Azure AD Conditional Access Demystified

Centric Craft – October 2021 edition

.CRFT

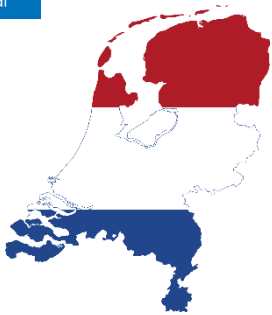wpninjas.nl

About "Kenneth van Surksum"

Focus

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

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

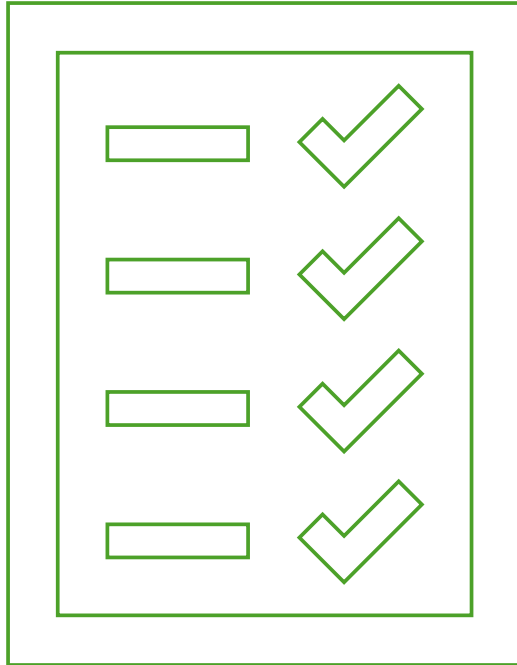https://www.linkedin.com/in/kennethvansurksum

Our topics for Today!

- **What is Conditional Access?**

- **How does Conditional Access work?**

- **Designing Conditional Access**

- **Implementing Conditional Access**

- **Troubleshooting Conditional Access**

Yesterday's Infrastructure ;)
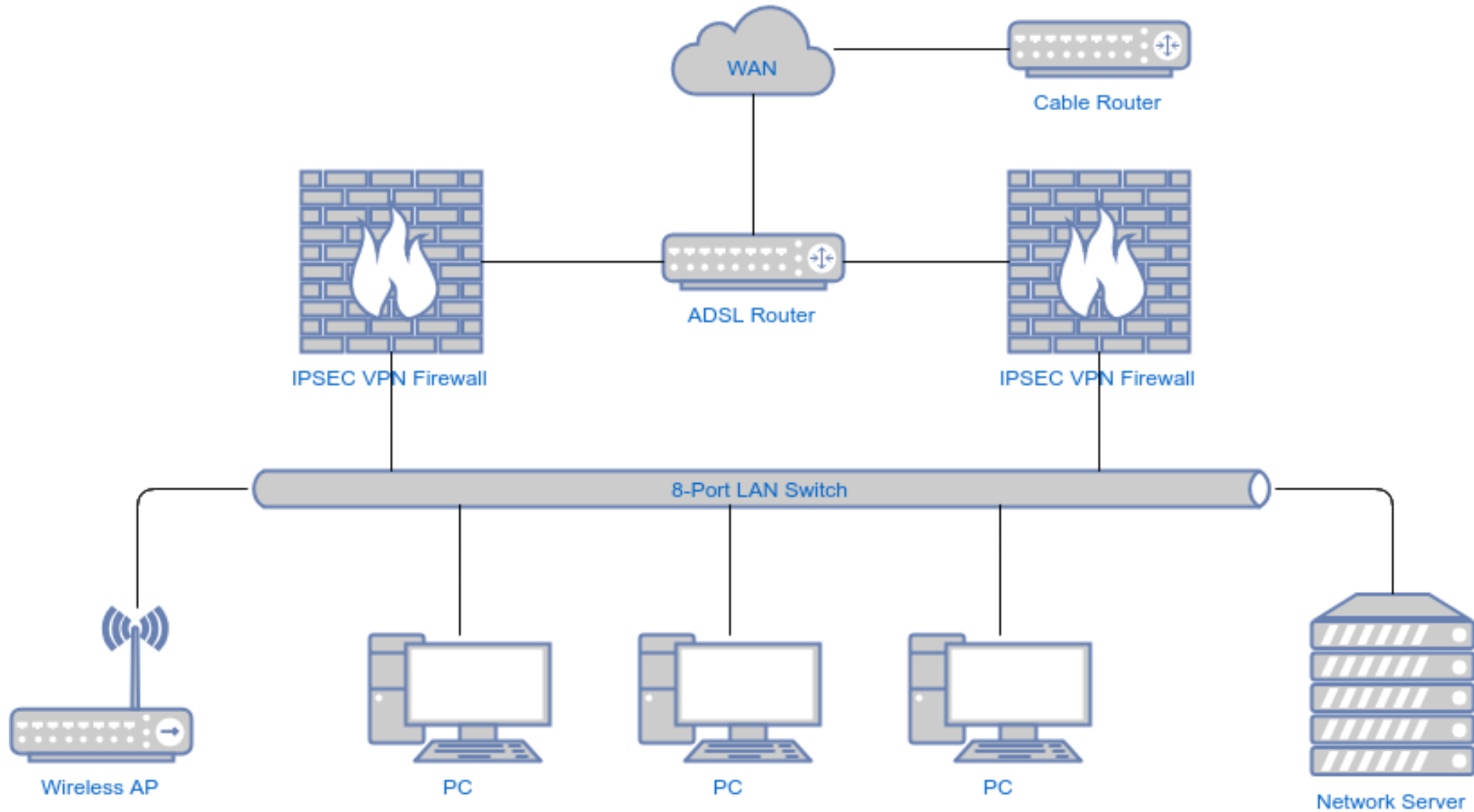
Traditional IT environment
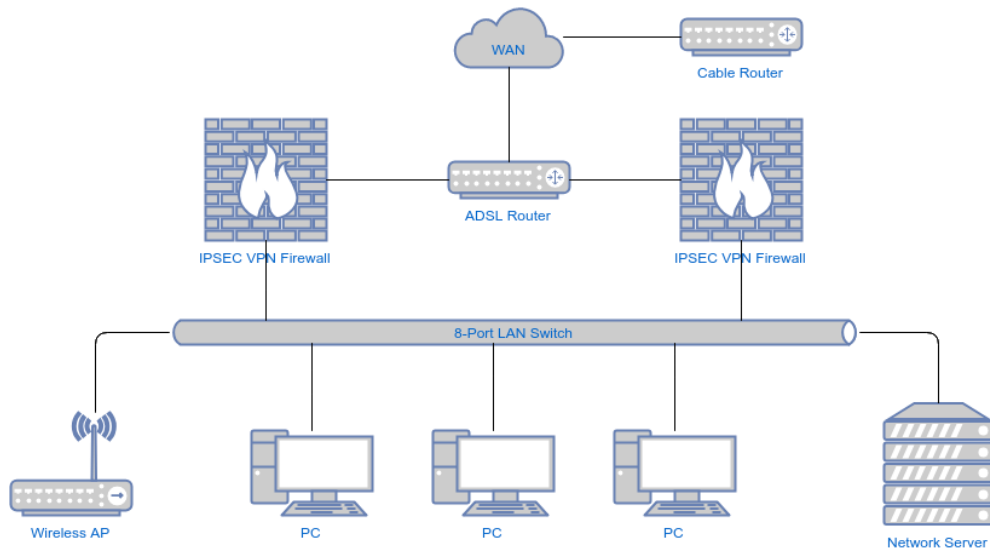
- 1 Personal Computer
- Multiple Personal Computers
- Network
- Authentication
- Management via LAN
- Internal collaboration, sending documents to each other via email/working of fileshares
- Files are stored centrally on fileshares
- Printing using print servers
- Client/Server applications
- Email/Internet
- LAN extension (VPN)
- Security by using Firewalls

