



Microsoft Device Compliance and Jamf Pro



Sean Rabbitt

Sr Consulting Engineer,
Identity and Access Mgmt

PRESENTING TO

University of Utah - MacAdmins
March 2024

Agenda

1 | Conditional Access Recap

Why do I need this thing and how does Conditional Access affect my life as an Apple Administrator?

2 | Deployment

Buttons you press in Jamf Pro, Microsoft Intune, and Microsoft Entra ID to make things happen

3 | Common Ooopsies

Deployment issues, what's the plan for on-premises customers, and Q&A



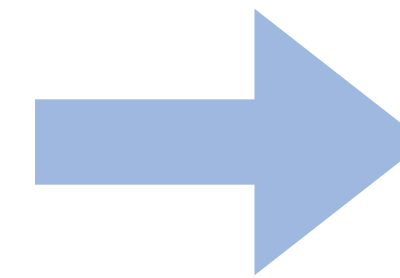
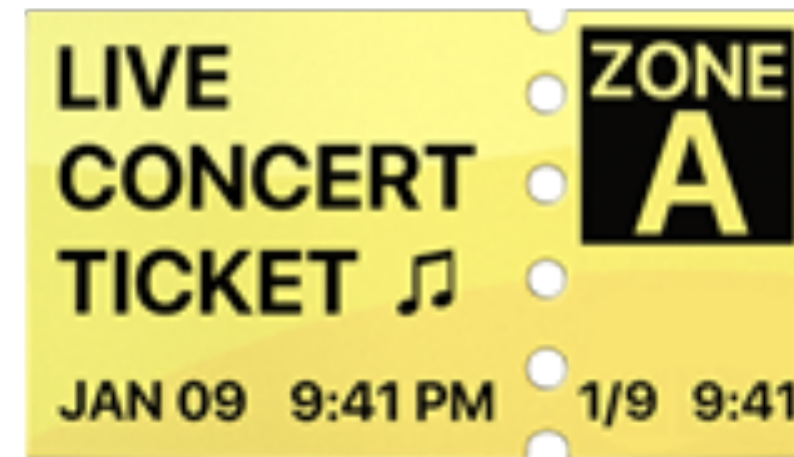
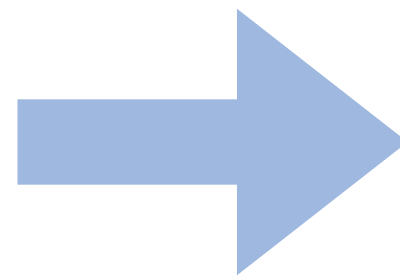
What is Conditional Access?



“I need backstage access!”



“Pass, please.”



“Rock on.”

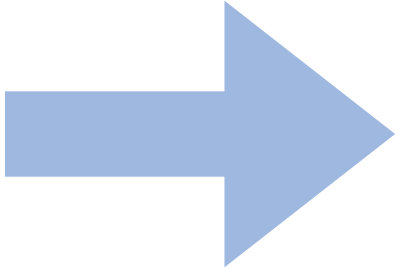
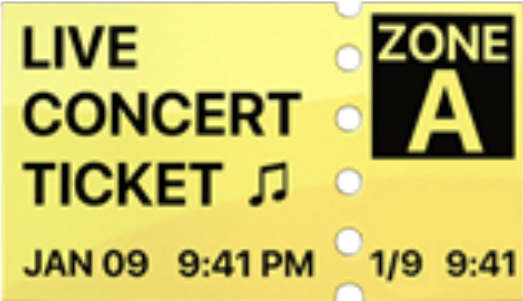
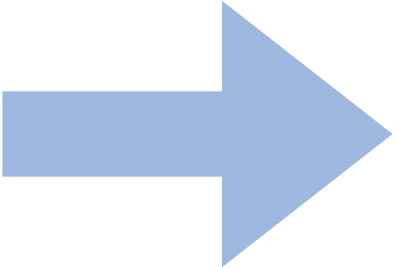
What is Conditional Access?



“I need backstage access!”



“Pass, please.”



“Rock on.”

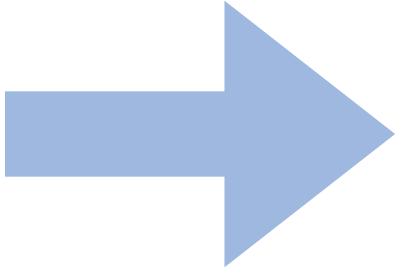
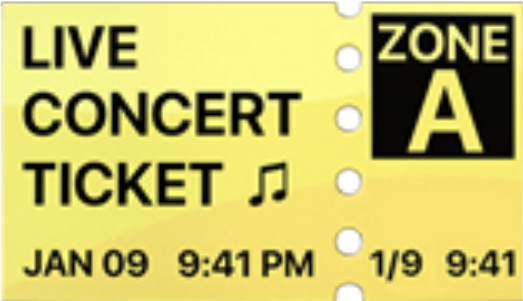
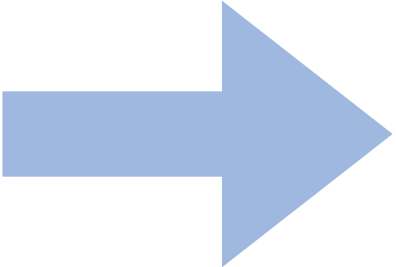
What is Conditional Access?



“I need backstage access!”



“Pass, please.”

