

# Conditional Access demystified

WHITEPAPER ON IMPLEMENTING CONDITIONAL ACCESS  
KENNETH VAN SURKSUM | [WWW.VANSURKSUM.COM](http://WWW.VANSURKSUM.COM) |  
VERSION 1.1 | MAY, 2020





## Table of contents

1	Introduction.....	3
1.1	Why this whitepaper? .....	3
2	What is Conditional Access?.....	3
2.1	Licensing .....	4
2.2	Secure score .....	4
2.3	What's with the preview label?.....	6
3	How does Conditional Access work?.....	7
3.1	General .....	11
3.2	Assignments (a.k.a. conditions).....	11
3.2.1	Users and Groups .....	11
3.2.2	Cloud apps or actions .....	11
3.2.3	Sign-in Risk (additional license needed).....	12
3.2.4	Device Platforms.....	12
3.2.5	Locations.....	13
3.2.6	Client apps .....	13
3.2.7	Device state .....	14
3.3	Access Controls.....	14
3.3.1	Grant.....	14
3.3.2	Session Controls .....	15
4	Designing a Conditional Access strategy .....	16
5	Implementing Conditional Access .....	18
6	Testing and Troubleshooting Conditional Access.....	22
6.1	What if tool.....	22
6.2	Report-only Mode .....	23
6.3	Azure Active Directory sign-ins logging .....	24
6.4	Where to find help and provide feedback .....	26
7	Modifying Conditional Access to suit your special needs .....	27
8	Resources and further references.....	29
8.1	Microsoft documentation .....	29
8.2	Other interesting blogs.....	30





**About:** Kenneth van Surksun

Kenneth van Surksun works as a senior consultant at [Insight24](#) and is specialized in public and private cloud solutions based on Azure and System Center. Kenneth also works with client management solutions based on System Center Configuration Manager and Intune (part of EMS+S). Kenneth is Microsoft Certified Trainer (MCT) and has multiple certifications. Kenneth has received the MVP and VMware vExpert award multiple times.



Kenneth has worked with System Center Configuration Manager/SMS since 1998 and has been responsible for implementing the product in large and small enterprise environments. Kenneth regularly shares his knowledge by speaking on national and international events. Kenneth is co-founder of the [Windows Management User Group Netherlands](#) (WMUG NL) and Speaker Manager for [ExpertsLive Netherlands](#). He organizes community meetings on a regular basis.

A special thanks to Peter Daalmans for reviewing the content.

Disclaimer: This information is provided "AS IS" with no warranties, confers no rights and is not supported by the author.

Copyright © 2020 by Kenneth van Surksun. All rights reserved. No part of the information on this web site may be reproduced or posted in any form or by any means without the prior written permission of the publisher.





# 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's 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?

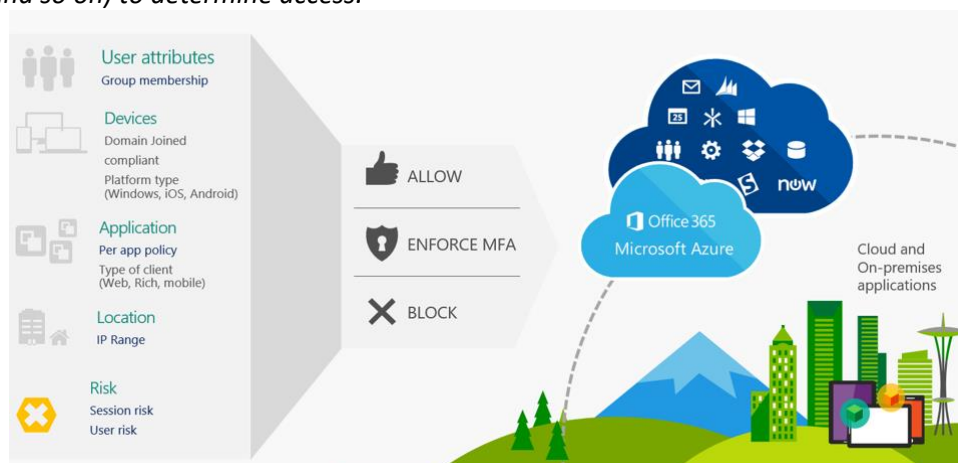
There is already some good documentation from Microsoft and many blogpost by fellow bloggers detailing Conditional Access scenario's, but not really a one-stop shopping overview. With this whitepaper I hope to achieve this.

