the Microsoft applications you can also select any application which is configured as an Enterprise Application within your Azure AD.

The Office 365 app is a special application since it allows you to target all of the Office 365 services at once.



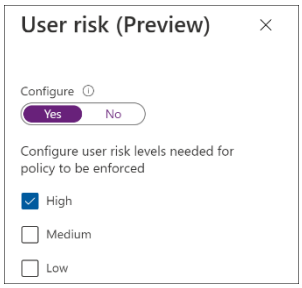
Actions refer to tasks a user can perform. For now, the only action available is “Register security information”, which requires the user to register security information needed to start using MFA. More information on that here: Combined security information registration for Azure Active Directory overview. Actions are a nice addition since they can help to make sure that prerequisites, like MFA are met, before enabling or applying other conditional access policies.

Keep in mind that if you do not use the User actions, you must select as least one cloud application for the Conditional access policy to work.

3.2.2.3 Conditions

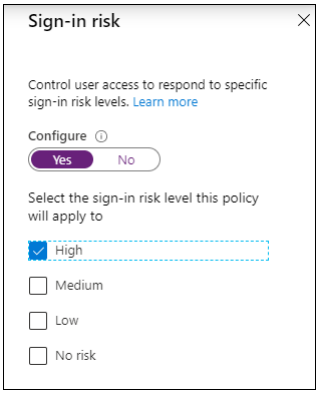
There are many conditions you can use, and Microsoft is sometimes adding even more available conditions depending on new functionality becoming available in Azure AD. Below are the current conditions described.

3.2.2.3.1 User Risk (additional license needed)



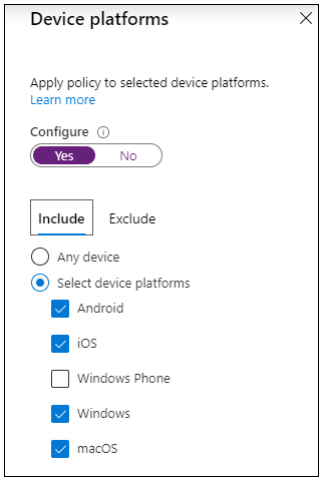
If you have licensed Azure Active Directory Identity Protection as part of Azure AD Premium P2 you can use this condition as a criterion to determine to which situation the conditional access policy will apply. Azure Active Directory Identity Protection will generate a so called "User risk level" and based on the level (High, Medium, and Low) you can make the conditional access policy applicable. More information about this scenario here: Conditional Access: Sign-in risk-based Conditional Access and in an article I wrote about the subject here: "Azure AD Identity Protection deep dive"

3.2.2.3.2 Sign-in Risk (additional license needed)



If you have licensed Azure Active Directory Identity Protection as part of Azure AD Premium P2 you can use this condition as a criteria to determine to which situation the conditional access policy will apply. Azure Active Directory Identity Protection will generate a so called "sign-in risk level" and based on the level (High, Medium, Low and No Risk) you can make the conditional access policy applicable. More information about this scenario here: Conditional Access: Sign-in risk-based Conditional Access and in a article I wrote about the subject here: "Azure AD Identity Protection deep dive"

3.2.2.3.3 Device Platforms



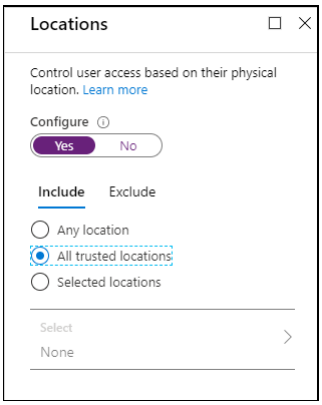
In the device platform condition, you can specify for which device platforms the policy is applicable. You can either include or optionally exclude device platforms from the condition. The following device platforms are available to select:

- Android
- iOS
- Windows Phone
- Windows
- macOS

You can also include All platforms, where you also include the platforms not in the list above (unsupported platforms, like for example Linux) and then exclude a certain supported platform from the list above. You can use the device platform condition in the case that you want to restrict access to cloud apps from managed devices, but also if you need to create several conditional access policies when you want to implement a feature which is not supported on all device platforms.

Note: The device platform feature in Conditional Access is depending on user agent strings sent by the application or the web browser, which can easily be spoofed. This is something you must keep in mind when designing your Conditional Access policies. See this article from Nicola Suter for more excellent information: Bypassing Conditional Access Device Platform Policies

3.2.2.3.4 Locations



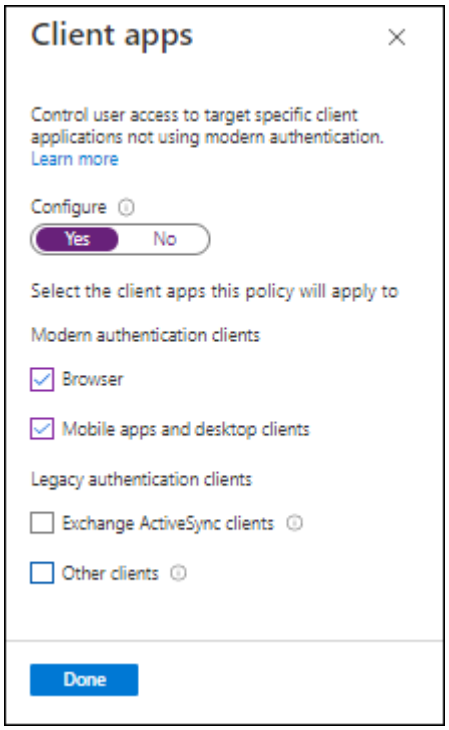
With locations you can specify conditions based on the network location the user is coming from, this is always the public IP address which is used on the internet and you cannot therefore use internal IP addresses to distinct in CA policies.

You can either include or exclude locations from the conditional access policy. Some use cases are that you want to restrict accessing the cloud app only from known locations (for example access to the Azure portal) or that you want to block access to a cloud app from a country or region for which you are sure your users will never use the cloud app service.

Note: Keep in mind that if within your company you provide guest network access but breakout to the internet using the same public IP address as your corporate devices, your guest network will fall under the same regime as your trusted network.

3.2.2.3.5 Client apps

Here you can specify the apps on the client for which the condition is applicable. These can be:



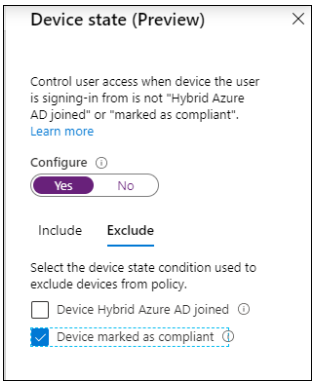
Modern Authentication Clients:

- Browser apps - apps accessed by a web browser on the client
- Mobile Apps and desktop clients

Legacy Authentication clients:

- Exchange Active Sync clients - apps which use Active Sync to connect to the cloud app - this option can only be selected if Exchange Online only is selected in the Cloud Apps selection. When Apply policy only to supported platforms is selected, only supported platforms like iOS, Android and Windows will be applicable.
- Other clients - apps which are not using "modern" authentication mechanisms, like IMAP, POP, SMTP etc... (for example, Outlook 2010). For more information about Modern and Legacy authentication see my article on that subject: "Microsoft is going to disable basic/legacy authentication for Exchange Online. What does that actually mean and does that impact me?"

3.2.2.3.6 Device state



When using the device state condition, you can exclude devices marked as compliant and devices which are Hybrid Azure AD joined (meaning Active Directory joined, and Azure AD registered) from the policy. Some scenarios are that you don't want the policy to apply to domain joined/azure ad registered devices, or that the managed device must report itself as compliant and if not the policy will apply (block access for example until the device is compliant again)

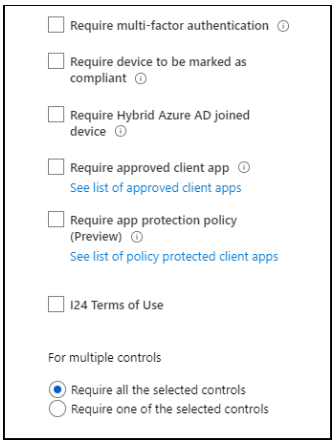
3.2.3 Access Controls

Access Controls define the "then do this" part of the conditional access policy. Based on the conditions the policy can:

- Block access to the cloud app
- Grant access to the cloud app
- Grant access to the cloud app but require an additional control (either one or all) from a list of selected controls (like MFA, must be compliant, Azure AD joined)

The grant access controls available are:

3.2.3.1 Grant



- Require multi-factor authentication (MFA)
  - Users are required to provide an extra authentication before access is granted
- Require device to be marked as compliant
  - Device from which the user is accessing the cloud app must be managed and compliant
- Require Hybrid Azure AD joined device
  - Device is Hybrid Azure AD joined, meaning member of Active Directory and registered in Azure AD
- Require approved client app
  - Approved client apps are apps which can be managed using MAM functionality in Intune, for a list of supported apps see: Supported mobile applications and desktop clients
- Require app protection policy
  - Here you can specify that besides the fact that the application must be capable of being managed using MAM, that also app protection policies must have been applied.
- Optional: Terms of use, or other custom controls

Microsoft want to move towards App Protection policy checks. Therefore, we now see that some applications are supported under the Require App Protection Policy part, where these are not listed as Approved Client App. On the other hand, having the require Approved Client App functionality available could be handy if you only have Azure AD P1 and no Enterprise Mobility + Security license (giving you MAM capabilities).

The Microsoft documentation currently raises a lot of questions, when trying to figure out my options I decided to create a matrix comparing the options available:

- Intune Protected Apps, the Official list that Microsoft references

- Approved Client App, the list of supported Apps when using a CA policy with Grant access controls
- Require App Protection policy, the list of supported Apps when using a CA policy with Grant access controls
- Applications listed under either iOSiPadOS or Android when creating an App Protection Policy.

Based on this comparison, the only Apps with full support on all points are (note that Teams for example is missing):

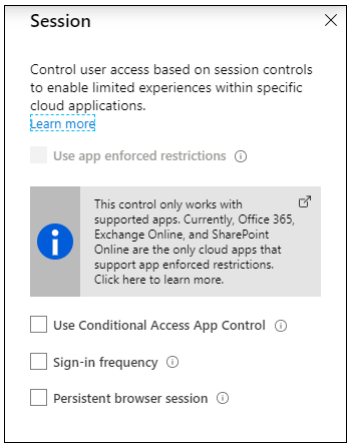
- Microsoft Cortana
- Microsoft Edge
- Microsoft Excel
- Microsoft Office
- Microsoft OneDrive
- Microsoft OneNote
- Microsoft Outlook
- Microsoft Planner
- Microsoft Power BI
- Microsoft PowerPoint
- Microsoft SharePoint
- Microsoft Word

3.2.3.2 Session Controls

Session controls are also part of the Access controls and can be applied after the session is granted, they allow for a limited experience within a cloud app and have the following options:

- Use app enforced restrictions

When this option is enabled, Conditional Access passes the device information to the cloud app, for now only SharePoint Online (SPO) and Exchange Online (EXO). In the cloud app a limited or full experience is offered depending on the device information.



- Use Conditional Access App Control

Routes the session through Microsoft Cloud App Security, which protects data by applying access and session controls acting as a reverse proxy. Some examples are: Prevent data exfiltration, protect on download, prevent upload of unlabeled files and monitor user session for compliance. The options available here are: Monitor only (preview), Block downloads (preview) and Use custom policy.

- Sign-in frequency

With sign-in frequency you can specify the time period before a user is asked to sign in again when attempting to access a resource. You can either choose Hours (between 1 and 23) or days (between 1 and 365)

- Persistent browser session

A persistent browser session allows users to remain signed in after closing and reopening their browser window. With this control, which can only be set when all cloud apps are selected you can choose between Always persistent or Never persistent. Never persistent requires the user to login again after the browser window is closed.

App enforced restrictions are only supported with Exchange Online and SharePoint Online. When enabled for SharePoint Online, users without a compliant device will see the following when

accessing SharePoint via a web browser. See “Control access from unmanaged devices” for more information

If a browser session to Exchange Online is configured to use App enforced restrictions, what can be done in Outlook Web Access can be restricted, for example offline mode and downloads can be restricted. The restrictions are defined in a so called OWA Mailbox Policy which can be set using PowerShell. See “Conditional Access in Outlook on the web for Exchange Online” for more information on how to configure the Mailbox policy.

For more information about how to use Conditional Access App Control, please read the following article on my blog: “Extending Conditional Access to Microsoft Cloud App Security using Conditional Access App Control”

4 Designing a Conditional Access strategy

When you are designing a Conditional Access strategy we first need to start with an inventory of the environment, in the most ideal situation you would design and implement conditional access in a green field scenario, but I for sure never had that luxury before so it's better to assume that the customer is already using cloud apps and wants to implement conditional access as a security measure.

The points to be inventoried are (but not limited to):

- What kind of devices does the customer use to access cloud apps?
    - Are the devices company owned, and fully managed?
    - Are the devices user owned, and non-managed?
- What kind of applications are currently used to access cloud apps?
- Is this a green field implementation, or are the cloud apps already in use without any conditional access policies in action?
- Does the customer use Intune and which scenarios are built into Intune?
    - Mobile Device Management
    - Mobile Application Management
- Is every user treated equally when it comes to access to the cloud apps, or can we distinct persona's with different requirements when it comes to Conditional Access?
- Which licensing is the customer using? My opinion is that you need E5 functionality for administrators at least nowadays.
- How are licenses being assigned to users (groups, directly)
- Are there any service accounts used that interact with the cloud apps?
- Is Modern Authentication already enabled for Exchange Online and Skype for Business online?
- Is the company storing password hashes in Azure Active Directory?
- Are there cloud apps depending on each other?

When it comes to licensing while administrating Microsoft 365 services, please be aware that there are some things you need to be aware of, see also this article on my blog: “License requirements for administering Microsoft 365 services”

Microsoft has a document available helping in planning setting up Conditional Access, called the "Azure Active Directory Conditional Access Deployment Plan". The document in word format can be downloaded from the following location: https://aka.ms/CADPDownload. Microsoft also provides planning documentation online at: Plan a Conditional Access deployment - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

When designing a Conditional Access strategy in my experience it is important to really think on a high level on what you want to accomplish. It is very easy to start creating Conditional Access all kinds of individual Conditional Access policy and get lost from what you wanted to accomplish along the way.

Based on my experience the main goal of implementing Conditional Access is that you want to prevent access to your company data in situations where you do not have control over the data. That means that ideally cloud apps can only be accessed by:

1. Devices which are under company control and are compliant
2. Applications which are under company control and are compliant

3. Browser sessions on managed devices where data can be stored locally.
4. Browser sessions on non-managed devices where data can only be opened in the browser session and no data is left behind on the device.

All the other scenario's possible are either to fulfill requirements to successfully use Conditional Access or are additional security measures like always enforcing MFA when Azure AD administrators log in. It might also be that you need some "temporary" conditional access policies while migrating to the designed situation.

Below are some example scenario's which can be the outcome of your design

- Scenario 1: Allow devices managed by Intune access all the cloud apps using Apps and Desktop Clients and Modern Authentication Clients if compliant

Access to "All Cloud Apps" by "Users with EMS License" using "Any" device platform" coming from "any location" using "Mobile Apps and Desktop Clients" or "Modern authentication clients" is allowed, but device must be compliant.

- Scenario 2: Only allow Apps we can manage to access cloud apps when device is not managed.

Allow users with EMS License using devices not managed by Intune to access (portion of) cloud apps, using clients which we can manage using MAM policies (approved clients list)

- Scenario 3: Allow browser access to all the cloud apps from a trusted location

When users access the cloud apps from a trusted location, they can login without using any additional form of authentication

- Scenario 4: Allow browser access to all the cloud apps from an untrusted location but use MFA and restrict the browser session (when possible)

When users access the cloud apps from a non-trusted location they can login but have to use MFA and when possible the browser session is restricted.

- Scenario 5: Block browser access to all the cloud apps from some geographic areas

Users cannot access cloud apps from regions where the company does not operate.

Once you know your scenario's try to model the conditional access policy in a spreadsheet, by doing this you can determine if policies can be combined, or if more than one policy needs to be created to meet the requirements of the scenario. Keep in mind that the less is more.

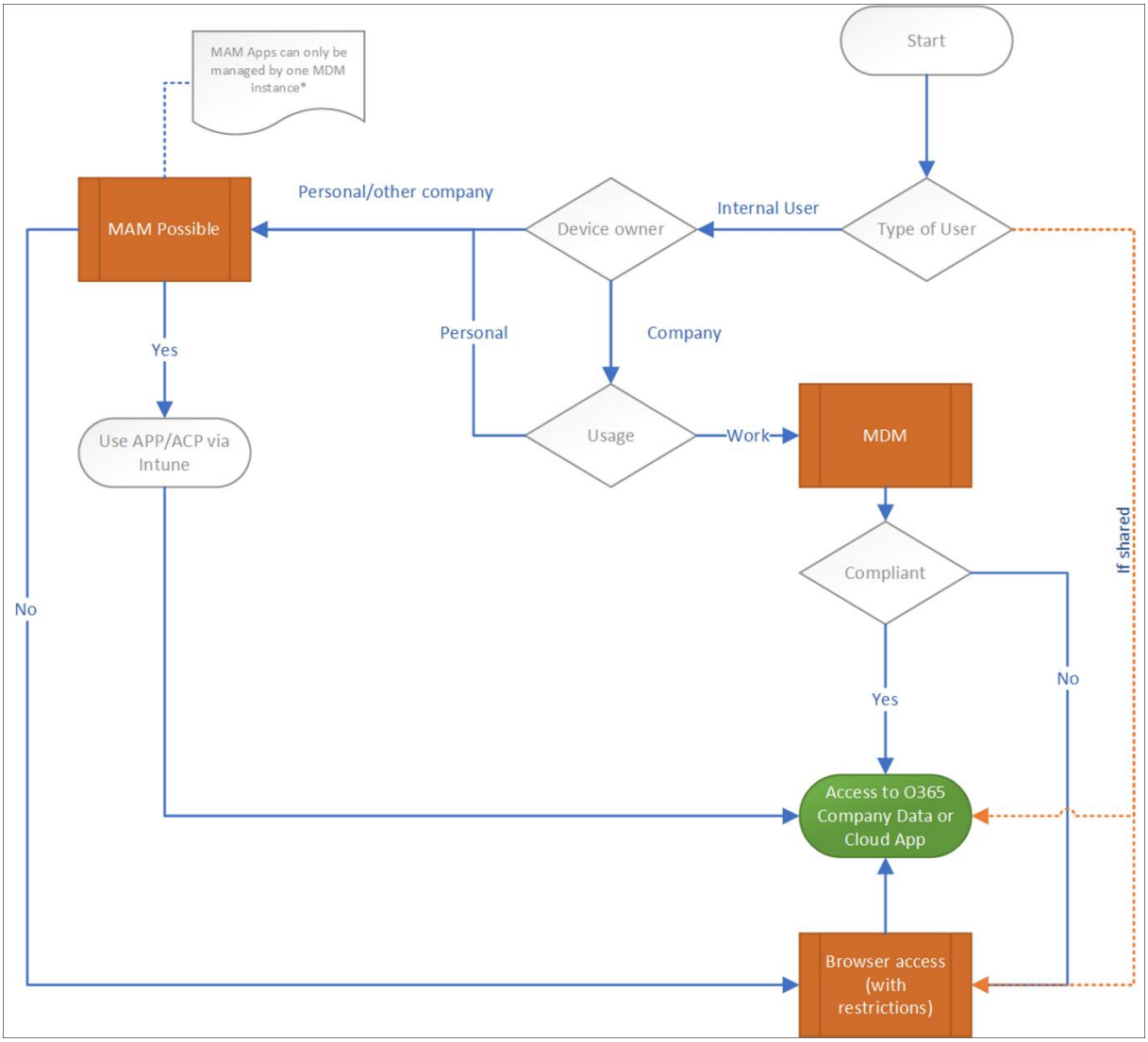
Service dependencies

Many cloud apps have dependencies to other cloud apps, Microsoft Teams is a good example since it also provides access to SharePoint Online, and Planner for example. When this situation occurs, you have to know how the application will behave, since policies may be applied either early-bound or late-bound. See the following article with more information about this: "What are service dependencies in Azure Active Directory Conditional Access?"

I've created a spreadsheet which can hopefully help you to document and write down your conditional access policies, the spreadsheet is available for download from the following location: [Conditional Access Policy Description-v1.2.xlsx]

4.1 Functional Design

The functional flowchart below gives an overview of what I want to accomplish, I always use this flowchart and adjust it where needed to determine the use cases which must be supported.



As you can see, the flowchart is situated around giving access to company data, since I think that Data is the asset you must protect using Conditional Access policies.

So basically we support several scenario's in this flowchart, let me describe some of them:

4.1.1 Guest users

In a default Microsoft 365 configuration, each user can invite Guest users into your Azure Active Directory. This is mostly done by either sharing a specific file hosted on OneDrive/SharePoint with

that Guest user, or by inviting that Guest user to a Microsoft Teams environment, where that Guest user can participate in the team.

With Conditional Access policies we can control how Guest users can access the environment. The options we have are:

4.1.2 Allow full access to the environment

When you allow full access to the environment (which is the default), Guest users can use Desktop applications to access the data hosted by your company. In teams they are able to switch to your tenant and work in the teams that they are member of just like an internal user. They can even setup synchronization of SharePoint sites and have the data in that site available on their device.

You should ask yourself If you want to allow this, this totally depends on the data you are sharing with these guest users, in my opinion, if that data is confidential you shouldn't allow that data to be one a device which you not manage. It's also advised to implement a Governance procedure for Guest users and clean up once in a while, because without that Guest users can keep unlimited access the files shared and the Teams/SharePoint sites they have access to.

4.1.3 Allow Browser/Browser restricted access to the environment

We can also disable access via Desktop clients, and offer browser based access only. In this way we have some better control since we can apply App Enforced Restrictions to the browser session and by doing so denying users the ability to download and print any company data. I've described this scenario in the following article: Limit Access to Outlook Web Access, SharePoint Online and OneDrive using Conditional Access App Enforced Restrictions. We can have the restrictions on all the data, or on just a part of the data by using the sensitivity label functionality for containers.

4.1.4 Device Owner and usage

When it comes to device owner and usage, we have several options:

4.1.4.1 Company owned

Company owned devices in most cases are devices, mostly Windows and macOS laptops which are enrolled and managed using Microsoft Endpoint Manager/Intune. The device has several policies applied, and we are able to measure if the device is compliant to our security policies by using Compliance policies. Mobile devices, can also enrolled and managed, but with the current capabilities of what MAM can offer, and the way these devices are being used, I see that less often. Even though there are endless possibilities to manage mobile devices using MDM, these implementations are complex and must also be maintained.

4.1.4.2 Personally owned

Personally owned devices, are owned by the user. In my opinion it doesn't make sense to start managing those devices, and most of the time these devices aren't even suitable to be company managed. If you ask the user bringing the device if he or she wants IT to manage the device, they will probably say NO. The Bring Your Own Device (BYOD) principle was a nice idea, but when it comes to managing a device and measure its integrity by using compliance policies, in the end you have to make the choice on whether you want to manage the device as a company yes or no. Managing a device comes at a cost and you should really ask yourself if the benefits outweigh the costs.

