

Conditional Access Demystified

- Kenneth van Surksum
- Modern Workplace Ninja at Insight24
- Twitter: @kennethvs
- Blog: <https://www.vansurksum.com>

Azure AD Conditional Access

Demystified – February 2021 edition

Our topics for Today!

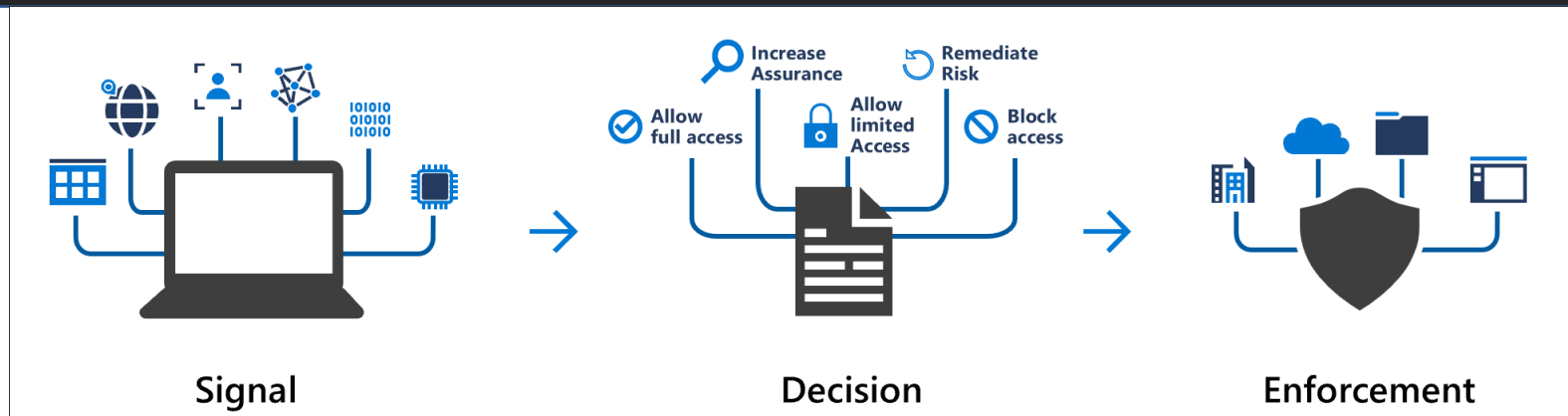


- What is Conditional Access?
- How does Conditional Access work?
- Designing a Conditional Access environment
- Implementing Conditional Access
- Troubleshooting Conditional Access (if time permits)

What is Conditional Access?

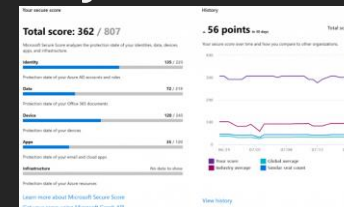
Microsoft Description:

*"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."*



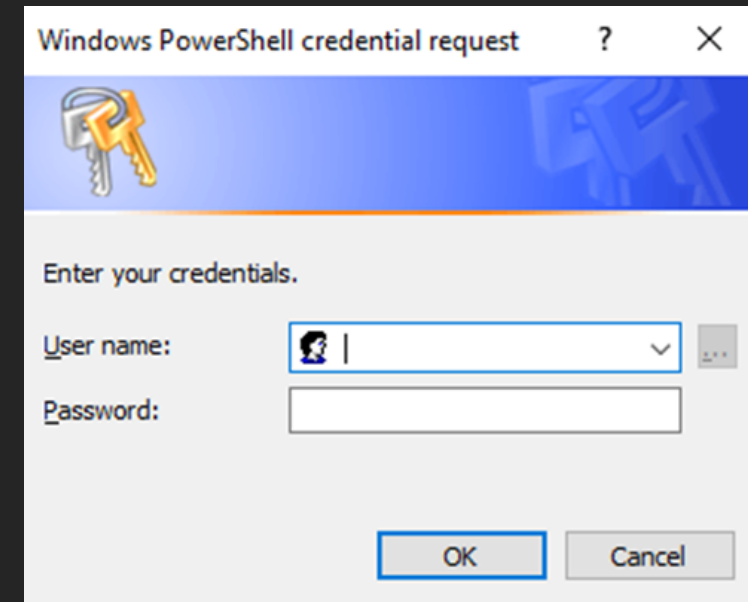
What is Conditional Access?

- 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



Prerequisites

- 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



101010
010101
101010



- How does it work?