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 and 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?

[Microsoft describes Conditional Access](#) as followed: "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 your cloud applications.

With cloud applications Microsoft means applications which use Azure Active Directory (Azure AD) for authentication. Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. So, if you access an 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 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 only the credentials of the application in Azure AD, and through Azure AD you can login using SSO making use of Conditional Access, but when accessing the SaaS application directly you can also provide your userid and password. So, it's important that you modify the SaaS identity provider to leverage Azure Active Directory.

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.

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 of course have MCAS licensed as well.

Keep in mind though, 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 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

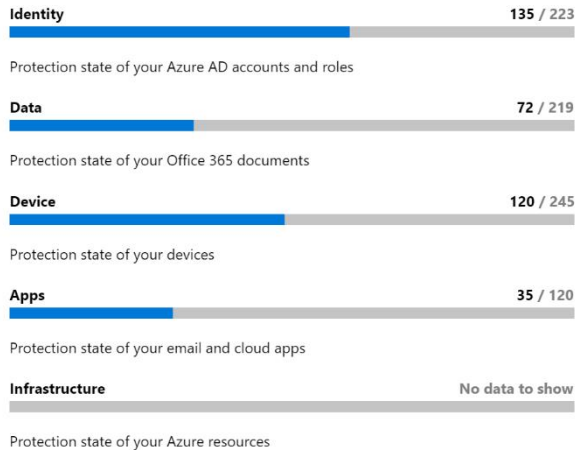




## Your secure score

**Total score: 362 / 807**

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps, and infrastructure.



[Learn more about Microsoft Secure Score](#)

[Get your score using Microsoft Graph API](#)

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

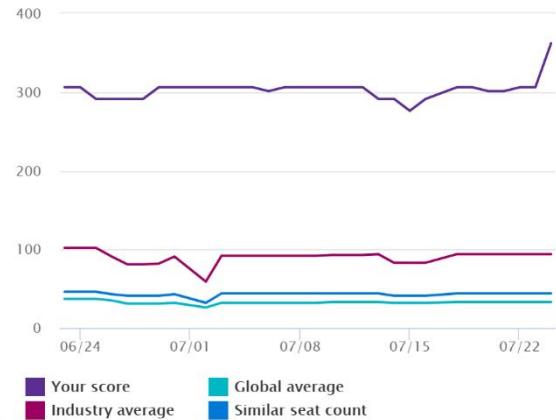
Conditional access provides functionality, which is part of a secure identity infrastructure, more actions than just implementing conditional access are needed. See this article for more information on the steps needed to secure your identity infrastructure: Five steps to securing your identity infrastructure - <https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps#step-2---reduce-your-attack-surface>

## History

**56 points** in 30 days

Total score ▾

Your secure score over time and how you compare to other organizations.



[View history](#)





## 2.3 What's 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"



**Kenneth van Surksun**  
@kennethvs



@alex\_a\_simons can you give me some guidelines on support for (Preview) options within #ConditionalAccess? IS there any support available when implementing these in production? #AzureAD

9:18 PM · Jul 23, 2019 · [Twitter Web App](#)

||| View Tweet activity



**Alex Simons** @Alex\_A\_Simons · 3m  
Replying to @kennethvs



Yes, all public preview features in Azure AD are fully supported.

