Microsoft 365
SECURITY & COMPLIANCE
USER GROUP

Azure AD Conditional Access

Demystified – June 2021 edition

About “Kenneth van Surksum”

Focus

Modern Workplace Consultant at Insight24, Microsoft Certified Trainer, Co-founder and organizer at ~~Windows Management User Group Netherlands~~ Workplace Ninja User Group Netherlands

Microsoft® Most Valuable Professional MVP

From

The Netherlands

My Blog

https://www.vansurksum.com

Certifications

Microsoft 365 Certified Enterprise Administrator

Microsoft Certified Azure Solutions Architect

Hobbies

Cooking on my Kamado Joe & Sports

Contact

kenneth@vansurksum.com

https://twitter.com/kennethvs

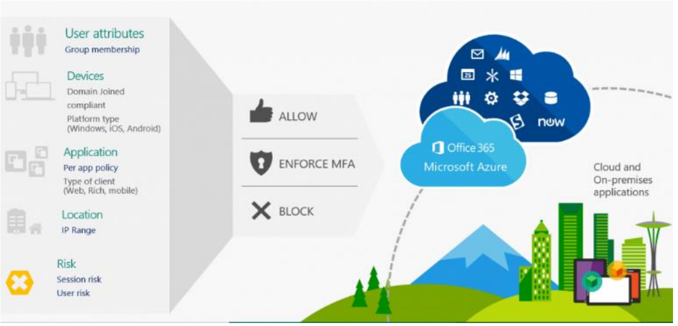
https://www.linkedin.com/in/kennethvansurksum

Our topics for Today!

- What is Conditional Access?
- How does Conditional Access work?
- Designing Conditional Access
- Implementing Conditional Access
- Troubleshooting Conditional Access

Identity is the new perimeter

What is Conditional Access?

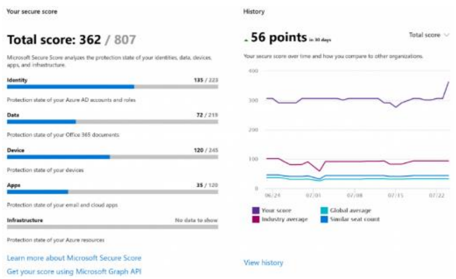


Microsoft Description:

“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.”*

What is Conditional Access?

- Put **conditions** in place to **access** to company data and apps. (Identity and device)
- Can be compared with a Network Firewall but then for your identity
- Resources being accessed must use Azure AD as authentication provider
- Even though you can use it, doesn't mean you are licensed
- When using ADFS, it can become quite complex – [ask yourself whether you still need ADFS]()
- Adds points to your Secure Score



Your secure score

Total score: 362 / 807

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

Identity 135 / 223

Protection state of your Azure AD accounts and roles

Data 72 / 219

Protection state of your Office 365 documents

Device 120 / 245

Protection state of your devices

Apps 35 / 120

Protection state of your email and cloud apps

Infrastructure No data to show

Protection state of your Azure resources

Learn more about Microsoft Secure Score

Get your score using Microsoft Graph API

History

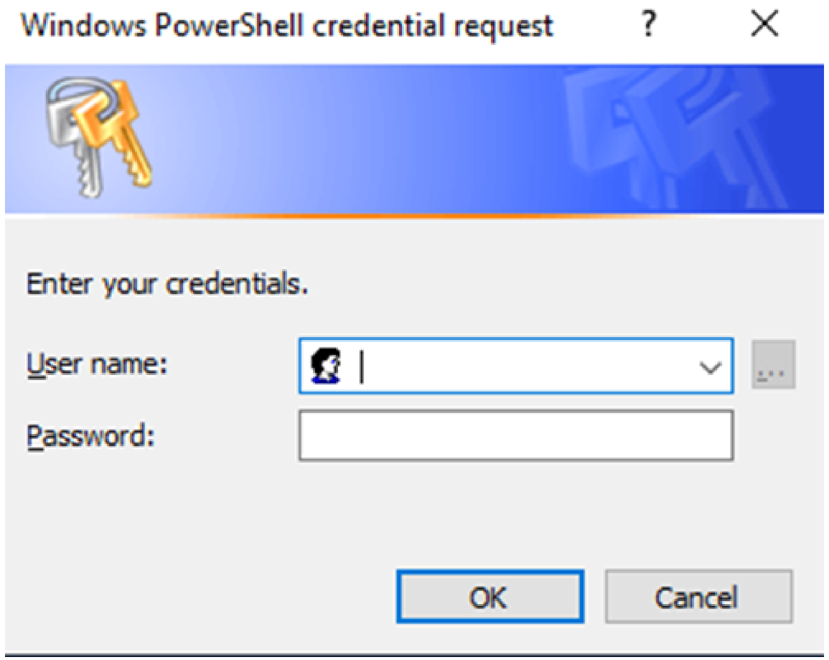
56 points in 30 days

Total score

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

View history

Prerequisites



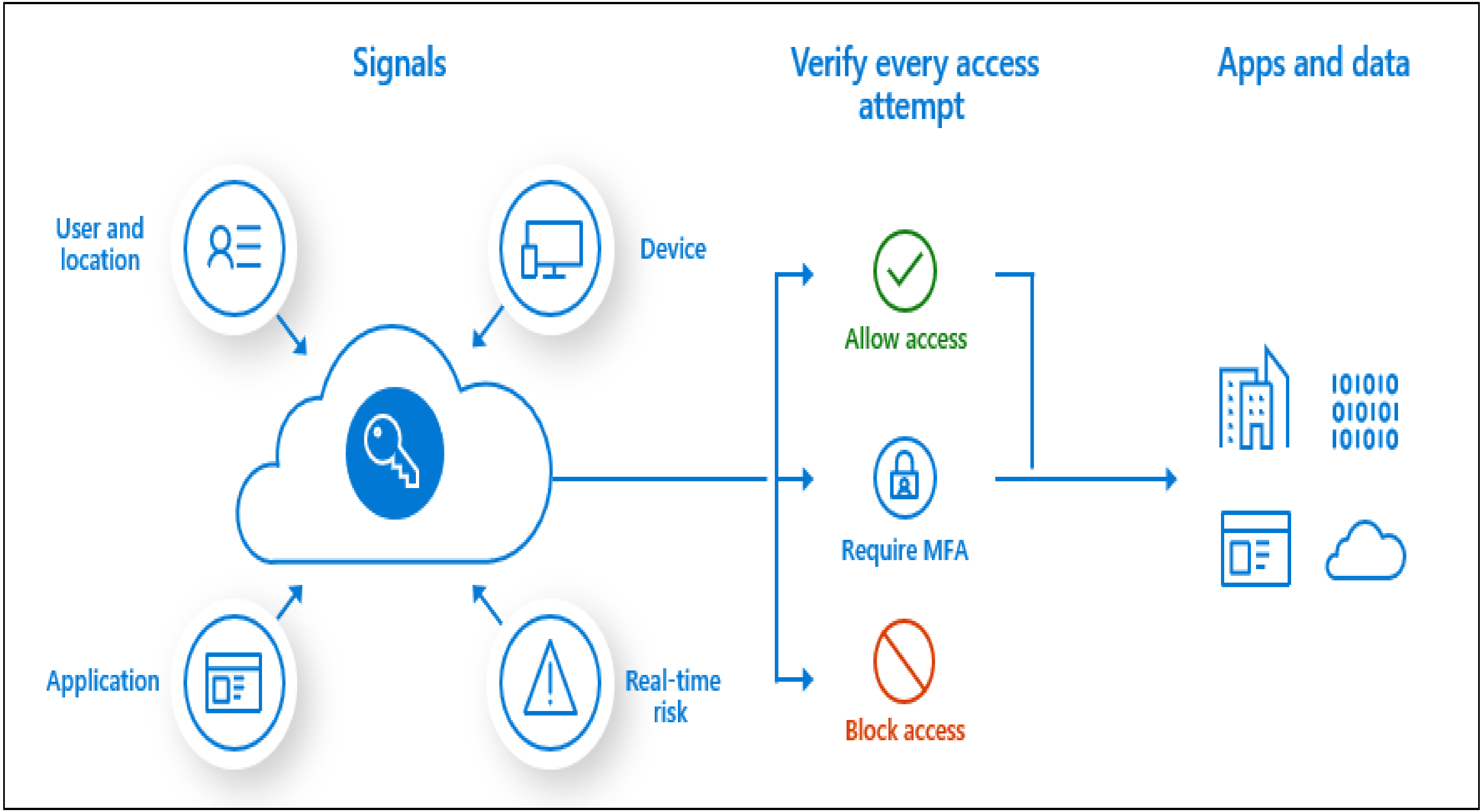
Windows PowerShell credential request

Enter your credentials.