4.1.4.3 *Company owned, personally used*

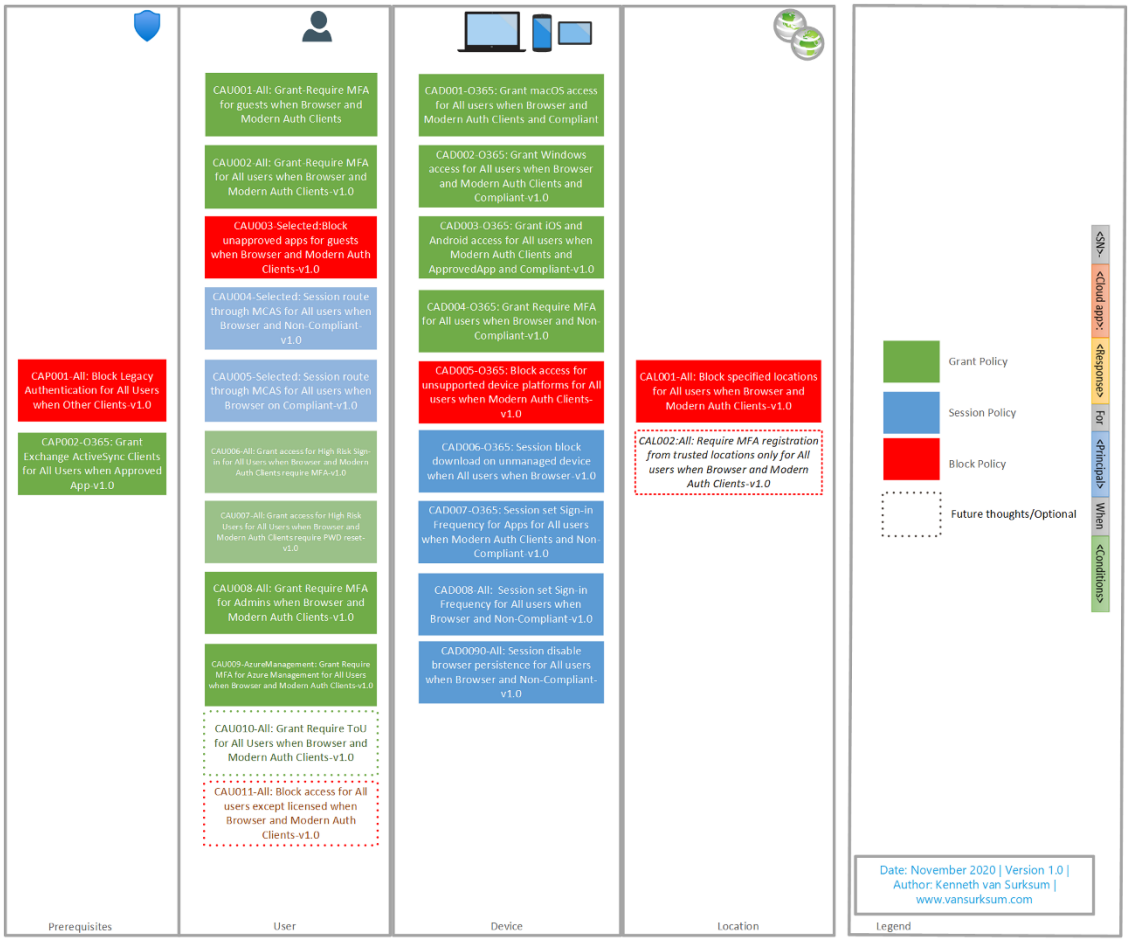
When it comes to mobile devices, this is actually the scenario encountered the most. Even though the company bought the device, the user using the device considers it personal. So besides hosting applications containing company data, the device will contain personal email, personal pictures, personal apps and more personal data as well. If that is the current status of the device, you will have a real hard story to tell your end users if you want to bring that device back under MDM and fully manage it from that point forward.

4.1.4.4 *Other Company owned*

If you work with external consultants, but do supply those consultants with an Azure AD account (because you want those consultants to act on behalf of your company) it might be that those consultants already have a device managed by their own company. One of the limitations of MAM is that you cannot have more than one MDM solution managing the App. In that case the only option left over is to allow those external consultants to read their email using the web browser (which works quite well if you ask me).

The functional flowchart is my recommendation, it might be that you have another opinion or other requirements which require you to revise the flowchart. I think that the flowchart is a good starting point, in my work as a consultant I see many implementations where the IT department started with the Conditional Access policies, not having a clear idea on what they want to accomplish functionally.

Based on the Functional specifications I created a set of Default Conditional Access policies, these policies are described in more detail in chapter 5.



4.2 Browser restrictions and configuration when using Conditional Access

Even though you are working in the browser on a compliant device, does not necessarily mean that Azure AD can detect that. Therefore, you must make sure that your browsers are configured correctly before you implement the Conditional Access policy.

Some examples I often encounter: End user is working on a compliant device, but cannot download or print files when using the web interface to connect to SharePoint online, this is caused by the App Enforced Restrictions policy being active (see: Limit Access to Outlook Web Access, SharePoint Online and OneDrive using Conditional Access App Enforced Restrictions). Or, MCAS blocks the download of a file, even though the user is working on a compliant device. (see: Extending Conditional Access to Microsoft Cloud App Security using Conditional Access App Control)

4.2.1 Browser support

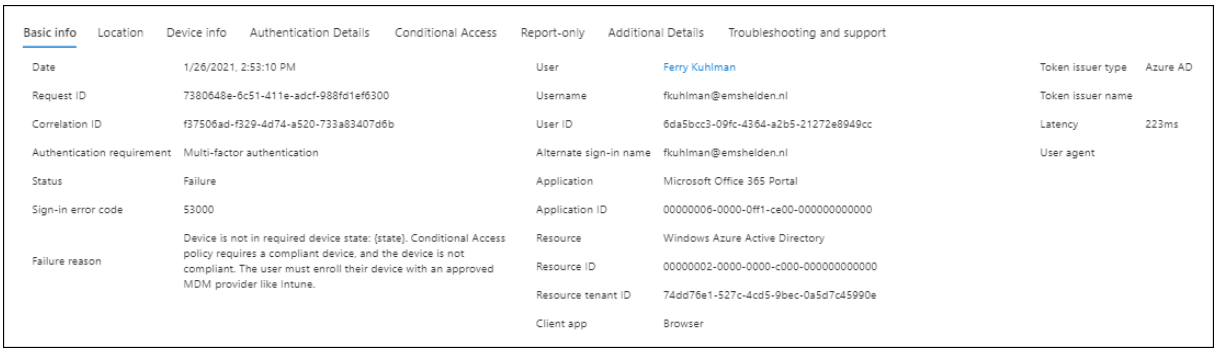
This all has to do with browser support and configuration, below is an overview of the requirements and what is, and what is not supported. Currently Microsoft supports the following browsers:

OS	Browsers
Windows 10	Microsoft Edge, Internet Explorer, Chrome
Windows 8 / 8.1	Internet Explorer, Chrome
Windows 7	Internet Explorer, Chrome
iOS	Microsoft Edge, Intune Managed Browser, Safari
Android	Microsoft Edge, Intune Managed Browser, Chrome
Windows Phone	Microsoft Edge, Internet Explorer
Windows Server 2019	Microsoft Edge, Internet Explorer, Chrome
Windows Server 2016	Internet Explorer
Windows Server 2012 R2	Internet Explorer
Windows Server 2008 R2	Internet Explorer
macOS	Chrome, Safari

4.2.1.1 Sign-in Logging

When users are using a non-supported configuration, this might reflect as followed in the Azure AD sign-in logging. As you can see the Conditional Access policy requires a compliant device before

access to the resource can be given. And in this case, our test user Ferry was working on a compliant device (you have to take my word for it).

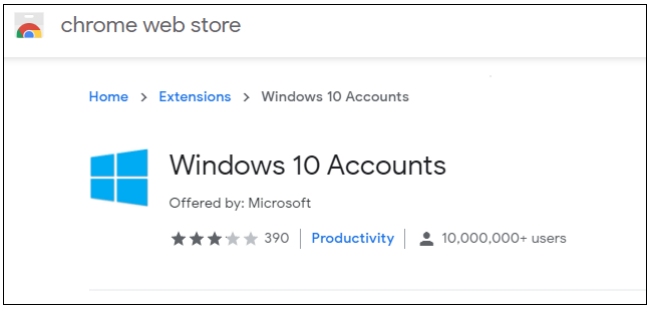


4.2.2 Mozilla FireFox

Mozilla Firefox isn't a supported browser when it comes to Conditional Access. If you configure a conditional access policy enforcing App Enforced Restrictions for example, you will experience these restrictions even when working on a compliant device. Keep in mind that there are also other browsers who use the Mozilla engine, like Tor Browser, Waterfox, and SeaMonkey to name a few. All these browsers will not work in this scenario.

4.2.3 Google Chrome

In order for the Google Chrome browser to support the device authentication you must deploy the Windows 10 accounts extension in the Chrome browser to your devices. You'll need this extension if you want to use the device compliancy within your Conditional Access policies.



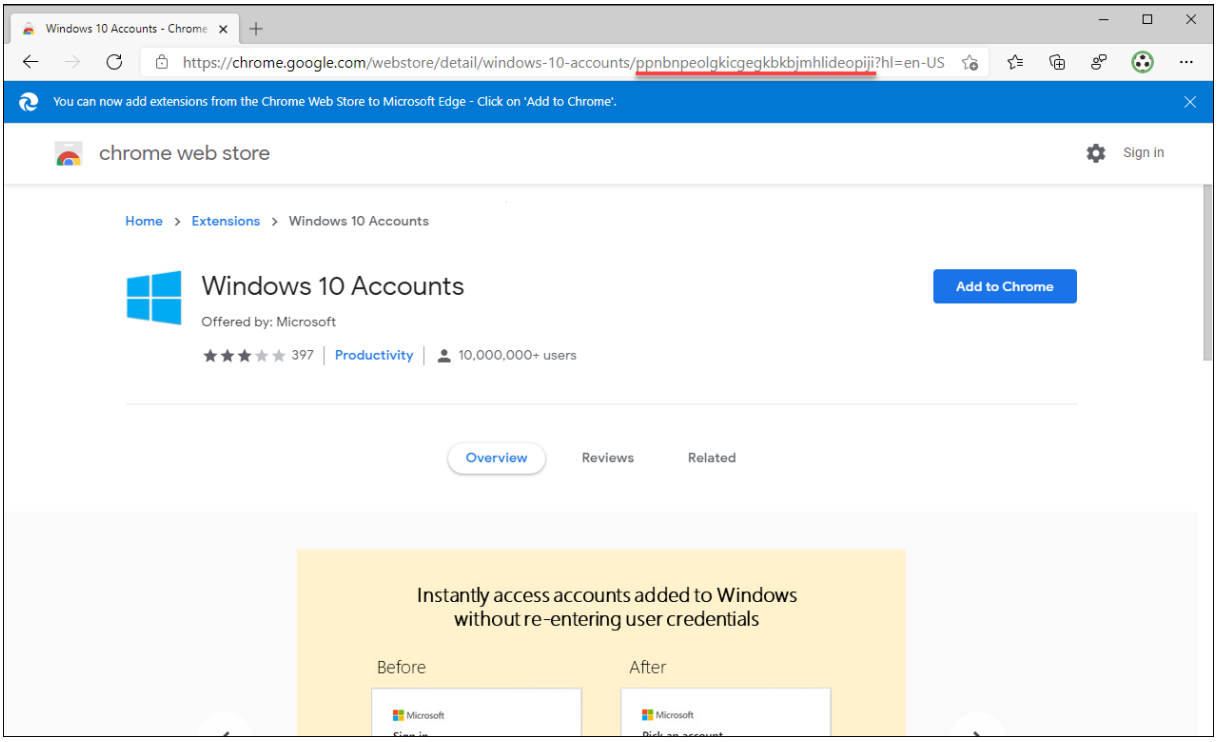
4.2.3.1 Deploying extensions for Google Chrome using Microsoft Endpoint Manager

You can configure the Google Chrome browser running on a Intune/MEM managed Windows 10 device by using a Configuration Profile with a custom profile type.

For this to work, we first need to download the Google Chrome Bundle. Within that bundle you can find a folder called ADMX. From that folder you will need the chrome.admx file. Within the ADMX file we will use the ExtensionInstallForceList parameter to define the extensions we want to have installed.

```
<policy class="Both" displayName="$(string.ExtensionInstallForcelist)" explainText="$(string.ExtensionInstallForcelist_Explain)"
key="Software\Policies\Google\Chrome" name="ExtensionInstallForcelist" presentation="$(presentation.ExtensionInstallForcelist)">
  <parentCategory ref="Extensions"/>
  <supportedOn ref="SUPPORTED_WIN7"/>
  <elements>
    <list id="ExtensionInstallForcelistDesc" key="Software\Policies\Google\Chrome\ExtensionInstallForcelist" valuePrefix=""/>
  </elements>
</policy>
```

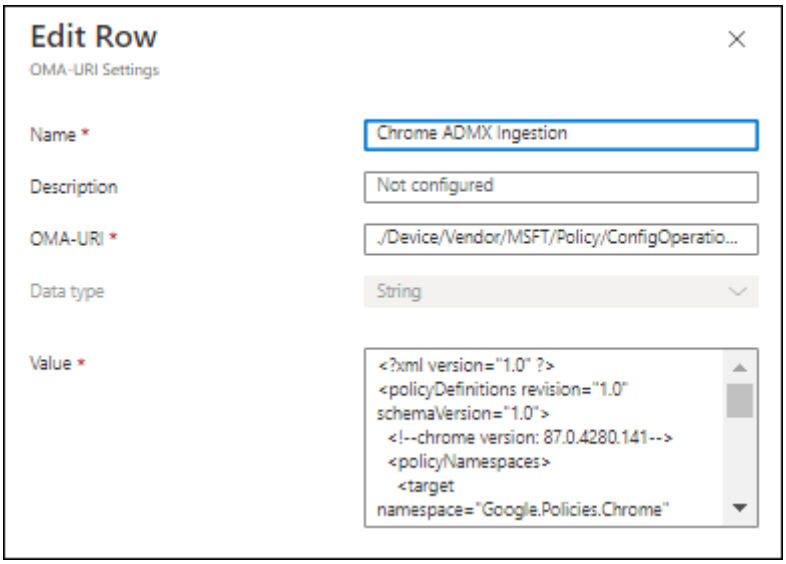
Secondly we must determine the unique identifiers for the extension(s) we want to install. You can determine this by browsing to the chrome web store. From the chrome web store we need the Windows 10 Accounts extension, which at time of writing has the following id:"ppnbnpeolgkicgegkbkbjmhlideopiji" make sure that if you are configuring this yourself to doublecheck whether the id still matches.



After downloading the ADMX file and figuring out which extensions we want to install by their ID in the chrome web store we can define our Configuration Policy.

First make sure that the custom policy ingests the ADMX file, use the following OMA-URI settings to configure this:

Name: Chrome ADMX Ingestion (can be any name, but make it easy to understand what it does)
Description: <Your description if you prefer>
OMA-URI:
./Device/Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/Chrome/Policy/ChromeAdmx
Data type: String
Value: Copy/Paste here the contents of the ADMX file.



Secondly we can define the setting we want to make as defined in the ingested ADMX file. Be very careful here.

Name: ExtensionInstallForcelist (can be any name, but make it easy to understand what it does)
Description: <Your description if you prefer>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/Chrome~Policy~googlechrome~Extensions/ExtensionInstallForcelist
Data type: String
Value: <enabled/> <data id="ExtensionInstallForcelistDesc" value="1ppnbnpeolgkicgegkbkbjmhlideopiji;https://clients2.google.com/service/update2/crx2bkbeeeffjjeopflfhgeknacdieedcoml;https://clients2.google.com/service/update2/crx"/>

In the example above I also install another extension (The Microsoft Defender Browser Protection) as you can see the value must be carefully composed.

First of all, the ExtensionInstallForceList will eventually end up as a REG_MULTISZ registry string. Which means that each entry must be separated by the Unicode character 0xF000 (or  when encoded). You can also see that the URL https://clients2.google.com/service/update2/crx is being used. That URL is needed for the browser to determine the download path once its ready to download the extension. Each extension is also numbered, so the Windows 10 Accounts extension is number 1 and the Microsoft Defender Browser Protection extension is number 2. If you want to add more use 3, 4, etc…

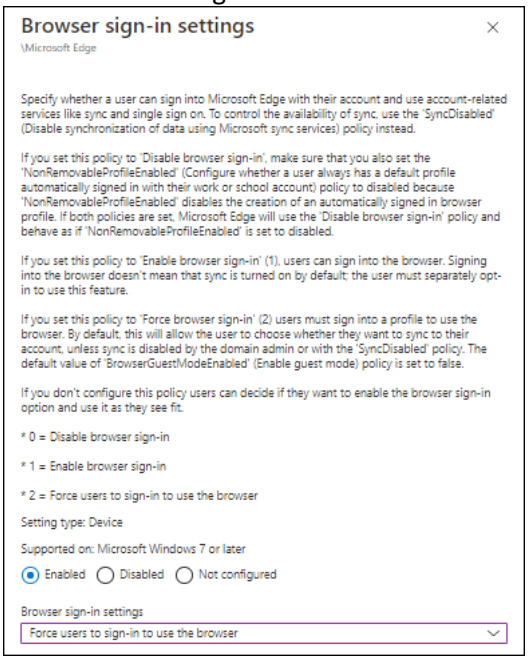
Once configured assign the policy to a group and you verify whether the necessary extensions are installed within the Google Chrome browser.

4.2.4 Microsoft Edge

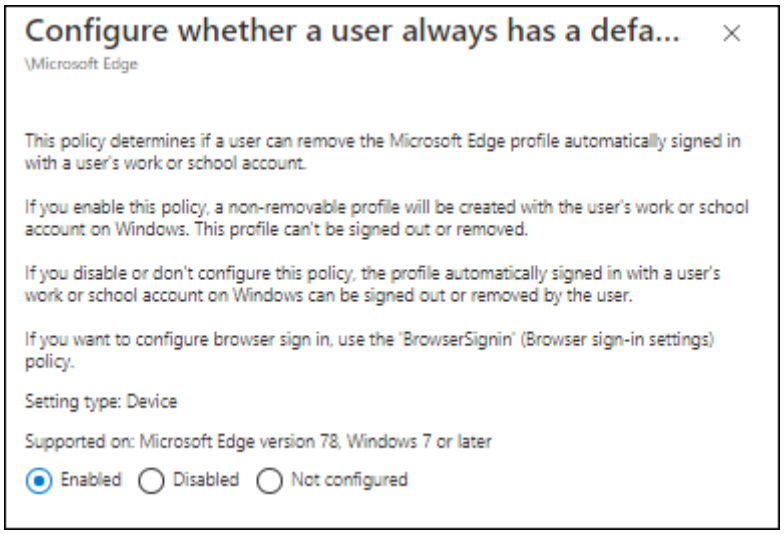
Microsoft Edge obviously supports device authentication, but whether this is being used is depending on the profile you are signed into. When you are signed into a Microsoft Edge profile with enterprise Azure AD credentials, Microsoft Edge allows seamless access to enterprise cloud resources protected using Conditional Access. On a compliant device, the identity accessing the resource should match the identity on the profile. See: [Accessing Conditional Access protected resources in Microsoft Edge] for more information.

If you want to configure this sign-in for your devices you can use two settings using a Configuration Profile with an Administrative Template.

The first setting we must modify is the "Browser sign-in settings", make sure that the setting is enabled, and that the option "Force users to sign-in to use the browser" is selected.

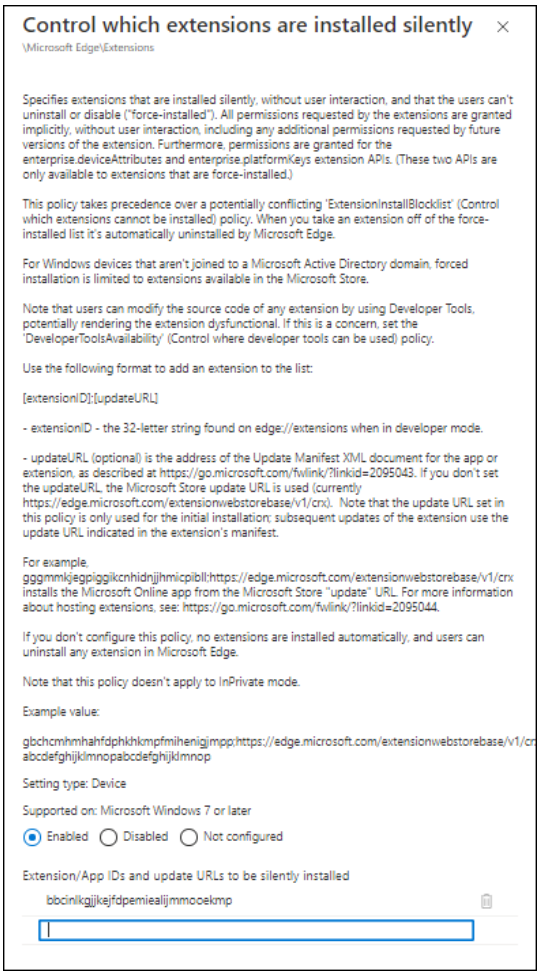


The second setting we must modify is called: "Configure whether a user always has a default profile automatically signed in with their work or school account". Make sure that this setting is enabled.



Finish the Configuration Profile and assign it to a group of your choosing.

On a sidenote, installing extensions in Microsoft Edge is much easier, since it is also part of the Administrative Templates, search for "Control which extensions are installed silently" and just supply the unique id or more in a list.



4.3 Understanding and governing reauthentication settings in Azure Active Directory

Governing when users receive authentication prompts when authenticating to Azure Active Directory (Azure AD) is depending on more than one setting, on which functionalities are in use and in which scenario you authenticate (Browser, Modern clients or other). Reauthentication can take place by asking for a single factor, like password, FIDO, the password less option in the Microsoft Authenticator app or by using Multi Factor Authentication (MFA)

So you might understand that how reauthentication must be configured really depends per company and per scenario, so luckily Microsoft provides options which you can configure.

Some examples:

- You want users to reauthenticate more often when they come from a non-managed or non-registered device
- You want users to reauthenticate more often when using a certain cloud application which you make available via Azure AD single sign on
- You might want some users in your organization to authenticate more often than others based on their risk profile

4.3.1 The settings which make up the experience

Azure AD has a default sign-in frequency of 90 days, this might seem like a long time but there are some scenario's which require the user to sign in again, like:

- A change in the compliancy status of the managed device
- Disabling the account
- Revoking the sessions for the user
- Changing the password

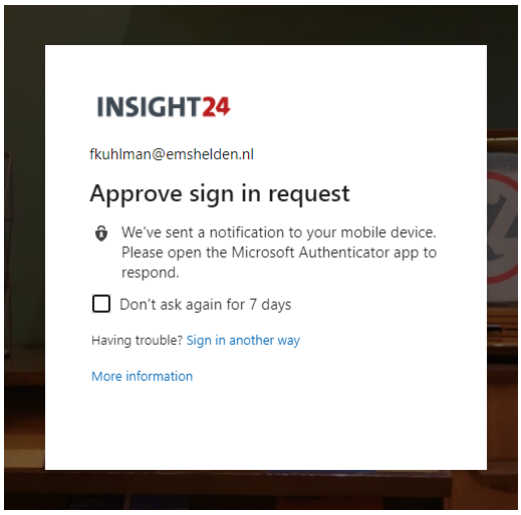
Microsoft explains this default configuration as followed: "*don't ask users to provide their credentials if security posture of their sessions has not changed*", and states: "*If users are trained to enter their credentials without thinking, they can unintentionally supply them to a malicious credential prompt.*"

Personally I think this default sign-in frequency makes sense when users work on managed devices, for other scenario's some adjustments might be necessary.