When this happens

Then do this

Conditional access policy

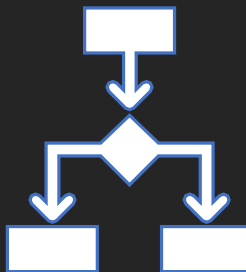
Conditions

Access controls

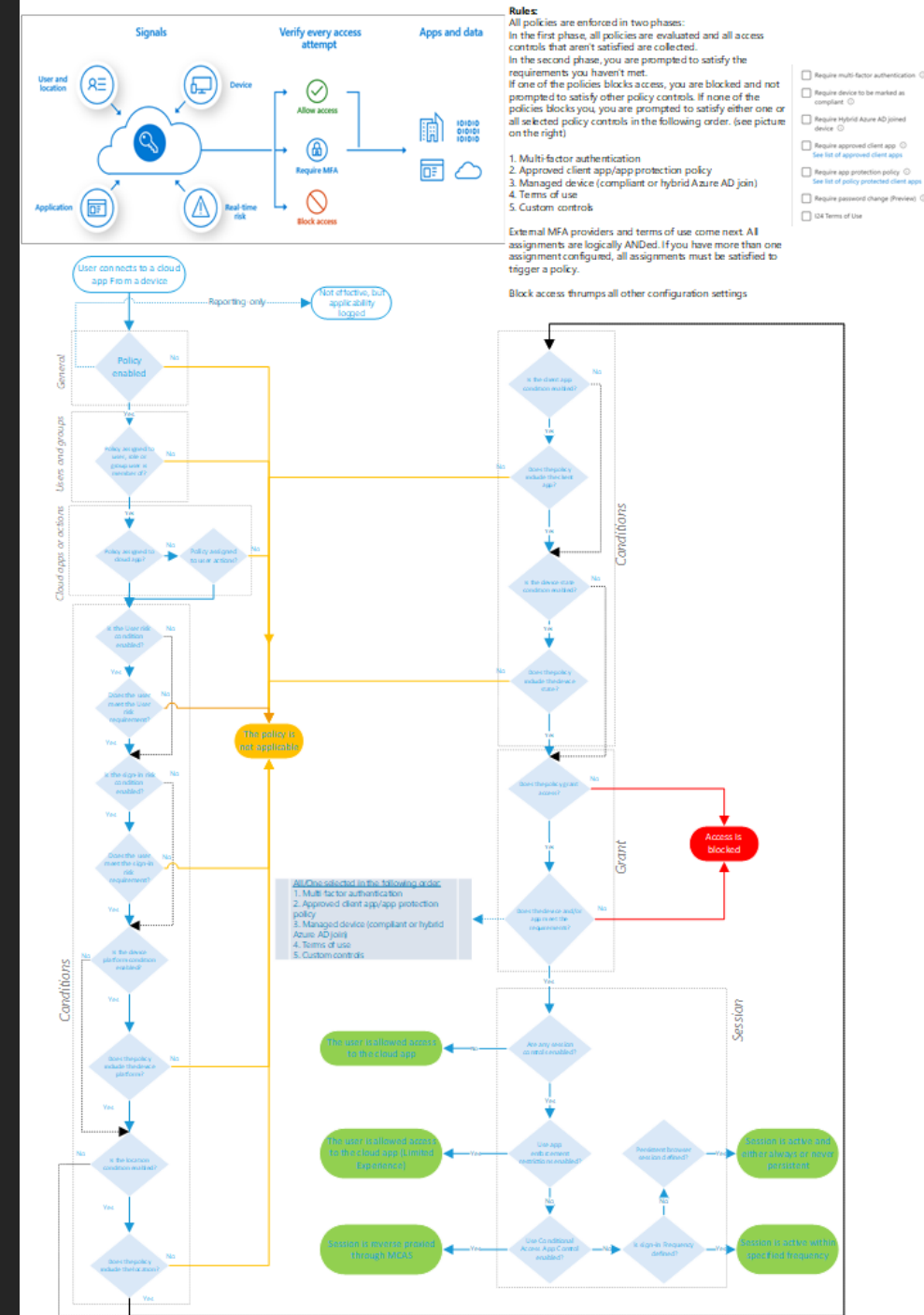
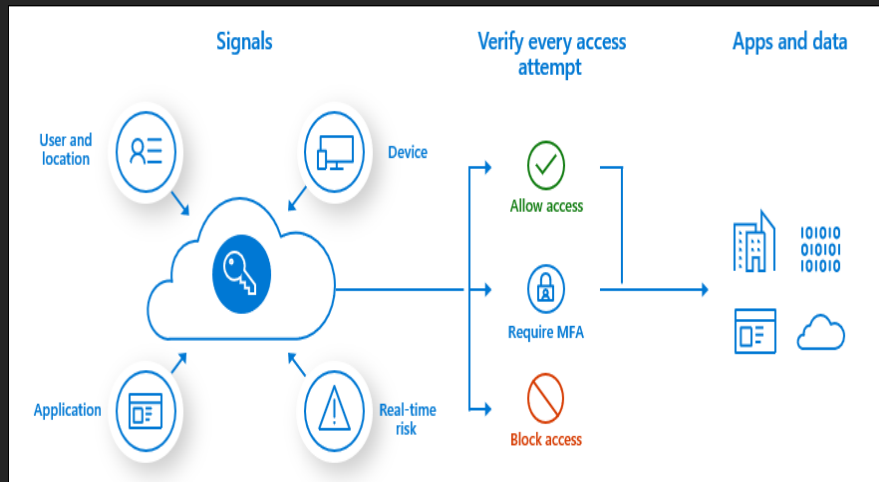
How does it really work?