- We must block legacy authentication for Conditional Access to work in all scenarios.
  - Legacy authentication is vulnerable to brute force or password spray attacks
  - ~~Microsoft announced that it will disable support for legacy authentication for EXO in H2 2021~~
- Azure AD Premium P1 or P2 license (if not you can use Security defaults)
- Microsoft Endpoint Manager (if you want to leverage compliance)
- Rethink your reauthentication settings (MFA global settings/KMSI)
- Make sure that you define 2 break glass accounts - https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access

Legacy Authentication

Usage within your tenant?



Signals

Verify every access attempt

Apps and data

User and location

Device

Application

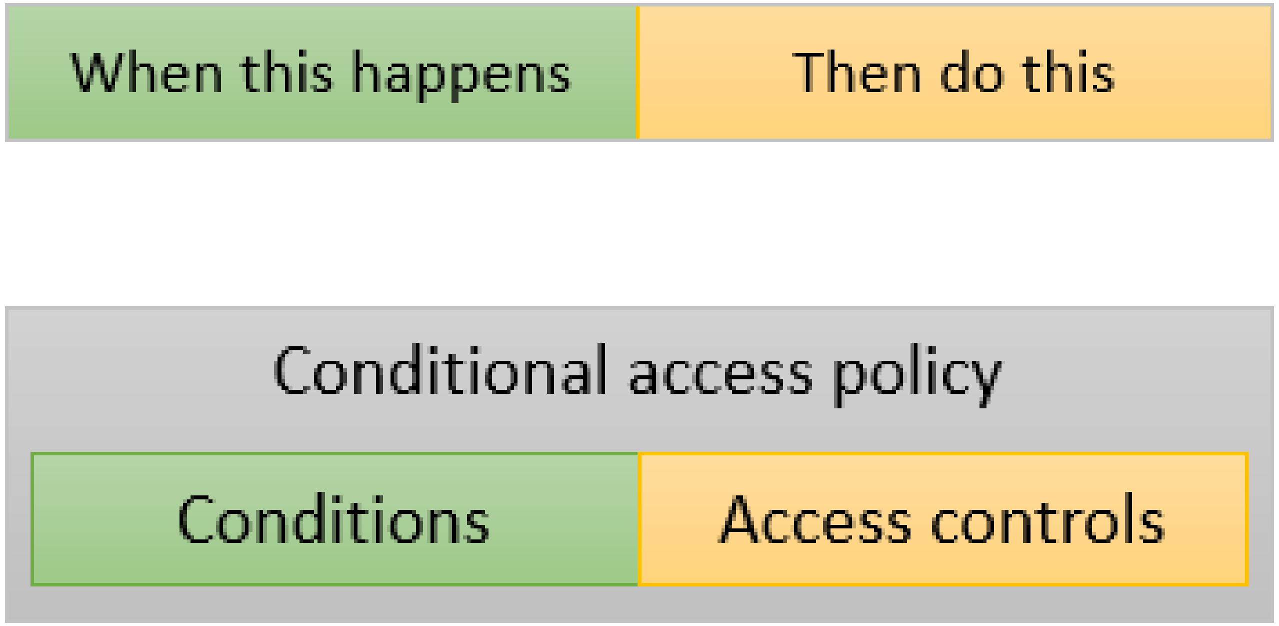
Real-time risk

Allow access

Require MFA

Block access

How does it work?



When this happens

Then do this

Conditional access policy

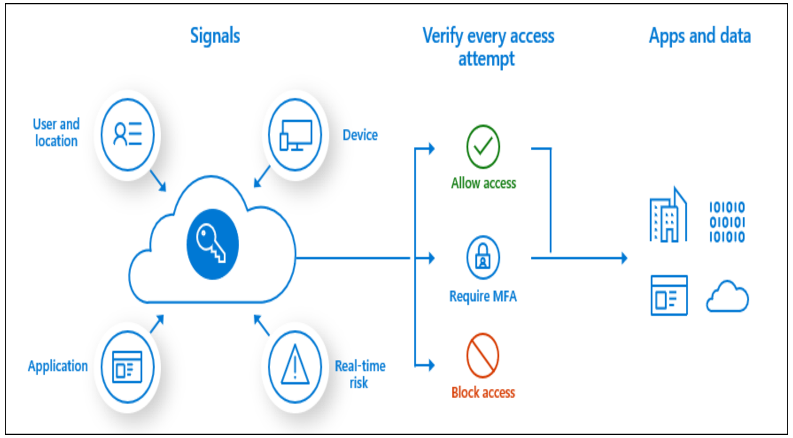
Conditions

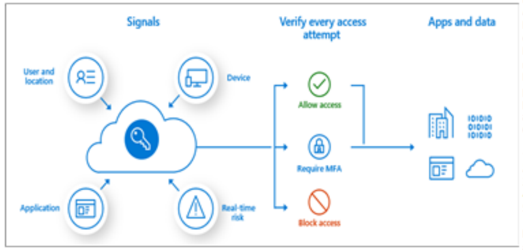
Access controls

How does it really work?

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.

How does it really work



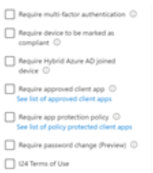


Rules:
All policies are enforced in two phases:
In the first phase, all policies are evaluated and all access controls that aren't satisfied are collected.
In the second phase, you are prompted to satisfy the requirements you haven't met.
If one of the policies blocks access, you are blocked and not 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)

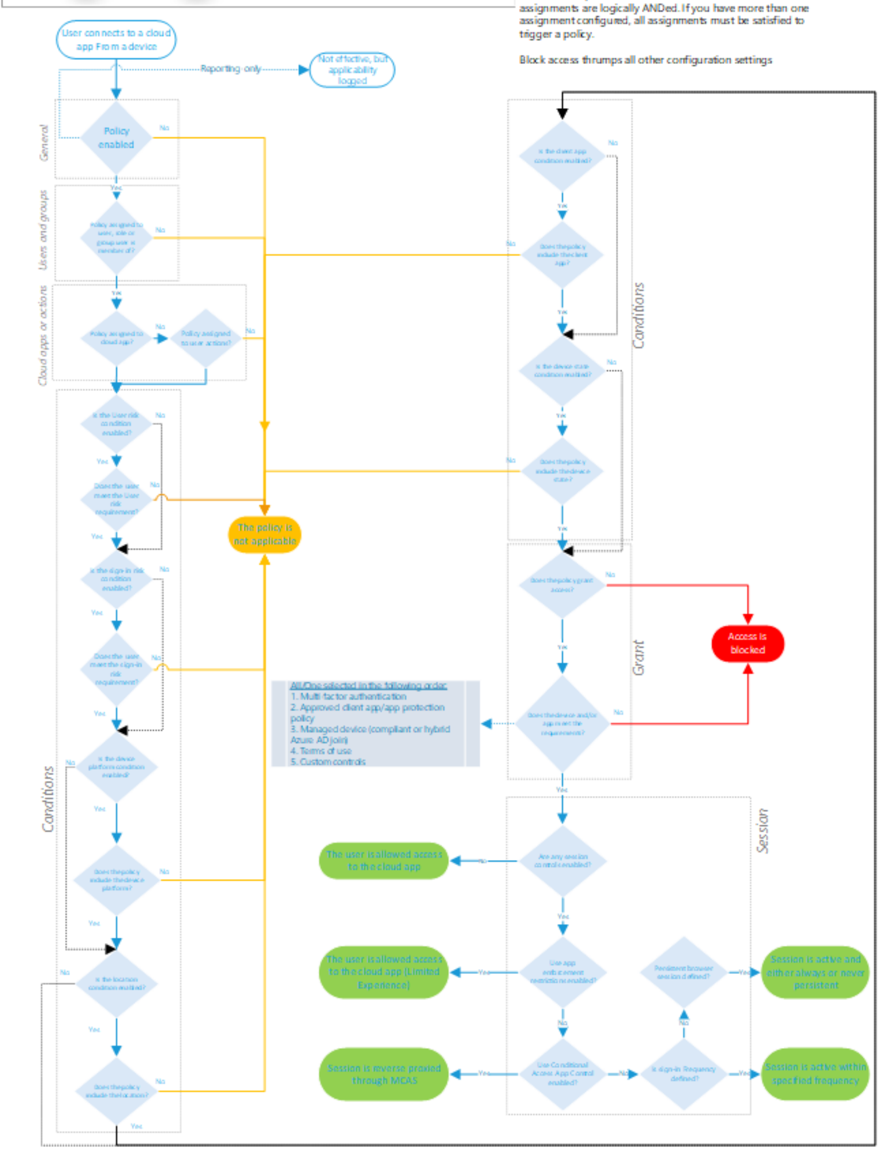
1. Multi-factor authentication
2. Approved client app/app protection policy
3. Managed device (compliant or hybrid Azure AD join)
4. Terms of use
5. Custom controls