4.3.1.1 Azure Multi Factor Authentication Settings

When configuring Multi Factor Authentication you have the option to remember the multi factor authentication on trusted devices. When configured, the option allows you to bypass verifications for a specified number of days.

When using the Browser this is achieved by setting a cookie which expires after the specified time. In the screenshot below this has been set to 7 days.

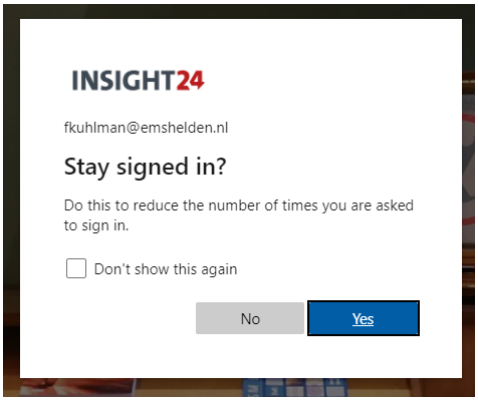


Non-browser apps use refresh tokens with a default validity of 1 hour, while validating the refresh token the check for MFA is performed as well.

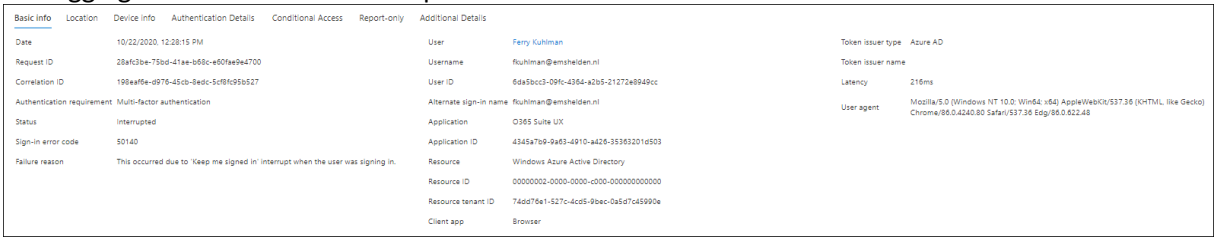
Microsoft recommends that you set this setting to 90 days, in line with the default sign-in frequency. If needed, you must revoke the MFA session to force the user to re authenticate using MFA.

4.3.1.2 Show option to remain signed in (KMSI)

Another option influencing the experience is the option "Show option to remain signed in, also known as "Keep me signed in (KMSI)" for which the configurable settings can be found in a really strange place, the Company Branding settings.

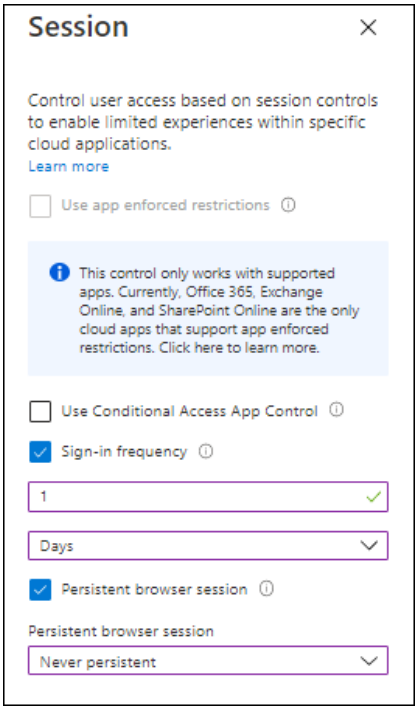


When users are presented with the Stay signed in option but abandon it, this is reflected in the Azure AD logging with a status of "Interrupted" and error code 50140.



4.3.1.3 Conditional Access

Conditional Access policies can be used to override some of the default settings in certain scenario's. By using session controls you can control how users must authenticate in different scenarios.



4.3.1.4 Sign-in Frequency

By setting the Sign-in Frequency session control you can override the default setting of 90 days to a lower setting, you can do this for example if users access your Office 365 environment from a non-managed device via the Browser, in the screenshot above we have set a sign-in frequency for 1 day.

See: Policy 1: Sign-in frequency control for an example on how to create a Conditional Access policy leveraging the sign-in frequency session control.

4.3.1.5 Persistent Browser session

A persistent browser session setting controls if users remain signed in after closing and reopening their browser window. We have 2 options here, either "Always persistent" or "Never persistent".

- This setting works correctly when "All cloud apps" are selected
- This does not affect token lifetimes or the sign-in frequency setting.
- This will **override** the "Show option to stay signed in" policy in Company Branding.
- "Never persistent" will override any persistent SSO claims passed in from federated authentication services.
- "Never persistent" will prevent SSO on mobile devices across applications and between applications and the user's mobile browser.

See: Policy 2: Persistent browser session for an example on how to create a Conditional Access policy leveraging the "Persistent browser session" session control.

4.3.2 The scenarios which make up the experience

The scenarios under which users authenticate to your Azure AD environment are diverse, and you should understand which scenarios you will encounter and want to support within your organization. Below are some topics which should be considered when defining your scenarios.

4.3.2.1 Supported applications

This sign-in frequency works with applications that have implemented Open Authorization (oAuth2) or OpenID Connect (OIDC) authentication protocols, which is supported for most applications working with Azure AD. Sign-in frequency also works with applications implementing the Security Assertion Markup Language (SAML) protocol for authorization and authentication as well.

When working in a Microsoft 365 modern environment you can assume that the Office desktop and mobile apps will work, also accessing the Office 365 web portals will support this without any issue. When it comes to 3rd party applications it depends. For example if an applications drops its cookies for some reason and therefore redirects back to Azure AD, then the sign-in frequency can be less.

4.3.2.2 Non registered devices

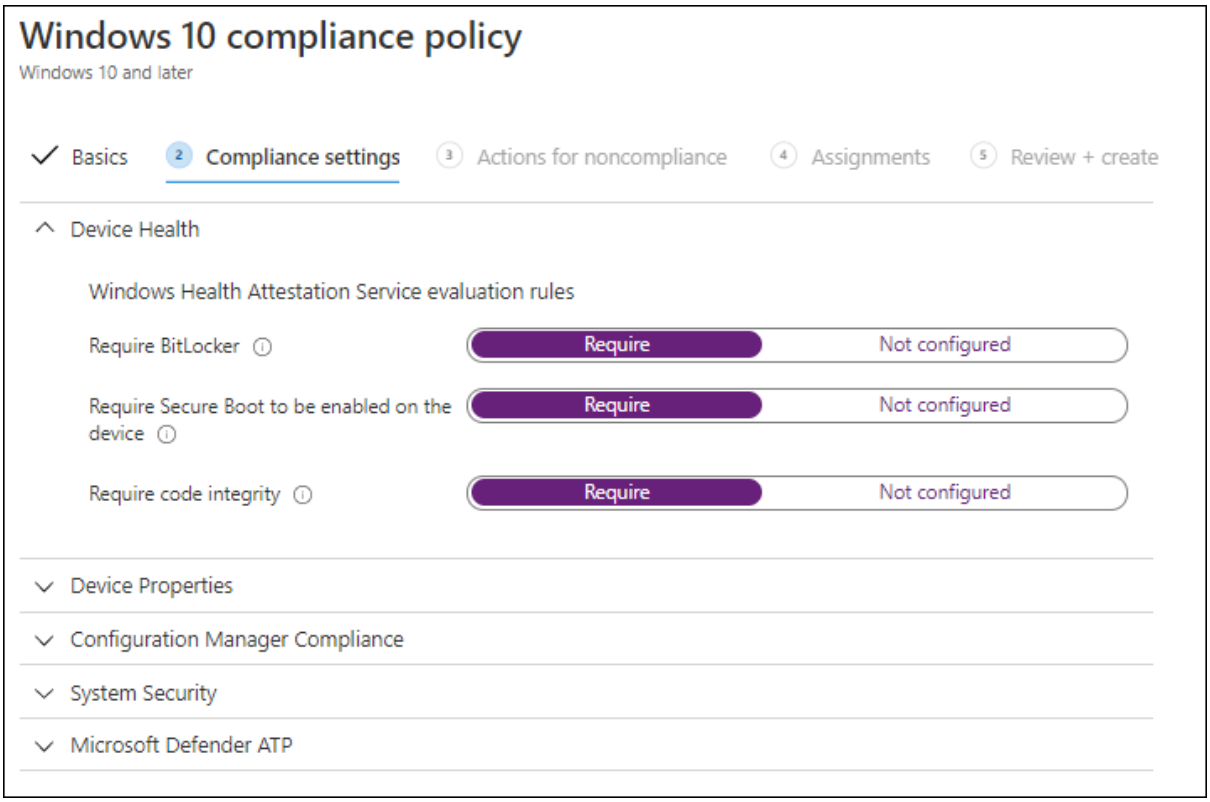
If you work on devices which are not registered in Azure AD, it might also be that applications running on top of that device are not sharing their oAuth refresh token with each other, requiring the user to authenticate multiple times.

4.3.2.3 Azure AD joined or Registered devices

Devices which are either Azure AD Joined, or Active Directory Joined/Azure AD registered via Hybrid AD join receive a so called Primary Refresh Tokens (PRT) allowing them to use this token for Single Sign-on (SSO) functionality. A PRT is valid for 14 days and continuously renewed (every 4 hours at least) as long as the user actively uses the device. For more information about how the PRT works, I suggest to read the following article: "What is a Primary Refresh Token?" on the Microsoft website.

4.3.3 Managed devices

Managed devices are devices on which you can measure compliance using Microsoft Endpoint Manager/Intune. Even though these devices are also registered, you also have the option to measure whether other security requirements are met, like for example BitLocker and Secure Boot being enabled on the device.



4.3.4 Browser used

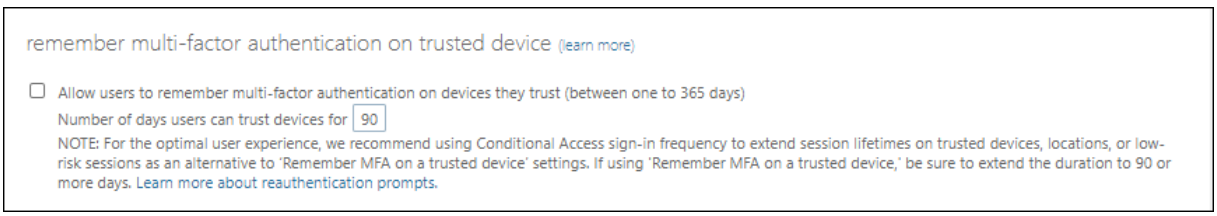
Which browser is used is an important factor when determining the scenarios. Is the browser being used an old browser like Internet Explorer, or a modern browser like Google Chrome, the new Microsoft Edge and Mozilla Firefox

4.3.5 Default settings when creating a new tenant

When you create a new tenant today, the following default settings are available.

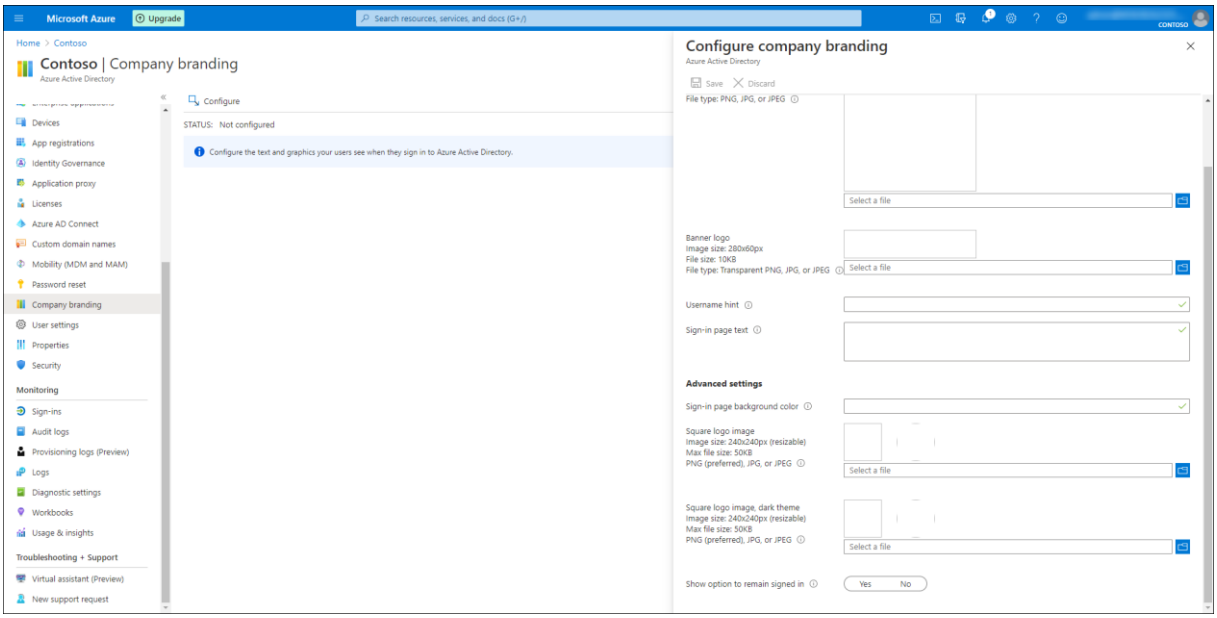
4.3.5.1 Multi factor authentication

Multi Factor Authentication by default is configured to not remember MFA on devices people trust. If you enable the setting the default number of days is set to 90 days.



4.3.5.2 Show option to remain signed in

By default in a new tenant, Company branding is not enabled and therefore the setting "Show option to remain signed in" is off.



4.3.5.3 *Conditional Access*

A new tenant does not have any Conditional Access policies configured. In the tenant I provisioned even the default security settings were not applied, but that can have something to do with the fact that I used a temporary tenant which was already hydrated.

The Default Security settings provide the following settings by default.

- Requiring all users to register for Azure Multi-Factor Authentication.
- Requiring administrators to perform multi-factor authentication.
- Blocking legacy authentication protocols.
- Requiring users to perform multi-factor authentication when necessary.
- Protecting privileged activities like access to the Azure portal.

For more information, see: [Microsoft deprecates Conditional Access baseline policies in favour of Security Defaults, here is what you need to know and do]

4.3.6 Bringing it all together

So now that we know the different options on how to configure reauthentication behavior and have an idea of the different scenarios we can face we can start designing our reauthentication scenarios.

4.3.6.1 *Managed devices*

For MDM managed devices, having the option to measure compliance gives us options to check whether the device is secure. Because of this I would advise to keep the defaults of the supplier in this case to keep the sign-in frequency to 90 days. MFA

4.3.6.2 *Managed applications*

For applications which you manage using Mobile Application Management (App Protection Policies) you can set a more strict sign-in frequency policy. For example set this 7 days using a Conditional Access policy.

4.3.6.3 Non-managed devices

On non-managed devices (devices not compliant or not hybrid AD joined), especially when accessing the environment using the web browser (which is at this moment the real manageable option to keep your company data protection IMHO), you should even set a more restrict sign-in policy and also disable browser persistence. An example would be to set the sign-in frequency to 1 day/4 hours and disable browser persistence.

Microsoft also provides some recommended settings depending on whether you have Azure AD Premium yes or no, which you can find here: Recommended settings

5 Implementing Conditional Access

Before you start implementing your Conditional Access policies you should define an implementation strategy, some things to consider are:

1. Make sure that Modern Authentication is enabled for Exchange Online (EXO) and Skype for Business Online (SfBO), SharePoint online has modern authentication enabled out of the box
2. Create 2 break glass accounts, these accounts, which are global administrator should have complex passwords and will be excluded from any conditional access policy created and must have MFA disabled (or at least on one of the two accounts). More information about creating break glass accounts can be found here: Manage emergency access accounts in Azure AD.
3. For each conditional access policy created, we will create an exclusion group, so that we can deal with exceptions in our environment. These exception groups will be setup with Access review functionality (if available) to make sure that the memberships of these groups are evaluated on a regular basis.

Based on this we can define the following steps needed to implement your Conditional Access policies in the most ideal way.

Step 1: Check if modern authentication is enabled for Exchange Online and Skype for Business Online

Steps to check if modern authentication is enabled for Exchange Online and if not enable can be found here: Enable modern authentication in Exchange Online

Steps to check if modern authentication is enabled for Skype for Business Online and if not enable can be found here: Enable modern authentication for Skype for Business Online -

Step 2: Disable the legacy authentication protocols which are not used from the Office 365 accounts

This is not a small step since this can be a major change in your environment. Basically, it starts by monitoring how Exchange Online and Skype for Business Online are accessed, based on that determine the impact of this change. It might be that clients need to be updated to a newer version or that some special applications/services are accessing your environment using legacy protocols. The inventory should make this clear though and we have options to exclude certain accounts from our setup. In the end though it should be the goal to fully eliminate the use of legacy protocols.

Reference: Protect Your Office 365 Accounts By Disabling Basic Authentication, and Microsoft is going to disable basic/legacy authentication for Exchange Online. What does that actually mean and does that impact me?

Step 3: Create 2 Breakglass accounts.

If you do not have them already, create 2 break glass accounts which will be excluded from any policy which could potentially block access to the Azure environment in case something goes wrong

See the following article from Microsoft for more information: Manage emergency access accounts in Azure AD

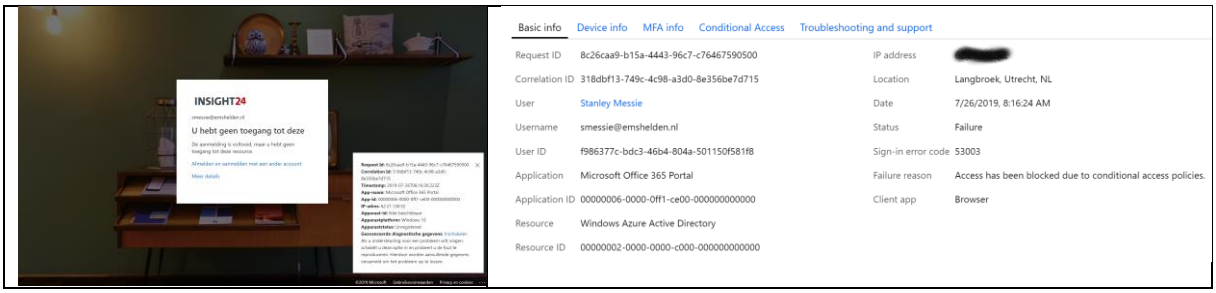
Step 4: Implement your own custom Conditional Access policies based on your Conditional Access design, make sure that for every policy that you exclude a specific group for that policy and make

sure that the break glass accounts are excluded as well. Make sure that you have a decent test plan to test the policies and modify your Conditional Access policies if needed in case something does not work as expected.

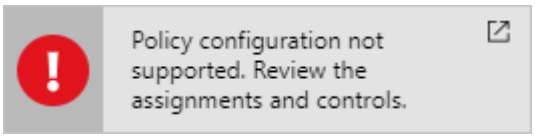
Testing conditional access policies can be quite tricky. Main reason for this is that once a policy is enabled it is not necessarily directly effective and it can take a while for it to become effective for your clients. This has to do with the fact that clients are not logging in all the time. Therefore, make sure that before you enable your Conditional Access policy that you know where you can find the logging (more on that in the next chapter) to centrally determine if something is possibly wrong. Also make sure that all company procedures are followed for a change like this.

Step 5: Create a block all policy to make sure that you do not miss anything and that holes in your conditional access strategy exist. The way this works is that you create the policy but exclude all the groups used (include and exclude groups) for the Conditional Access policies and of course exclude the break glass accounts. In this case we are **absolutely sure** that all users are covered by Conditional Access policy

Users not authorized within any of the Conditional Access groups will not be able to sign in from that point forward.



Azure has a safety feature that prevents you from creating a policy which violates the best practices for Conditional Access policies, so you cannot enable a policy for all cloud apps, for all users which denies access.



The safety feature is necessary because block all users and all cloud apps have the potential to block your entire organization from signing on to your tenant. You must exclude at least one user to satisfy the minimal best practice requirement.

Some other things to consider are:

For all the exception groups make sure that you enable the "Access review" functionality (Azure AD Premium P2 feature), for which you can find more information here:

- Use Azure AD access reviews to manage users excluded from Conditional Access policies -
- Create an access review of groups or applications in Azure AD access reviews
- Which users must have licenses?

Make sure that you have defined operational procedures on what to do if certain functionality provided by Microsoft is down. A good example of this is the fact that in the past the Microsoft Multi Factor Authentication service has been down for a significant time. Having an operational procedure

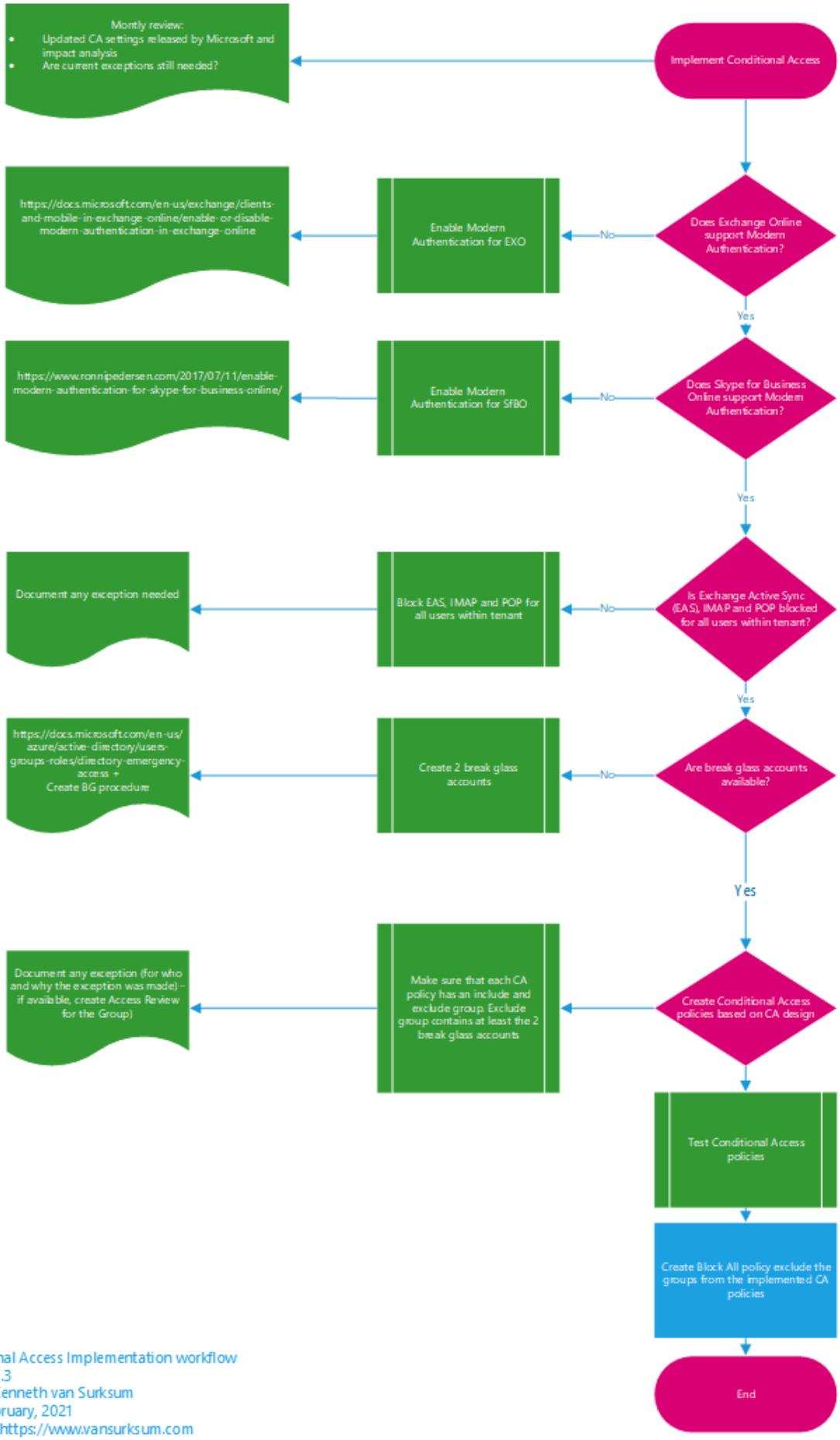
which allows you to make cloud apps available only from on premises when that happens without using MFA by disabling the "standard" policy and enabling a "temporary" policy might be a good idea.