1

1

1

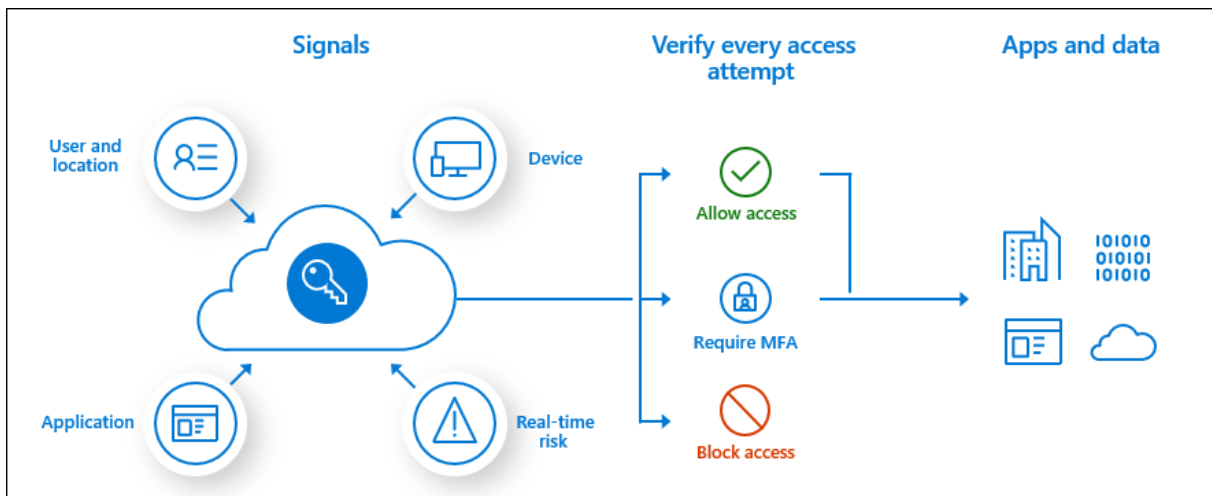


**Kenneth van Surksun** @kennethvs · 31s  
Great, thanks for the quick response!





### 3 How does Conditional Access work?



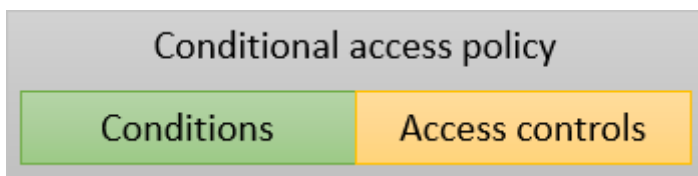
Microsoft [explains Conditional Access](#) in the following way.

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 used to provide some already configured policies for you to use, called "Baseline policies", these policies protect against many common tasks, at time of writing the following baseline policies exist:

- Require MFA for admins
- End user protection (preview)
- Block legacy authentication (preview)
- Require MFA for service management (preview)

While these policies might still be visible in your tenant, Microsoft doesn't support them anymore and is planning on removing them. See my blogpost: "[Microsoft deprecates Conditional Access baseline policies in favour of Security Defaults, here is what you need to know and do](#)". Basically it comes down to either enabling Security Defaults (which disables the option to use Conditional Access







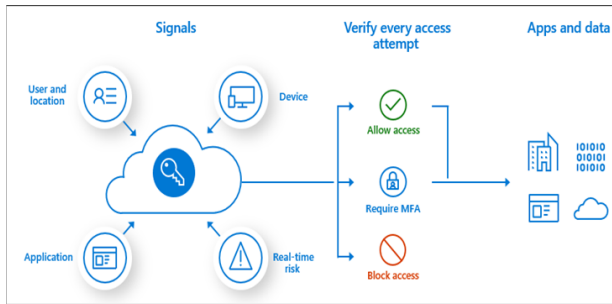
policies) or create your own policies. For the old baseline policies Microsoft provides documentation on how to create them yourself.

1. [Conditional Access: Require MFA for administrators](#)
2. [Conditional Access: Require MFA for Azure management](#)
3. [Conditional Access: Block legacy authentication](#)
4. [Conditional Access: Risk-based Conditional Access](#)

Besides some of the common policies, customers can also create their own "custom" Conditional Access policies, the figure below 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 - v4.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.