Tomorrow's Infrastructure
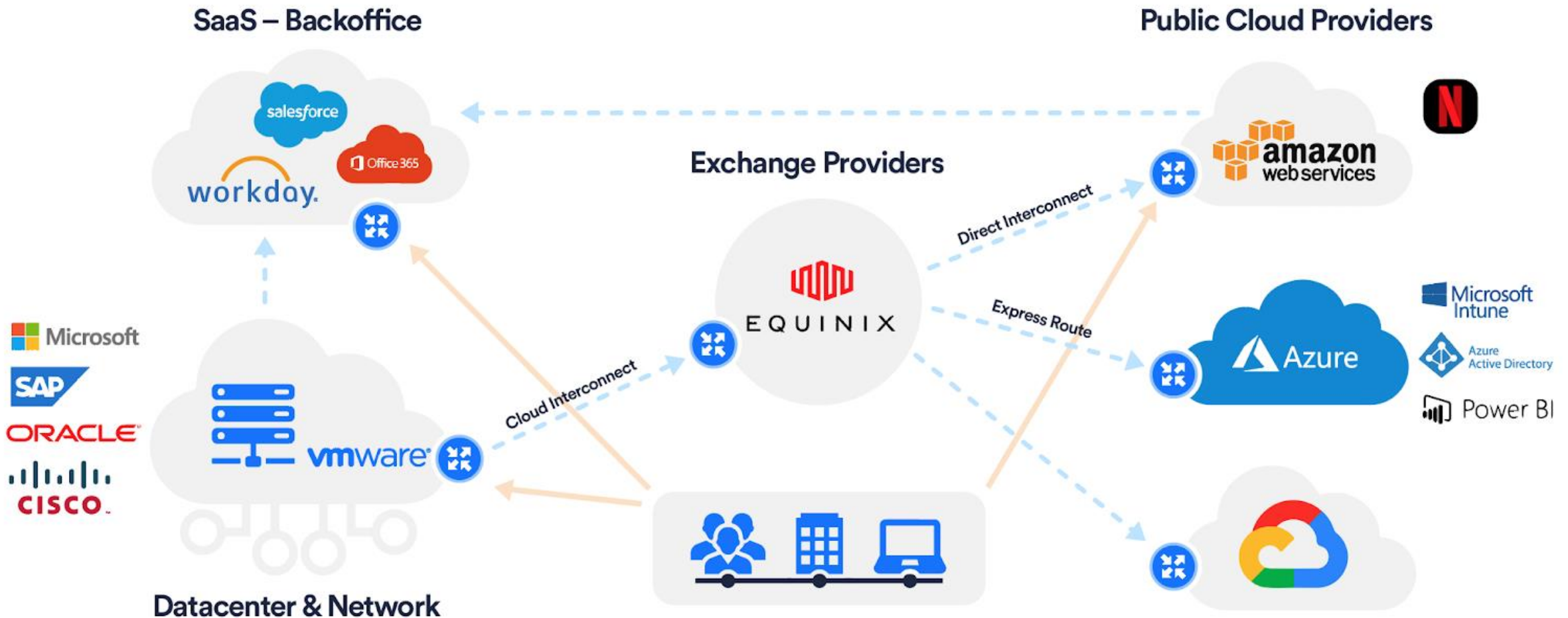
Tomorrows Workplace
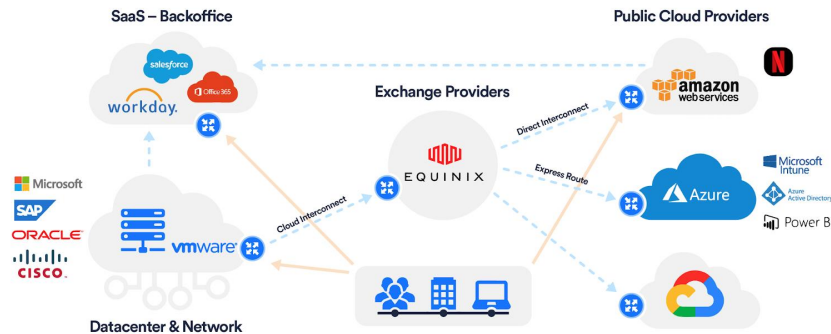
Work anywhere at any time