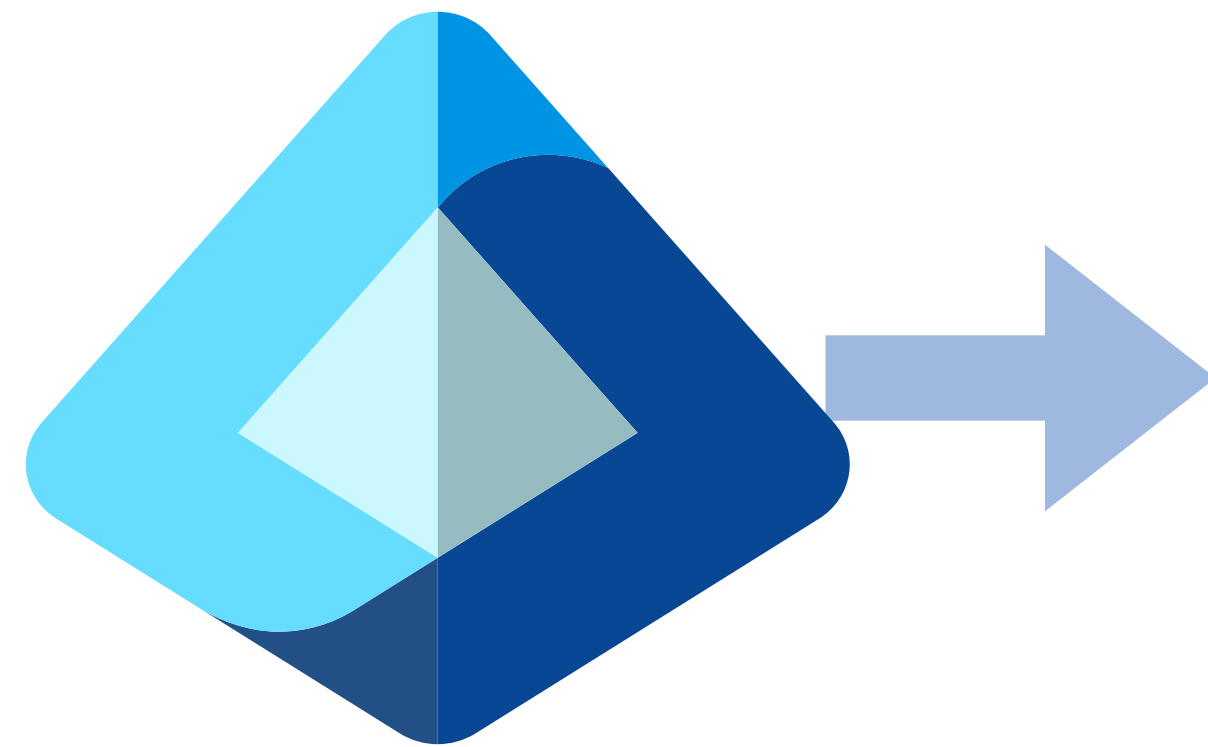


“Beat it!”

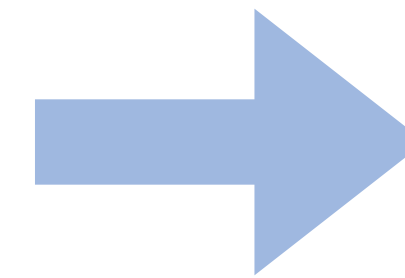
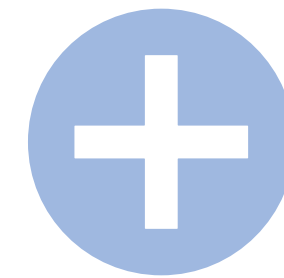
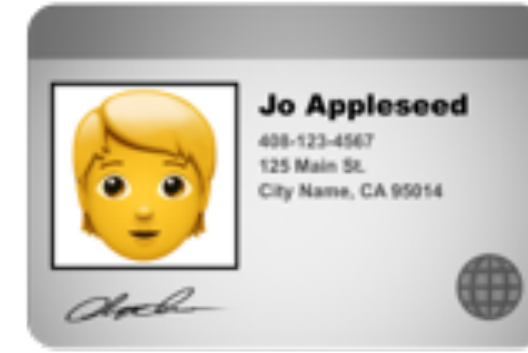
What is Conditional Access?



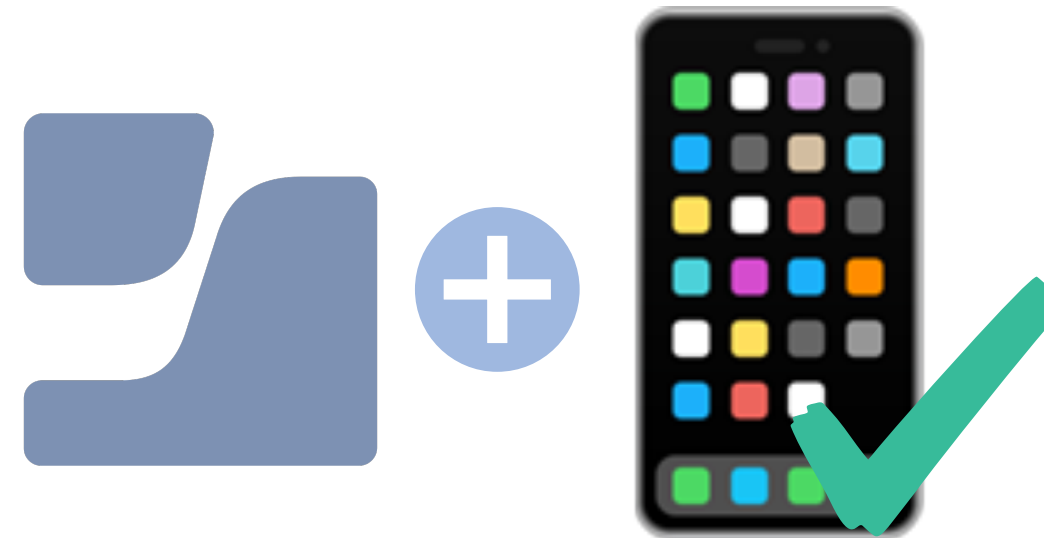
“Let me into Jira, plz.”



Authentication



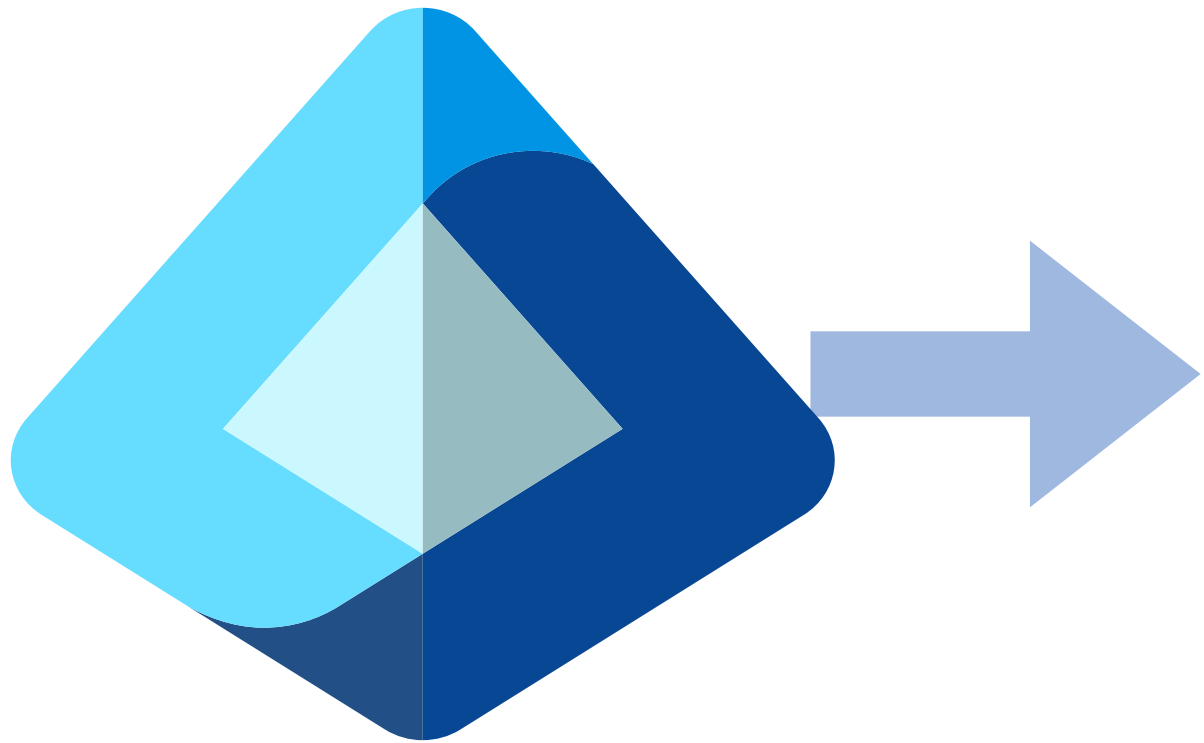
“Get to work.”