The 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.

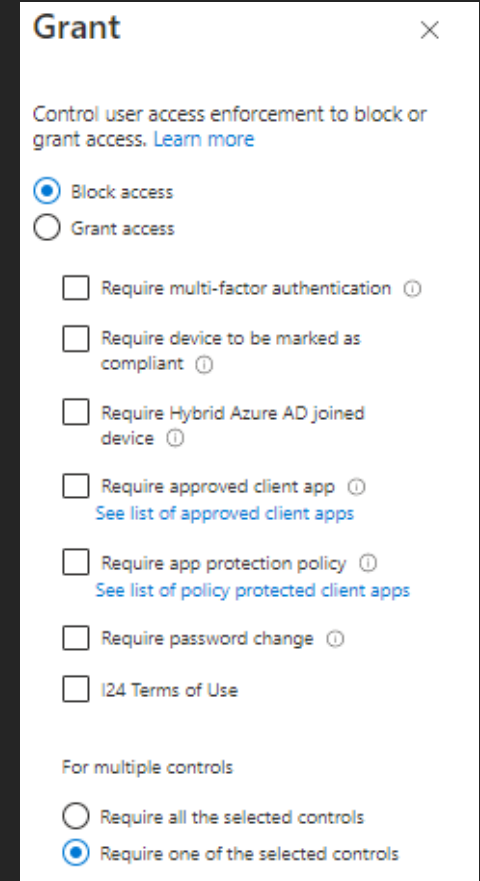


How does it really work?



Important rules

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



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

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

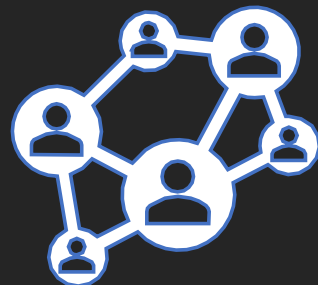
- Azure Active Directory Conditional Access Deployment Plan:
 - <https://aka.ms/CADPDownload>
- How To: Plan your Conditional Access deployment in Azure Active Directory – <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access>
- Conditional Access documentation 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.*