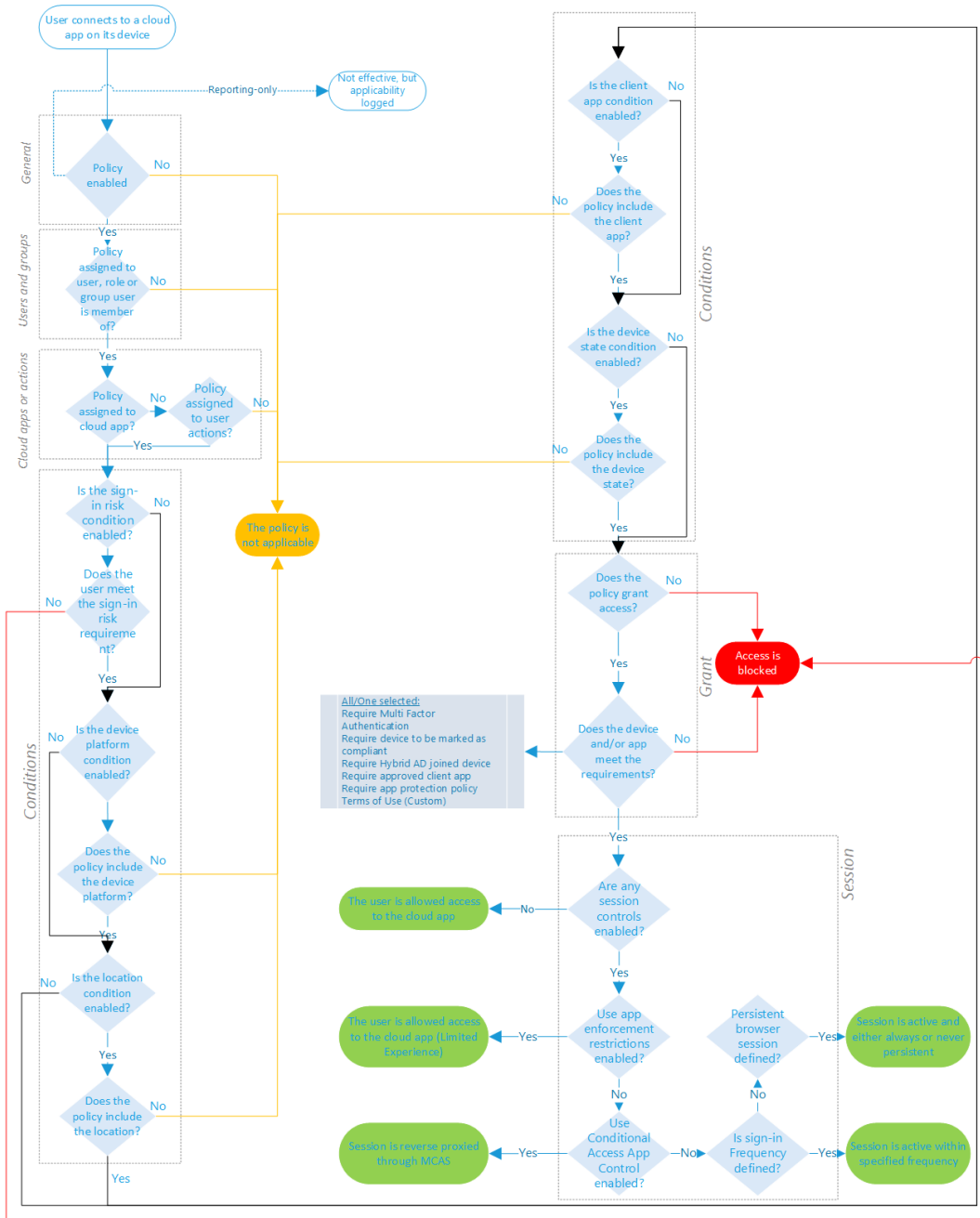
In the second phase, you are prompted to satisfy the requirements you haven't met.