Internal & external collaboration in a central location

Divers set of Workplaces (Laptops, Desktops, Mobile)

Managed from the Internet

High usage of SaaS offerings (Office 365, Salesforce, Dynamics)

Company data stored in the cloud

Less need to print

Safety provided by the identity

Cloud Service Types

Private (On-Premise)	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Runtimes	Runtimes	Runtimes	Runtimes
Security & Integration	Security & Integration	Security & Integration	Security & Integration
Databases	Databases	Databases	Databases
Servers	Servers	Servers	Servers
Virtualization	Virtualization	Virtualization	Virtualization
Server HW	Server HW	Server HW	Server HW
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

You manage

You manage

You manage

Managed by vendor

Managed by vendor

Managed by vendor

Today's Infrastructure = Hybrid

Yesterday
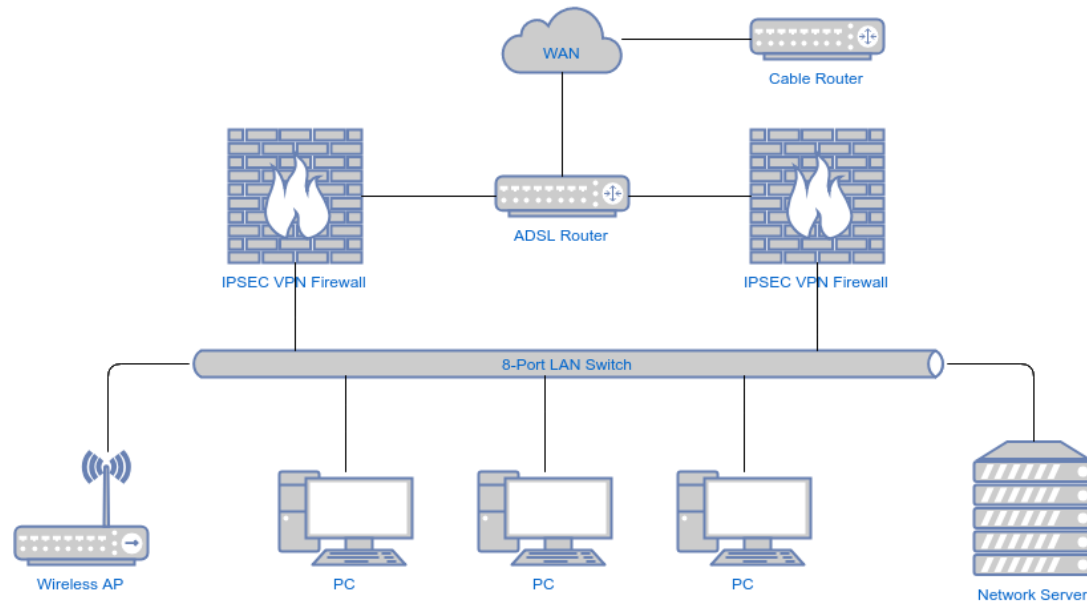
Tomorrow
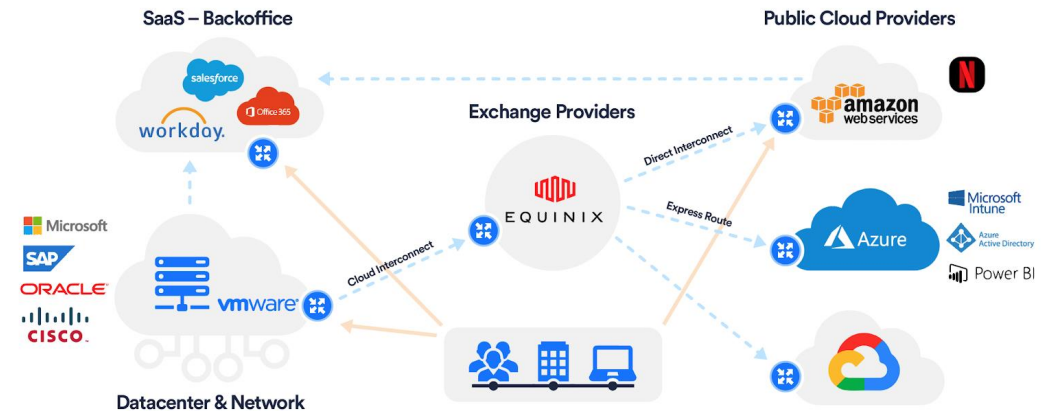
Identity is the new perimeter