Azure Active Directory Conditional Access changes on a regular basis, make sure that you have a procedure to check occasionally what is cooking on this topic. Make sure you understand what is coming, what is in preview and what is released. Invest time to determine the possible impact of these changes to the Conditional Access policies and requirements in place. You can see what's new in Azure Active Directory and on the Azure Updates webpage.

Some cloud apps have dependencies with other cloud apps, for example Microsoft Teams has dependencies of Exchange Online, SharePoint and Planner and perhaps even more.

More information here: What are service dependencies in Azure Active Directory Conditional Access?

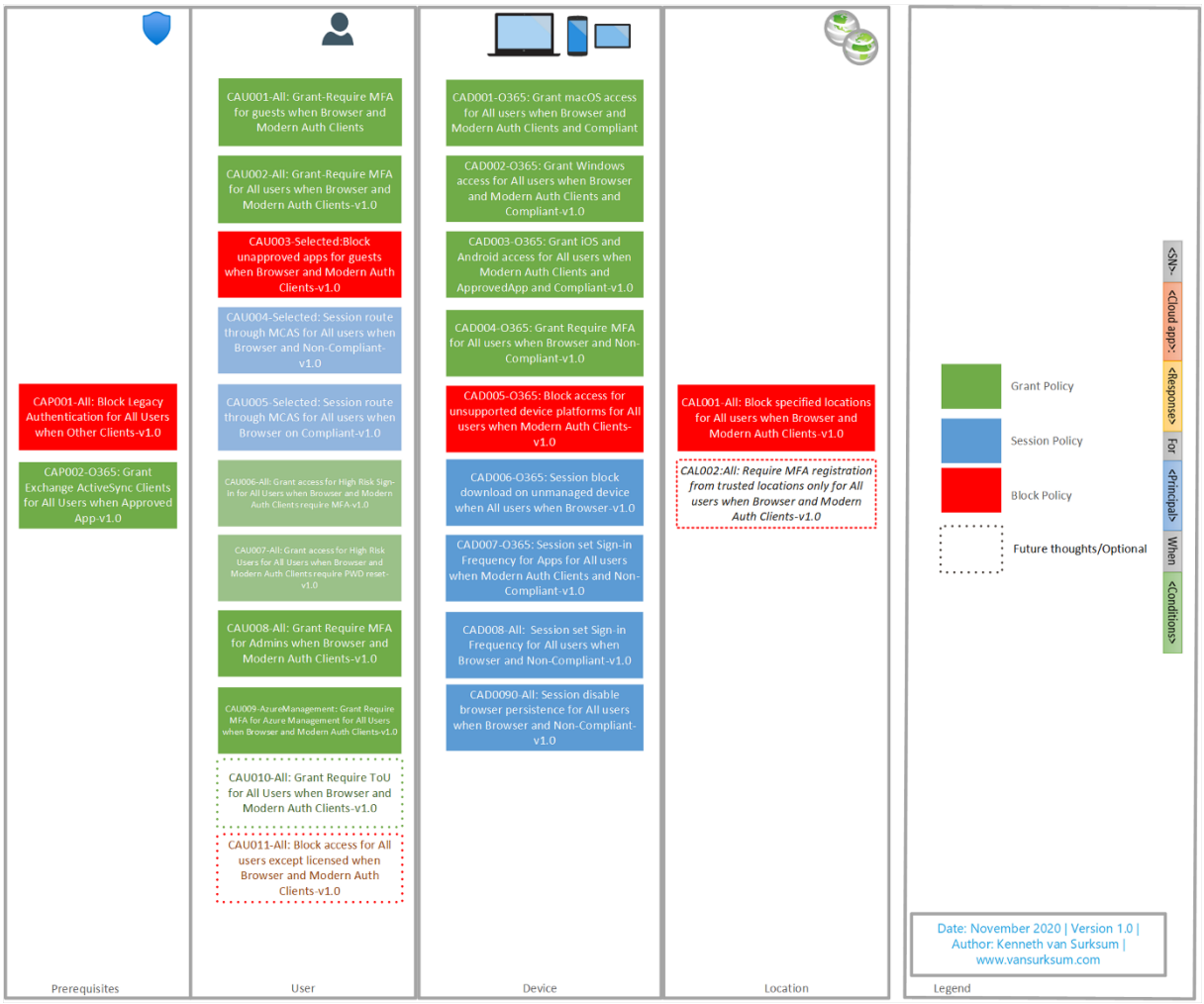
I've created a flowchart which describe the steps described above, you can download this flowchart for your reference here: Conditional Access Implementation Workflow - V1.3.pdf



Conditional Access Implementation workflow
Version 1.3
Author: Kenneth van Surksum
Date: February, 2021
Website: https://www.vansurksum.com

5.1 My recommended default set of policies

Once you have consensus about how you want to allow access to your company data, you can start describing your Conditional Access policies, below is an overview of the Conditional Access policies based on the functional design described in chapter 4.



As you can see, the policies are divided into several categories which I use in the naming of the policies as well. For the naming I use the Microsoft recommended naming policy as described in this article: [Set naming standards for your policies]

The detailed settings of the policies described, can be found in the new version of the Conditional Access Documentation spreadsheet which can be found here: [Conditional Access Policy Description-v1.2.xlsx]

For each policy, an exclusion group is created, and for each policy the group containing the break glass accounts will also be excluded from the policy.

5.1.1 Versioning

Each policy has a version number in it, by doing so we can update policies with a new version, test this new policy on a select set of users and/or Report-Only mode and then make the switch by turning the old version off and implementing the new one.

5.1.2 Prerequisites

The first category are the prerequisites and contains two policies.

5.1.2.1 CAP001-All: Block Legacy Authentication for All users when OtherClients-v1.0

This policy blocks all Legacy authentication when clients not supporting Modern Authentication are being used. For more information about this policy, please read the documentation from Microsoft: [How to: Block legacy authentication to Azure AD with Conditional Access]

Keep in mind that just disabling Legacy authentication in an existing environment isn't a good idea. The end-users might still use applications only capable of performing legacy authentication and they might need your help first to transition to apps which support modern authentication. Please read the following article for more context and how to start your own project to phase out legacy authentication. [Microsoft is going to disable basic/legacy authentication for Exchange Online. What does that actually mean and does that impact me?]

CAP001-All: Block Legacy Authentication for All users when OtherClients-v1.0				
Assignments			Access Controls	
Users	*Cloud Apps*	*Conditions*	*Grant*	*Session*
All Users	All	Client Apps: Other	Block	
Except				
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAP001-Exclude				

5.1.2.2 CAP002-O365: Grant Exchange ActiveSync Clients for All users when Approved App-v1.0

Based on the functionalities provided, there is no use case to keep using Exchange Active Sync, that is the reason that we block Exchange Active Sync clients as well. Even though the policy grants, it actually blocks access to EAS clients because an Approved App is needed. (Outlook in our case). By using this mechanism, users still using EAS actually receive a message that they must transition to an application supporting Modern Authentication. If we would use a block policy, the user simply won't get any email messages anymore.

CAP002-O365: Grant Exchange ActiveSync Clients for All users when Approved App-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Exchange Active	Grant	
Except				
AAD_AA_ConAcc-Breakglass			Require Approved App	
AAD_AA_CAP002-Exclude				

5.1.3 User

The second category contains the policies for users and contains nine policies. Some of these policies require a Azure AD Premium P2 subscription, like CAU005 and CAU006 which require Azure AD Identity Protection and CAU004 which requires Microsoft Cloud App Security(MCAS).

5.1.3.1 CAU001-All: Grant Require MFA for guests when Browser and Modern Auth Clients-v1.0

This one makes sure that guest users are required to use Multi Factor Authentication (MFA) when accessing resources that you host.

CAU001-All: Grant Require MFA for guests when Browser and Modern Auth Clients-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
Guest and External Users *Except* AAD_AA_ConAcc-Breakglass AAD_AA_CAU001-Exclude	All	Client Apps: Browser Mobile Apps and Desktop Clients	Grant Require multi-factor authentication	

5.1.3.2 CAU002-All: Grant Require MFA for All users when Browser and Modern Auth Clients-v1.0

This policy requires each user to use MFA when accessing cloud apps.

CAU002-All: Grant Require MFA for All users when Browser and Modern Auth Clients-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users *Except* Guest and External Users *And* AAD_AA_ConAcc-Breakglass AAD_AA_CAU002-Exclude	All	Client Apps: Browser Mobile Apps and Desktop Clients	Grant Require multi-factor authentication	

5.1.3.3 CAU003-Selected: Block unapproved apps for guests when Browser and Modern Auth Clients-v1.0

With this policy, you can create a list of Cloud Apps for which guest users are not allowed to use them. These apps can be apps containing sensitive company data for example

CAU003-Selected: Block unapproved apps for guests when Browser and Modern Auth Clients-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
Guest and External Users *Except* AAD_AA_ConAcc-Breakglass AAD_AA_CAU003-Exclude	<Selected>	Client Apps: Browser Mobile Apps and Desktop Clients	Block	

5.1.3.4 CAU004-Selected: Session route through MCAS for All users when Browser on Non-Compliant-v1.0

With this policy you can route the session through MCAS and its reverse-proxy capability, allowing you to either block downloads and monitor the session for strange behavior. In this example we block downloads for Cloud Applications specified if the device is not compliant.

CAU004-Selected: Session route through MCAS for All users when Browser on Non-Compliant-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	<Selected>	Client Apps: Browser		Use Conditional Access App Control: Block downloads (Preview)
Except		Device state: All except Device marked as Compliant		
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAU004-Exclude				

5.1.3.5 CAU005-Selected: Session route through MCAS for All users when Browser on Compliant-v1.0

With this policy you can route the session through MCAS and its reverse-proxy capability, allowing you to either block downloads and monitor the session for strange behavior. In this example we just monitor the session on devices which are compliant.

CAU005-Selected: Session route through MCAS for All users when Browser on Compliant-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	<Selected>	Client Apps: Browser Mobile Apps and Desktop Clients		Use Conditional Access App Control: Monitor (Preview)
Except				
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAU005-Exclude				

5.1.3.6 CAU006-All: Grant access for High Risk Sign-in for All Users when Browser and Modern Auth Clients require MFA-v1.0

This policy will require MFA for sign-ins flagged as high-risk by Azure AD identity protection. See my article: [Azure AD Identity Protection deep dive] for more information

CAU006-All: Grant access for High Risk Sign-in for All Users when Browser and Modern Auth Clients require MFA-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Browser Mobile Apps and Desktop Clients	Grant	
Except		Sign-in Risk: High		
AAD_AA_ConAcc-Breakglass			Require multi-factor authentication	
AAD_AA_CAU006-Exclude				

5.1.3.7 CAU007-All: Grant access for High Risk Users for All Users when Browser and Modern Auth Clients require PWD reset-v1.0

This policy will grant access for High Risk users after but only after they have reset their password. This functionality is also provided by Azure AD Identity Protection.

CAU007-All: Grant access for High Risk Users for All Users when Browser and Modern Auth Clients require PWD reset-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Browser Mobile Apps and Desktop Clients	Grant	
Except		User Risk: High		
AAD_AA_ConAcc-Breakglass			Require Password Change	
AAD_AA_CAU007-Exclude				

5.1.3.8 CAU008-All: Grant Require MFA for Admins when Browser and Modern Auth Clients-v1.0

This policy makes sure that Admins must always use MFA before signing in to any cloud application.

CAU008-All: Grant Require MFA for Admins when Browser and Modern Auth Clients-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
User Account Administrator SharePoint Service Administrator Security Administrator Password Administrator Helpdesk Administrator Company Administrator Exchange Service Administrator Conditional Access Administrator Billing Administrator Authentication Administrator	All	Client Apps: Browser Mobile Apps and Desktop Clients	Grant	
Except				
AAD_AA_ConAcc-Breakglass			Require multi-factor authentication	
AAD_AA_CAU008-Exclude				

5.1.3.9 CAU009-AzureManagement: Grant Require MFA for Azure Management for All Users when Browser and Modern Auth Clients-v1.0

This policy makes sure that MFA is required when the Azure Management portal is requested. The reason for this policy is that when using PIM, your admin users might first go to the Admin portal, to request their rights using PIM afterwards. See: [Lessons learned while implementing Azure AD Privileged Identity Management (PIM)] for more information.

CAU009-AzureManagement: Grant Require MFA for Azure Management for All Users when Browser and Modern Auth Clients-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All	Windows Azure Service Management API	Client Apps: Browser Mobile Apps and Desktop Clients	Grant	
Except				
AAD_AA_ConAcc-Breakglass			Require multi-factor authentication	
AAD_AA_CAU009-Exclude				

5.1.3.10 CAU010-All: Grant Require ToU for All Users when Browser and Modern Auth Clients-v1.0 (Optional)

This one is optional, but the policy requires users to agree to the Terms of Use (TOU) first, before they are allowed to access the resources.

CAU010-All: Grant Require ToU for All Users when Browser and Modern Auth Clients				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Browser Mobile Apps and Desktop Clients	Grant	
Except				
AAD_AA_ConAcc-Breakglass			Terms of Use	
AAD_AA_CAU010-Exclude				

5.1.3.11 CAU011-All: Block access for All users except licensed when Browser and Modern Auth Clients-v1.0 (Optional)

This one is optional as well, but I personally recommend it even though it's a risky one. It will block access to any user which is not licensed. Make sure that you also exclude your admins from this policy. If you implement this policy you can really govern who can access the environment, but requires careful planning.

CAU011-All: Block access for All users except licensed when Browser and Modern Auth Clients-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users *Except* AAD_AA_ConAcc-Breakglass AAD_AA_CAU011-Exclude License groups	All	Client Apps: Browser Mobile Apps and Desktop Clients	Block	

5.1.4 Device

The device policies relate to the device the user is coming from. Keep in mind here that if a device which is managed but for some reason is not compliant, other policies apply targeted to non-compliant devices. In this case for example, the user will not receive any email anymore within the Outlook desktop client, but can login to the Office portal with browser based restrictions.

5.1.4.1 CAD001-O365: Grant macOS access for All users when Browser and Modern Auth Clients and Compliant-v1.0

Only grant access if the macOS device is compliant. In the policy below we exclude Guests and External users, allowing them to use Client Applications to access a Teams environment hosted in your tenant. If you only want to allow browser access (either full access or restricted) you should exclude Guest and External users.

CAD001-O365: Grant macOS access for All users when Browser and Modern Auth Clients and Compliant-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users *Except* Guest and External Users *And* AAD_AA_ConAcc-Breakglass AAD_AA_CAD001-Exclude	Office 365	Client Apps: Browser Mobile Apps and Desktop Clients Device Platform: macOS	Grant Require device to be marked as compliant	

5.1.4.2 CAD002-O365: Grant Windows access for All users when Browser and Modern Auth Clients and Compliant-v1.0

Only grant access if the Windows device is compliant. In the policy below we exclude Guests and External users, allowing them to use Client Applications to access a Teams environment hosted in your tenant. If you only want to allow browser access (either full access or restricted) you should exclude Guest and External users.

CAD002-O365: Grant Windows access for All users when Browser and Modern Auth Clients and Compliant-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users *Except* Guest and External Users *And* AAD_AA_ConAcc-Breakglass AAD_AA_CAD002-Exclude	Office 365	Client Apps: Browser Mobile Apps and Desktop Clients Device Platform: Windows	Grant Require device to be marked as compliant	

5.1.4.3 CAD003-O365: Grant iOS and Android access for All users when Modern Auth Clients and ApprovedApp and Compliant-v1.0

Only grant access if the iOS or Android device is compliant or if an Approved Client App is used. In the policy below we exclude Guests and External users, allowing them to use Client Applications to

access a Teams environment hosted in your tenant. If you only want to allow browser access (either full access or restricted) you should exclude Guest and External users.

Microsoft is transitioning towards apps having a protection policy applied to eventually replace the Approved Apps functionality in some of the scenario's. For now using this option isn't advised yet since the Microsoft Teams app is not yet supported. See my article: [Mobile Application Management for Mobile Devices with Microsoft Endpoint Manager/Intune deep dive]

Did you know that even if your apps are managed by another company, you can switch profiles with Microsoft Edge. So in this case, even though the apps are managed by company A, you can switch the logged in session in the Microsoft Edge browser to company B requiring an Approved App as well. If you just want to be able to use any browser, don't include the Browser option, and the user will then receive "CAD006-O365: Session block download on unmanaged device when All users when Browser" which uses App enforced restrictions. (no download and no printing) just as on non-compliant Windows and macOS devices. If you require that web access on mobile devices should only be possible from a managed browser (Microsoft Edge) you must include the Browser in the Client App selection.

CAD003-O365: Grant iOS and Android access for All users when Modern Auth Clients and ApprovedApp or Compliant-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	Office 365	Client Apps: Mobile Apps and Desktop Clients	Grant	
Except		Device Platform: iOS and Andr		
Guest and External Users			Require device to be marked as compliant	
And			or	
AAD_AA_ConAcc-Breakglass			Require Approved Client App	
AAD_AA_CAD003-Exclude				

5.1.4.4 CAD004-O365: Grant Require MFA for All users when Browser and Non-Compliant-v1.0

Require MFA if the device falls out of compliance.

CAD004-O365: Grant Require MFA for All users when Browser and Non-Compliant-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	Office 365	Client Apps: Browser	Grant	
Except		Device state: All except Device marked as Compliant		
AAD_AA_ConAcc-Breakglass			Require multi-factor authentication	
AAD_AA_CAD004-Exclude				

5.1.4.5 CAD005-O365: Block access for unsupported device platforms for All users when Modern Auth Clients-v1.0

Block unsupported device platforms, like Linux and Windows Phone from accessing the environment.

CAD005-O365: Block access for unsupported device platforms for All users when Modern Auth Clients-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	Office 365	Client Apps: Browser	Block	
Except		Device Platform: Any, except: Android iOS Windows macOS		
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAD005-Exclude				

Before you enable this policy, make sure that you have no "unknown" clients accessing the environment. You should check Azure AD sign-in logging as described in the article: [Microsoft is going

to disable basic/legacy authentication for Exchange Online. What does that actually mean and does that impact me?

5.1.4.6 CAD006-O365: Session block download on unmanaged device when All users when Browser-v1.0

This policy uses the App Enforced Restrictions, blocking download of files in OneDrive/SharePoint and Outlook Web Access. See: Limit Access to Outlook Web Access, SharePoint Online and OneDrive using Conditional Access App Enforced Restrictions.

CAD006-O365: Session block download on unmanaged device when All users when Browser-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	Office 365	Client Apps: Browser		Use App Enforced Restrictions
Except		Device state: All except Device marked as Compliant		
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAD006-Exclude				

5.1.4.7 CAD007-O365: Session set Sign-in Frequency for Apps for All users when Modern Auth Clients and Non-Compliant-v1.0

With this policy, you force users using Modern Authentication Clients to reauthenticate after a specified amount of hours/days. I normally set this to once per 7 days.

CAD007-O365: Session set Sign-in Frequency for Apps for All users when Modern Auth Clients and Non-Compliant-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	Office 365	Client Apps: Mobile Apps and Desktop Clients		Sign-in Frequency: 7 Days
Except		Device state: All except Device marked as Compliant		
AAD_AA_ConAcc-Breakglass		Device Platform: iOS Android		
AAD_AA_CAD007-Exclude				

5.1.4.8 CAD008-All: Session set Sign-in Frequency for All users when Browser and Non-Compliant-v1.0

With this policy, you force users using the Browser to reauthenticate after a specified amount of hours/days. I normally set this to once per day.

CAD008-All: Session set Sign-in Frequency for All users when Browser and Non-Compliant-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Browser		Sign-in Frequency: 1 Days
Except		Device state: All except Device marked as Compliant		
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAD008-Exclude				

5.1.4.9 CAD009-All: Session disable browser persistence for All users when Browser and Non-Compliant-v1.0

This policy makes sure that the session is not persisted in the Browser when the browser is closed. See: Understanding and governing reauthentication settings in Azure Active Directory for more information.

CAD0009-All: Session disable browser persistence for All users when Browser and Non-Compliant-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Browser		Persistent Browser Session
Except		Device state: All except Device marked as Compliant		
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAD009-Exclude				

5.1.5 Location

Location based Conditional Access policies relate to the location the user is coming from. I'm personally not a fan of excluding company locations from MFA policies. I had some cases for example where company cases were excluded, but came to the conclusion that the Guest WiFi network allowing all customers used the same internet IP address, making this network trusted as well.

5.1.5.1 CAL001-All: Block specified locations for All users when Browser and Modern Auth Clients-v1.0

If your company doesn't do business in certain countries, you might as well block access from these countries. Even though there are ways to circumvent this (like using a VPN for example), it might make your security a little bit better than your neighbor.