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 other policy controls in the following order:

- 1 ☒ Require multi-factor authentication ①
- 2 ☒ Require device to be marked as compliant ②
- 2 ☒ Require Hybrid Azure AD joined device ②
- 3 ☒ Require approved client app ③  
See list of approved client apps

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 trumps all other configuration settings



Date: May 2020 | Version 1.1 | Author: Kenneth van Surksum | [www.vansurksum.com](http://www.vansurksum.com)





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

*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> 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.*

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”

☐ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

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

☐ Require app protection policy (Preview) ⓘ  
[See list of policy protected client apps](#)

☐ I24 Terms of Use

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected 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.

## 3.1 General

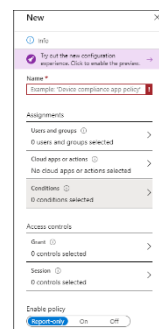
The conditional access policy must have a unique name, use a name which gives an idea of what the policy is doing under what circumstances. Policies can either be enabled (On), disabled (Off) or defined in Report-only mode which can help to determine whether the policy is working as supposed to. More on Report-only mode in chapter 5, Implementing Conditional Access.

## 3.2 Assignments (a.k.a. conditions)

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

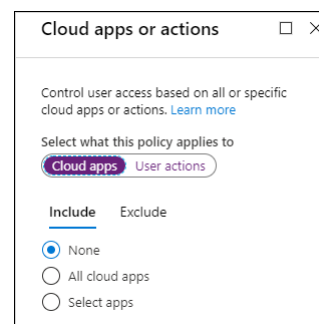
### 3.2.1 [Users and Groups](#)

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.



### 3.2.2 [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 can be found in the following list: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps#microsoft-cloud-applications>. Some of the cloud apps are Office 365, Office 365 Exchange Online, Office 365 SharePoint Online and Microsoft Azure Management (the Azure Portal). The [Office 365 app](#), 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:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-registration-mfa-sspr-combined>.

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.

Cloud apps or actions

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

Select what this policy applies to

Cloud apps **User actions**

Select the action this policy will apply to

☐ Register security information

### 3.2.3 [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: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-sign-in-risk> and in a article I wrote about the subject here: "[Azure AD Identity Protection deep dive](#)"

Sign-in risk

Control user access to respond to specific sign-in risk levels. [Learn more](#)

Configure ⓘ

**Yes** No

Select the sign-in risk level this policy will apply to

☒ High

☐ Medium

☐ Low

☐ No risk

### 3.2.4 [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.

Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure ⓘ

**Yes** No

**Include** Exclude

☐ Any device

☒ Select device platforms

☒ Android

☒ iOS

☐ Windows Phone

☒ Windows

☒ macOS

**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: <https://tech.nicolonsky.ch/bypassing-conditional-access-device-platform-policies/>





### 3.2.5 [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.

Locations

Control user access based on their physical location. [Learn more](#)

Configure ⓘ

☒ Yes ☐ No

**Include** Exclude

☐ Any location

☒ All trusted locations

☐ Selected locations

Select >

None

**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.

### 3.2.6 [Client apps](#)

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

- Browser apps - apps accessed by a web browser on the client
- Mobile Apps and desktop clients
  - Apps using Modern authentication - these are apps which can use "modern", meaning secure authentication mechanisms
  - 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?"](#)

Client apps (Preview)

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ

☒ Yes ☐ No

Select the client apps this policy will apply to

☐ Browser

☒ Mobile apps and desktop clients

☐ Modern authentication clients

☐ Exchange ActiveSync clients

☒ Other clients ⓘ





### 3.2.7 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)

Device state (Preview)

Control user access when device the user is signing-in from is not "Hybrid Azure AD joined" or "marked as compliant". [Learn more](#)

Configure ⓘ  
**Yes** No

Include **Exclude**

Select the device state condition used to exclude devices from policy.