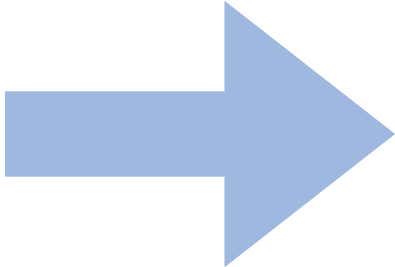
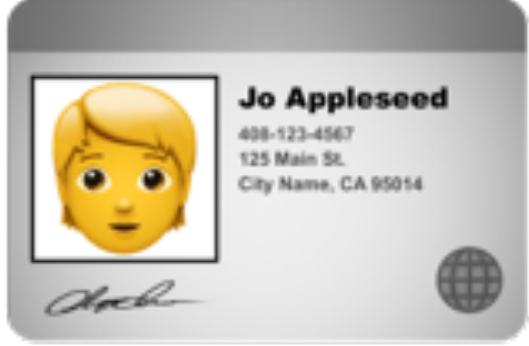
What is Conditional Access?



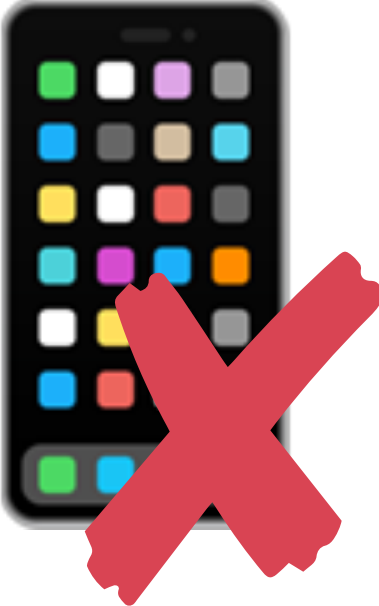
“Let me into Jira, plz.”



Authentication



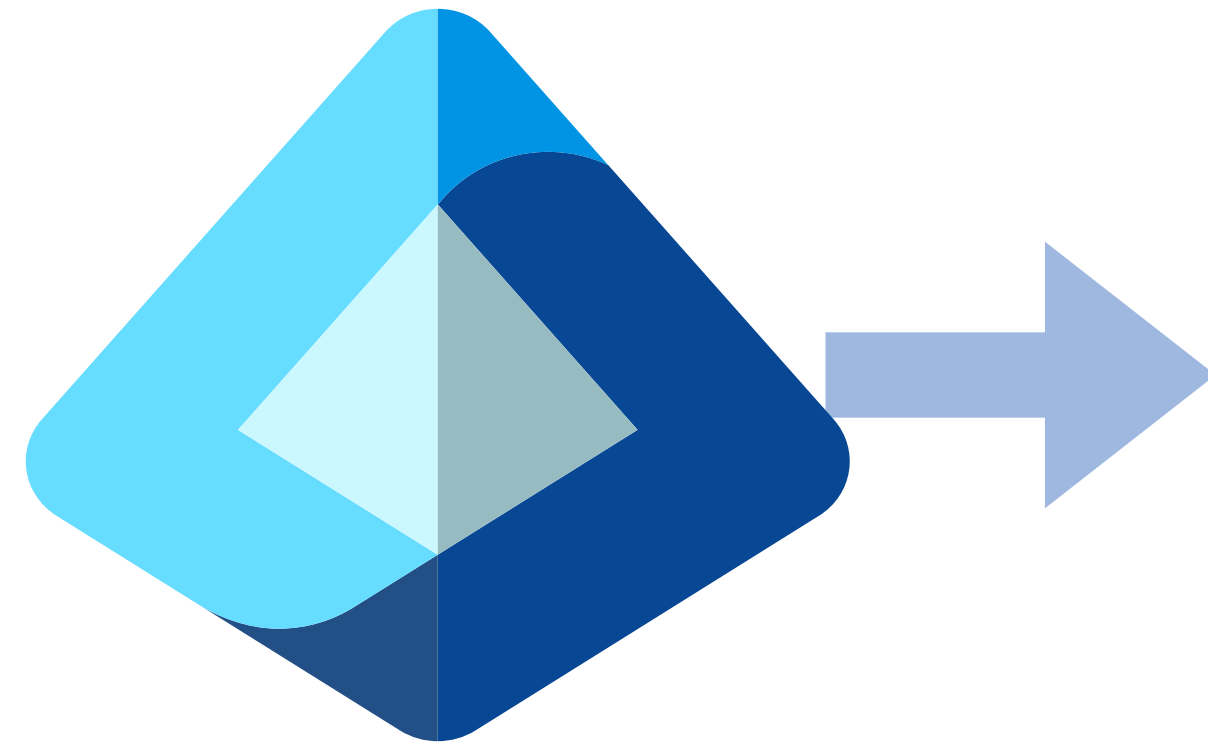
“Go update your iOS.”



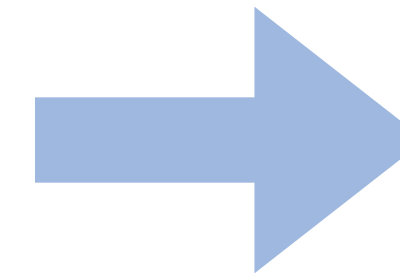
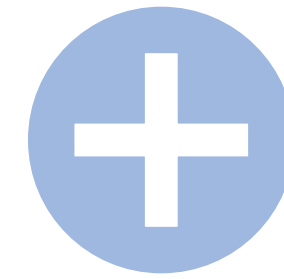
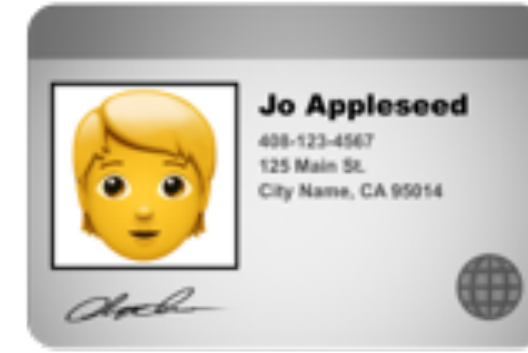
What is Conditional Access?