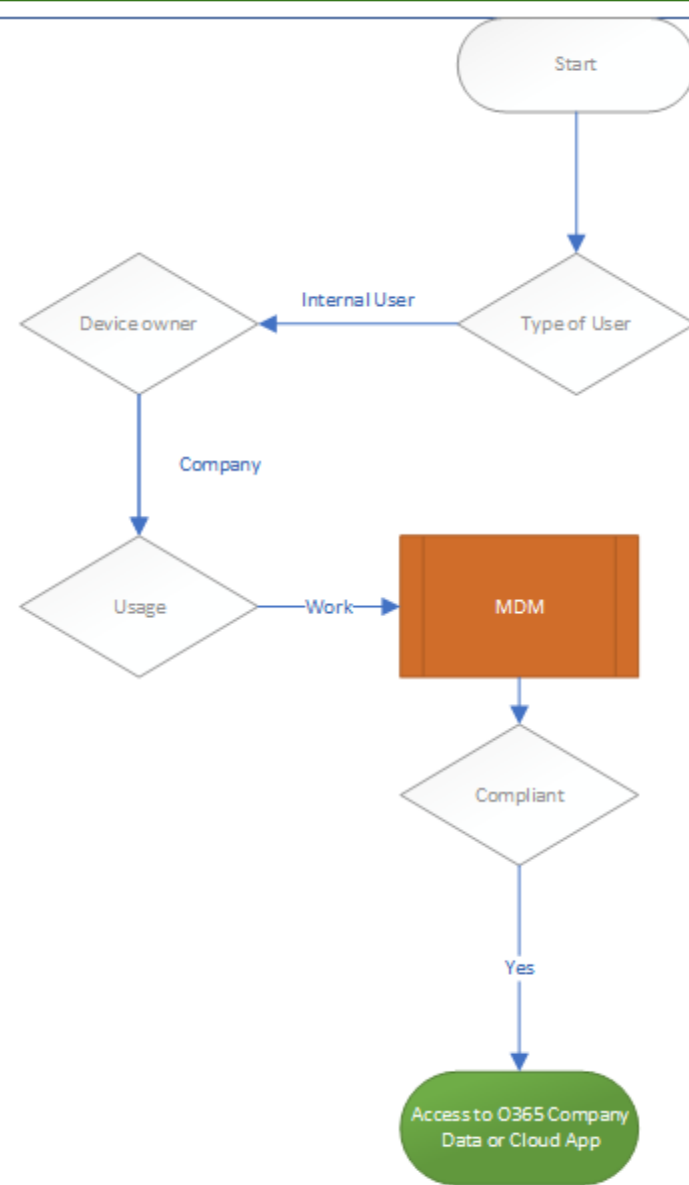


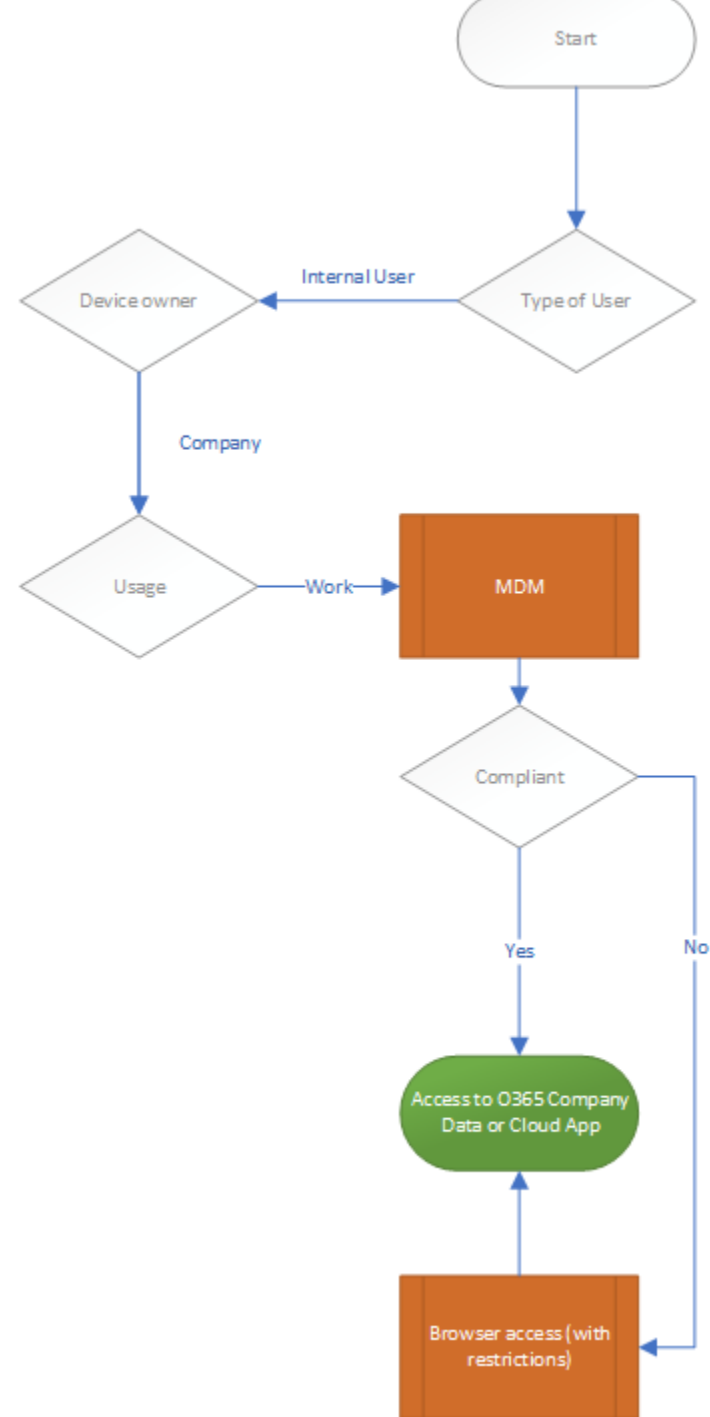
Goals