☐ Device Hybrid Azure AD joined ⓘ  
☒ Device marked as compliant ⓘ

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

The grant access controls available are:

### 3.3.1 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: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/technical-reference#approved-client-app-requirement>
- 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

☐ Require multi-factor authentication ⓘ  
☐ Require device to be marked as compliant ⓘ  
☐ Require Hybrid Azure AD joined device ⓘ  
☐ Require approved client app ⓘ  
[See list of approved client apps](#)  
☐ Require app protection policy (Preview) ⓘ  
[See list of policy protected client apps](#)  
☐ I24 Terms of Use

For multiple controls  
☒ Require all the selected controls  
☐ Require one of the selected controls

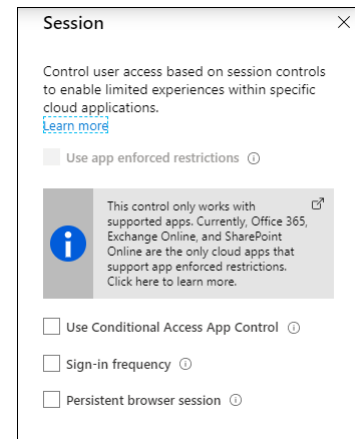




### 3.3.2 Session Controls

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

ⓘ 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.

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 distinguish 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 administering 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 in order 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, the spreadsheet is available for download from the following location: [Conditional Access Policy Description-v1.1.xlsx](#)





## 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 - <https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/enable-or-disable-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 - <https://www.ronnipedersen.com/2017/07/11/enable-modern-authentication-for-skype-for-business-online/>

**Step 2:** Disable the legacy authentication protocols from the Office 365 accounts

Writing this down as a step is not fair 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:** Enable the "Block Legacy Authentication" policy

Follow the steps as described in the following article: "[Block Legacy Authentication](#)". By enabling this policy and excluding the users which you identified in step 2 you make sure that legacy authentication cannot be used.





**Step 4:** 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

**Step 5:** If you have licensed Azure Active Directory Identity Protection consider implementing the user risk policy and force a user to change its password if the password is leaked. This is either determined by Microsoft finding leaked credentials, or by using Azure AD threat intelligence which can compare user activity with known attack patterns.

In this step you can also enable the following baseline policies:

- [Require MFA for administrators](#)
- [Require MFA for Azure management](#)
- [Risk-based Conditional Access](#)

Make sure that you exclude the break glass accounts from these policies.

**Step 6:** 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 also 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.

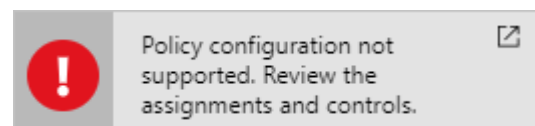
Testing conditional access policies can be quite tricky. Main reason for this is that once a policy is enabled it is not necessarily directly effective and it can take a while for it to become effective for your clients. This has to do with the fact that clients are not logging in all the time. Therefore,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

**Step 7:** 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.

Basic info	Device info	MFA info	Conditional Access	Troubleshooting and support
Request ID	8c26caa9-b15a-4443-96c7-c76467590500			IP address
Correlation ID	318dbf13-749c-4c98-a3d0-8e356be7d715			Location
User	Stanley Messie			Date
Username	smessie@emshelden.nl			Status
User ID	f986377c-bdc3-46b4-804a-501150f581f8			Sign-in error code
Application	Microsoft Office 365 Portal			Failure reason
Application ID	00000000-0000-0001-ce00-000000000000			Client app
Resource	Windows Azure Active Directory			
Resource ID	00000002-0000-0000-c000-000000000000			

Azure has a safety feature that prevents you from creating a policy which violates the best practices for Conditional Access policies, so you can't 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.