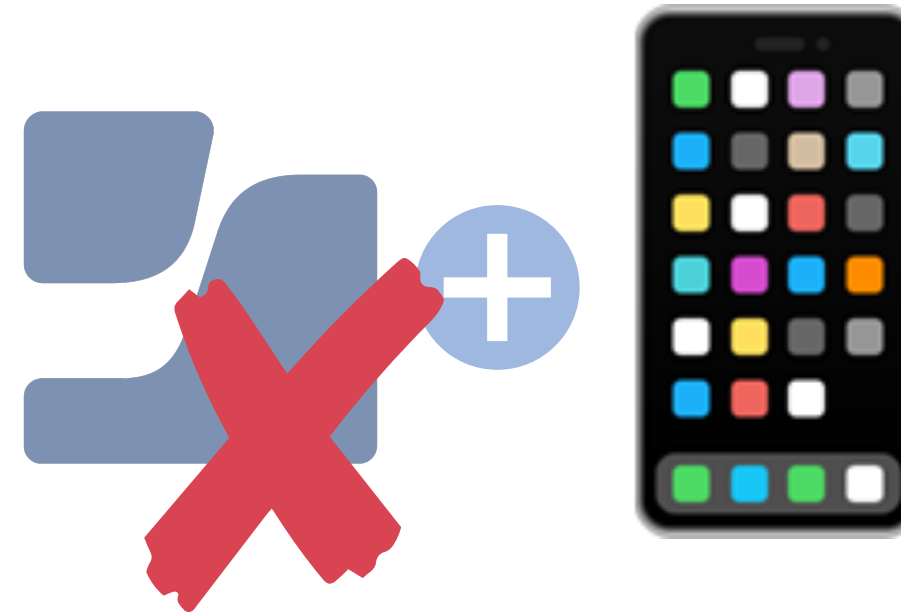
“Let me into Jira, plz.”



Authentication



“Go enroll your device.”



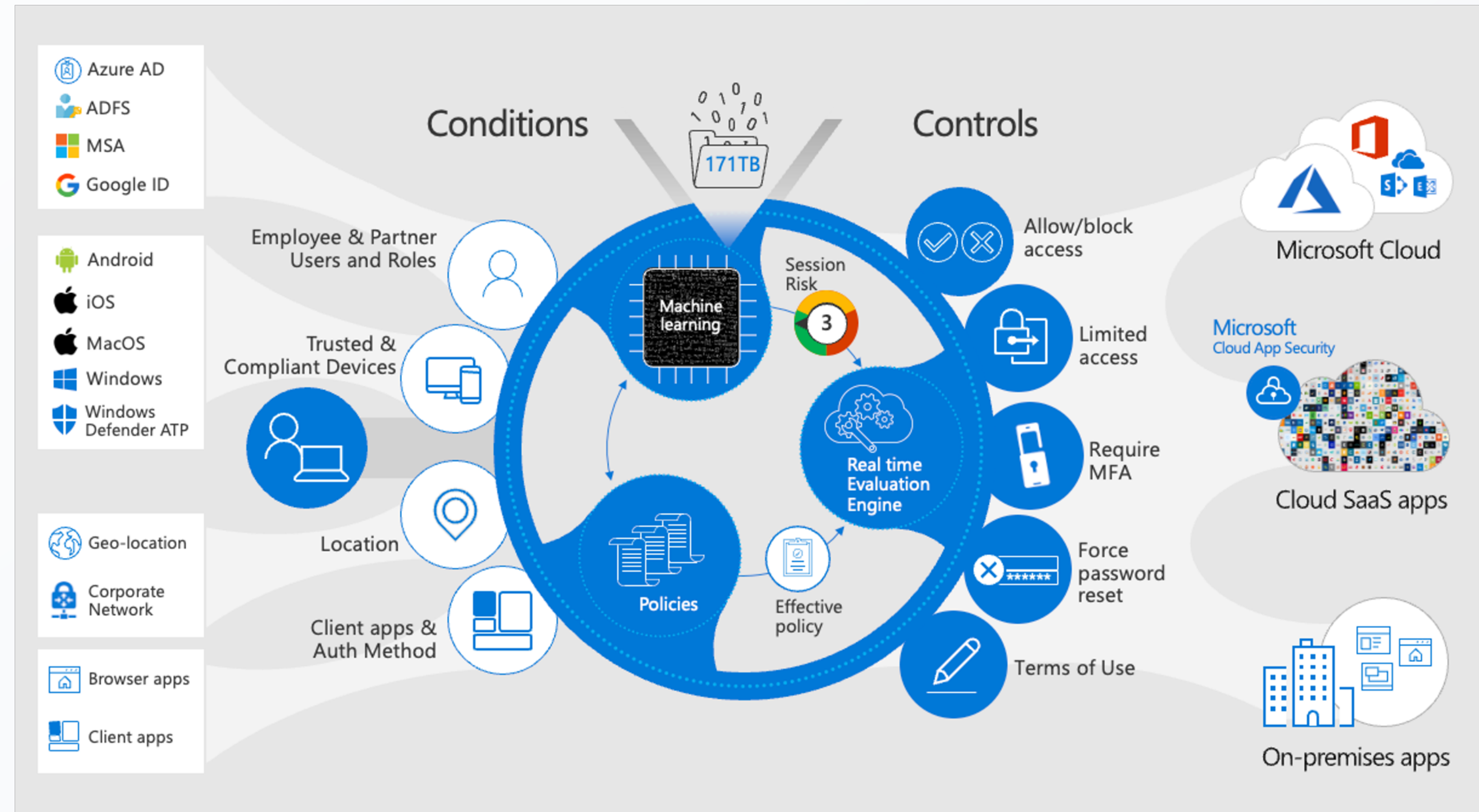
Microsoft Entra ID

- Formerly known as Azure Active Directory
- Part of Microsoft Entra
- Full blown IDaaS
- Rich set of features
 - SSO, Provisioning
 - Governance, Passwordless
 - Conditional Access



Microsoft Entra Conditional Access

- Zero-trust engine
- CA understands user's activity
 - User Location
 - User Risk
 - App Requirements
 - State of Device (Critical!)
- Applies to “Cloud Apps”
- Goal: CA policy in scope for every request



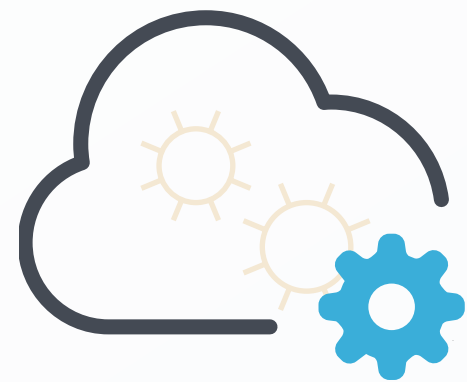
What are cloud apps?