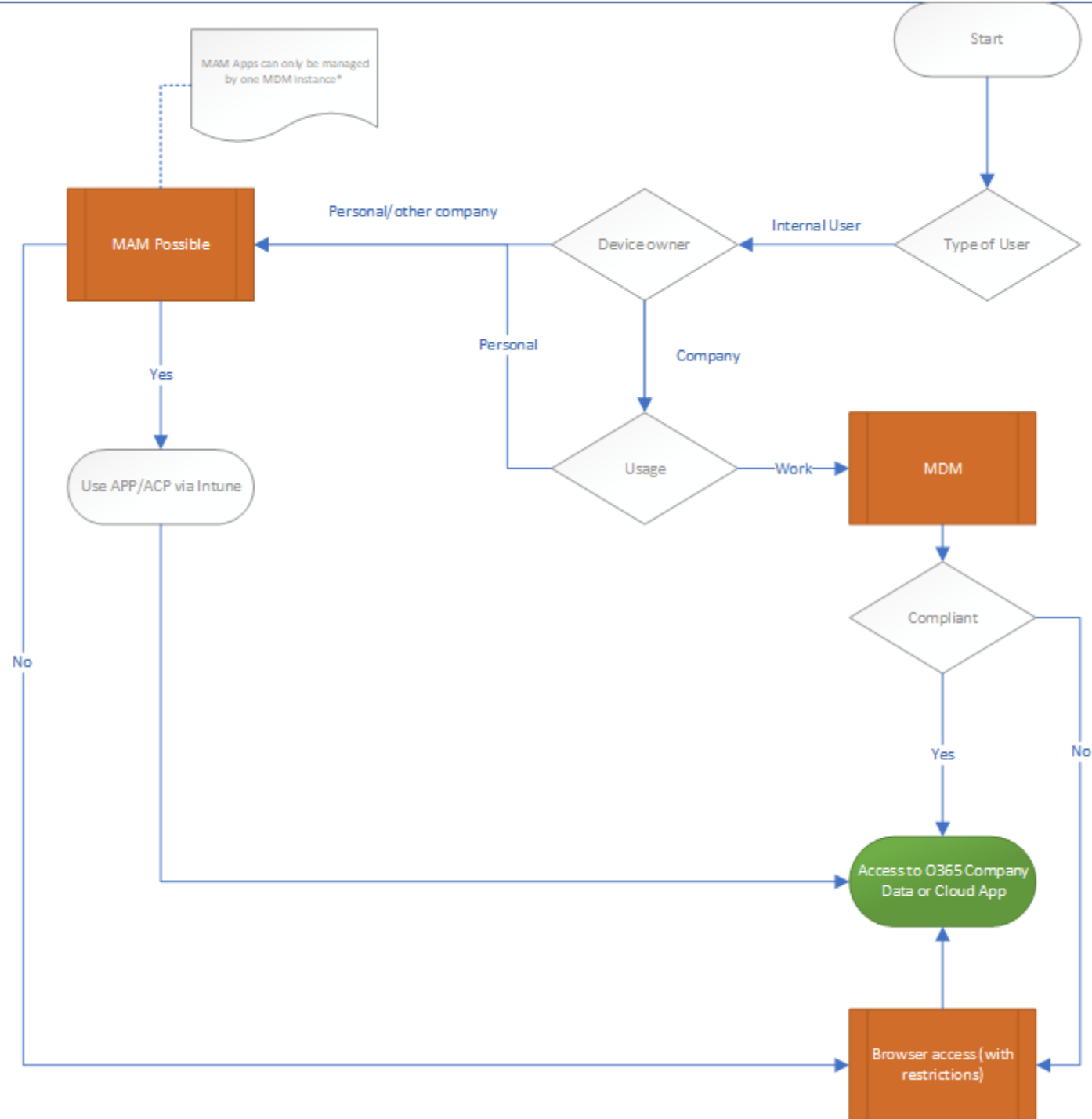
- Protect company data hosted in Office 365 and protect identity of users