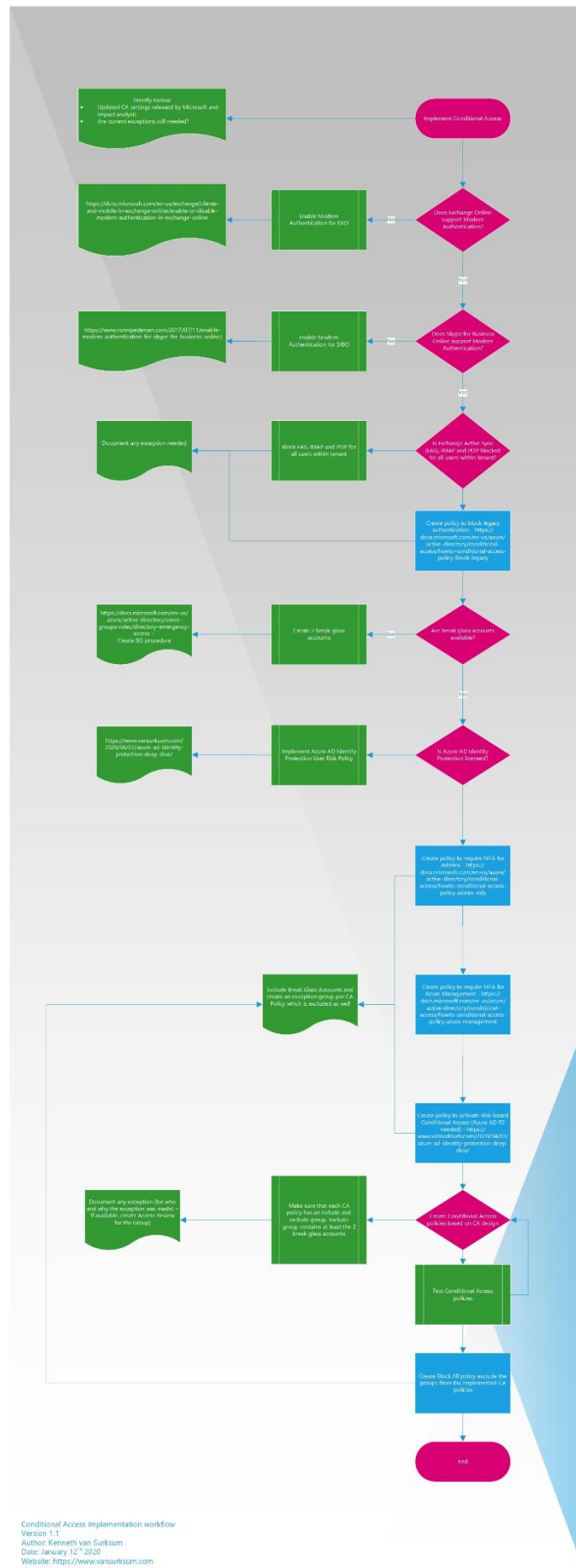
Azure Active Directory Conditional Access changes on a regular basis, make sure that you have a procedure to check occasionally what is cooking on this topic. Make sure you understand what is coming, what is in preview and what is released. Invest time to determine the possible impact of these changes 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 - V1.2.pdf](#)





Conditional Access Implementation workflow  
Version 1.1  
Author: Kenneth van Surksom  
Date: January 12<sup>th</sup> 2020  
Website: <https://www.vanvurksum.com>





## 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.

**What If** Info ×

Info

Test the impact of conditional access on a user when signing in under certain conditions.  
[Learn more](#)

★ User ⓘ

0 users selected

>

Cloud apps or actions ⓘ

Any cloud app

>

IP address ⓘ  
Enter IP address (ex: 40.77.182.32)

Country ⓘ  
Select country...

Device platform ⓘ  
Select device platform...

Client apps (preview) ⓘ  
Select a client app...

Device state (preview) ⓘ  
Select device state...

Sign-in risk ⓘ  
Select sign-in risk...


What If

Reset

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:

Evaluation result

 You have one or more classic policies configured. This includes policies in enabled or disabled state. [Click here to view policies.](#)

Policies that will apply

Policies that will not apply

POLICY NAME	GRANT CONTROLS	SESSION CONTROLS
Baseline policy: Block legacy authentication (Preview)	Block access	...
I24 - Browser Access via MFA	Require multi-factor authentication	...
I24 - Block legacy authentication Exchange Online	Block access	...
I24 - Block Active Sync Exchange Online	Block access	...
I24 - Block login from certain countries	Block access	...