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

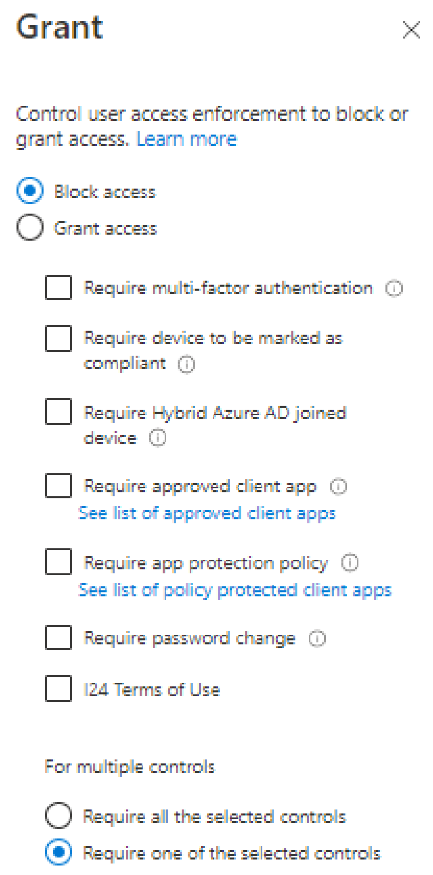


□ Require multi-factor authentication ⓘ
□ Require device to be marked as compliant ⓘ
□ Require Hybrid Azure AD joined device ⓘ
□ Require approved client app ⓘ
See list of approved client apps
□ Require app protection policy ⓘ
See list of policy protected client apps
□ Require password change (Preview)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


User connects to a cloud app From a device
Reporting only
Not effective, but applicability logged
General
Policy enabled
Users and groups
Policy assigned to user, role or group user is member of?
Cloud apps or actions
Policy assigned to cloud app?
Policy assigned to user actions?
Conditions
Is the User risk condition enabled?
Does the user meet the User risk requirement?
Is the sign-in risk condition enabled?
Does the user meet the sign-in risk requirement?
Is the device platform condition enabled?
Does the policy include the device platform?
Is the location condition enabled?
Does the policy include the location?
The policy is not applicable
Is the client app condition enabled?
Does the policy include the client app?
Is the device state condition enabled?
Does the policy include the device state?
Grant
Does the policy grant access?
Does the device and/or app meet the requirements?
Access is blocked
All/One selected in the following order:
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
Session
Are any session controls enabled?
Use app enforcement restrictions enabled?
Use Conditional Access App Control enabled?
Persistent browser session defined?
Is sign-in Frequency defined?
The user is allowed access to the cloud app
The user is allowed access to the cloud app (Limited Experience)
Session is reverse proxied through MCAS
Session is active and either always or never persistent
Session is active within specified frequency
Yes
No

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

Important rules



Grant

Control user access enforcement to block or grant access. Learn more

● Block access
○ Grant access

□ Require multi-factor authentication ⓘ

□ Require device to be marked as compliant ⓘ

□ Require Hybrid Azure AD joined device ⓘ

□ Require approved client app ⓘ
See list of approved client apps

□ Require app protection policy ⓘ
See list of policy protected client apps

□ Require password change ⓘ

□ I24 Terms of Use

For multiple controls

○ Require all the selected controls
● Require one of the selected controls

1. All policies are enforced in two phases
   1. In the first phase, all policies are evaluated (in parallel) and all access controls that aren’t satisfied are collected.
   2. In the second phase, you are prompted to satisfy the requirements you haven’t met.
2. 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. 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
3. Policies are not effective immediately
4. With Continuous Access Evaluation (currently in preview) we will get quicker results

Designing a Conditional Access Strategy

- What kind of devices does the customer use to access cloud apps?
- What kind of applications are 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 personas 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 or people who are local administrator at least nowadays.
- How are licenses being assigned to users (groups, directly)
- Are there any service accounts used that interact with the cloud apps?
- What are the reauthentication settings for the customer?
- 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?

Designing a Conditional Access Strategy

- Azure Active Directory Conditional Access Deployment Plan:
- https://aka.ms/CADPDownload

- How To: Plan your Conditional Access deployment in Azure Active Directory – https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

- Conditional Access documentation spreadsheet - https://gallery.technet.microsoft.com/Conditional-Access-dc903421

Define Scenarios

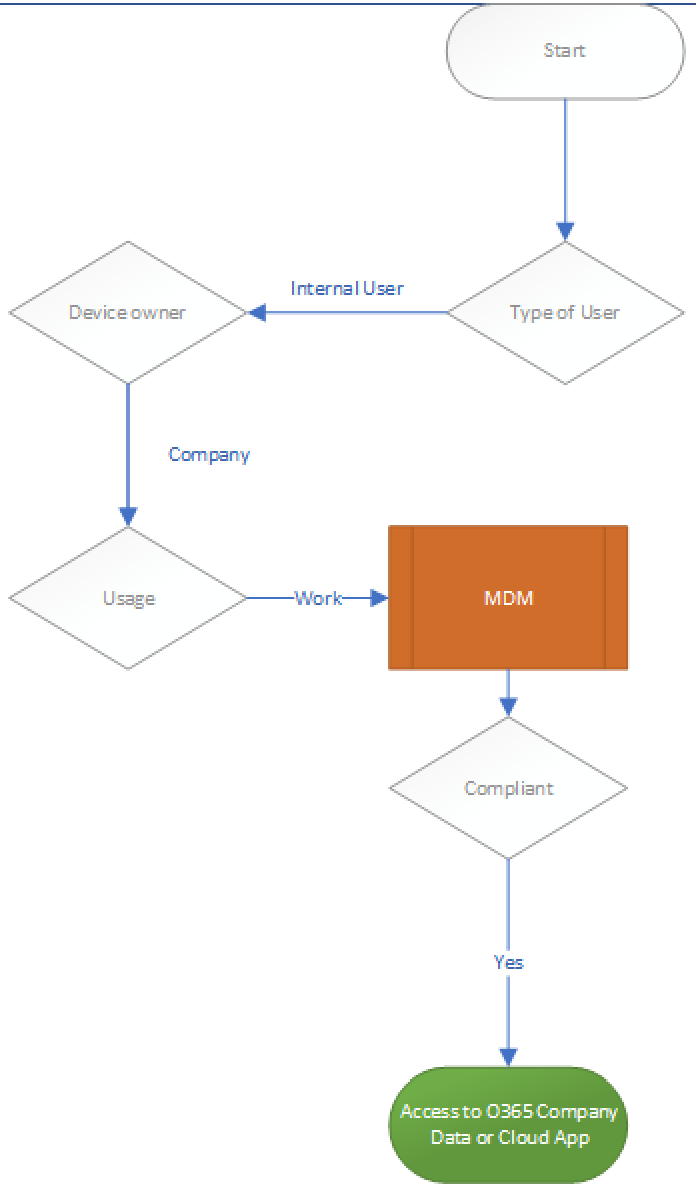
Scenario 1: Allow devices managed by Intune access all the cloud apps using Apps and Desktop Clients and Modern Authentication Clients if compliant

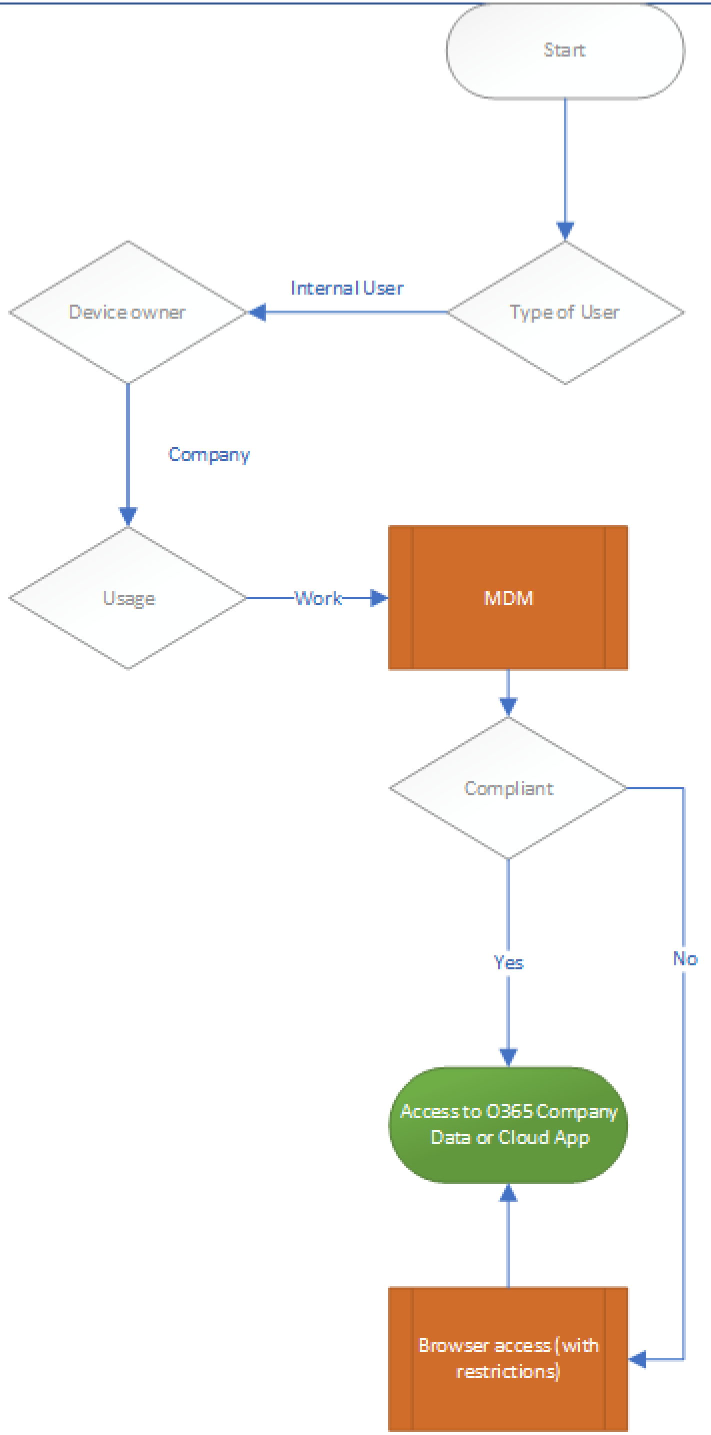
- *Access to “All Cloud Apps” by “Users with EMS License” using “Any” device platform” coming from “any location” using “Mobile Apps and Desktop Clients” or “Modern authentication clients” is allowed, but device must be compliant.*
- **Scenario 2:** Only allow Apps we can manage to access cloud apps when device is not managed.
- *Allow users with EMS License using devices not managed by intune to access (portion of, t.b.d.) 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 doesn’t operate.*