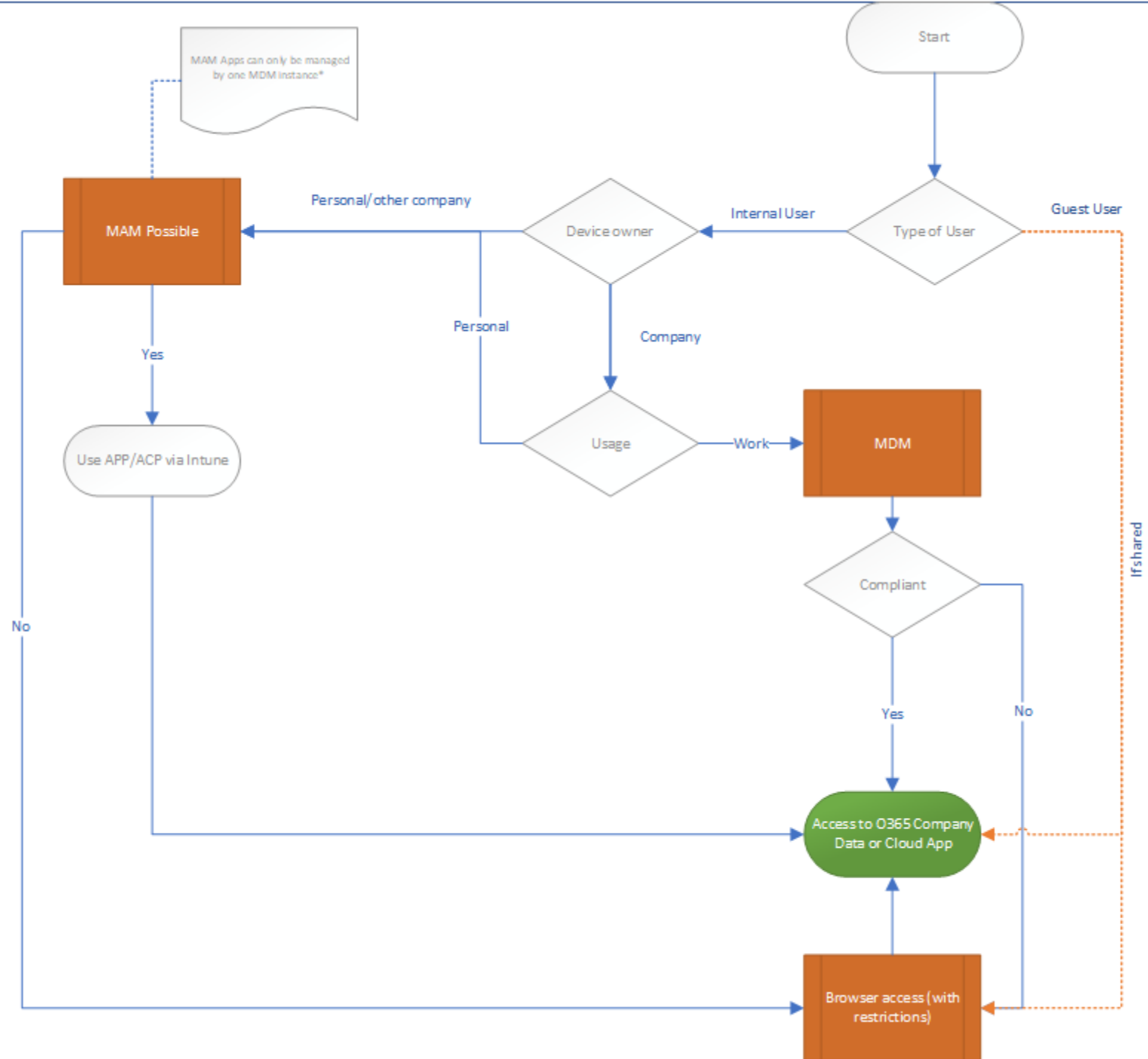


Access to O365 Company
Data or Cloud App



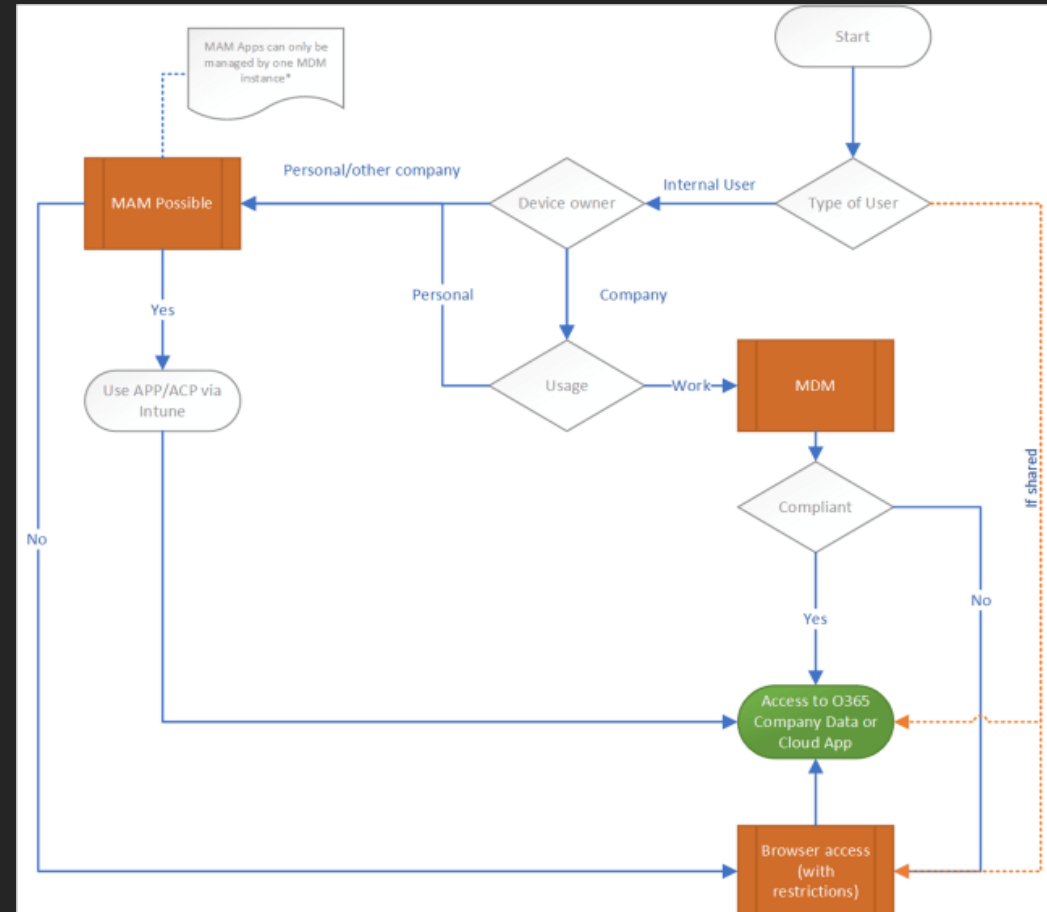






Consequences

- 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)