CAL001-All: Block specified locations for All users when Browser and Modern Auth Clients-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Browser Mobile Apps and Desktop Clients	Block	
Except		Locations: Blocked Locations		
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAL001-Exclude				

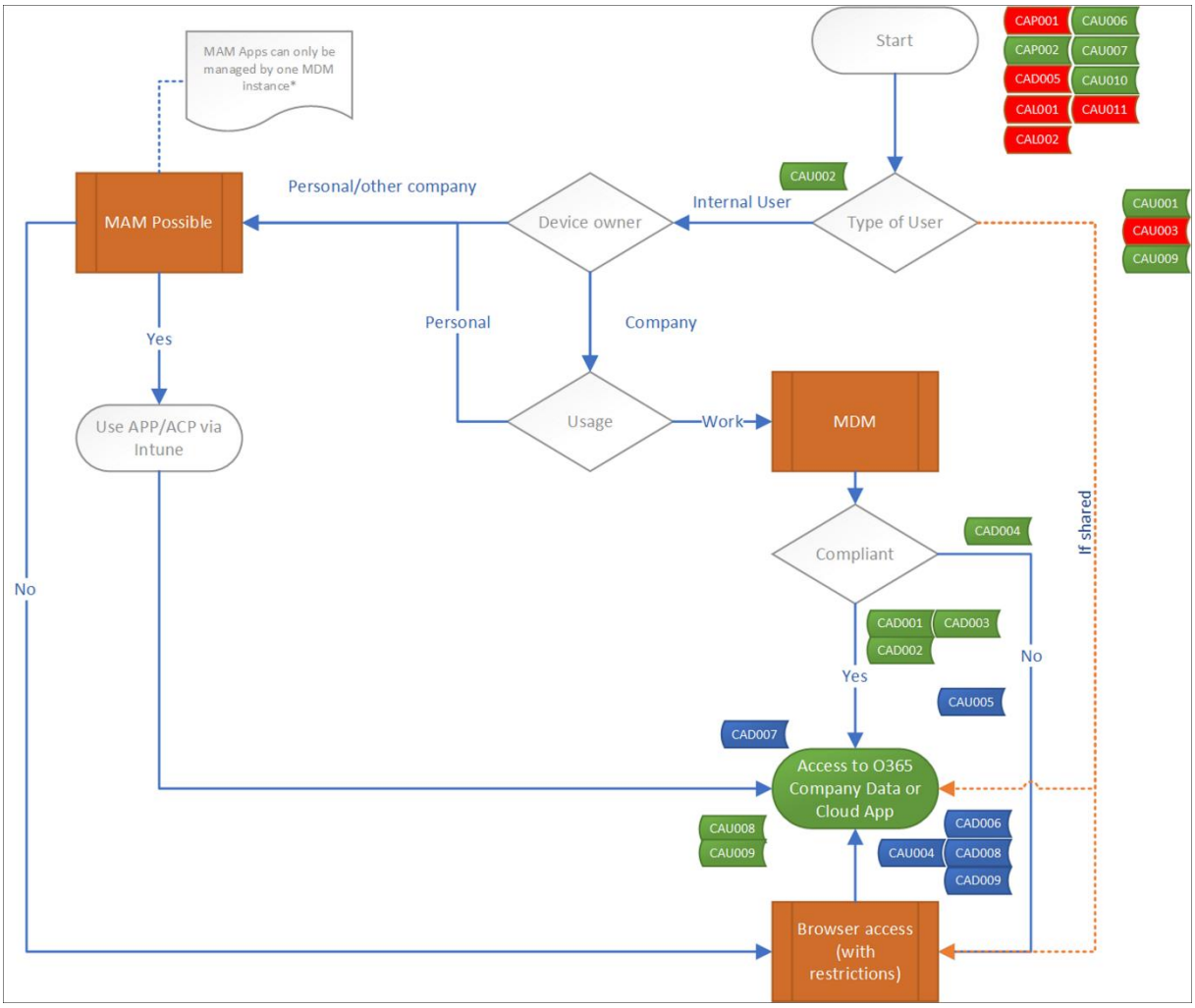
5.1.5.2 CAL002:All: Require MFA registration from trusted locations only for All users when Browser and Modern Auth Clients-v1.0

MFA registration, is something that you might want to allow only when the user is in a trusted location. For example when onboarding the user.

CAL002:All: Require MFA registration from trusted locations only for All users when Browser and Modern Auth Clients-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Browser Mobile Apps and Desktop Clients	Block	
Except	Actions: Register Security Information	Locations: All Locations, except Trusted Locations		
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAL002-Exclude				

5.1.6 Translating the functional design to the technical implementation

Below is an overview of the functional flowchart, with tags for the Conditional Access policies. Even though the position of the CA policy is not always fully correct or can be applicable in more than one scenario, it gives an idea on where the policy is applied and might help while troubleshooting.



5.2 Limit Access to Outlook Web Access and SharePoint Online and OneDrive using Conditional Access App Enforced Restrictions

One of the scenario's we can build with Conditional Access, is the scenario where we restrict access inside the web application itself. By doing so, you could for example limit the functionality of the web applications on non-managed devices, or when accessing the web application from a country where your company normally does not operate. The web applications can be configured to behave differently if the user is applicable for a Conditional Access policy where App Enforced restrictions are configured.

Within the Office 365 suite of applications, the following web applications are supported for App Enforced Restrictions:

- Outlook Web Access
- SharePoint and OneDrive

5.2.1 Configure Outlook Web Access for limited access via App Enforced Restrictions

Before you can enable Conditional Access App Enforced Restrictions you first need to enable the feature in the default OWA mailbox policy, since by default this functionality is turned off, this can be done using the Set-OwaMailBoxPolicy cmdlet as part of the Exchange Online PowerShell module.

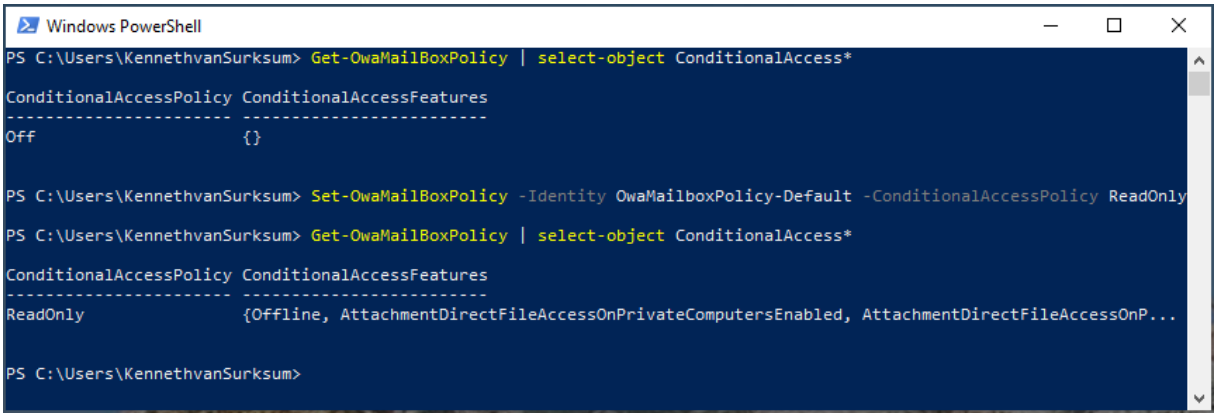
First request the current status of the OWA mailbox policy by executing the following command: Get-OwaMailBoxPolicy |select-object ConditionalAccess*. This command will return the current status of the ConditionalAccessPolicy (On or Off) and the ConditionalAccessFeatures.

If the ConditionalAccessPolicy is set to Off, you can enable the functionality which allows for restrictions when used in combination with a Conditional Access App Enforced Restriction policy. You have either the option to configure the policy in two modes:

- ReadOnly, where users can't download attachments to their local computer, and can't enable Offline Mode on non-compliant computers
- ReadOnlyPlusAttachmentsBlocked, in the ReadOnly setting viewing attachments in the browser is possible, when using this setting viewing attachments in the browser is blocked.

In this example we are going to enable the ConditionalAccessPolicy in the OWA Mailbox Policy and use the ReadOnly mode, this can be accomplished by executing the following command: Set-OwaMailbBoxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly

After executing the command make sure that you check whether the setting was succesfull by executing the Get-OwaMailBoxPolicy |select-object ConditionalAccess* command again and check whether the ConditionalAccessPolicy is set to ReadOnly



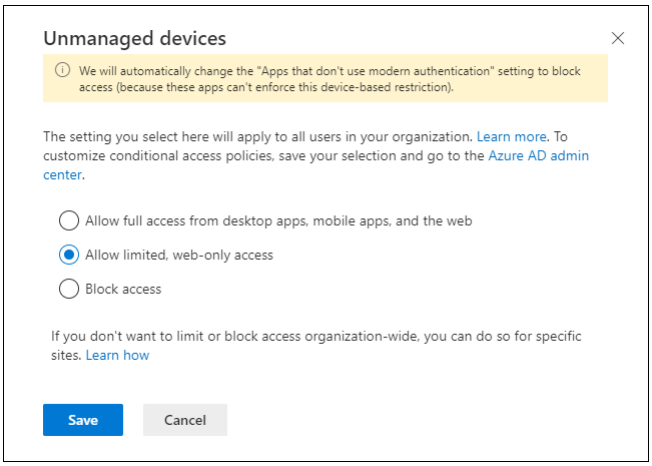
5.2.2 Configure SharePoint Online and OneDrive for limited access via App Enforced Restrictions

SharePoint Online and OneDrive can be configured in several ways. The first option is to set a Global setting which becomes effective for all SharePoint Online and OneDrive sites in your environment, and the Per site option allows you to specify options per site.

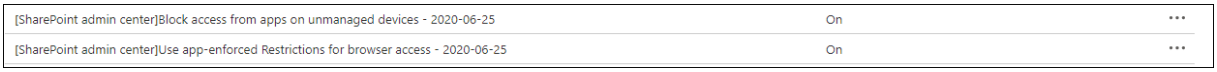
5.2.2.1 Global settings

The Global or organizational-wide settings can be configured from the SharePoint admin center (https://<tenantname>-admin.sharepoint.com). In the SharePoint Admin center select Policies | Access Control and select Unmanaged devices.

By default, for unmanaged devices the option "Allow full access from desktop apps, mobile apps, and the web" is selected, and by modifying the option to either "Allow limited, web-only access" or "Block access" you configure limited access for your whole environment.



If you configure the unmanaged devices settings, 2 new Conditional Access policies will be created. While I'm not a big fan of letting a setting like create the Conditional Access policies for you, they do provide some valuable information. I would therefore suggest to let the wizard create them, and that you turn them off immediately after creation. Keep in mind that if you are playing with these, it might be that several Conditional Access policies are created (one per day, since the day when created in defined in the name)



The first one "[SharePoint admin center]Block access from apps on unmanaged devices - 2020-06-25" has the following properties

Name: [SharePoint admin center]Block access from apps on unmanaged devices - 2020-06-25
Assignments
    Users and Groups: All Users
    Cloud apps or actions: Office 365 SharePoint Online
    Conditions
        Client apps: Modern Authentication clients
Access controls
    Grant: Require device to be marked as compliant OR Require Hybrid Azure AD joined device

So, to summarize this policy grants access to either Compliant Azure AD joined devices or Hybrid joined (AD joined, Azure AD registered) devices when the client supports Modern Authentication while accessing SharePoint Online.

So having clients which support Modern Authentication is crucial for this, I've already written a lot more on this topic for which you can find the latest information here: "May 2020 update of the Conditional Access Demystified Whitepaper, Workflow cheat sheet, Implementation workflow and Documentation spreadsheet"

The second one "[SharePoint admin center]Use app-enforced Restrictions for browser access - 2020-06-25" has the following properties

Name: [SharePoint admin center]Use app-enforced Restrictions for browser access - 2020-06-25
Assignments
Users and Groups: All Users
Cloud apps or actions: Office 365 SharePoint Online
Conditions
Client apps: Browser
Access controls
Session: Use app enforced restrictions

This conditional access policy when applicable gives SharePoint online, the signal that the limited access is applicable.

5.2.2.2 Per site settings

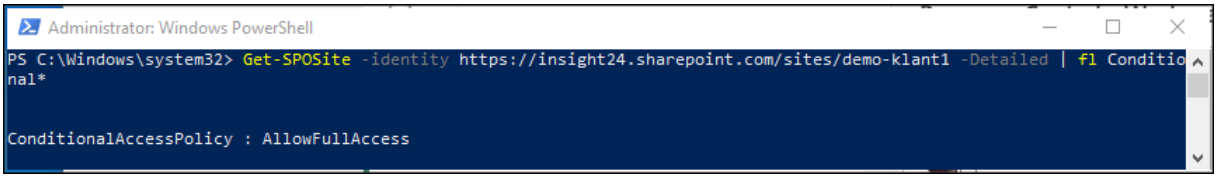
For a basic environment, having these global settings might be enough, but perhaps you want to more granularly control whether you want the limited access applied to a SharePoint or OneDrive site. This can be accomplished by using PowerShell (for now, more on that later) and described in the following section "Block or limit access to a specific SharePoint site or OneDrive" of the article: "Control access from unmanaged devices" in the SharePoint online documentation.

In order to use PowerShell you must have the SharePoint Online Management Shell installed, once installed, you can connect using

Connect-SPOService -Url https://<tenantname>-admin.sharepoint.com which will log you in, into the Management Shell

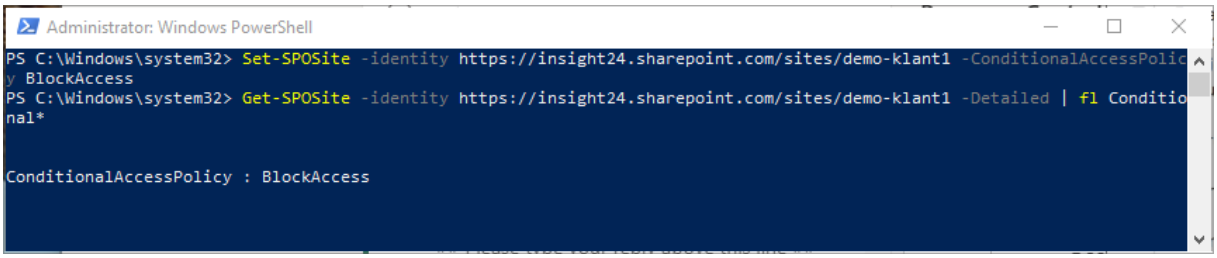
From there you can determine the current status of a particular SharePoint site using the following command.

Get-SPOSite -Identity https://<SharePoint online URL>/sites/<name of site or OneDrive account> -Detailed | fl Conditional*



As you can see, this command has a strange outcome, since on a Global level we just defined Read Only Access. Turns out that if you specify the setting on site level, this will override the global policy. So for example, you could set the option "Allow limited, web-only access" as described above in the Global policy, but define a setting to Block Access on the Site level.

You can set the policy on a site level by executing the following command: Set-SPOSite -Identity https://<SharePoint online URL>/sites/<name of site or OneDrive account> -ConditionalAccessPolicy <value>



For the ConditionalAccessPolicy parameter the following values are available:

- AllowFullAccess: The default setting
- AllowLimitedAccess: The setting allowing limited access
- BlockAccess: Blocks access

When using the AllowLimitedAccess option, you can supply additional parameters to further define the behavior, as detailed in "Advanced Configurations", for example you can provide the option -LimitedAccessFileType OtherFiles after the -ConditionalAccess AllowLimitedAccess parameter to allow users to download files that can't be previewed, such as .ZIP files.

If you have to specify this for a lot of SharePoint sites, you can of course automate these settings, but wouldn't it be nice if we could enable this from the GUI while creating the SharePoint site, or while the SharePoint site is created as part of a Teams environment .

5.2.2.3 Using sensitivity labels for containers

What if you want more granularity and want to decide on a per SharePoint site basis whether or not these App Enforced Restrictions should be applicable?

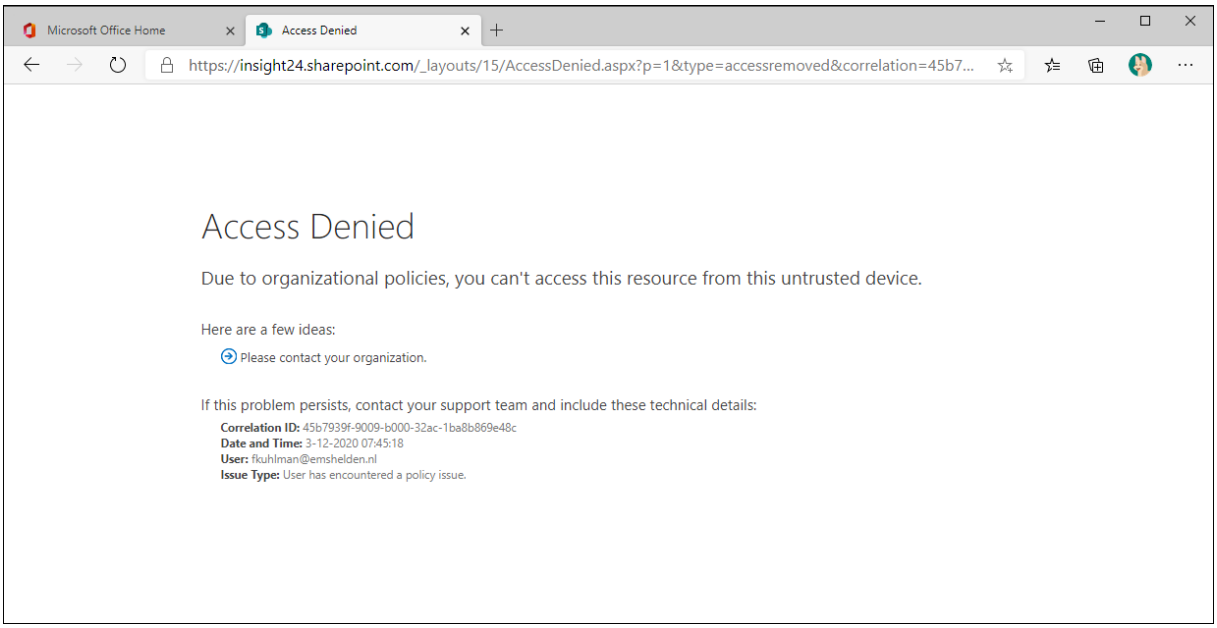
Luckily there are options.

5.2.2.3.1 Option 1: Block or limit access to a specific SharePoint site or OneDrive

This option is explained in the following article: Control access from unmanaged devices, the article explains that by using PowerShell you can limit access by using the Set-SPOSite commandlet.

Set-SPOSite -Identity https://<SharePoint online URL>/sites/<name of site or OneDrive account> -ConditionalAccessPolicy AllowLimitedAccess

When using this option, you must remove the global setting, since setting another setting on a subsite only works when its less restrictive. If you would for example set the global policy to "Allow limited, web-only access" and use the Set-SPOSite commandlet to set the Conditional Access Policy for a specific site to "Allow full access from desktop apps, mobile apps, and the web" using the AllowFullAccess parameter, the access will still be limited. If however you would set the Conditional Access Policy for a specific site to "Block Access" using the BlockAccess parameter, the access to the site will be blocked.



Using this method, has major disadvantages, since you have to execute the necessary PowerShell command for each SharePoint and OneDrive after its created. This can easily be forgotten and can lead to inconsistency

5.2.2.3.2 Option 2: Use Sensitivity labels for Containers

There is far more to tell when it comes to Sensitivity labels then explained in this blogpost. For this blogpost we are going to make use of Sensitivity labels for contains, which can be used to define certain settings when creating a Teams or SharePoint environment.

By using sensitivity labels for containers we can control the following settings:

- Privacy and external user access settings
    - Use the label to determine whether the site privacy is set to Public, Private or None
    - Define whether Microsoft 365 Group owners can add Guest users to the group
- Device access and external sharing settings
    - You can determine if external sharing settings already on the site will be replaced or respected
    - You can determine the access from unmanaged devices (same options as on global level - Full, Limited and Block)

So by defining Sensitivity labels for contains we can actually determine the access from unmanaged devices setting that will be used when the Conditional Access policy which enforces the App Enforced Restrictions will be hit.

The settings of this policy is explained in my article: "Conditional Access demystified: My recommended default set of policies", the name of the policy providing this functionality is called: "CAD006-O365: Session block download on unmanaged device when All users when Browser-v1.0"

CAD006-O365: Session block download on unmanaged device when All users when Browser-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	Office 365	Client Apps: Browser		Use App Enforced Restrictions
Except		Device state: All except Device marked as Compliant		
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAD006-Exclude				

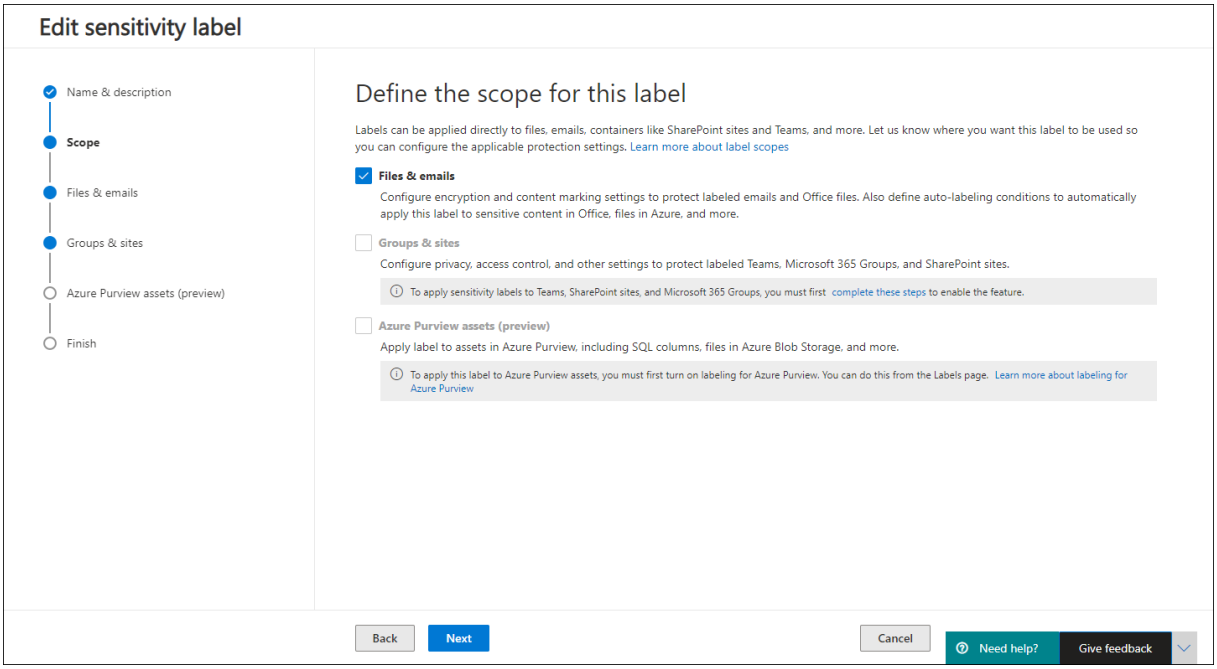
After creating the sensitivity labels you can use them for each new Teams/SharePoint site created, and based on the defined Sensitivity label the correct access from unmanaged devices setting will be applied.

This is not a perfect solution, since it will not solve the issue for all SharePoint sites already created, and you still have to build a solution for OneDrive sites which are created automatically and do not have the option to define a "default" sensitivity label at creation.

Let's go a little bit more into detail in how to build this from scratch, let's walk through the steps.