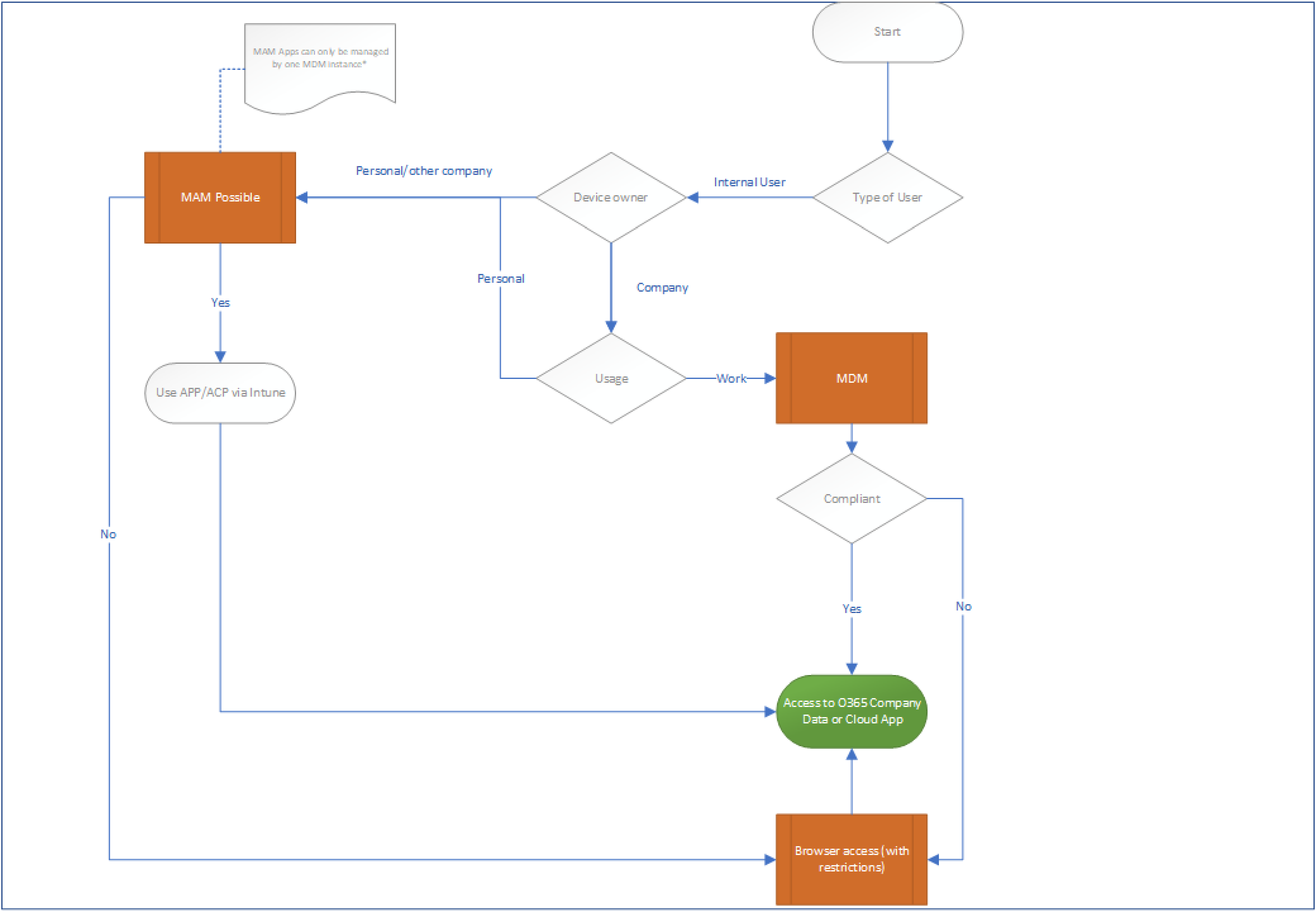
Goals

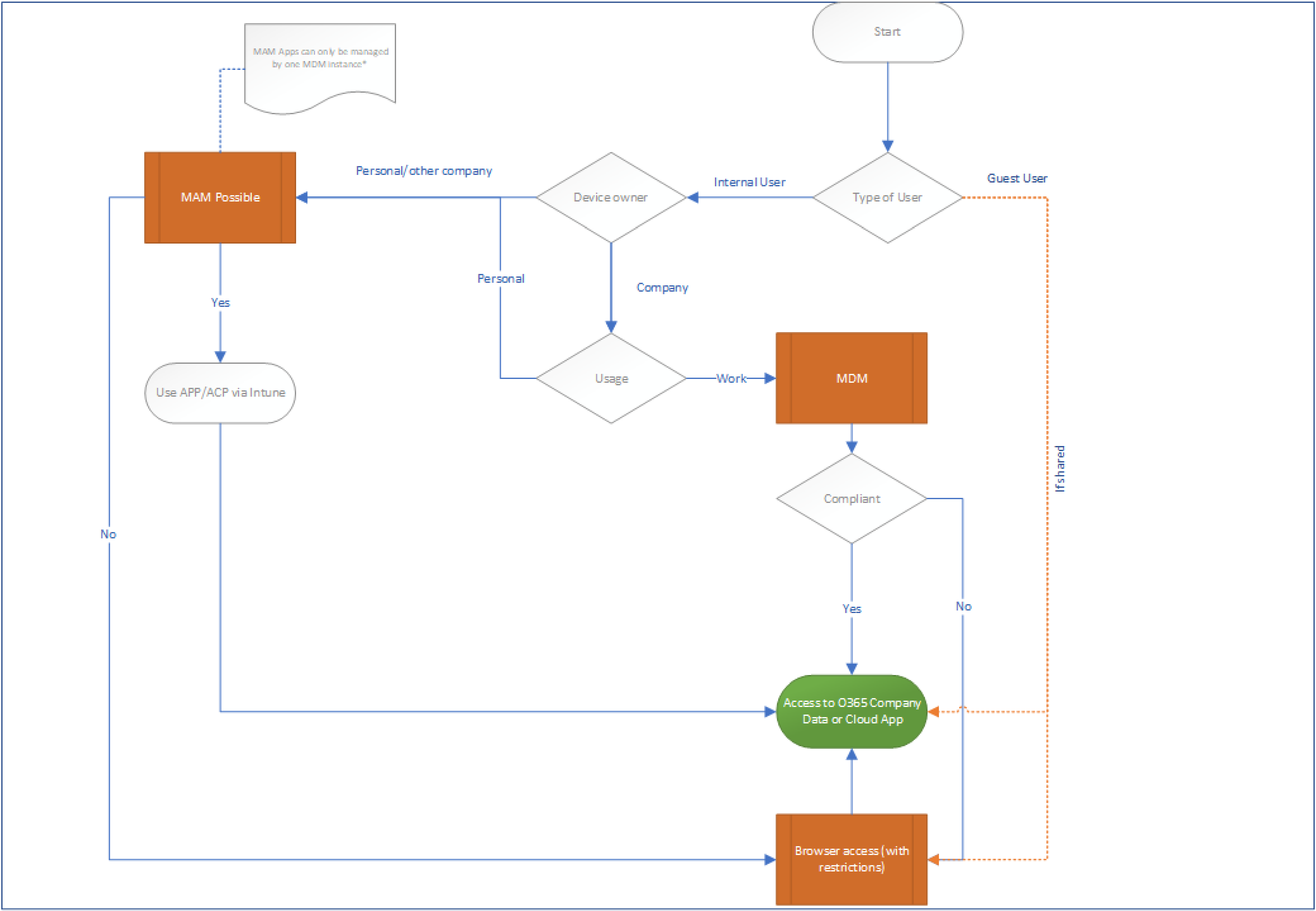
Protect company data hosted in Office 365 and protect identity of users