Cloud Apps **ARE**



Web sites

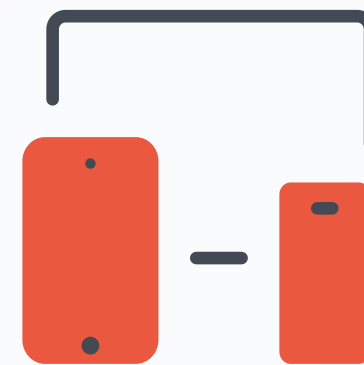
OpenID Connect / OAuth 2.0
confidential clients
SAML



Web services

APIs

Cloud Apps **ARE NOT**



Mobile or desktop apps

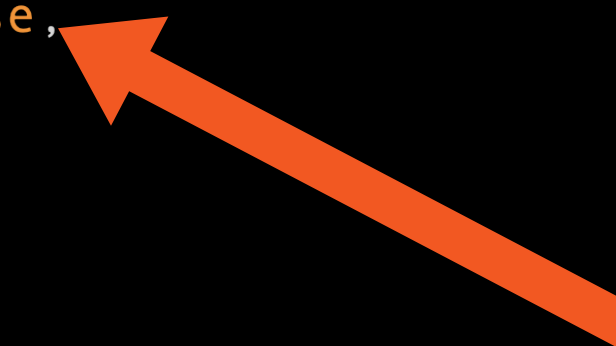
OpenID Connect / OAuth 2.0 native clients

Conditional Access is applied to the RESOURCE
Ex: You apply it to Exchange Online, NOT Outlook

Conditional Access Policy Evaluation

- All CA policies are ANDed together
- Is Policy in scope of the request
- Block controls satisfied first
- Grant controls applied in order
 - Risk
 - MFA
 - Device
 - Approved client app/app protection
- Tries to satisfy policy without user interaction
 - Example: Control MFA or device compliant. If device is NOT compliant, will THEN prompt for MFA

```
{
  "userDisplayName": "Michael Epping",
  "appDisplayName": "Azure Portal",
  "ipAddress": "97.113.39.216",
  "clientAppUsed": "Browser",
  "conditionalAccessStatus": "success",
  "riskDetail": "none",
  "riskLevelAggregated": "none",
  "riskLevelDuringSignIn": "none",
  "riskState": "none",
  "resourceDisplayName": "Windows Azure Service Management API",
  "deviceDetail": {
    "deviceId": "",
    "displayName": "",
    "operatingSystem": "MacOs",
    "browser": "Edge 102.0.1245",
    "isCompliant": false,
    "isManaged": false,
    "trustType": ""
  },
  "location": {
    "city": "Seattle",
    "state": "Washington",
    "countryOrRegion": "US",
    "geoCoordinates": {
      "altitude": null,
      "latitude": 47.61837,
      "longitude": -122.3142
    }
  }
}
```



Policy Number	When <i>this</i> happens	Then do <i>this</i>
1	An access attempt is made: <ul style="list-style-type: none"> - To Exchange Online - By Jane Smith 	Grant access with: <ul style="list-style-type: none"> - MFA
2	An access attempt is made: <ul style="list-style-type: none"> - To Exchange Online - By Jane Smith 	Grant Access with: <ul style="list-style-type: none"> - Compliant Device

Condition	Controls Required
Jane Smith is attempting to access Exchange Online	MFA <u>AND</u> Compliant Device

Access Token Request for Resource

Condition	Controls Required
Jane Smith is attempting to access Exchange Online	MFA <u>AND</u> Compliant Device

Is the user assigned to the resource directly or assignment not required?

Yes

Are there Conditional Access policies in scope of the request?

Yes

Do any policies have a BLOCK control?

No

Are all the Grant Controls satisfied?

Yes

Apply Session Controls, if required

No

Access Token is NOT issued

No

Access Token is issued

Yes

Access Token is NOT issued

No

Access Token is NOT issued

↓

Access Token is issued

Common Conditional Access Policies

- Requiring strong authentication (MFA, phishing-resistant credentials)
- Blocking legacy auth
- Blocking access by country location
- Require compliant or hybrid join device
- Stricter Controls for non-corp managed devices (is this macOS in your environment?)
- Sign-In Frequency to 2 hours for everything not filtered out
- Applying policies to “All Apps”

The screenshot displays the Microsoft Conditional Access configuration interface. It features two overlapping panels: 'Filter for devices' and 'Session'.

Filter for devices panel:

- Header: Filter for devices
- Instruction: Configure a filter to apply policy to specific devices. [Learn more](#)
- Configure: Yes No
- Devices matching the rule:
 - Include filtered devices in policy
 - Exclude filtered devices from policy
- Text: You can use the rule builder or rule syntax text box to create or edit the filter rule.
- Table:

And/Or	Property	Operator	Value
	isCompliant	Equals	True
- + Add expression
- Rule syntax: `device.isCompliant -eq True`

Session panel:

- Header: Session
- Instruction: Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)
- Use app enforced restrictions
- Info box: This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.
- Use Conditional Access App Control
- Sign-in frequency
 - Periodic reauthentication
 - Input field: 2
 - Unit: Hours

Jamf Pro, or why this is really
important to Apple administrators

Device Compliance



Microsoft Entra ID
(formerly Azure AD)