Step 1: Enable sensitivity labels for containers

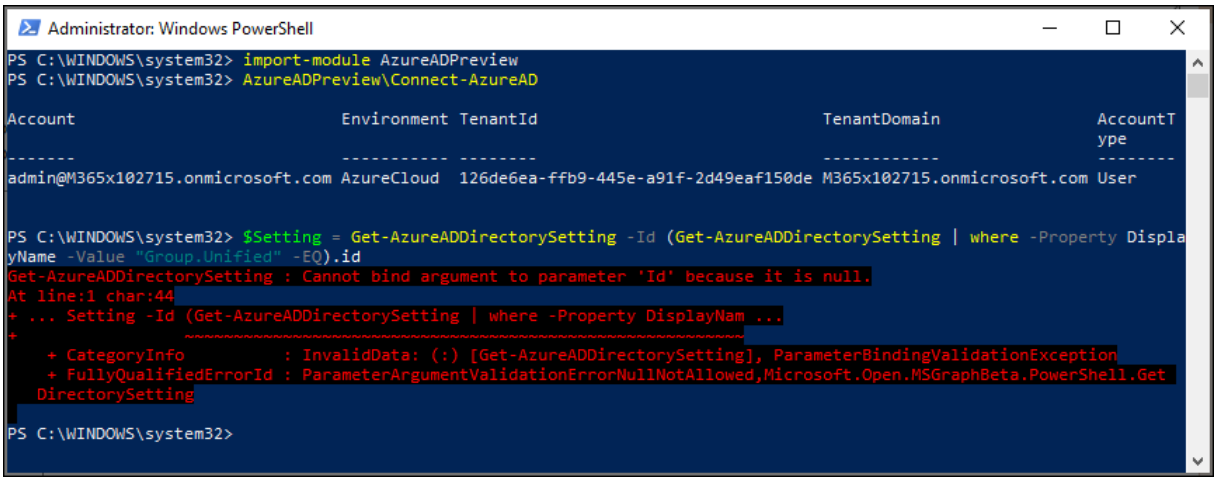
By default, support for sensitivity labels for containers is not enabled, you can easily determine this by creating a new sensitivity label or by trying to modify an existing one. If the option to select Group & sites is greyed out, you first have to execute some steps to enable this functionality.



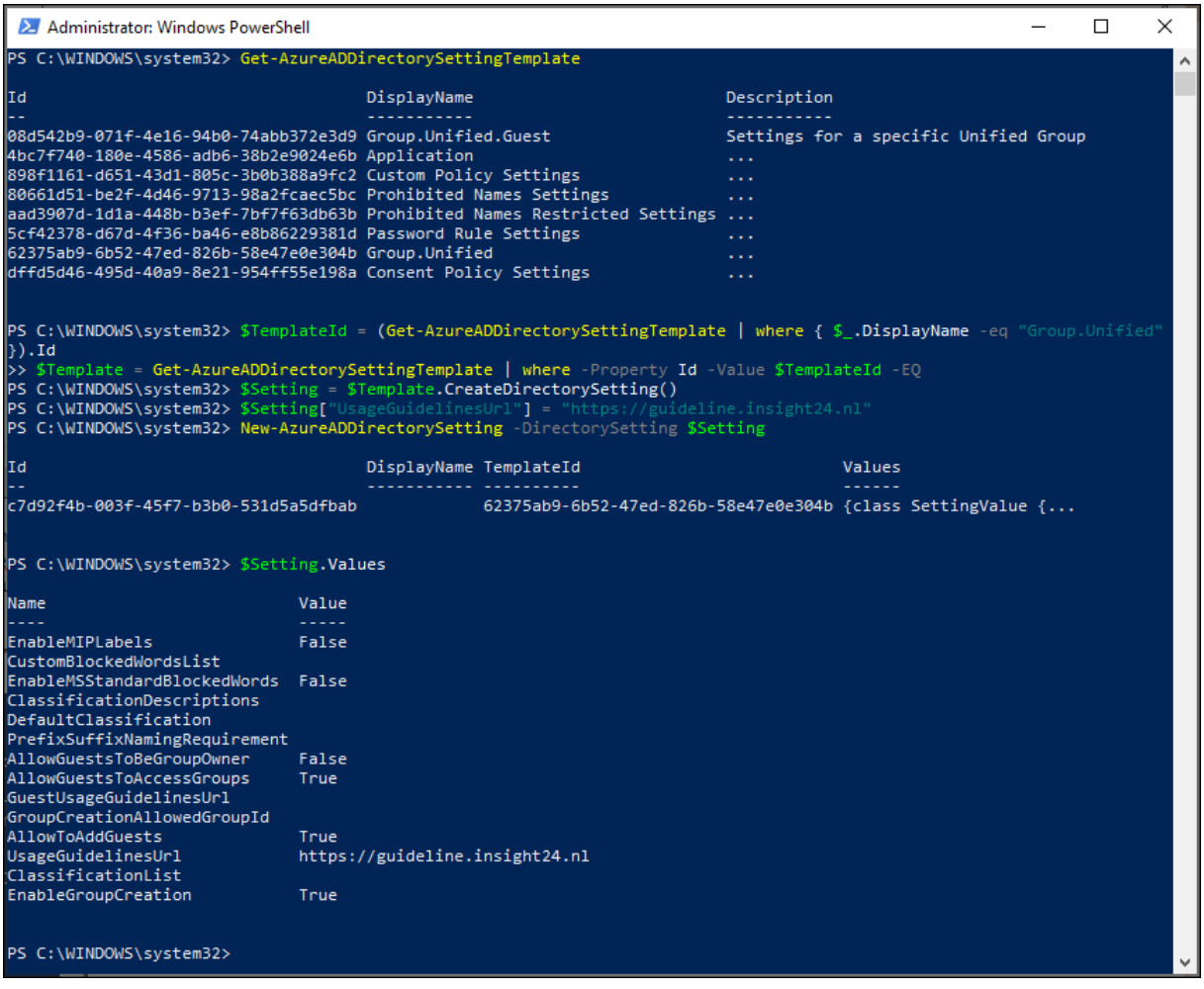
The following procedure is explained in the following article: [How to enable sensitivity labels for containers and synchronize labels] and one of the first steps is to enable the feature to apply sensitivity labels to groups as explained in this article: [Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory]

The first thing we need to do, is to import the AzureADPreview module using the import-module AzureADPreview and connect using the Connect-AzureAD commandlet. Make sure that you use the

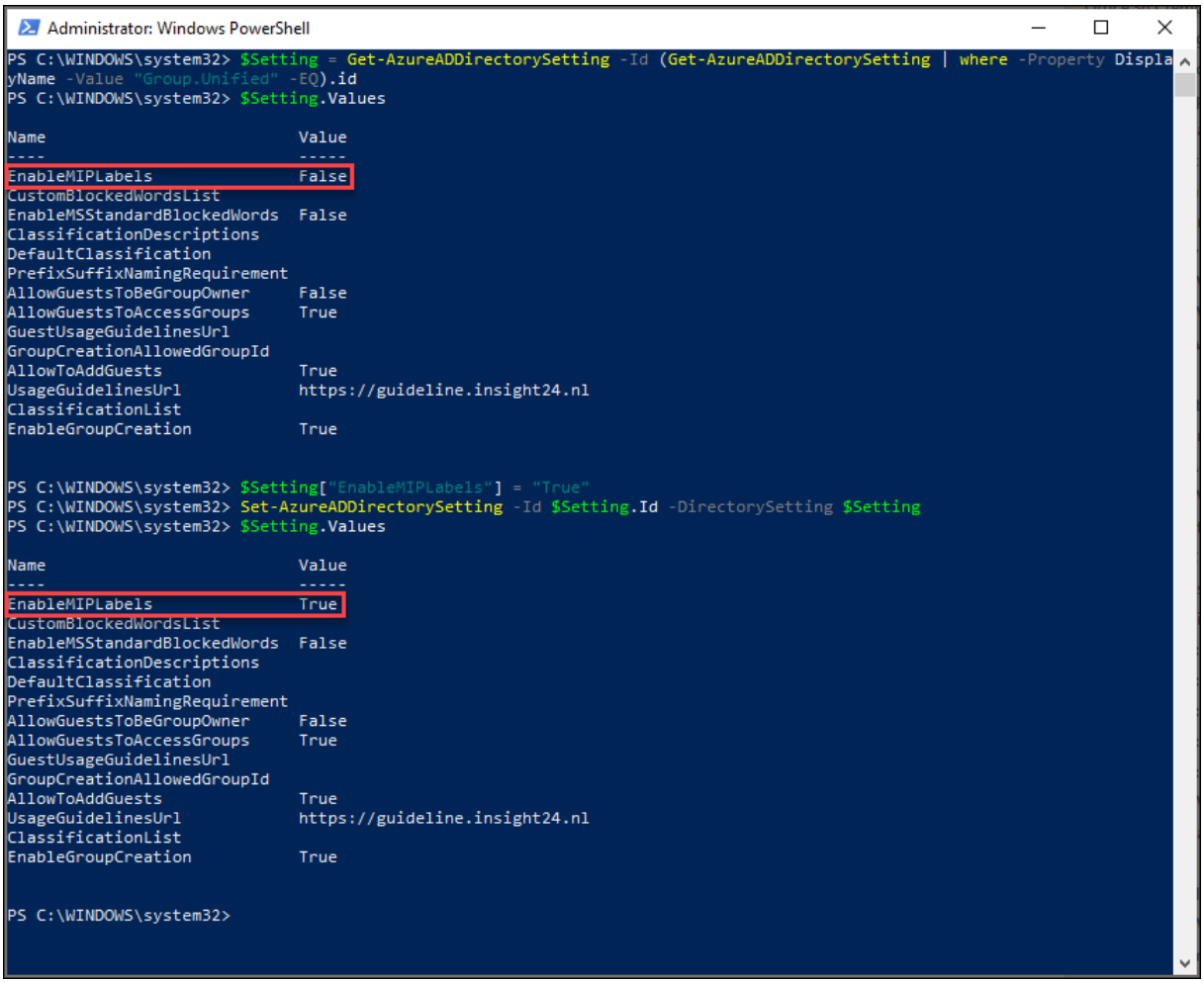
Connect-AzureAD commandlet from the Azure AD Preview module by putting AzureADPreview\ in front of it. Once connected verify if group settings have been set for the Azure AD organization. If no group settings are applied, you'll get the same error as in the picture below.



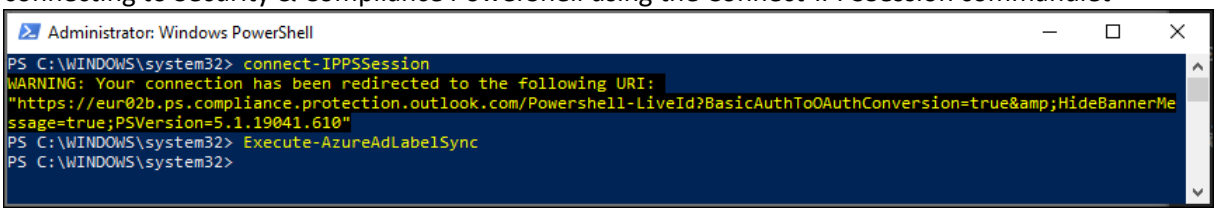
If this is the case you first have to create the settings, as explained in the following article: [Azure Active Directory cmdlets for configuring group settings]



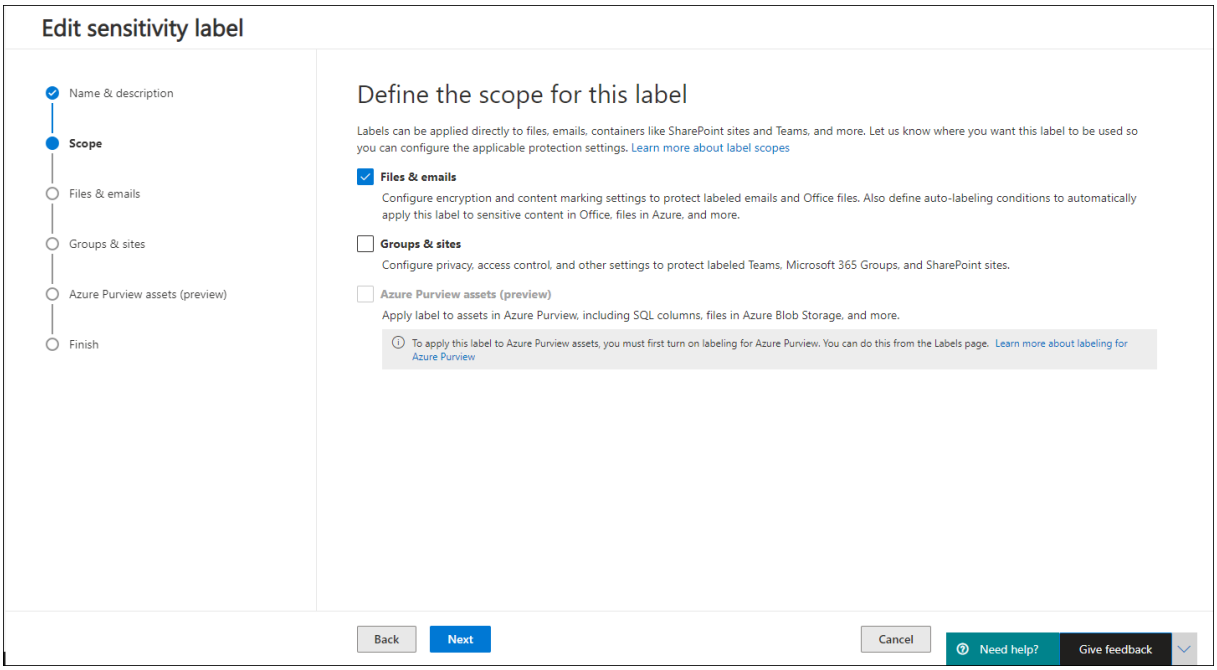
After performing these steps, you can continue with enabling the Microsoft Information Protection labels functionality as shown in the figure below. You can see that the EnableMIPLabels value is set to True.



After this is done, you must synchronize your sensitivity labels to Azure AD. You can do this by connecting to Security & Compliance PowerShell using the Connect-IPPSSession commandlet



Once finished, the end result should be that you are able to specify the "Groups & Sites" option when modifying an existing Sensitivity label or creating a new one.

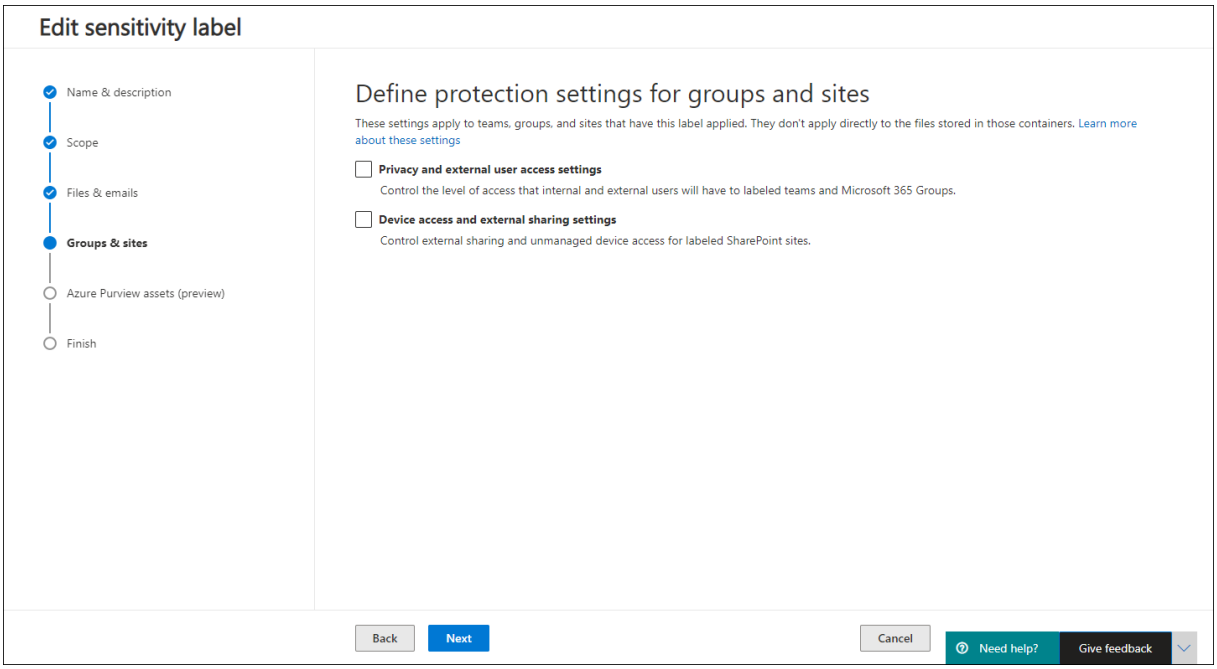


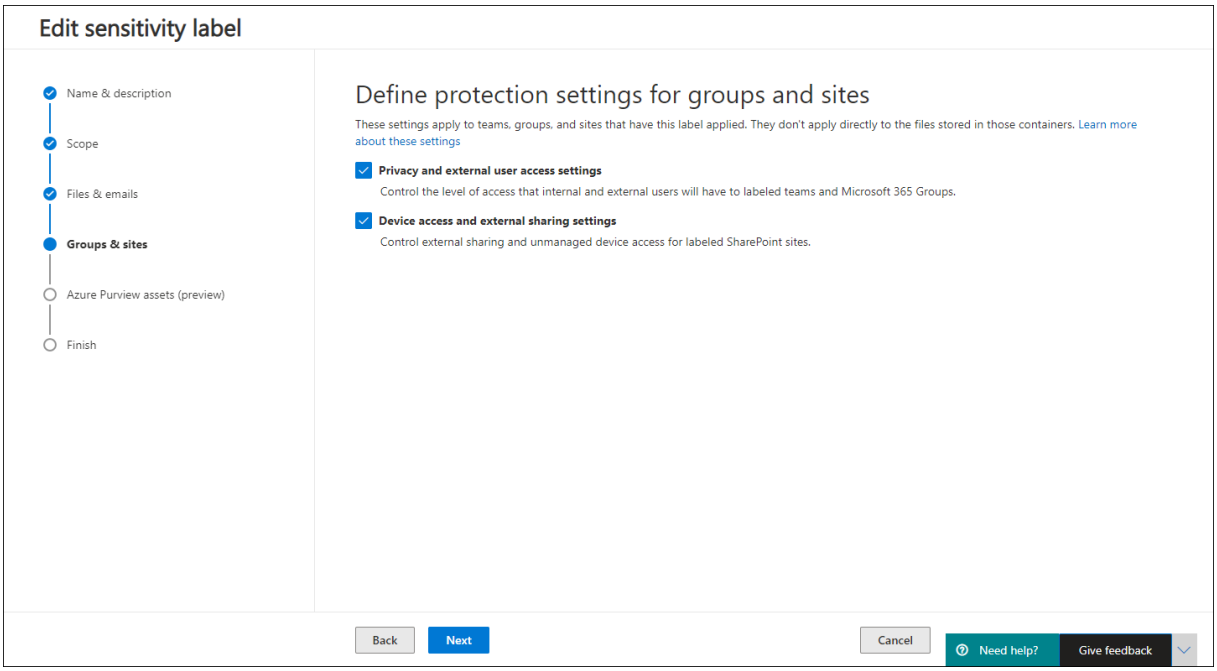
Step 2: Create or Modify your Sensitivity Labels

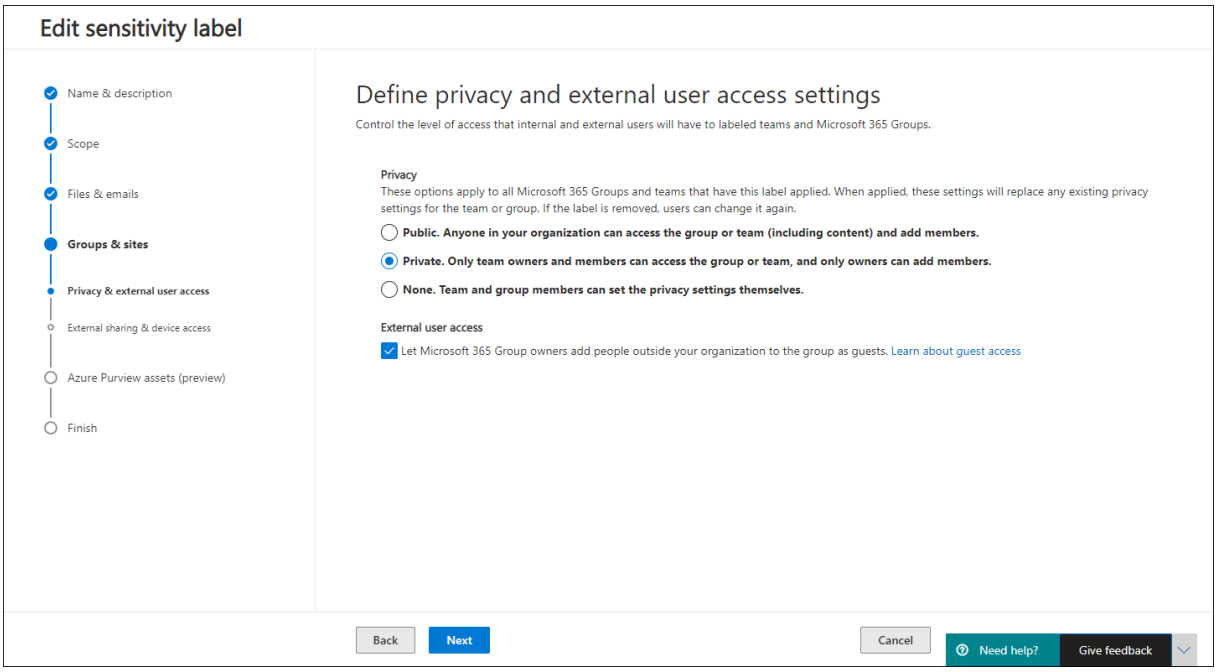
So, now that we have the functionality available, we can define our settings. In this blogpost I used the following settings