Access to O365 Company Data or Cloud App

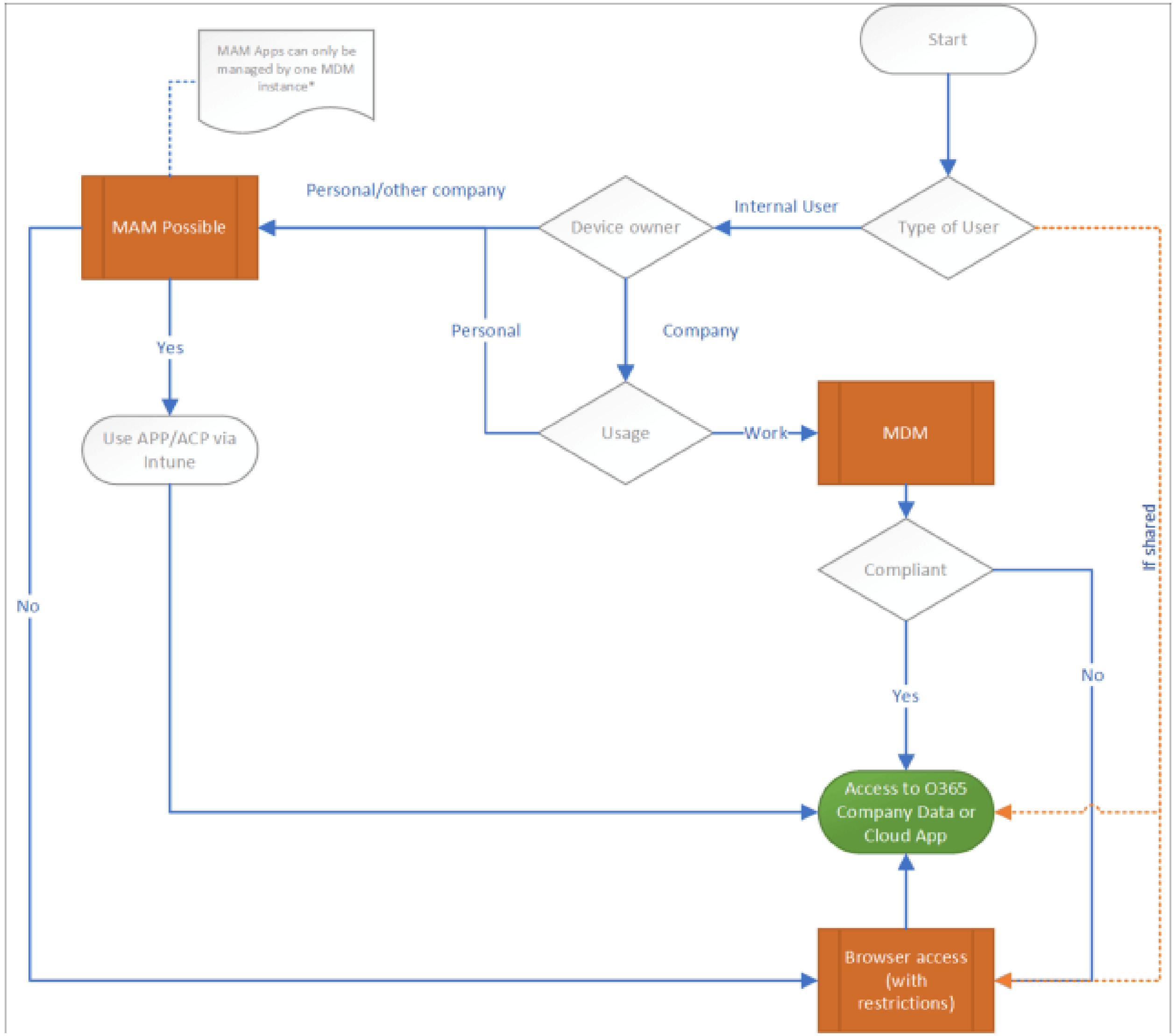

Start
Type of User
Internal User
Device owner
Company
Usage
Work
MDM
Compliant
Yes
Access to O365 Company Data or Cloud App


Start
Type of User
Internal User
Device owner
Company
Usage
Work
MDM
Compliant
Yes
No
Access to O365 Company Data or Cloud App
Browser access (with restrictions)

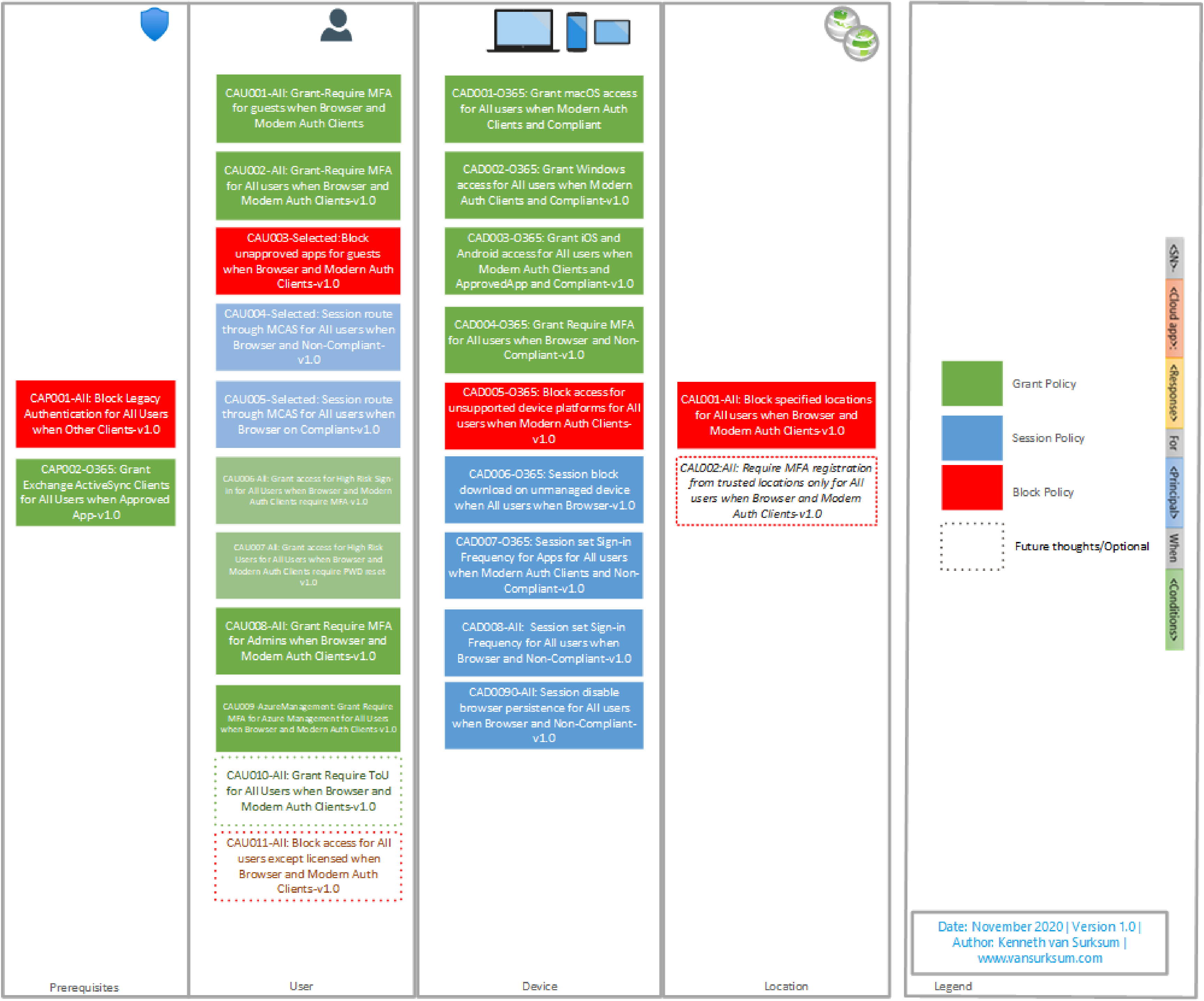

Start
Type of User
Internal User
Device owner
Personal/ other company
MAM Apps can only be managed by one MDM instance*
MAM Possible
Yes
Use APP/ACP via Intune
Personal
Company
Usage
Work
MDM
Compliant
Yes
No
No
Access to O365 Company Data or Cloud App
Browser access (with restrictions)