Microsoft Description:

What is Conditional Access?

"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?

o Put **conditions** in place to **access** to company data and apps. (Identity and device)

o Can be compared with a Network Firewall but then for your identity

o Resources being accessed must use Azure AD as authentication provider

o Even though you can use it, doesn't mean you are licensed

o When using ADFS, it can become quite complex – ask yourself whether you still need ADFS

o Adds points to your Secure Score
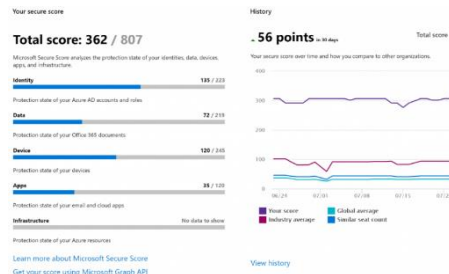
Prerequisites

- We must block legacy authentication for Conditional Access to work in all scenarios.

- 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

What is legacy authentication?

When using Basic/Legacy Authentication application sends a username and password with every request to f.e. Exchange Online which either forwards the credentials towards Azure AD or a federated authentication provider like Active Directory Federation Services (ADFS).

What is the issue with legacy authentication?

The problem with Basic/Legacy authentication is that it is vulnerable to brute force or password spray attacks.

And therefore:

The Exchange Team announced that effective October 1st, 2022 basic authentication, regardless of usage will be permanently disabled in all tenants.

Some additional reasons

- In order to fully implement Conditional Access we must make sure that the services that we want to protect using Conditional Access make use of Modern Authentication

- If we want to move towards Passwordless we must stop using Legacy Authentication
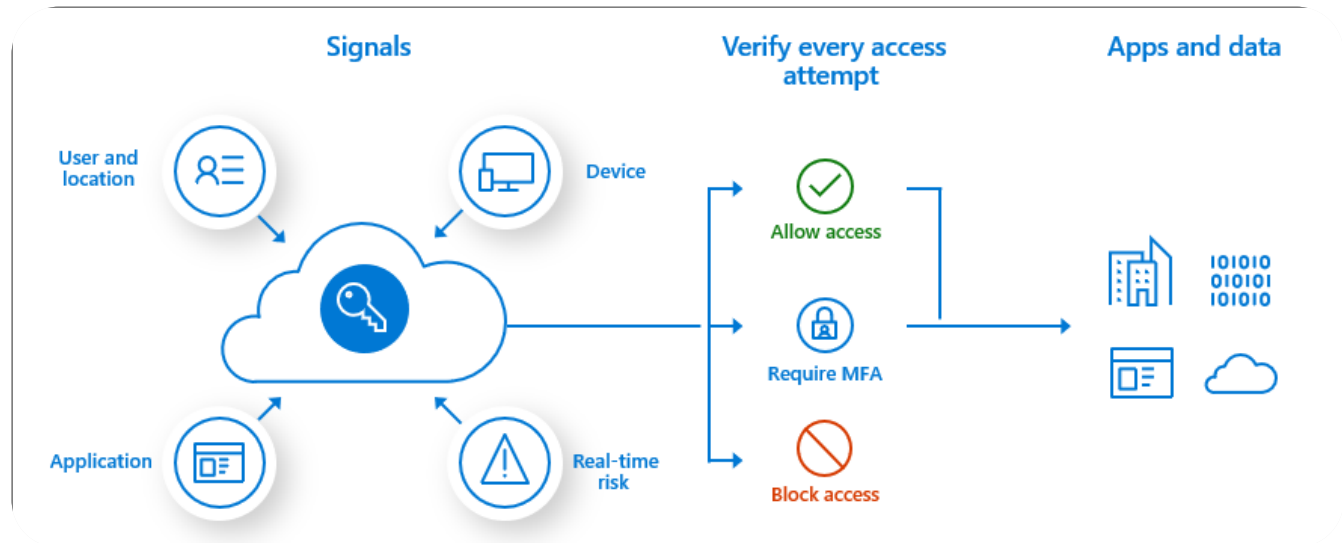
Legacy Authentication

Usage within your tenant?