Rules

- OS/Platform Compliant
- Obtained Policy Device ID
- App Displacement

Compliant

Device Compliance



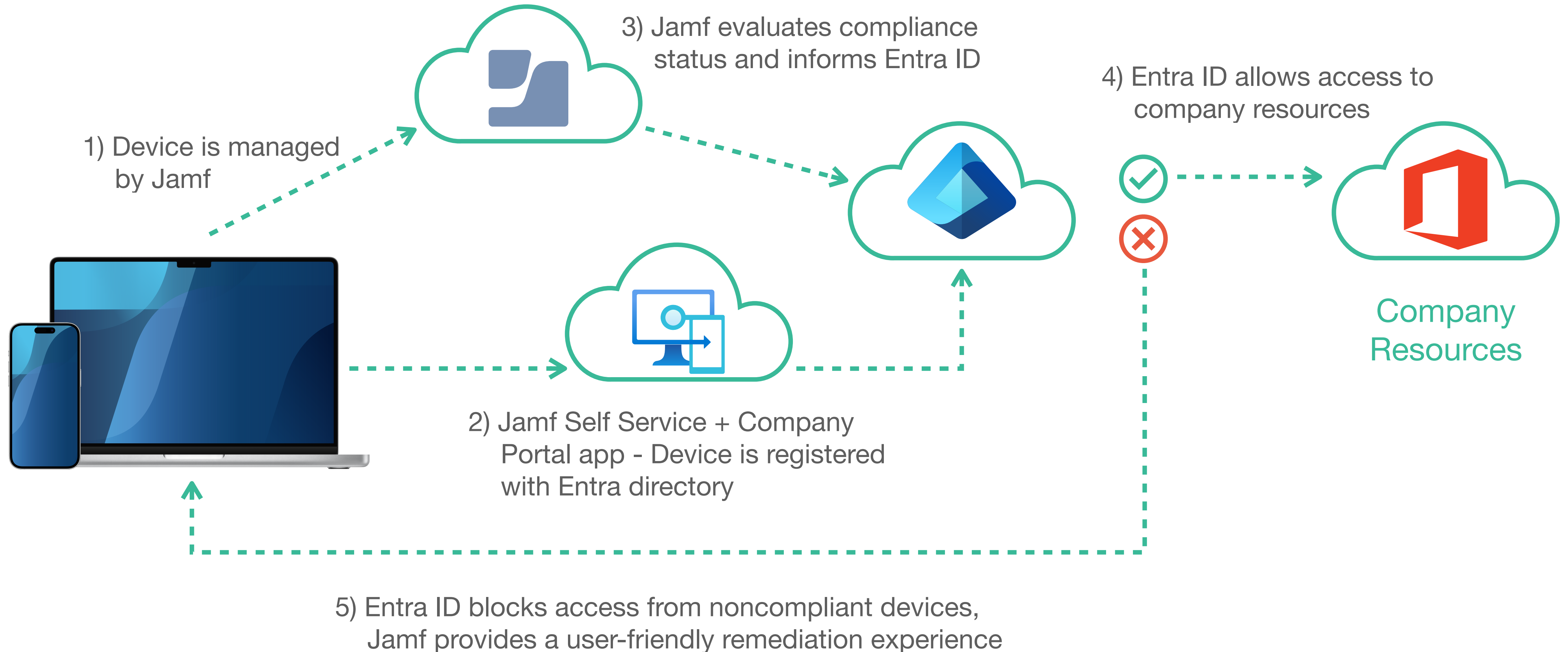
**Microsoft Entra ID
(formerly Azure AD)**



 **Compliant**

Device Compliance

with Jamf and Microsoft



Jamf Pro Setup

Prerequisites:

- Jamf Pro - 10.43 or greater - cloud hosted
- Microsoft Endpoint Manager / Intune administrator
- Microsoft Entra ID administrator
- VPP licenses for Microsoft Authenticator app
- Microsoft Company Portal app



learn.jamf.com

Search: Device Compliance

Jamf Pro Setup - Mobile and Wearable devices

Mobile Devices : Smart Device Groups

← Microsoft Conditional Access - Registration Eligible

Mobile Device Group Criteria Automated Management Reports

Display Name Display name for the smart mobile device group

Microsoft Conditional Access - Registration Eligible

Send email notification on membership change
When group membership changes, send an email notification to the user.

Site Site to add the smart mobile device group

None ▼

Mobile Devices : Smart Device Groups

← Microsoft Conditional Access - Registration Eligible

Mobile Device Group **Criteria** Automated Management Reports

AND/OR	CRITERIA	OPERATOR	VALUE	
	App Identifier	is	com.microsoft.azureauthenticat	Delete
and	App Identifier	is	com.jamfsoftware.selfservice	Delete

+ Add

Jamf Pro Setup - Mobile and Wearable devices

Mobile Devices : Smart Device Groups

← Microsoft Conditional Access - Compliant

Mobile Device Group Criteria Automated Management Reports

Display Name Display name for the smart mobile device group

Microsoft Conditional Access - Compliant

Send email notification
When group membership changes

Site Site to add the smart mobile device group

None

Mobile Devices : Smart Device Groups

← Microsoft Conditional Access - Compliant

Mobile Device Group Criteria Automated Management Reports

AND/OR	CRITERIA	OPERATOR	VALUE			
	Passcode Compliance	is	Compliant	...		Delete
and	App Name	does not have	Onion Browser	...		Delete
and	iOS Version	greater than or equal	16.6	...		Delete

+ Add

Jamf Pro Setup - macOS

Computers : Smart Computer Groups

← Microsoft Conditional Access - Register

Computer Group Criteria Reports

Display Name Display name for the smart computer group

Microsoft Conditional Access - Register

Send email notification on membership changes
When group membership changes

Site Site to add the computers to

None

Computers : Smart Computer Groups

← Microsoft Conditional Access - Register

Computer Group Criteria Reports

AND/OR	CRITERIA	OPERATOR	VALUE		
<input type="button" value="▼"/>	Application Title	is <input type="button" value="▼"/>	Company Portal.app	<input type="button" value="⋮"/>	<input type="button" value="Delete"/>
<input type="button" value="+ Add"/>					

Jamf Pro Setup - macOS

Computers : Smart Computer Groups

← Microsoft Conditional Access - Compliant

Computer Group **Criteria** Reports

AND/OR		CRITERIA	OPERATOR	VALUE			
	▼	FileVault 2 Partition Encryption State	is ▼	Encrypted	⋮	▼	Delete
and ▼	▼	Jamf Protect: Installation	is ▼	Installed		▼	Delete
and ▼	▼	Application Title	is ▼	Company Portal.app	⋮	▼	Delete
and ▼	▼	Computer Group	not member of ▼	Jamf Protect: HIGH	⋮	▼	Delete

+ Add

Jamf Pro Setup

The screenshot displays the Jamf Compliance Editor interface. On the left, a sidebar shows the selected benchmark: "CIS Benchmark - Level 1 macOS 13.0". Below this, a "Sections" menu lists categories like Auditing, macOS, Password Policy, System Settings, and Supplemental. The main area is titled "Jamf Compliance Editor" and features a search bar at the top right. Below the search bar, it shows "Rules 85 Rules, 85 included, 85 found" with a "Sort - ID" dropdown. A list of rules is displayed, each with a blue checkmark indicating it is enabled. The rule "2.3.1.1 Disable AirDrop" is highlighted. To the right of the rules list is a "Rule Details" panel with an "Edit" button. This panel shows the rule's ID as "os_airdrop_disable" and lists various fields: Title, Discussion, Check, Result, Fix, References, and Tags, each with a "Show" button. The "Mobileconfig" section is checked and has a "Hide" button, showing the configuration: "com.apple.applicationaccess: allowAirDrop: false". At the bottom of the interface, there are buttons for "Jamf Pro Upload" and "Create Guidance".



trusted.jamf.com

Jamf Pro Setup

Computers : Configuration Profiles

← Microsoft Enterprise Single Sign-On Plug-in

Options Scope Show in Jamf Pro Dashboard

Search...