Start
Type of User
Guest User
Internal User
Device owner
Personal/other company
MAM Apps can only be managed by one MDM instance*
MAM Possible
Personal
Company
Usage
Work
MDM
Yes
Use APP/ACP via Intune
Compliant
Yes
No
If shared
No
Access to O365 Company Data or Cloud App
Browser access (with restrictions)

Consequences



- Users on mobile devices must be migrated to either MDM or MAM (Outlook and other Office apps on the approved apps list)
- We must implement Guest user governance
    - Ask yourself if you want to allow full access to Guests from unmanaged devices?
- We must review the usage of non-personal accounts (Service Accounts)



Prerequisites

CAP001-All: Block Legacy Authentication for All Users when Other Clients-v1.0

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

User

CAU001-All: Grant-Require MFA for guests when Browser and Modem Auth Clients

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

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

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

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

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

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

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

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

CAU010-All: Grant Require ToU for All Users when Browser and Modem Auth Clients-v1.0

CAU011-All: Block access for All users except licensed when Browser and Modem Auth Clients-v1.0

Device

CAD001-O365: Grant macOS access for All users when Modern Auth Clients and Compliant

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

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

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

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

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

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

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

CAD0090-All: Session disable browser persistence for All users when Browser and Non-Compliant-v1.0

Location

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

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

Legend

🟩 Grant Policy

🟦 Session Policy

🟥 Block Policy

⬚ Future thoughts/Optional

Date: November 2020 | Version 1.0 | Author: Kenneth van Surksum | www.vansurksum.com

Additional Notes

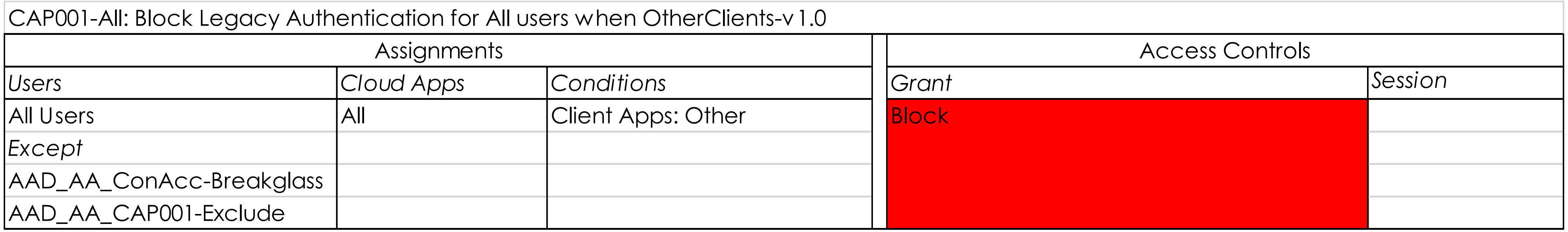
- Even though MS recommends less is better when it comes to CA policies, I prefer granularity
  - Conditional Access policy per functionality
  - For each Conditional Access policy there is a specific exclude group (which also includes the Breakglass accounts)
    - Therefore, if exceptions are made, they can be very specific
    - Consider implementing access reviews on those exclude groups if you have Azure AD P2
- Naming convention is very important, follow MS best practices

<SN>-	<Cloud app>:	<Response>	For	<Principal>	When	<Conditions>

- The Conditional Access policies are numbered, **and** versioned
  - CAP = Conditional Access Prerequisite
  - CAU = Conditional Access User
  - CAD = Conditional Access Device
  - CAL = Conditional Access Location
  - Example: CAD007-O365: Session set Sign-in Frequency for Apps for All users when Modern Auth Clients and Non-Compliant-v1.0

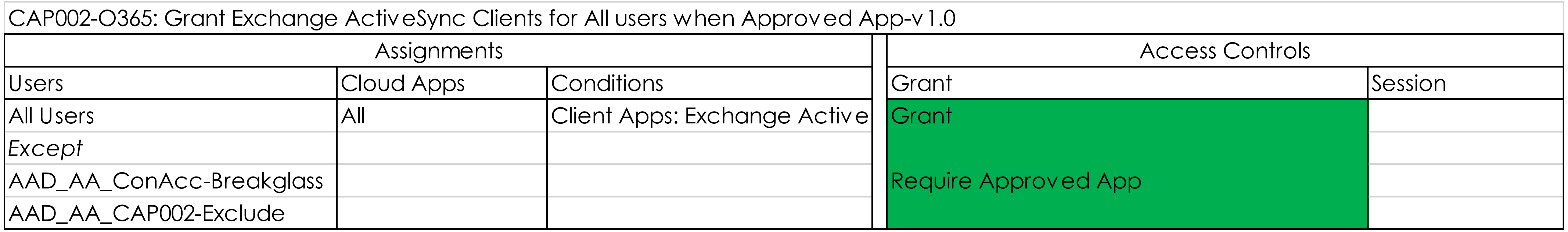
Some examples

- Prerequisite policies



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				



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

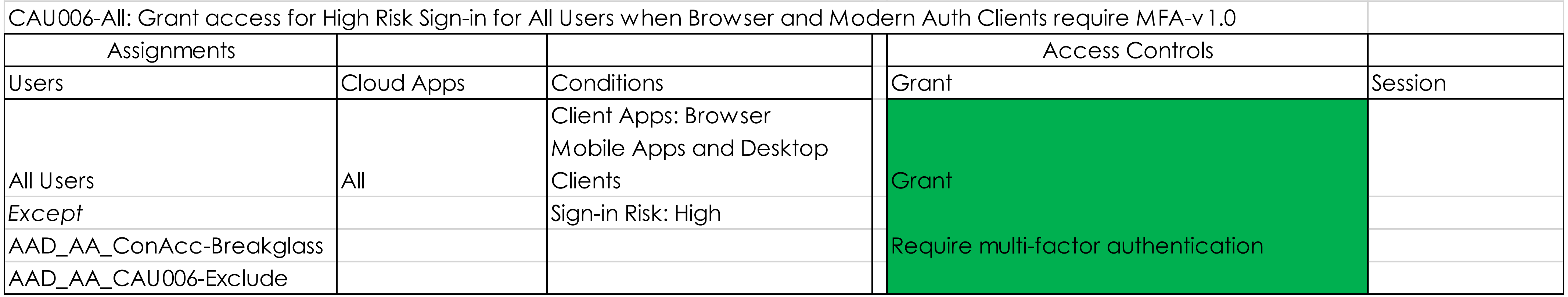
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Exchange Active	Grant	
Except				
AAD_AA_ConAcc-Breakglass			Require Approved App	
AAD_AA_CAP002-Exclude				

Some examples

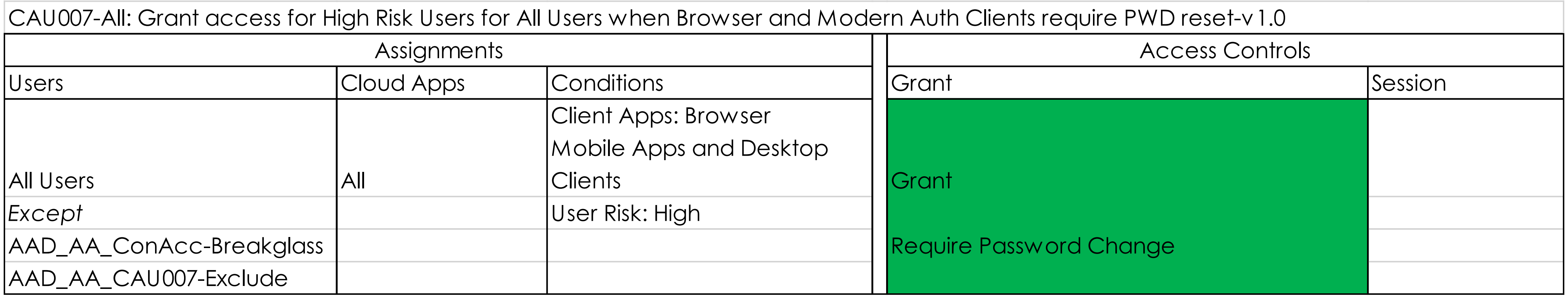
CAU004-Selected: Session route through MCAS for All users when Browser on Non-Compliant-v1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	<Selected>	Client Apps: Browser		Use Conditional Access App Control: Block downloads (Preview)
Except		Device state: All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