Signals

User and location

Device

Application

Real-time risk

Verify every access attempt

Allow access

Require MFA

Block access

Apps and data

101010
010101
101010

How does it work?

When this happens	Then do this

Conditional access policy

Conditions	Access controls

How does it really work?
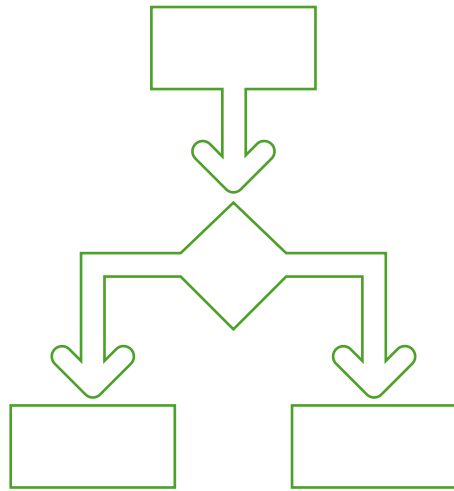
Access to <provided> Clouds Apps except <provided> Cloud apps by <provided> users and/or <provided> roles and/or <provided> groups except <provided> users and/or <provided> groups using <provided> User Risk and/or <provided> Sign-in Risk and/or <provided> Device Platform except <provided> Device Platform 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

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

Conditional Access

Creating your conditional access policy

Designing a Conditional Access Strategy
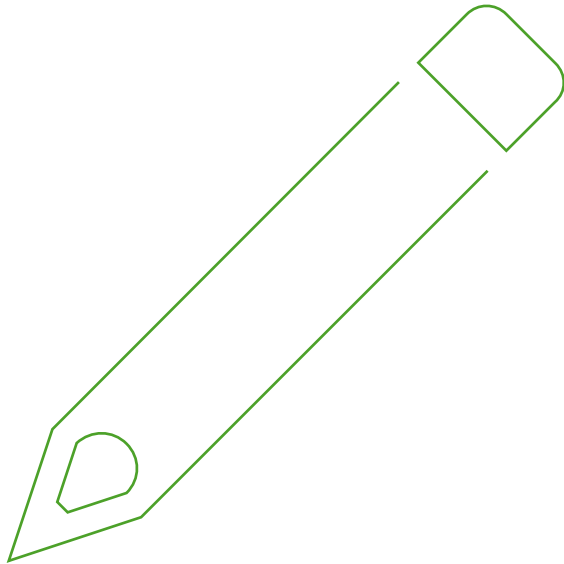
- What kind of devices does the customer use to access cloud apps?
- What kind of applications are used to access cloud apps?
- Is this a green field implementation, or are the cloud apps already in use without any conditional access policies in action?
- Does the customer use Intune and which scenarios 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
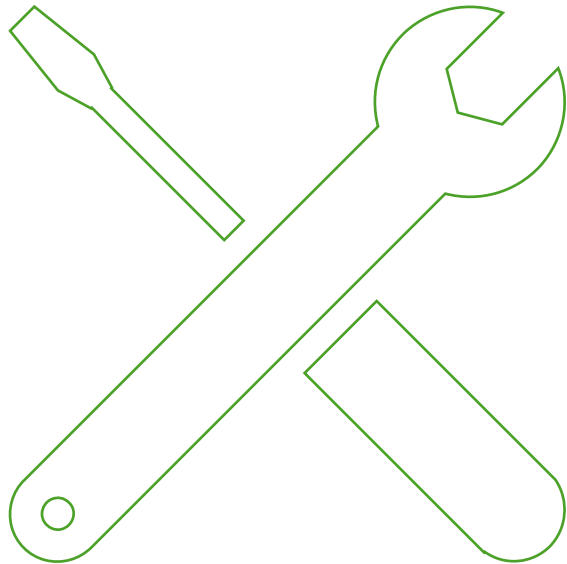
- How To: Plan your Conditional Access deployment in Azure Active Directory – https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

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

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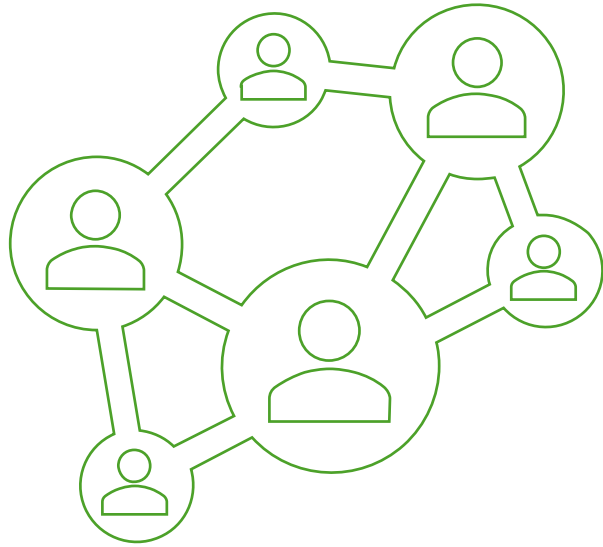
Scenario 1: Allow devices managed by Intune access all the cloud apps using Apps and Desktop Clients and Modern Authentication Clients if compliant