General

Application & Custom Settings 1 payload configured

Upload

Single Sign-On Extensions 1 payload configured

Single Sign-on Extensions

1 payload configured

Single Sign-on Extension Configure app extensions that perform single sign-on (macOS 10.15 or later, User Approved MDM required).	^
Payload Type The payload type	SSO
Extension Identifier Bundle identifier of the app extension that performs single sign-on	com.microsoft.CompanyPortalMac.ssoextension
Team Identifier The team identifier of the app extension that performs single sign-on	UBF8T346G9
Sign-on Type Sign-on authorization type	Redirect
URLs URLs of identity providers where the app performs single sign-on. The URLs must begin with http:// or https:// and be unique for all configured Single Sign-On Extensions payloads. Query parameters and URL fragments are not allowed.	

https://login.microsoftonline.com

https://login.microsoft.com

https://sts.windows.net

https://login.partner.microsoftonline.cn

https://login.chinacloudapi.cn

History Logs Download Clone Delete Edit



jamf.it/entraSSOe



<https://jamf.it/entrassoe-ios>

Jamf Pro Setup

Jamf Pro Settings ->
Global ->
Device Compliance

Settings : Global
← Device Compliance

Configuration status
Use the switch to enable or disable the connection.

Platform Select platform type to configure.

macOS

Compliance Group Smart computer group Jamf Pro will use to calculate device compliance.
Microsoft Conditional Access - Compliant

Applicable Group Smart group containing all computers Jamf Pro uses to send a compliance status to Microsoft Intune. This also makes the Register button available in Self Service.
Microsoft Conditional Access - Register Applicable Group

iOS and iPadOS

Compliance Group Smart device group Jamf Pro will use to calculate device compliance.
Microsoft Conditional Access - Compliant

Applicable Group Smart group containing all devices Jamf Pro uses to send a compliance status to Microsoft Intune. This also makes the Register button available in Self Service.
Microsoft Conditional Access - Registration Eligible

Allowed Duration Of Inactivity Number of days after a device's last check in with Jamf Pro before the device is marked as "Unspecified" in Azure AD.
120 Required

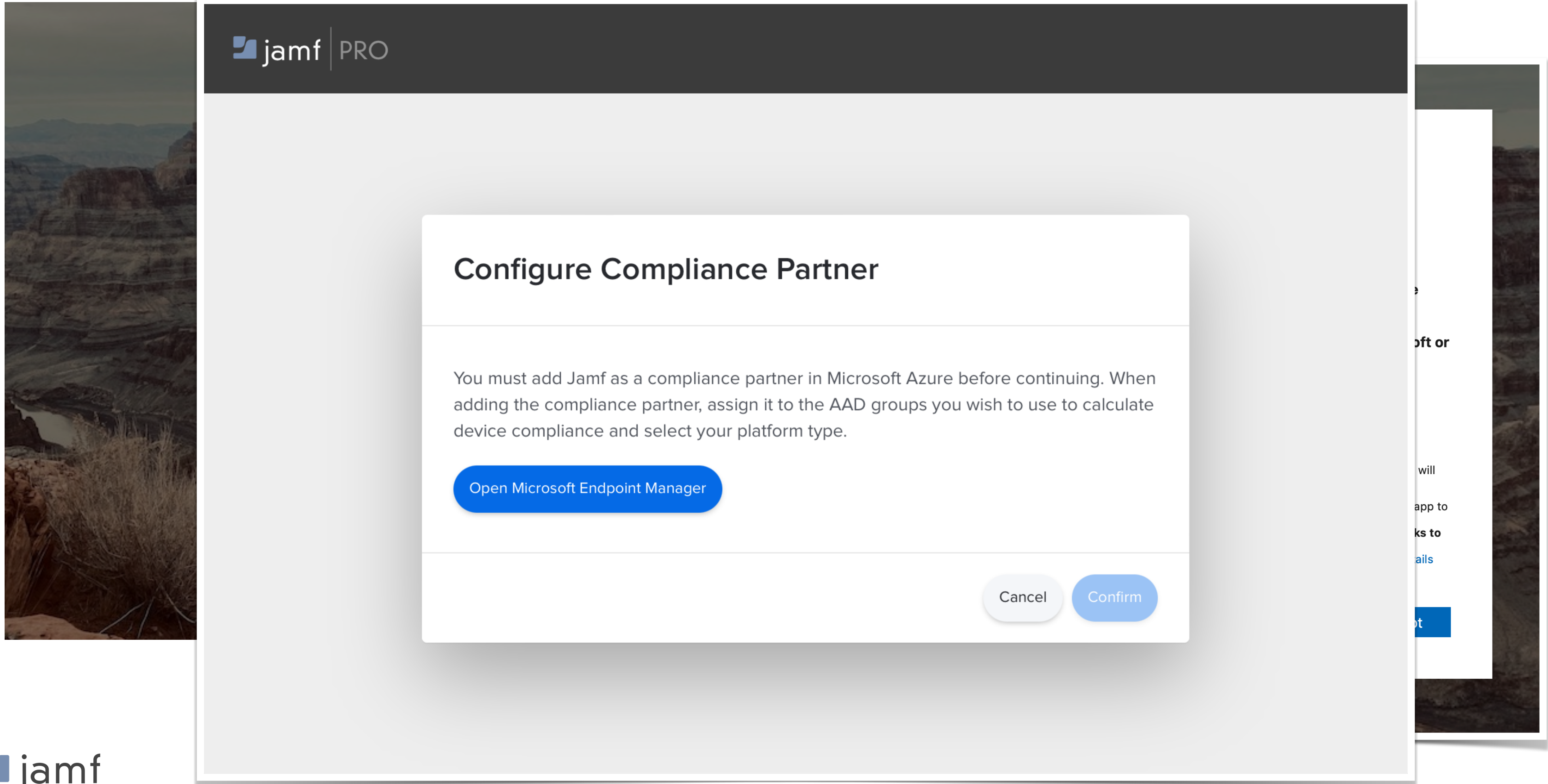
Landing Page For Devices Not Recognized By Microsoft Azure Webpage where users are redirected to if their device is not registered with Azure AD or not enrolled with Jamf Pro.

Default Jamf Pro Device Registration page
 Access Denied page
 Custom URL:

Registration Page Name Descriptive name of the enrollment page option for redirection from Microsoft unregistered CA block. This will display to end users to pick. Name could relate to division or organization for each Jamf Pro listed.

Cancel Save

Jamf Pro Setup



Jamf Pro Setup

Microsoft Intune admin center

sean.rabbitt@jamfse.io
JAMFSE.IO (OBITHECAT.ONMICR...)