<div data-bbox="606 0 652 57"></div> <div data-bbox="435 544 657 636">CAP001-All: Block Legacy Authentication for All Users when Other Clients-v1.0</div> <div data-bbox="435 654 657 746">CAP002-0365: Grant Exchange ActiveSync Clients for All Users when Approved App-v1.0</div>	<div data-bbox="861 0 907 57"></div> <div data-bbox="723 105 983 198">CAU001-All: Grant-Require MFA for guests when Browser and Modern Auth Clients</div> <div data-bbox="723 219 983 312">CAU002-All: Grant-Require MFA for All users when Browser and Modern Auth Clients-v1.0</div> <div data-bbox="723 319 983 419">CAU003-Selected:Block unapproved apps for guests when Browser and Modern Auth Clients-v1.0</div> <div data-bbox="723 434 983 526">CAU004-Selected: Session route through MCAS for All users when Browser and Non-Compliant-v1.0</div> <div data-bbox="723 548 983 641">CAU005-Selected: Session route through MCAS for All users when Browser on Compliant-v1.0</div> <div data-bbox="723 662 983 755">CAU006-All: Grant access for High Risk Sign-in for All Users when Browser and Modern Auth Clients require MFA v1.0</div> <div data-bbox="723 762 983 855">CAU007-All: Grant access for High Risk Users for All Users when Browser and Modern Auth Clients require PWD reset v1.0</div> <div data-bbox="723 869 983 962">CAU008-All: Grant Require MFA for Admins when Browser and Modern Auth Clients-v1.0</div> <div data-bbox="723 983 983 1076">CAU009-AzureManagement: Grant Require MFA for Azure Management for All Users when Browser and Modern Auth Clients v1.0</div> <div data-bbox="723 1083 983 1176">CAU010-All: Grant Require ToU for All Users when Browser and Modern Auth Clients-v1.0</div> <div data-bbox="723 1183 983 1283">CAU011-All: Block access for All users except licensed when Browser and Modern Auth Clients-v1.0</div>	<div data-bbox="1105 0 1314 71"></div> <div data-bbox="1054 105 1327 198">CAD001-0365: Grant macOS access for All users when Modern Auth Clients and Compliant</div> <div data-bbox="1054 219 1327 312">CAD002-0365: Grant Windows access for All users when Modern Auth Clients and Compliant-v1.0</div> <div data-bbox="1054 319 1327 419">CAD003-0365: Grant iOS and Android access for All users when Modern Auth Clients and ApprovedApp and Compliant-v1.0</div> <div data-bbox="1054 434 1327 526">CAD004-0365: Grant Require MFA for All users when Browser and Non-Compliant-v1.0</div> <div data-bbox="1054 548 1327 641">CAD005-0365: Block access for unsupported device platforms for All users when Modern Auth Clients-v1.0</div> <div data-bbox="1054 648 1327 741">CAD006-0365: Session block download on unmanaged device when All users when Browser-v1.0</div> <div data-bbox="1054 748 1327 855">CAD007-0365: Session set Sign-in Frequency for Apps for All users when Modern Auth Clients and Non-Compliant-v1.0</div> <div data-bbox="1054 862 1327 962">CAD008-All: Session set Sign-in Frequency for All users when Browser and Non-Compliant-v1.0</div> <div data-bbox="1054 969 1327 1069">CAD0090-All: Session disable browser persistence for All users when Browser and Non-Compliant-v1.0</div>	<div data-bbox="1589 0 1671 85"></div> <div data-bbox="1386 548 1658 641">CAL001-All: Block specified locations for All users when Browser and Modern Auth Clients-v1.0</div> <div data-bbox="1386 648 1658 748">CAL002-All: Require MFA registration from trusted locations only for All users when Browser and Modern Auth Clients-v1.0</div>	<div data-bbox="1755 512 1844 584"></div> Grant Policy <div data-bbox="1755 591 1844 662"></div> Session Policy <div data-bbox="1755 669 1844 741"></div> Block Policy <div data-bbox="1755 748 1844 819"></div> Future thoughts/Optional <div data-bbox="2074 334 2104 926"> <div data-bbox="2074 334 2104 405"><SN></div> <div data-bbox="2074 412 2104 484"><Cloud app></div> <div data-bbox="2074 491 2104 562"><Response></div> <div data-bbox="2074 569 2104 641">For</div> <div data-bbox="2074 648 2104 719"><Principal></div> <div data-bbox="2074 726 2104 798">When</div> <div data-bbox="2074 805 2104 926"><Conditions></div> </div> <div data-bbox="1755 1305 2048 1376"> Date: November 2020 Version 1.0 Author: Kenneth van Surksun www.vansurksun.com </div>
Prerequisites	User	Device	Location	Legend

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-v 1.0				
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-v 1.0				
Assignments			Access Controls	
Users	Cloud Apps	Conditions	Grant	Session
All Users	All	Client Apps: Exchange Active	Grant Require Approved App	
Except				
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAP002-Exclude				