- *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
- Guest User

Device owner
- Personal/other company → MAM Possible
- Company → Usage
- Personal → Usage

MAM Apps can only be managed by one MDM instance*

MAM Possible
- Yes → Use APP/ACP via Intune → Access to O365 Company Data or Cloud App
- No → Browser access (with restrictions)

Usage
- Work → MDM
- Personal → Access to O365 Company Data or Cloud App

MDM → Compliant
- Yes → Access to O365 Company Data or Cloud App
- No → Browser access (with restrictions)

Guest User → If shared → Access to O365 Company Data or Cloud App / Browser access (with restrictions)

Browser access (with restrictions) → 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)

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 Modern Auth Clients

CAU002-All: Grant-Require MFA for All users when Browser and Modern 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-v1.1

CAU005-Selected: Session route through MCAS for All users when Browser on Compliant-v1.1

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 Modern 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 Modern Auth Clients-v1.0

CAU011-All: Block access for All users except licensed when Browser and Modern 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-v1.1

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-v1.1

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-v1.1

CAD009-All: Session disable browser persistence for All users when Browser and Non-Compliant-v1.1

CAD010-All: Require MFA for device join or registration when Browser and Modern Auth Clients-v1.0

Location

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

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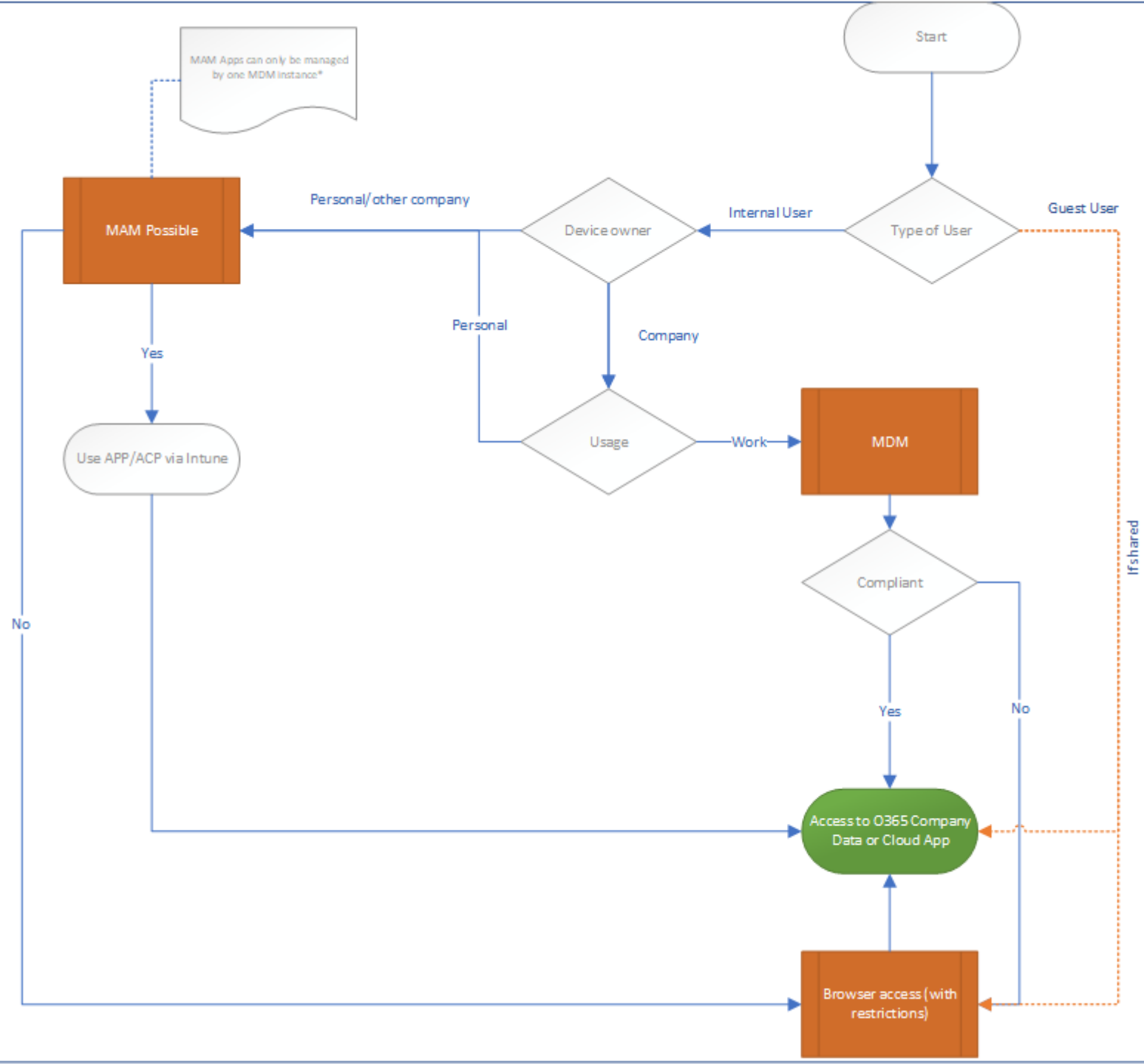
Legend