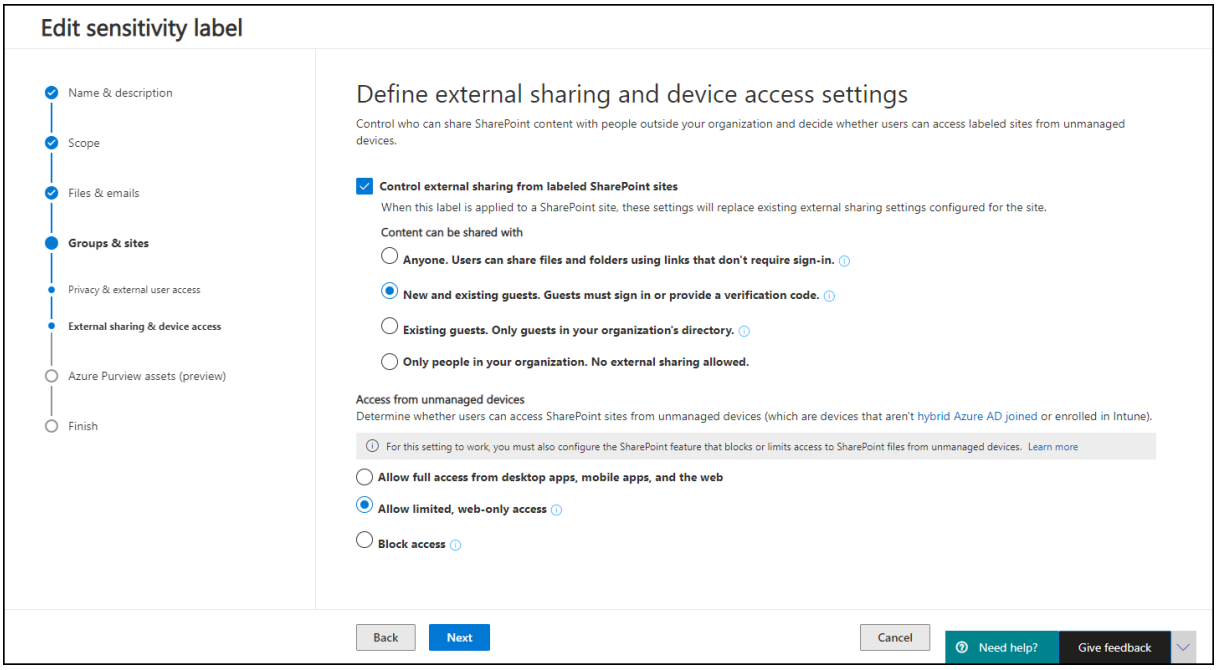
Label name	Privacy and external user access settings	Device access and external sharing settings
Public	Privacy: Public External user access: Enabled	Content can be shared with: Anyone. Users can share files and folders using links that don't require sign-in Access from unmanaged devices: Allow full access from desktop apps, mobile apps, and the web
General	Privacy: Private External user access: Enabled	Content can be shared with: New and existing guests. Guests must sign in or provide a verification code Access from unmanaged devices: Allow full access from desktop apps, mobile apps, and the web
Confidential	Privacy: Private External user access: Enabled	Content can be shared with: New and existing guests. Guests must sign in or provide a verification code Access from unmanaged devices: Allow limited, web only access
Highly Confidential	Privacy: Private External user access: Disable	Content can be shared with: Only people in your organization. No external sharing allowed Access from unmanaged devices: Block access

Next some figures showing the configuration of the Groups & Sites setting of my Confidential label


Edit sensitivity label
Name & description
Scope
Files & emails
Groups & sites
Azure Purview assets (preview)
Finish
Define protection settings for groups and sites
These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. Learn more about these settings
Privacy and external user access settings
Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.
Device access and external sharing settings
Control external sharing and unmanaged device access for labeled SharePoint sites.
Back
Next
Cancel
Need help?
Give feedback

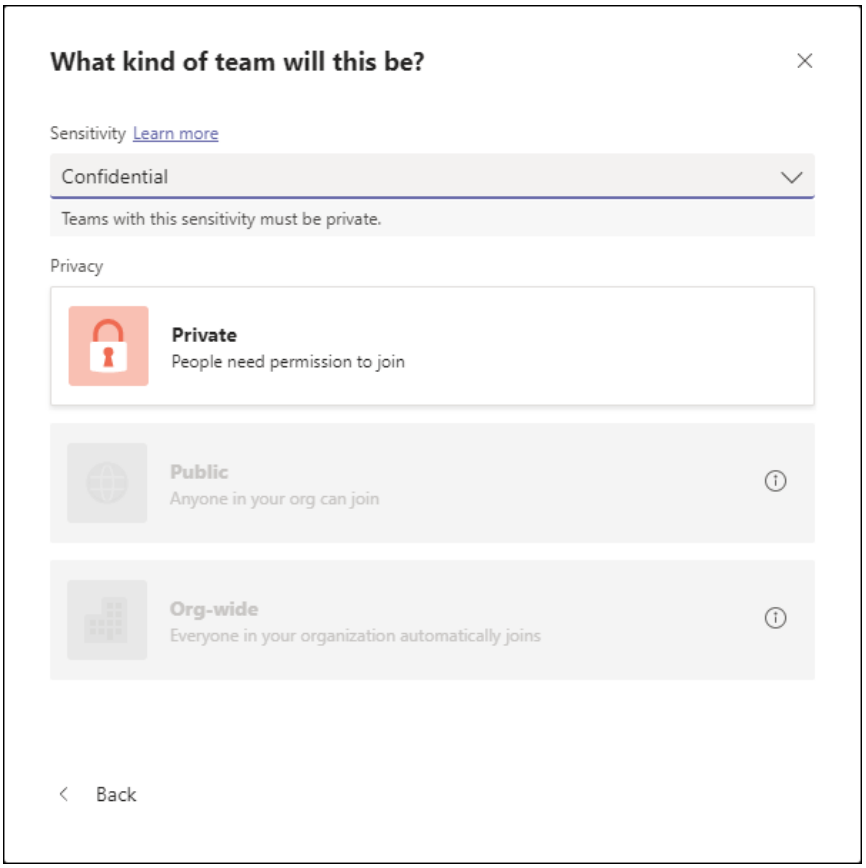

Edit sensitivity label
Name & description
Scope
Files & emails
Groups & sites
Azure Purview assets (preview)
Finish
Define protection settings for groups and sites
These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. Learn more about these settings
Privacy and external user access settings
Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.
Device access and external sharing settings
Control external sharing and unmanaged device access for labeled SharePoint sites.
Back
Next
Cancel
Need help?
Give feedback

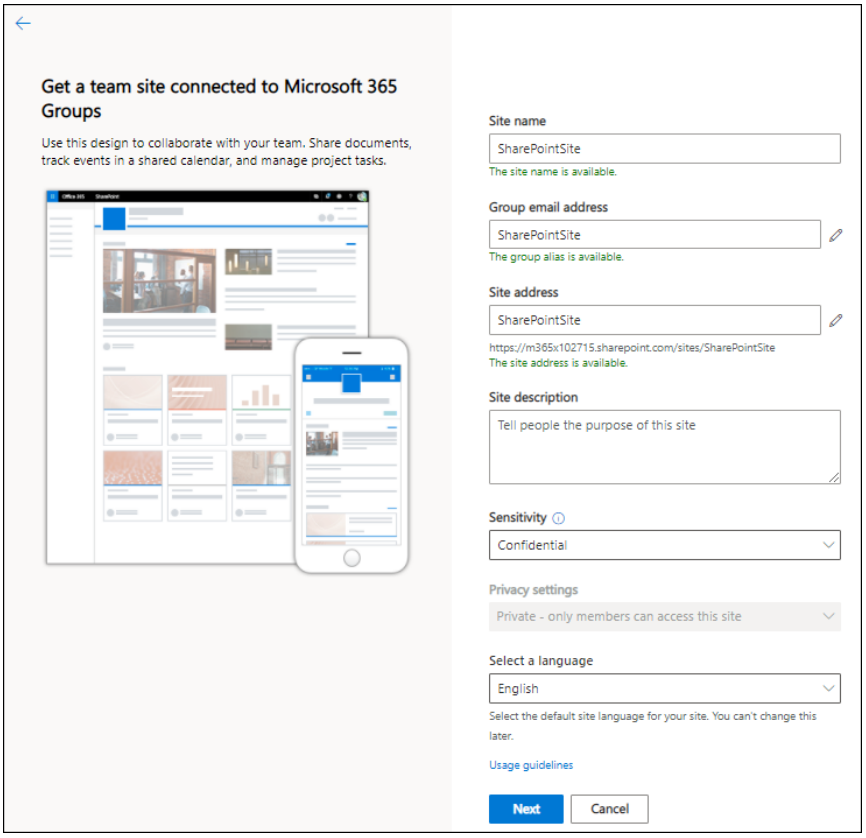


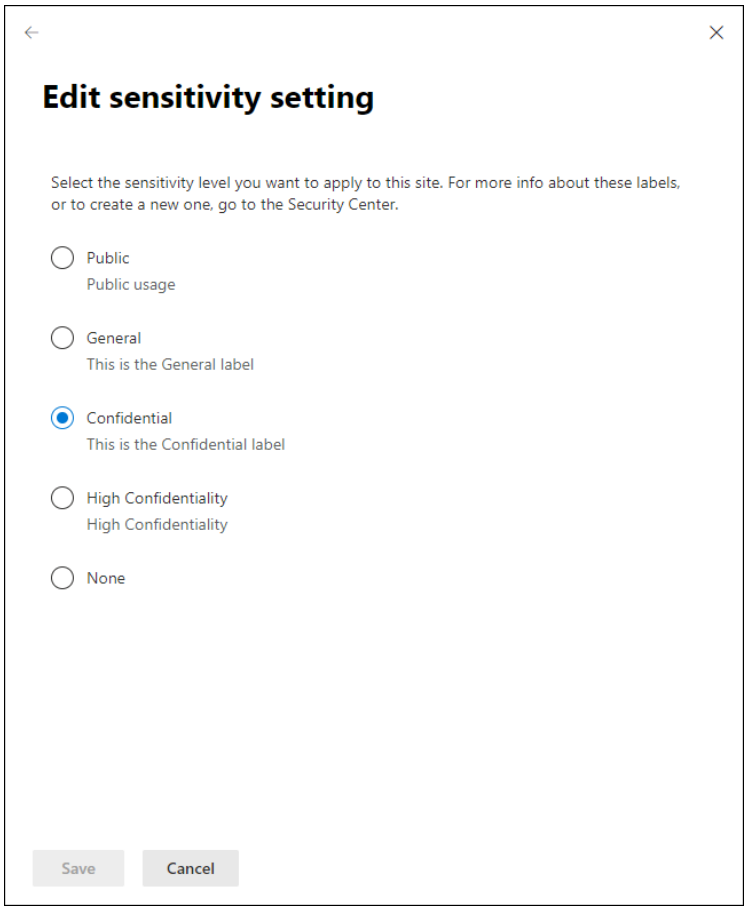


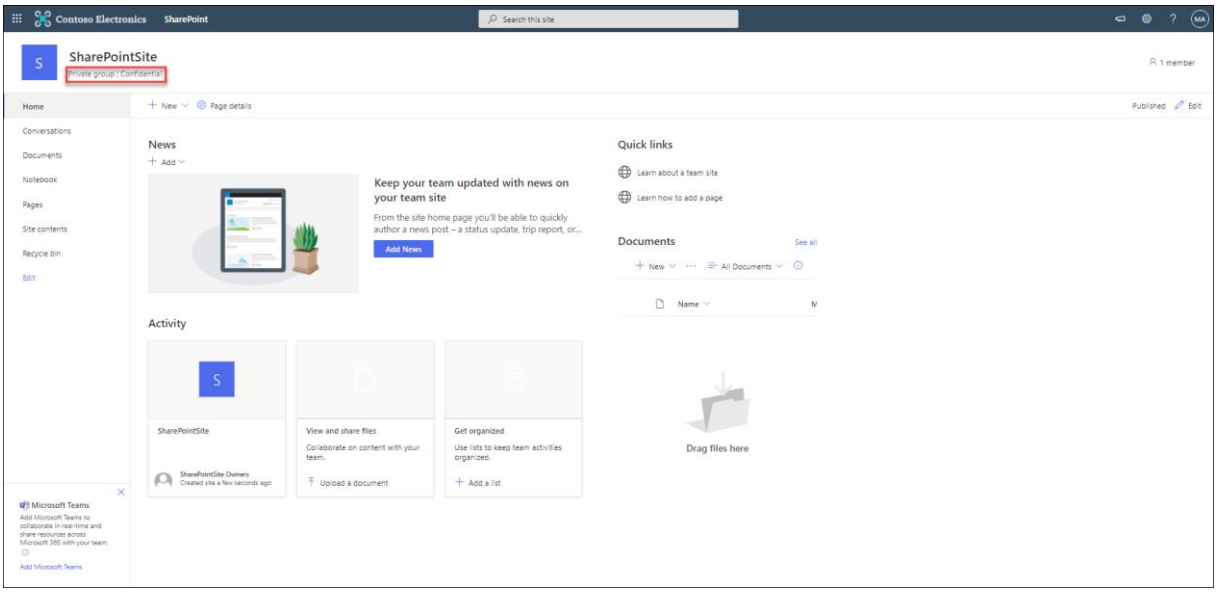
So now that the labels have been created, you will have the Sensitivity label options available when creating SharePoint and Teams environments as detailed in the slideshow below.

Note: It can take a while before you are able to use the sensitivity labels.


What kind of team will this be?
Sensitivity Learn more
Confidential
Teams with this sensitivity must be private.
Privacy
Private
People need permission to join
Public
Anyone in your org can join
Org-wide
Everyone in your organization automatically joins
Back


Get a team site connected to Microsoft 365 Groups
Use this design to collaborate with your team. Share documents, track events in a shared calendar, and manage project tasks.
Site name
SharePointSite
The site name is available.
Group email address
SharePointSite
The group alias is available.
Site address
SharePointSite
https://m365x102715.sharepoint.com/sites/SharePointSite
The site address is available.
Site description
Tell people the purpose of this site
Sensitivity
Confidential
Privacy settings
Private - only members can access this site
Select a language
English
Select the default site language for your site. You can't change this later.
Usage guidelines
Next
Cancel





5.2.2.3.3 How to provide a Sensitivity label to your already existing Teams and SharePoint sites?

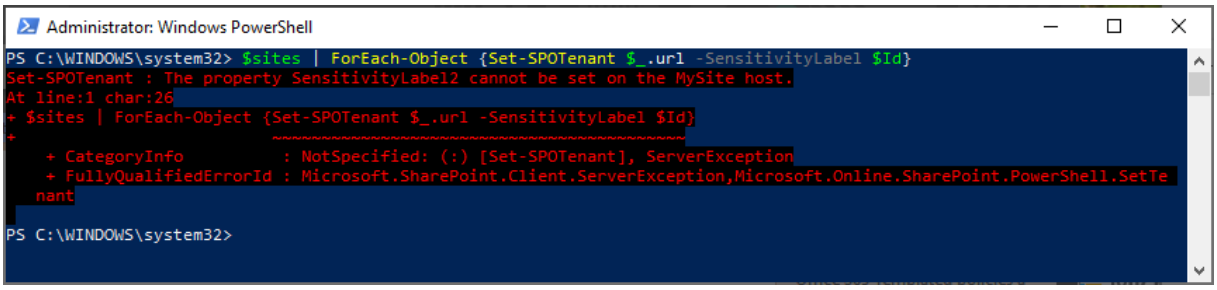
So, now that we have configured the sensitivity labels, and can use them to create new Teams or SharePoint sites, how can we handle that our current Teams and SharePoint sites are labelled as well?

For this we need PowerShell, as explained in the following article: [Use PowerShell to apply a sensitivity label to multiple sites]

Make sure that you have connected to SharePoint Online and to the Security & Compliance Center PowerShell environments by using the Connect-SPOService and Connect-IPPSSession commandlets. Retrieve the GUID of the label that you want to apply to all your existing sites using the Get-Label |ft Name, Guid command. Make sure to put the ID in a variable and enumerate the SharePoint sites by using a generic string representing your tenant. In my case this is "M365x102715"

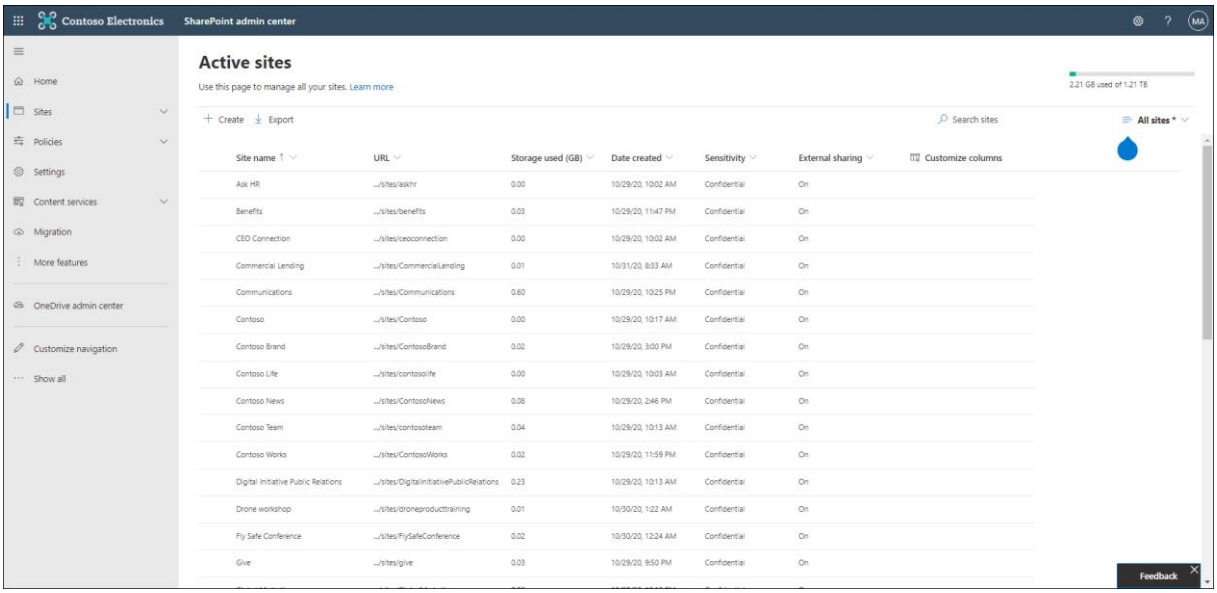
```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> $Id = [GUID]("8f9825d0-12d9-44b2-bb01-85bf2799fa88")
PS C:\WINDOWS\system32> $sites = Get-SPOSite -IncludePersonalSite $true -Limit all -Filter "Url -like 'M365x102715"
PS C:\WINDOWS\system32> write-output $sites

Url                                                                    Owner
---                                                                    -----
https://m365x102715-my.sharepoint.com/personal/christiec_m365x102715_onmicrosoft_com christiec@m365x102715.onmicroso...
https://m365x102715.sharepoint.com/sites/SharePointSite
https://m365x102715.sharepoint.com/sites/contosoteam
https://m365x102715.sharepoint.com/sites/GlobalMarketing                admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/SalesAndMarketing
https://m365x102715-my.sharepoint.com/personal/admin_m365x102715_onmicrosoft_com     admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/Communications                 admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/Contoso
https://m365x102715-my.sharepoint.com/
https://m365x102715-my.sharepoint.com/personal/alexw_m365x102715_onmicrosoft_com     alexw@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/GlobalSales                    admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/leadership-connection          admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/operations
https://m365x102715.sharepoint.com/sites/salesbestpractices
https://m365x102715-my.sharepoint.com/personal/lynner_m365x102715_onmicrosoft_com    lynner@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/portals/hub
https://m365x102715.sharepoint.com/sites/askhr
https://m365x102715.sharepoint.com/
https://m365x102715.sharepoint.com/sites/parentsofcontoso
https://m365x102715.sharepoint.com/sites/ReviewCenterForRetention
https://m365x102715-my.sharepoint.com/personal/diegos_m365x102715_onmicrosoft_com    diegos@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/ThePerspective                 admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/portals/Community
https://m365x102715.sharepoint.com/sites/CommercialLending
https://m365x102715.sharepoint.com/sites/newemployeeonboarding
https://m365x102715-my.sharepoint.com/personal/adelev_m365x102715_onmicrosoft_com    adelev@m365x102715.onmicrosoft.com
https://m365x102715-my.sharepoint.com/personal/pradeepg_m365x102715_onmicrosoft_com  pradeepg@m365x102715.onmicrosof...
https://m365x102715.sharepoint.com/sites/benefits                       admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/ceoconnection
https://m365x102715-my.sharepoint.com/personal/irvins_m365x102715_onmicrosoft_com    irvins@m365x102715.onmicrosoft.com
https://m365x102715-my.sharepoint.com/personal/debrab_m365x102715_onmicrosoft_com    debrab@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/ContosoBrand                   admin@m365x102715.onmicrosoft.com
https://m365x102715-my.sharepoint.com/personal/jonis_m365x102715_onmicrosoft_com     jonis@m365x102715.onmicrosoft.com
https://m365x102715-my.sharepoint.com/personal/alland_m365x102715_onmicrosoft_com    alland@m365x102715.onmicrosoft.com
https://m365x102715-my.sharepoint.com/personal/pattif_m365x102715_onmicrosoft_com    pattif@m365x102715.onmicrosoft.com
https://m365x102715-my.sharepoint.com/personal/nestorw_m365x102715_onmicrosoft_com   nestorw@m365x102715.onmicrosoft...
https://m365x102715.sharepoint.com/sites/SOCTeam
https://m365x102715.sharepoint.com/sites/leadership
https://m365x102715.sharepoint.com/sites/contosolife
https://m365x102715-my.sharepoint.com/personal/meganb_m365x102715_onmicrosoft_com    meganb@m365x102715.onmicrosoft.com
https://m365x102715-my.sharepoint.com/personal/miriamg_m365x102715_onmicrosoft_com   miriamg@m365x102715.onmicrosoft...
https://m365x102715.sharepoint.com/sites/ContosoWorks                   admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/ContosoNews                    admin@m365x102715.onmicrosoft.com
https://m365x102715-my.sharepoint.com/personal/leeg_m365x102715_onmicrosoft_com     leeg@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/FlySafeConference              admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/search
https://m365x102715-my.sharepoint.com/personal/lidiah_m365x102715_onmicrosoft_com    lidiah@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/safety
https://m365x102715-my.sharepoint.com/personal/gradya_m365x102715_onmicrosoft_com    gradya@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/Mark8ProjectTeam
https://m365x102715.sharepoint.com/sites/SalesPlanning
https://m365x102715.sharepoint.com/sites/USSales
https://m365x102715-my.sharepoint.com/personal/johannal_m365x102715_onmicrosoft_com  johannal@m365x102715.onmicrosof...
https://m365x102715.sharepoint.com/sites/give                           admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/Retail
https://m365x102715.sharepoint.com/sites/droneproducttraining           admin@m365x102715.onmicrosoft.com
https://m365x102715-my.sharepoint.com/personal/isaiahl_m365x102715_onmicrosoft_com   isaiahl@m365x102715.onmicrosoft...
https://m365x102715.sharepoint.com/sites/RetailOperations               admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/productsupport                 admin@m365x102715.onmicrosoft.com
https://m365x102715.sharepoint.com/sites/office365adoption
https://m365x102715.sharepoint.com/sites/DigitalInitiativePublicRelations
```

Now that we have enumerated all SharePoint sites (including OneDrive sites) we can apply the label we want, In my case I have chosen to use the Confidential label, so that by default I provide limited access and can use the GUI to make exceptions.



Apparently, you cannot set a sensitivity label on the MySite host, which is the https://m365x102715-my.sharepoint.com/ URL in my case. But this can be ignored.

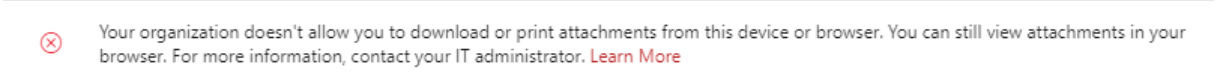
The end result is that all the SharePoint sites, and OneDrive sites will have the Confidential sensitivity label applied on the container level



Keep in mind though that you have to create a procedure from now on to make sure that the Sensitivity label gets applied to newly created OneDrive sites. Unfortunately I haven't found a way yet to set a default Sensitivity label for newly created OneDrive sites.