Some Examples

CAU004-Selected: Session route through MCAS for All users when Browser on Non-Compliant-v 1.0

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-v 1.0

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 Require multi-factor authentication	
Except		Sign-in Risk: High		
AAD_AA_ConAcc-Breakglass				
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 Require Password Change	
Except		User Risk: High		
AAD_AA_ConAcc-Breakglass				
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 Require device to be marked as compliant	
Except		Device Platform: Windows		
Guest and External Users				
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-v 1.0				
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

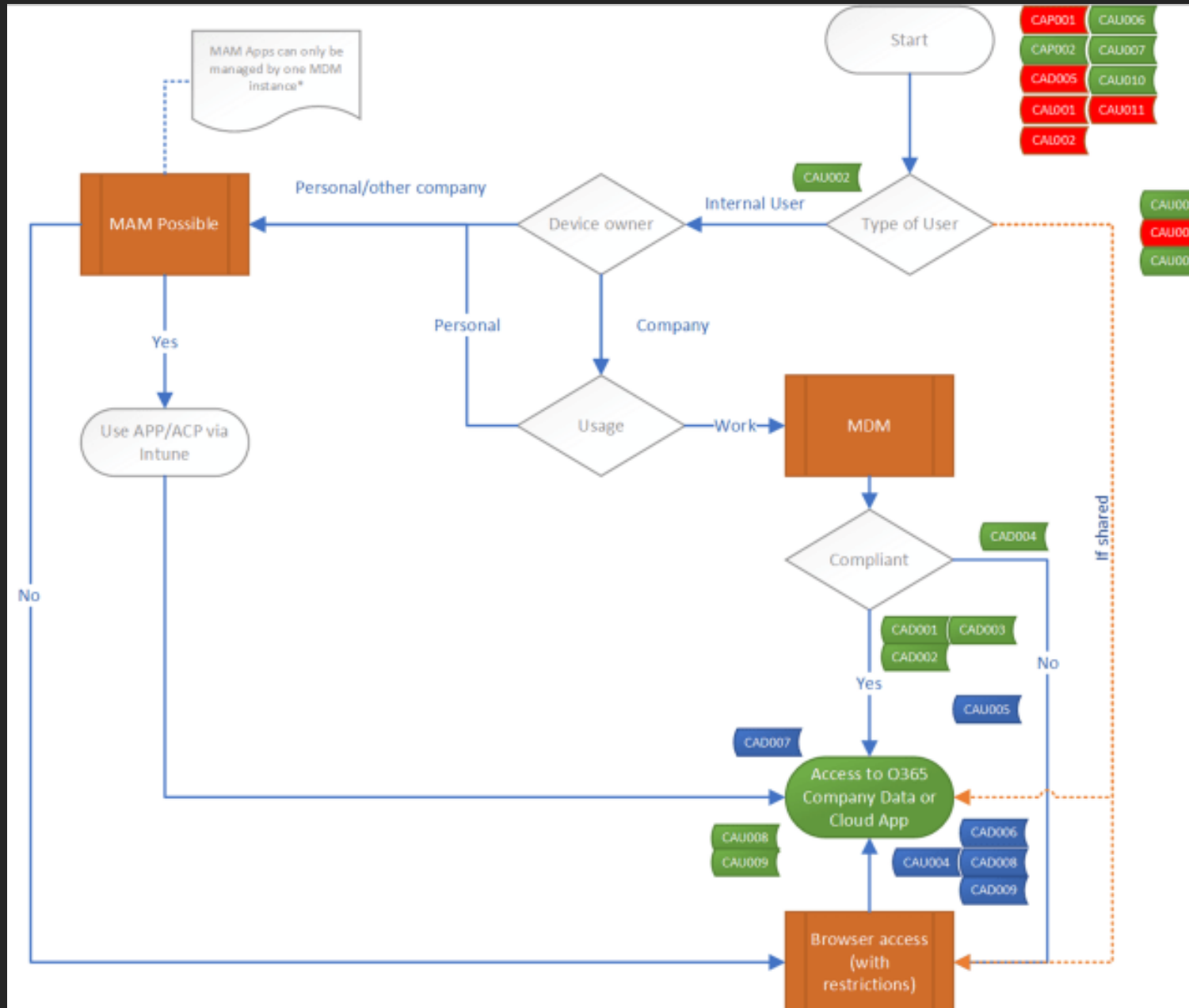
CAD008-All: Session set Sign-in Frequency for All users when Browser and Non-Compliant-v 1.0

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



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)
- Regularly **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

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](#)

Thank you!



MSEndPointMgr.com
#MSEndPointMgr

System Center User Group
Finland
#SCUGFI

System Center User Group
Denmark
#SCUGDK

System Center User Group
Sweden
#SCUGSE

Modern Management User Group
Norway
#MMUGNO