Grant Policy

Session Policy

Block Policy

Future thoughts/Optional

<SN> <Cloud apps> <Response> For <Principal> When <Conditions>

Date: October 2021 | Version 1.3 | 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
  - CAC = Conditional Access Custom
  - Example: CAD007-O365: Session set Sign-in Frequency for Apps for All users when Modern Auth Clients and Non-Compliant-v1.0
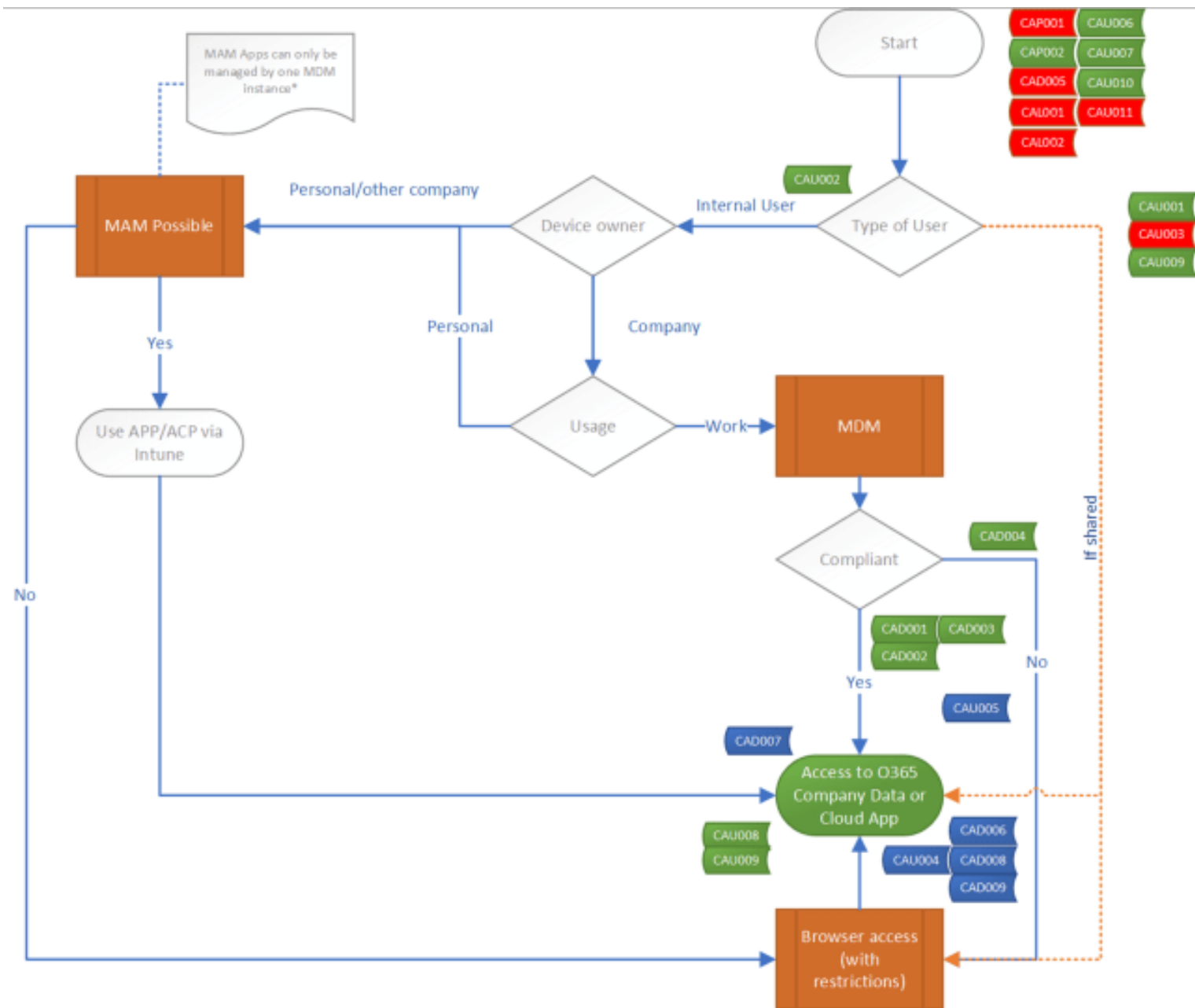
Some examples

- 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-v1.1					
Assignments				**Access Controls**	
Users	*Cloud Apps, User Actions or Authentication Context*	Conditions		Grant	Session
All Users *Except* AAD_AA_ConAcc-Breakglass AAD_AA_CAU004-Exclude	<Selected>	Client Apps: Browser Filter for devices: Exclude isCompliant Equals True			Use Conditional Access App Control: Block downloads (Preview)