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				

Some examples



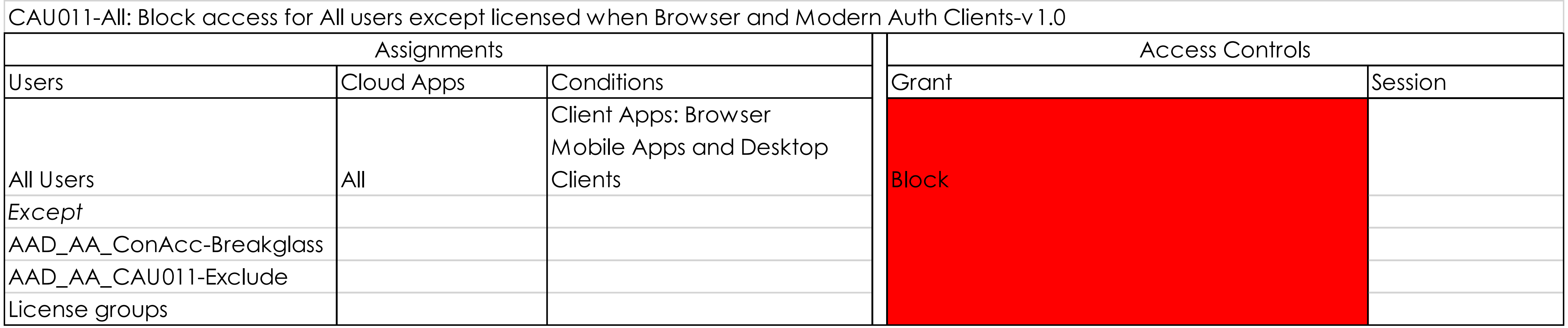
CAU006-All: Grant access for High Risk Sign-in for All Users when Browser and Modern Auth Clients require MFA-v 1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Browser Mobile Apps and Desktop Clients	Grant	
Except		Sign-in Risk: High		
AAD_AA_ConAcc-Breakglass			Require multi-factor authentication	
AAD_AA_CAU006-Exclude				



CAU007-All: Grant access for High Risk Users for All Users when Browser and Modern Auth Clients require PWD reset-v 1.0				
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				

Note: Disable the policies in Azure AD Identity Protection

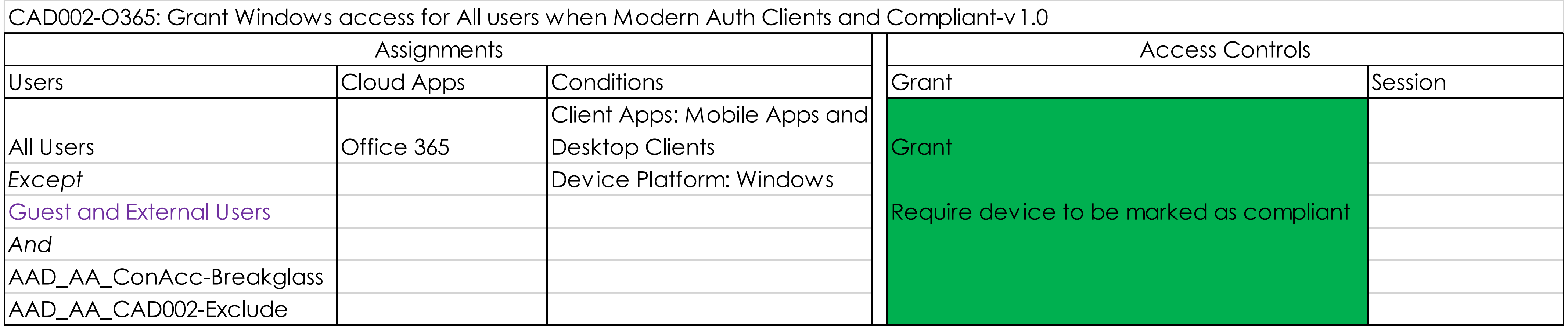
Some examples



CAU011-All: Block access for All users except licensed when Browser and Modern Auth Clients-v 1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Browser Mobile Apps and Desktop Clients	Block	
Except				
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAU011-Exclude				
License groups				

Note: Be Very Carefull!

Some examples

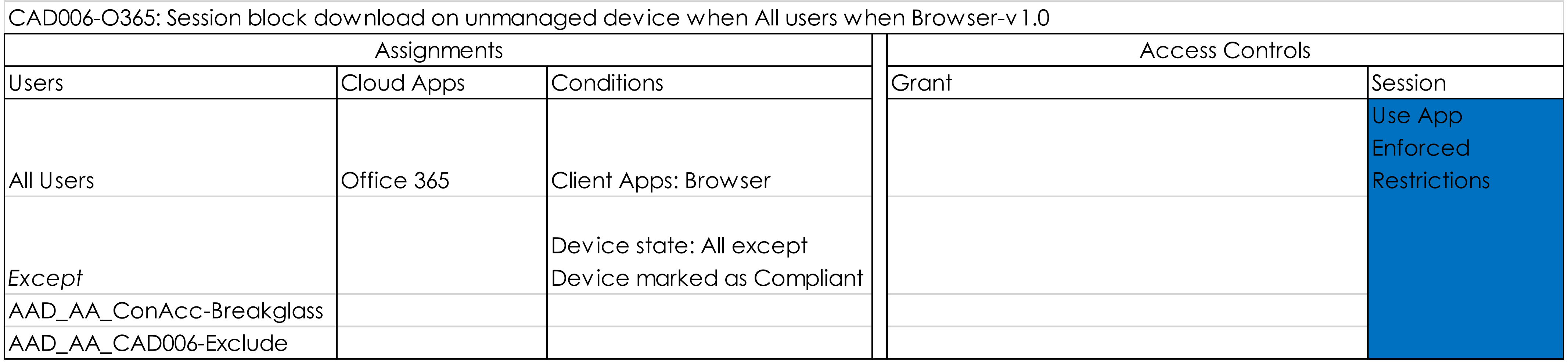


CAD002-O365: Grant Windows access for All users when Modern Auth Clients and Compliant-v 1.0

Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	Office 365	Client Apps: Mobile Apps and Desktop Clients	Grant	
Except		Device Platform: Windows		
Guest and External Users			Require device to be marked as compliant	
And				
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAD002-Exclude				

Note: Guest access depending on your design choices

Some examples



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				

Notes:

Be careful when setting the SharePoint settings, since that setting will create 2 enabled CA policies without asking

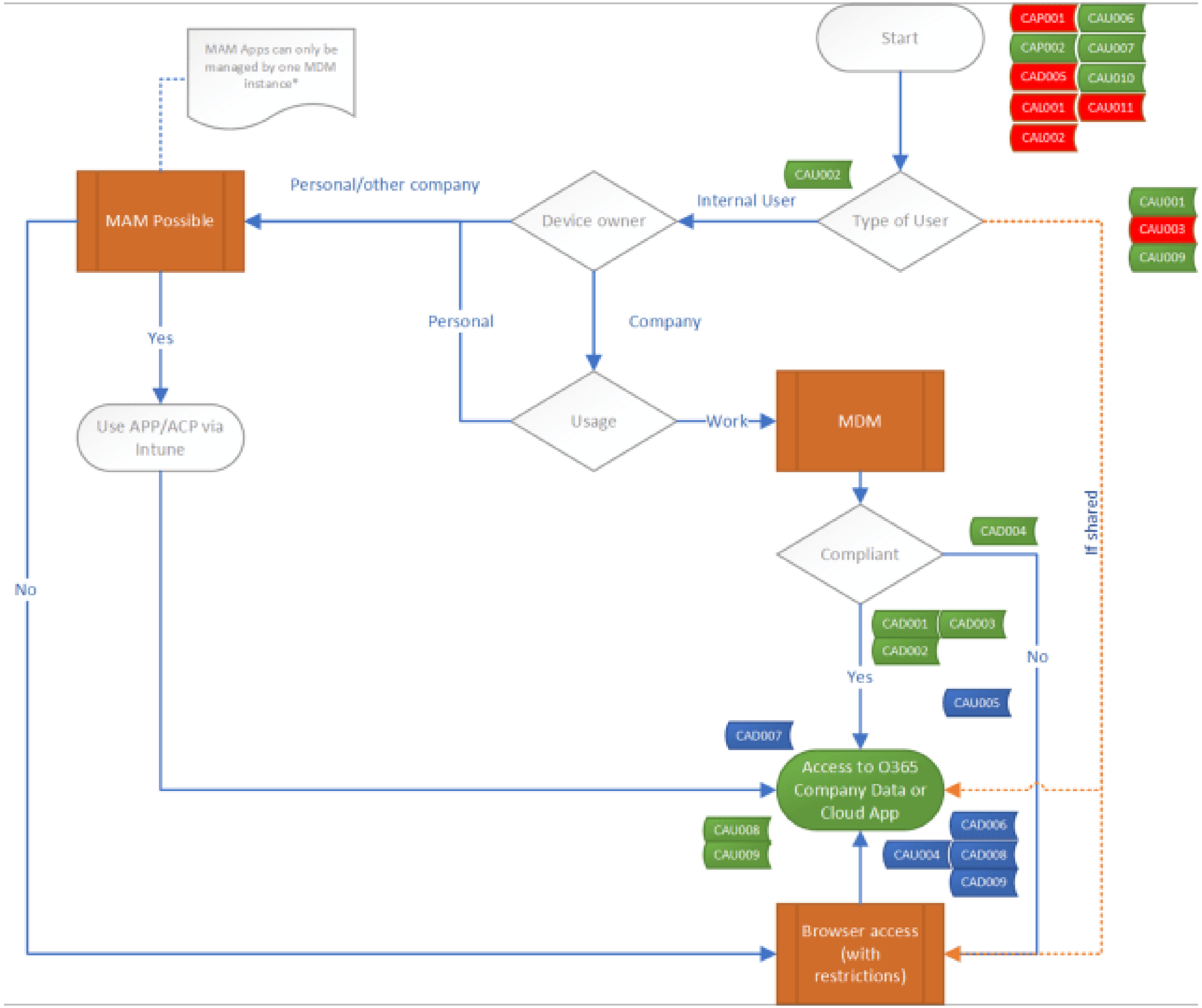
Consider implementing Sensitivity labels if you want more granularity