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"

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only (Preview)	Additional Details
Policy Name	↑↓	Grant Controls	↑↓	Session Controls	↑↓	Result
I24 - Accept User Terms		I24 Terms of Use				Report-only: User action required
A sign-in can also be interrupted (e.g. blocked, MFA challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.						

### 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.

## Conditional Access Insights (Preview)

Select one or more conditional access policies to evaluate their impact. To modify or enforce a policy [visit the Conditional Access blade](#). Submit public preview feedback [here](#).

Conditional Access policy: I24 - Accept User Terms - (R...  
Time range: Last 24 hours  
User: All users  
App: All apps  
Data view: users

To save your parameter selections for next time, save a copy of this workbook.

### Impact Summary

Select a tile to filter by result below







## 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).

Details					
Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Date	5/19/2020, 7:45:09 PM		User	Kenneth van Surksun	Token issuer type
Request ID	3156f757-85c6-4992-8f54-05cb10f69100		Username	ksurksun@insight24.nl	Azure AD
Correlation ID	64536636-5f3a-4848-ac99-154e1c927fe4		User ID	609b2486-922b-456b-ae5-63cec02f0873	Token issuer name
Status	Success		Alternate sign-in name		Latency
			Application	Office 365 Exchange Online	409ms
			Application ID	00000002-0000-0ff1-ce00-000000000000	User agent
			Resource	Office 365 Exchange Online	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.56 Safari/537.36
			Resource ID	00000002-0000-0ff1-ce00-000000000000	Edg/83.0.478.33
			Client app	Browser	

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.

Details					
Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Policy Name	↑↓	Grant Controls	↑↓	Session Controls	↑↓
I24 - Browser Access via MFA		require multi-factor authentication			Success
I24 - Sign-in frequency				persistent browser session, sign-in frequency	Success
I24 - Require MFA for Office Apps		require multi-factor authentication			Success
EAS					Disabled
MAM for EXO and SPO					Disabled
I24 - Block legacy authentication Exchange Online		block			Not Applied
I24 - Block Active Sync Exchange Online		block			Not Applied
I24 - Block login from certain countries		block			Not Applied
I24 - Block All (Safety Measure)		block			Not Applied
I24 - MFA for Intune Enrollment		require multi-factor authentication			Not Applied





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

Policy details (Preview)

Policy: I24 - Browser Access via MFA

Policy state: Enabled

Result: Success

Assignments

User

Kenneth van Surksum

✔ Satisfied

Application

Office 365 Exchange Online

✔ Satisfied

Conditions

Sign-in risk

None

● Not configured

Device Platform

Windows 10

● Not configured

Location

✔ Satisfied

Client app

Browser

✔ Satisfied

Device state

Compliant

● Not configured

Azure AD joined

Access controls

Grant Controls

✔ Satisfied





## 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

### New terms of use

#### Terms of use

Create and upload documents

* Name ⓘ	I24 Terms of Use ✓
* Display name ⓘ	Insight24 Terms of Use ✓
Terms of use document ⓘ	"I24 - Terms of use.pdf"  English ▼
<a href="#">+ Add language</a>	
Require users to expand the terms of use ⓘ	On <input checked="" type="radio"/> Off
Require users to consent on every device ⓘ	On <input checked="" type="radio"/> Off
Expire consents ⓘ	On <input checked="" type="radio"/> Off
Duration before re-acceptance required (days) ⓘ	90 ✓

#### Conditional access

* Enforce with conditional access policy templates ⓘ	Create conditional access policy later ▼
--	--



This terms of use will appear in the grant control list when creating a conditional access policy.



Create





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.

Grant

×

Select the controls to be enforced.

☐ Block access

☒ Grant access

☐ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ

[See list of approved client apps](#)

☐ Require app protection policy (preview) ⓘ

[See list of policy protected client apps](#)

☒ I24 Terms of Use

For multiple controls

☐ Require all the selected controls

☒ Require one of the selected controls

Select





## 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-what-is>
- 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>





## 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.sconfigmgr.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/>