CAU005-Selected: Session route through MCAS for All users when Browser on Compliant-v1.1					
Assignments				**Access Controls**	
Users	*Cloud Apps, User Actions or Authentication Context*	Conditions		Grant	Session
All Users *Except* AAD_AA_ConAcc-Breakglass AAD_AA_CAU005-Exclude	<Selected>	Client Apps: Browser Filter for devices: Include isCompliant Equals True		Require device to be marked as co	Use Conditional Access App Control: Monitor (Preview)

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 *Except* AAD_AA_ConAcc-Breakglass AAD_AA_CAU006-Exclude	All	Client Apps: Browser Mobile Apps and Desktop Clients Sign-in Risk: High	Grant Require multi-factor authentication	

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 *Except* AAD_AA_ConAcc-Breakglass AAD_AA_CAU007-Exclude	All	Client Apps: Browser Mobile Apps and Desktop Clients User Risk: High	Grant Require Password Change	

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 Device state: All except Device marked as Compliant		Use App Enforced Restrictions
Except				
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 *Except*	All	Client Apps: Browser Device state: All except Device marked as Compliant		Sign-in Frequency: 1 Days
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 *Except*	All	Client Apps: Browser Device state: All except Device marked as Compliant		Persistent Browser Session
AAD_AA_ConAcc-Breakglass				
AAD_AA_CAD009-Exclude				

Notes: Review your current reauthentication settings

Conditional Access

Implementation

Browser restrictions

OS	Browsers
Windows 10	Microsoft Edge, Internet Explorer, Chrome, Firefox 91+
Windows 8 / 8.1	Internet Explorer, Chrome
Windows 7	Internet Explorer, Chrome
iOS	Microsoft Edge, Intune Managed Browser, Safari
Android	Microsoft Edge, Intune Managed Browser, Chrome
Windows Phone	Microsoft Edge, Internet Explorer
Windows Server 2019	Microsoft Edge, Internet Explorer, Chrome
Windows Server 2016	Internet Explorer
Windows Server 2012 R2	Internet Explorer
Windows Server 2008 R2	Internet Explorer
macOS	Microsoft Edge, Chrome, Safari

Conditional Access

Browser restrictions

Authentication Context

- Conditional Access Authentication Context can trigger a Conditional Access policy when sensitive content is accessed. With this new functionality new scenarios become available; some examples are:
    - You can require MFA when a SharePoint site with a certain sensitivity label gets accessed on an unmanaged device.
    - You can block the session from a Conditional Access policy when a SharePoint site with a certain sensitivity label gets accessed on a unmanaged device.
    - You can require that Terms of Use must be accepted first before access to a SharePoint site with a certain sensitivity label gets accessed.
    - You can set the sign-in frequency to a low value when a SharePoint site with a certain sensitivity label gets accessed.
    - You can trigger the Authentication Context from within a session control policy defined in MCAS, for example to trigger MFA as defined in the Conditional Access policy. You could for example trigger MFA when a document with a certain sensitivity label gets downloaded, or require the user to accept a Terms of Use first.
    - App developers can leverage the authentication context in their own apps

Conditional Access examples

CAU012-AuthCon: Require MFA and compliant for sensitivity label confidential-v1.0

Assignments				Access Controls	
Users	Cloud Apps or Actions	Conditions		Grant	Session
All Users Except AAD_AA_ConAcc-Breakglass AAD_AA_CAU012-Exclude All Guest and External Users	Authentication Context: High Authentication Context	Client Apps: Browser Mobile Apps and Desktop Clients		Grant Require multi-factor authentication And Require device to be marked as compliant	

CAU013-AuthCon: Require MFA and Accept TOU for sensitivity label confidential-v1.0

| Assignments				Access Controls	
Users	Cloud Apps or Actions	Conditions		Grant	Session
All Guest and External Users Except AAD_AA_ConAcc-Breakglass AAD_AA_CAU013-Exclude	Authentication Context: High Authentication Context	Client Apps: Browser Mobile Apps and Desktop Clients		Grant Require multi-factor authentication And I24 - Terms of Use	

Conditional Access

Authentication Context

Tips
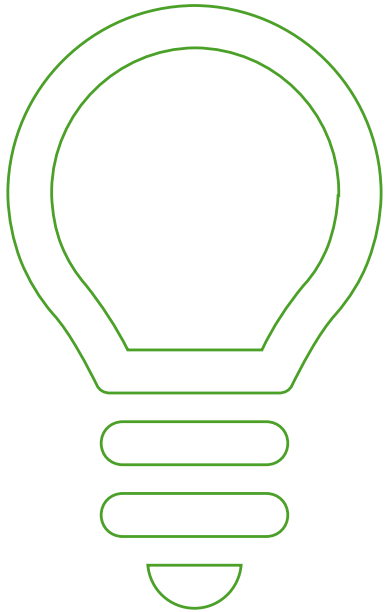
- Use the **Access Review** functionality if available (Azure AD P2)
- Define operational procedures to execute when **something out of your control goes down** (f.e. Azure MFA outage)
- Regulary **review what's new** in Azure AD conditional access and determine if it impacts your environment
  - You 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

Conditional Access

Troubleshooting Conditional Access policies

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

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](#)