Some examples

CAD008-All: Session set Sign-in Frequency for All users when Browser and Non-Compliant-v 1.0				
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				

CAD0009-All: Session disable browser persistence for All users when Browser and Non-Compliant-v 1.0				
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				

Notes: Review your current reauthentication settings


Start
CAP001
CAU006
CAP002
CAU007
CAD005
CAU010
CAI001
CAU011
CAI002
MAM Apps can only be managed by one MDM instance*
CAU002
Type of User
Internal User
CAU001
CAU003
CAU009
Device owner
Personal/other company
MAM Possible
Personal
Company
Yes
Use APP/ACP via Intune
Usage
Work
MDM
Compliant
CAD004
If shared
No
CAD001
CAD003
CAD002
Yes
No
CAU005
CAD007
Access to O365 Company Data or Cloud App
CAU008
CAU009
CAD006
CAU004
CAD008
CAD009
Browser access (with restrictions)

Tips

- Use the **Access Review** functionality if available (Azure AD P2)
- Define operational procedures to execute when **something out of your control goes down** (f.e. Azure MFA outage)
- Regulary **review what's new** in Azure AD conditional access and determine if it impacts your environment
  - You can see what's new in Azure Active Directory here: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/whats-new and on the Azure Updates webpage here: https://azure.microsoft.com/en-in/updates/?product=active-directory&status=all&updatetype=features
- 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.
  - What are service dependencies in Azure Active Directory Conditional Access? – https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/service-dependencies
- Make sure that you can **test your scenarios** (have equipment available)
  - Android device, Apple Device, Windows 10 device, VPN software….
- Create Alerts in Log Analytics to notify you when:
  - New Conditional Access policies are created
  - Existing Conditional Access policies are modified

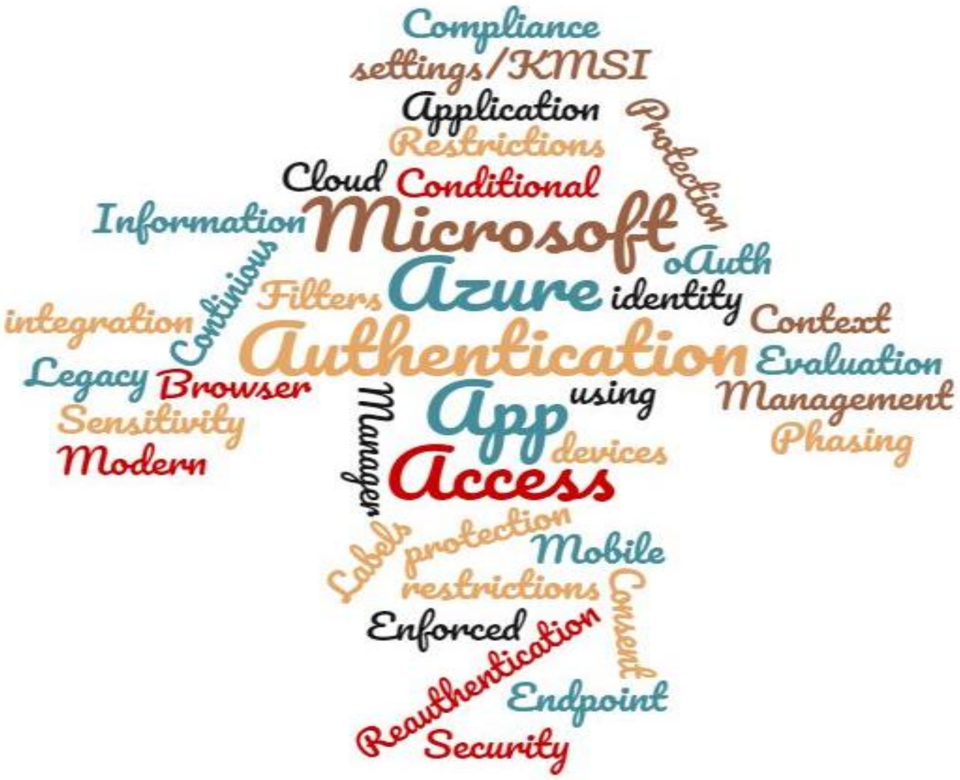
Further Resources

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

UserVoice: https://feedback.azure.com/forums/169401-azure-active-directory/category/167259-conditional-access

So much more to tell



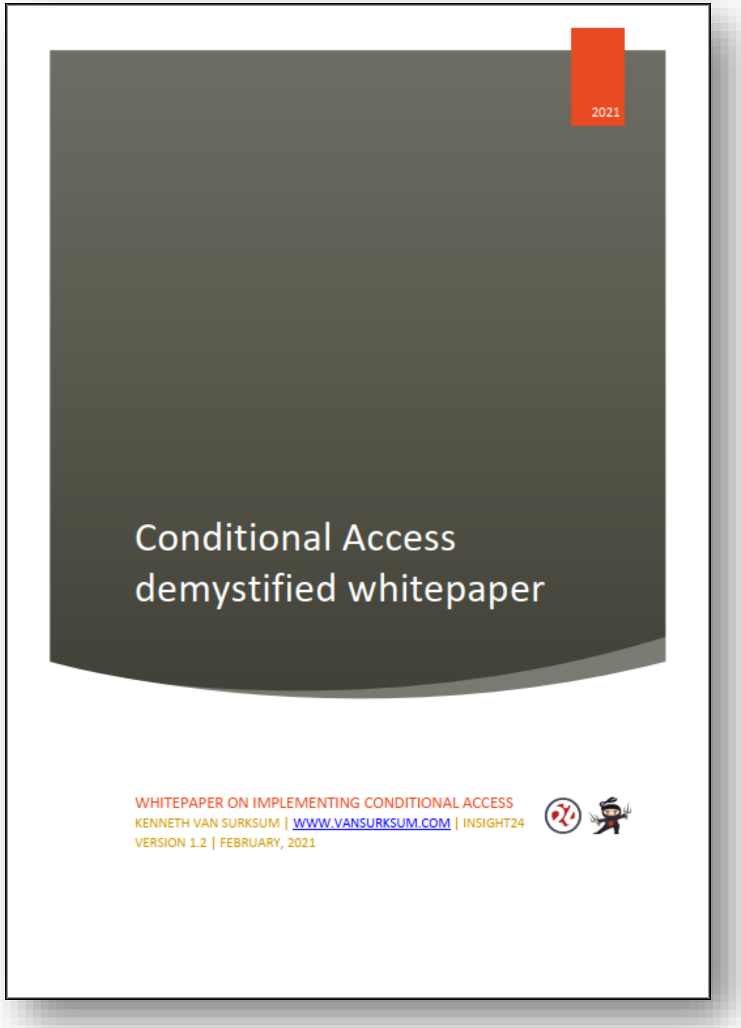
White paper

Latest released: The February 2021 update of the Conditional Access demystified whitepaper.

- Major release (from 30 to 77 pages)
- Includes updates workflow cheat sheet
- Much more information added

Download the paper from my blog at:

https://www.vansurksum.com/2021/02/16/february-2021-update-of-the-azure-ad-conditional-access-demystified-whitepaper-and-workflow-cheat-sheet/



2021

Conditional Access demystified whitepaper

WHITEPAPER ON IMPLEMENTING CONDITIONAL ACCESS
KENNETH VAN SURKSUM | WWW.VANSURKSUM.COM | INSIGHT24
VERSION 1.2 | FEBRUARY, 2021

References

- Microsoft is going to disable basic/legacy authentication for Exchange Online. What does that actually mean and does that impact me?
- Understanding and governing reauthentication settings in Azure Active Directory
- Extending Conditional Access to Microsoft Cloud App Security using Conditional Access App Control
- Azure AD Identity Protection deep dive
- Azure AD Continuous access evaluation (CAE), a first look
- Limit Access to Outlook Web Access, SharePoint Online and OneDrive using Conditional Access App Enforced Restrictions
- Defining more granularity for your Conditional Access App Enforced Restrictions using Sensitivity Labels
- Mobile Application Management for Mobile Devices with Microsoft Endpoint Manager/Intune deep dive
- Conditional Access demystified: My recommended default set of policies
- Defining more granularity for your Conditional Access App Enforced Restrictions using Sensitivity Labels
- Designing and building your Microsoft Endpoint Manager/Intune environment for Operations