Home > Tenant admin | Connectors and tokens > Connectors and tokens

Connectors and tokens | Partner compliance management

Search << + Add compliance partner Refresh

Windows

- Windows enterprise certificate
- Microsoft Endpoint Configuration Manager
- Windows 365 Citrix connector
- Windows data

Apple

- Apple VPP Tokens

Android and Chrome OS

- Managed Google Play
- Chrome Enterprise (preview)
- Firmware over-the-air update (preview)

Cross platform

- Microsoft Defender for Endpoint
- Mobile Threat Defense
- Partner device management
- Partner compliance management
- TeamViewer connector
- ServiceNow connector
- Certificate connectors

Intune compliance evaluates partner-managed devices in your organization. Set up the connection here.

A device must comply with the highest priority partner assigned to its user. Intune is the default compliance partner and has the lowest priority and cannot be edited or deleted.

[Find out more about connecting compliance partners to Intune.](#)

Android

Priority	Partner	Assigned	Partner status	Last Successful Sy...
Default	Intune	N/A	N/A	N/A

iOS

Priority	Partner	Assigned	Partner status	Last Successful Sy...
1	Jamf Device Complian...	Yes	Active	7/28/2023, 11:24:41 AM
Default	Intune	N/A	N/A	N/A

macOS

Priority	Partner	Assigned	Partner status	Last Successful Sy...
1	Jamf Device Complian...	Yes	Active	7/28/2023, 11:24:41 AM
Default	Intune	N/A	N/A	N/A

Jamf Pro Setup

Settings : Global

← **Device Compliance**

Configuration status

Use the switch to enable or disable the connection.



✔ Connection verification status: Success

Jamf Pro Setup - macOS

Computers : Policies

← Register Device with Microsoft

Options Scope Self Service User Interaction

Scripts
0 Scripts

Printers
0 Printers

Disk Encryption
Not Configured

Dock Items
0 Dock Items

Local Accounts
0 Accounts

Management Accounts
Not Configured

Directory Bindings
0 Bindings

EFI Password
Not Configured

Restart Options
Not Configured


Maintenance
Not Configured

Files and Processes
Configured

Microsoft Device Compliance >
Configured

Microsoft Device Compliance

Register computers with Azure Active Directory
Launches the Company Portal app for users, enabling them to register computers with Azure Active Directory. Registered computers submit updated inventory to Jamf Pro.

 The Microsoft Intune Company Portal app must be installed on computers in the scope of this policy prior to deploying the policy to users.

Cancel Save

Jamf Pro Setup - macOS

The screenshot displays the Jamf Pro web interface. At the top left, the 'Pro' logo is visible. The top right corner shows 'Full Jamf Pro' with a dropdown arrow, a notification bell with a red '3' badge, and a user profile icon. The left sidebar contains a navigation menu with categories: Computers, Inventory, Content Management, Mac Apps, Groups, and Enrollment. The 'Mac Apps' category is selected and highlighted. The main content area shows the configuration page for 'Microsoft Intune Company Portal - macOS Onboarding'. At the top of this page, it says 'Computers : Mac Apps' and has a back arrow. Below the title, there is a 'Deploy' toggle switch which is currently turned on. A horizontal menu below the title includes 'Configuration settings' (which is underlined and active), 'Deployment status', 'Self Service', and 'End user experience'. The 'App settings' section includes: 'Display Name' (Microsoft Intune Company Portal - macOS Onboarding), 'Site' (None), 'Category' (macOS Onboarding), and 'Target Group' (Prestage - Jamf Connect with Azure AD (FileVault)). The 'Initial Distribution Method' is set to 'Install automatically', and the 'Update Method' is set to 'Automatic'. A checkbox for 'Install supporting configuration profiles' is checked. At the bottom right of the page, there are four action buttons: 'History', 'Clone', 'Delete', and 'Edit'.

Jamf Pro Setup - Mobile and Wearable devices

Mobile Devices : Mobile Device Apps

← Microsoft Authenticator

General Scope Managed Distribution App Configuration

Display Name Display name for the app
Microsoft Authenticator

Enabled

Site Site to add the app to
None

Category Category to add the app to
Microsoft

Short Version Short Version of the app
6.7.12

Bundle Identifier Bundle identifier for the app
com.microsoft.azureauthenticator

Free
App is free

Distribution Method Method to use for distributing the app
Install Automatically/Prompt Users to Install

Display app in Self Service after it is installed

Require tethered network connection for app installation (iOS 10.3 or later)
Require the device to have a tethered network connection to download the app

Schedule Jamf Pro to automatically check the App Store for app updates
Automatically update app description, icon, and version in Jamf Pro

App Store Country Or Region Country or region to use when syncing app with the App Store
United States



Self Service

Search


Browse

- All
- Bookmarks
- Featured
- Device Compliance**
- Apple
- Microsoft
- Developer Tools
- Productivity Tools
- Certificates
- Compliance
- FileVault 2
- Jamf Connect
- Maintenance
- OS Installers
- TeamViewer
- Reprovisioning
- Security
- TnC

Log In


Device Compliance

A...Z



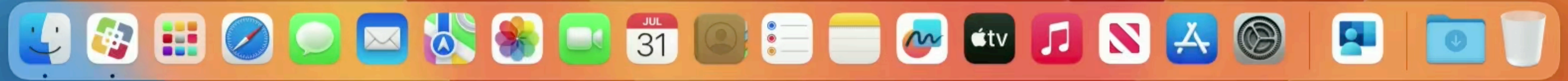
Firewall (Turn On)

Enable



Register Device with Microsoft

Re-Register



H2WGW2C9Q6NV | Properties

jamfse.io - Azure Active Directory

Manage Enable Disable Delete | Got feedback?

Manage

Properties

Roles and administrators

Administrative Units

Name	H2WGW2C9Q6NV
Device ID	a9289152-10f0-4b0a-8786-aab96ebf7e06
Object ID	d69bde9e-4625-4453-99aa-51ffeba3e354
Enabled	Yes
OS	MacOS
Version	13.5.0
Join Type	Azure AD registered
Owner	User Microsoft
User principal name	user.microsoft@jamfse.io
MDM	Microsoft Intune
Compliant	Yes
Registered	7/31/2023, 9:36:03 AM
Activity	7/31/2023, 9:36:03 AM
Groups	None
Extension Attributes	No Extension Attributes

Common Ooopsies or why
didn't this work, dang it!

Common Ooopsies

Using something other than Safari than the default browser

Device Registration Failures

Frequent Authentication Prompts

Compliant Device Check Fail

Confusion around which policy did what

Jamf Connect and Conditional Access w/ MFA

Q&A

support@jamf.com - info@jamf.com