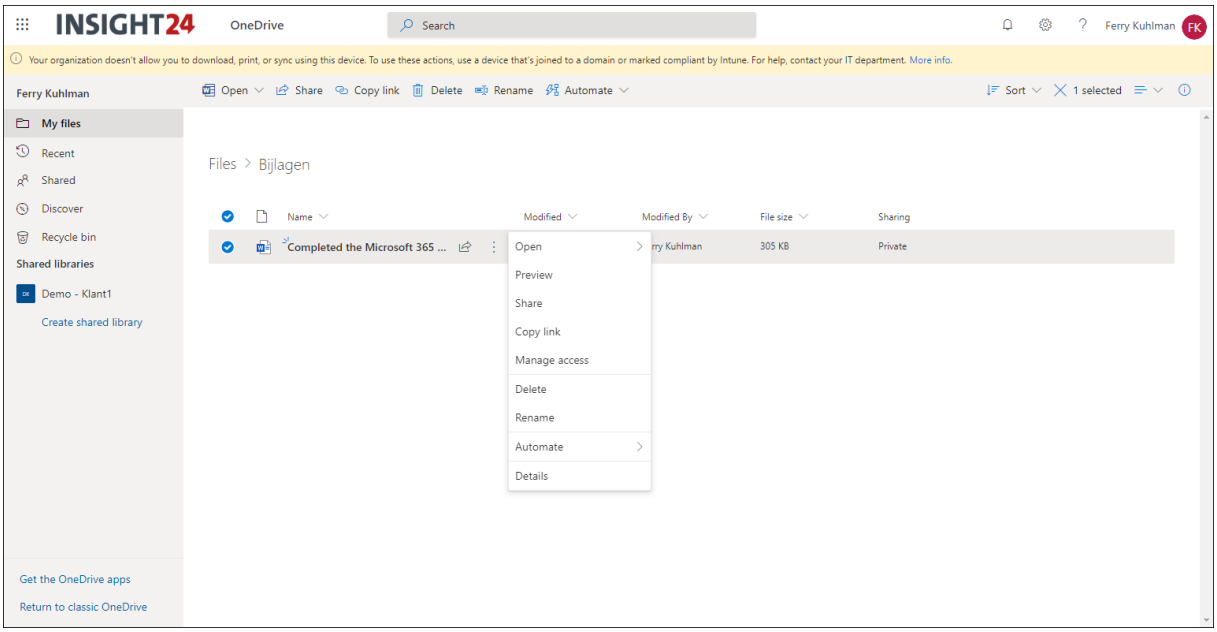
5.2.2.4 Policy behavior within Outlook Web Access

When the Conditional Access policy is applicable, the user accessing Outlook Web Access experiences the following behavior.



5.2.2.5 Policy behavior within SharePoint Online and OneDrive

When the Conditional Access policy is applicable, the user accessing SharePoint or OneDrive experiences the following behavior.


INSIGHT24
OneDrive
Search
Ferry Kuhlman
FK
Your organization doesn't allow you to download, print, or sync using this device. To use these actions, use a device that's joined to a domain or marked compliant by Intune. For help, contact your IT department. More info.
Ferry Kuhlman
Open
Share
Copy link
Delete
Rename
Automate
Sort
1 selected
My files
Recent
Shared
Discover
Recycle bin
Shared libraries
Demo - Klant1
Create shared library
Files > Bijlagen
Name
Modified
Modified By
File size
Sharing
Completed the Microsoft 365 ...
ry Kuhlman
305 KB
Private
Open
Preview
Share
Copy link
Manage access
Delete
Rename
Automate
Details
Get the OneDrive apps
Return to classic OneDrive

6 Testing and troubleshooting conditional access

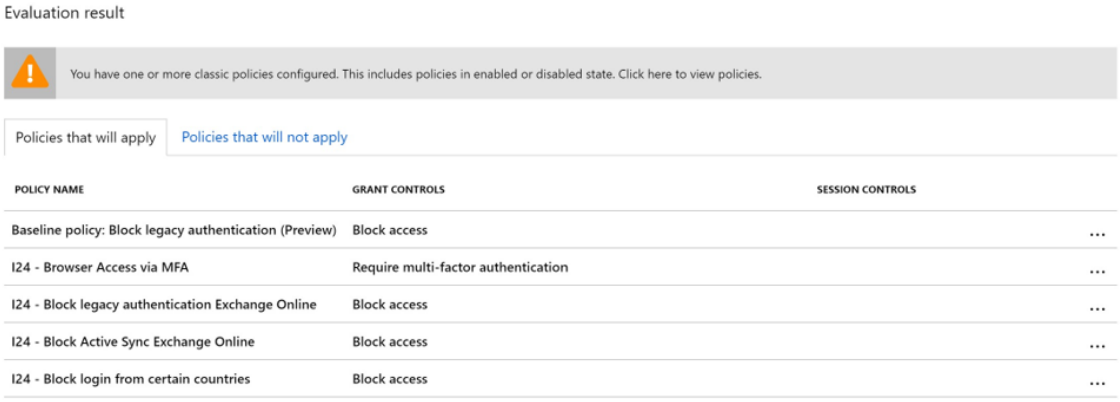
In this chapter we will go into more detail on where we can find information which can help us to test and troubleshoot Conditional Access policies.

6.1 What if tool

You can find the What if tooling by clicking on the What If icon on the Conditional Access policy overview page.

With the What if tooling you can determine which policies are applicable for a certain scenario. If you run the tooling it will give you an overview of which policies will apply, and which policies will not apply including the condition that has not been met.

A possible outcome can be:



There are some things the What if tooling is not capable of displaying though, that is that the effective outcome for the user, take for example the outcome of the example above - I'm still granted access to the cloud apps even though some "Block access" controls apply

6.2 Report-only Mode

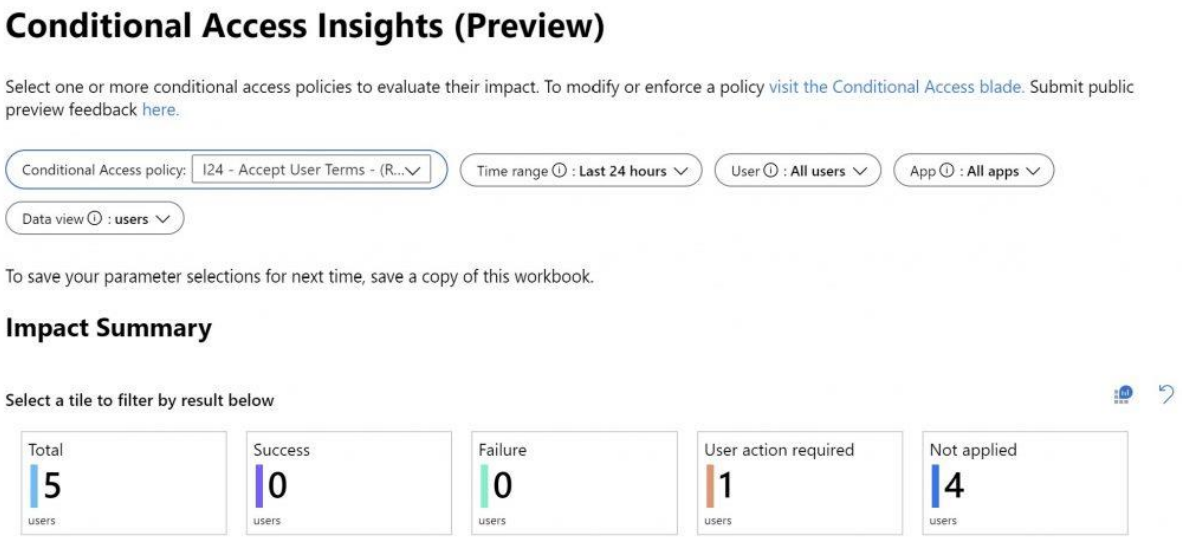
By enabling the Report-only mode the conditional access is evaluated on the client instead of enforced. By using the Azure AD sign-in logging functionality we can then determine the expected behavior of the Conditional Access Policy. This can be done in two ways:

1. Using Azure Active Directory Sign-in logging

Go to the Azure AD administration portal | Monitoring | Sign-ins and select one of the listed sign-ins. Once selected, within the sign-in logging, a tab titled: “Report-only” is available. Here you can see, in this example that the “I24 – Accept User Terms” conditional access policy reports the result: ” Report-only: User action required”

2. Using Azure AD Workbooks

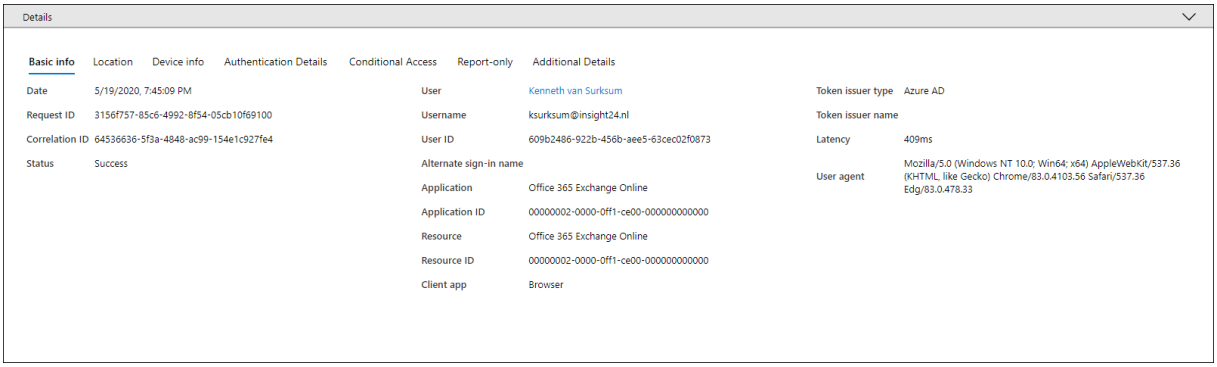
Using Azure AD workbooks requires that you have setup Log Analytics and forward your Azure AD sign-in logging to a Log Analytics Workspace.



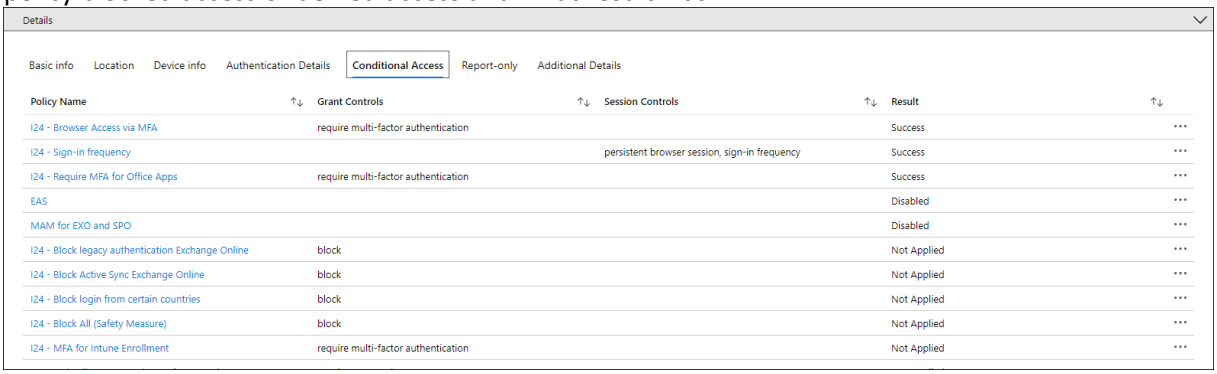
6.3 Azure Active Directory sign-ins logging

Once the policy is implemented you can use sign-ins logging from Azure Active Directory. Sign-ins logging is available under the monitoring section of Azure Active Directory, in the overview you can see all the sign ins and once a sign in is selected you can find more information about the circumstances under which the sign-in took place. On the Conditional Access tab, you can find all the Conditional Access related information.

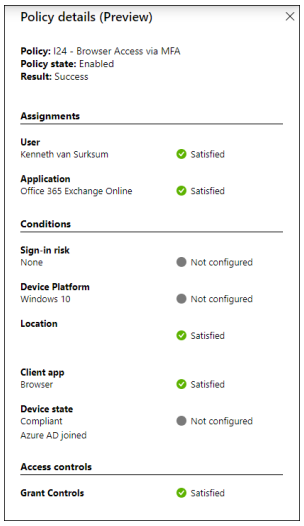
Below is an example of the outcome. On the basic page you can see the user involved, the date and time the sign in took place and what client app (Chrome browser) was used to access the cloud app (in this case Office 365 Exchange Online).



On the tab Conditional Access you can see which policies are applied for this login, whether the policy blocked access or denied access and what result was.



If you click on one of the Conditional Access policies, a new pane will pop up giving you additional information about this specific Conditional Access Policy



6.4 Where to find help and provide feedback

There are many resources where you can find help on Azure Active Directory Conditional Access, when troubleshooting at first Google/Bing is your best friend here. If those search engines don't give the expected result you can always ask at the following forums, or reach out using twitter and other social media channels.

- Azure Active Directory @ MSDN - https://social.msdn.microsoft.com/Forums/en-US/home?forum=WindowsAzureAD
- Azure Active Directory @ Stack Overflow - https://stackoverflow.com/questions/tagged/azure-active-directory

If something does not work as expected another good source could be to check the Azure Active Directory user voice page, where a certain functionality might already be noticed by somebody else who requested the product team to solve it. You can find the UserVoice page for Conditional Access here: https://feedback.azure.com/forums/169401-azure-active-directory/category/167259-conditional-access

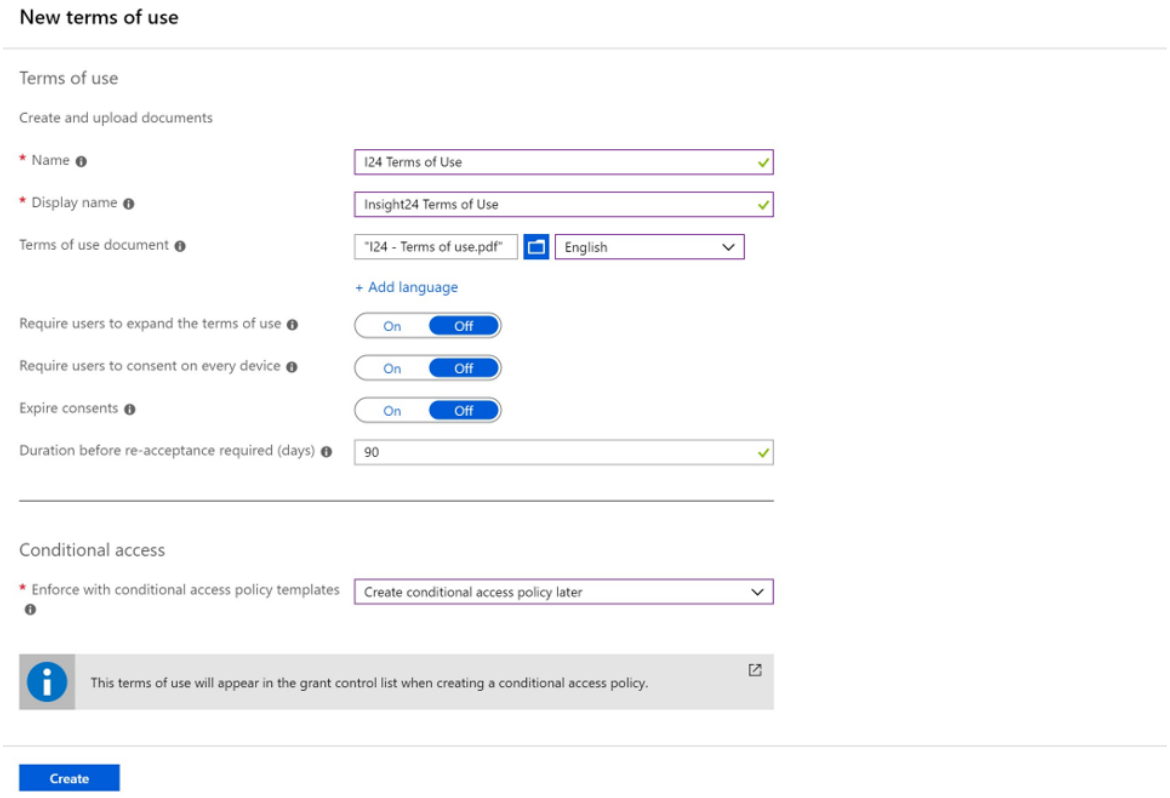
7 Modifying Conditional Access to suit your special needs

When you want to integrate other products into your Conditional Access environment you can use "Custom controls" to include products from other vendors into your Conditional Access conditions. If a custom control is used the browser is redirected to the external service, performs any required authentication or validation activities, and is then redirected back to Azure Active Directory. If the user was successfully authenticated or validated, the user continues in the Conditional Access flow.

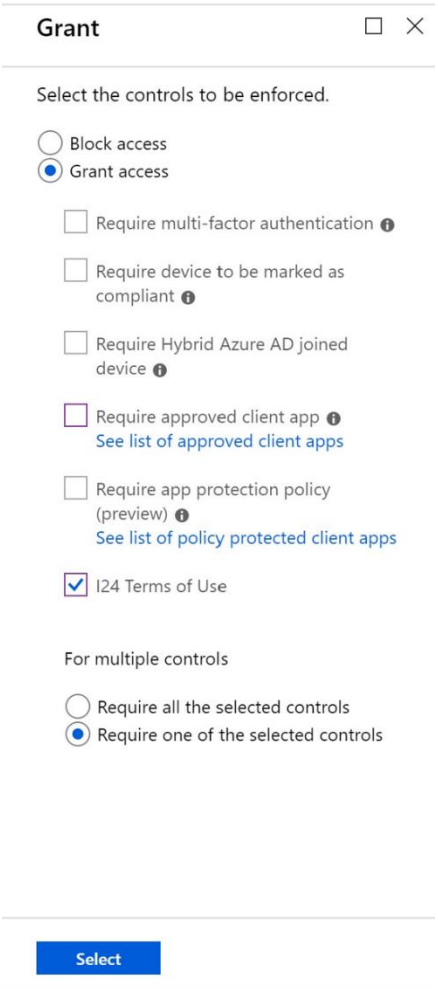
More information and some samples can be found here: Custom controls (preview)

Another thing you can do to extend the grant control with Terms of Use which users must consent with before they can access the cloud app. More information about creating the terms of use can be found here: Azure Active Directory terms of use - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

In the example below I have created the terms of use for my tenant Insight24



Once created if I open any Conditional Access policy, I have an extra control available which I can select in the Grant control. In this case the user is granted access to the cloud app if the I24 Terms of Use are accepted by the user.



8 Resources and further references

8.1 Microsoft documentation

- What is Conditional Access? - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview
- What is Azure Active Directory? - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis
- Azure Active Directory pricing - https://azure.microsoft.com/en-us/pricing/details/active-directory/
- Azure AD Adoption kits: https://www.microsoft.com/en-us/download/details.aspx?id=58321
- Microsoft 365 Business Service Description - https://docs.microsoft.com/en-gb/office365/servicedescriptions/microsoft-365-business-service-description
- QuickStart: Block access when a session risk is detected with Azure Active Directory conditional access - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-sign-in-risk
- Infographic: Control access to your data with intelligence using Microsoft EMS - https://gallery.technet.microsoft.com/Infographic-Control-access-81e7d79e
- Infographic: Comprehensive protection of Office 365 data on any device with EMS - https://gallery.technet.microsoft.com/Infographic-Comprehensive-e9a6c8c3
- Enable combined security information registration (preview) - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-registration-mfa-sspr-combined
- Enabling limited access with SharePoint Online - https://aka.ms/spolimitedaccessdocs
- Enabling limited access with Exchange Online - https://aka.ms/owalimitedaccess
- Use app enforced restrictions - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#application-enforced-restrictions
- Protect apps with Microsoft Cloud App Security Conditional Access App Control - https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad#how-it-works
- User sign-in frequency - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime#user-sign-in-frequency
- Configure authentication session management with Conditional Access - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime
- What are service dependencies in Azure Active Directory Conditional Access? - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/service-dependencies
- Reduce your attack surface - https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps#step-2---reduce-your-attack-surface
- Tutorial: Secure user sign-in events with Azure Multi-Factor Authentication - https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa
- Quickstart: Block access when a session risk is detected with Azure Active Directory Conditional Access - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-sign-in-risk
- Quickstart: Require terms of use to be accepted before accessing cloud apps - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-tou
- Control access from unmanaged devices - https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

- Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites - https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide#enable-this-preview-and-synchronize-labels
- Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory - https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels
- Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites - https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide
  - Optimize reauthentication prompts and understand session lifetime for Azure Multi-Factor Authentication - https://docs.microsoft.com/en-us/azure/active-directory/authentication/concepts-azure-multi-factor-authentication-prompts-session-lifetime
  - What is a Primary Refresh Token? - https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-primary-refresh-token
  - Configure the 'Stay signed in?' prompt for Azure AD accounts - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/keep-me-signed-in
  - Configure authentication session management with Conditional Access - https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime
  - Azure AD registered devices - https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register
  - Accessing Conditional Access protected resources in Microsoft Edge - https://docs.microsoft.com/en-us/deployedge/security-overview#accessing-conditional-access-protected-resources-in-microsoft-edge
  - Enable passwordless sign-in with the Microsoft Authenticator app (preview) - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phone
-

8.2 Other interesting blogs

- Conditional Access posts by Peter van der Woude - https://www.petervanderwoude.nl/post/category/microsoft-intune/conditional-access/
- Conditional Access posts by Peter Daalmans - https://www.configmgrblog.com/tag/conditional-access/
- Conditional Access posts by Per Larsen - https://osddeployment.dk/tag/conditional-access/
- How to get started with Conditional Access, by Per Larsen - https://osddeployment.dk/2018/07/01/how-to-get-started-with-conditional-access/
- Conditional Access - are you really getting the most out of it?, by Joni Nieminen - https://bloggerz.cloud/2019/01/02/conditional-access-are-you-really-getting-the-most-out-of-it-part-2-of-2/
- Implementing Modern Security Tools – Part 3 – Conditional Access, by Maurice Daly - https://www.scconfigmgr.com/2019/02/19/implementing-modern-security-tools-part-3-conditional-access/
- Azure Active Directory and Office 365: Conditional Access, by Jethro Seghers - https://regarding365.com/azure-active-directory-and-office-365-conditional-access-8bc616a392b2
- My favorite Conditional Access Policies for the SMB, by Alex Fields - https://www.itpromentor.com/conditional-access-faves/

- Conditional access (zero trust) is the most important EUC movement since mobile and cloud, by Jack Madden - https://www.brianmadden.com/opinion/Conditional-access-zero-trust-is-the-most-important-EUC-movement-since-mobile-and-cloud
- Diverse articles on Conditional Access from the Practical 365 team - https://practical365.com/tag/conditional-access/
- Bypassing Conditional Access Device Platform Policies, by Nicola Suter - https://tech.nicolonsky.ch/bypassing-conditional-access-device-platform-policies/