Device Identity

Managed devices

- Registration with Azure AD
- Creates an identity for the device
- This object is used by Azure

To get a device in Azure AD,

You have multiple options:

Azure AD registered	Azure AD joined	Hybrid Azure AD joined
Typically personally owned or mobile devices	Devices are owned by an organization and are signed in with an Azure AD account. They exist only in the cloud.	Devices that are owned by an organization and are signed in with an Active Directory account. They exist in the cloud and on-premises.

Azure AD registered devices

Definition	Registered to Azure AD without requiring organizational account to sign in to the device
Primary audience	Applicable to all users with the following criteria:
	Bring your own device (BYOD)
	Mobile devices
Device ownership	User or Organization
Operating Systems	Windows 10, iOS, Android, and MacOS
Provisioning	Windows 10 – Settings
	iOS/Android – Company Portal or Microsoft Authenticator app
	MacOS – Company Portal

Azure AD joined devices

Definition	Joined only to Azure AD requiring organizational account to sign into the device
Primary audience	Suitable for both cloud-only and hybrid organizations.
	Applicable to all users in an organization
Device ownership	Organization
Operating Systems	All Windows 10 devices except Windows 10 Home
Provisioning	Self-service: Windows OOBE or Settings
	Bulk enrollment
	Windows Autopilot

Hybrid Azure AD joined devices

Definition	Joined to on-premises AD and Azure AD requiring organizational account to sign into the device
Primary audience	Suitable for hybrid organizations with existing on-premises AD infrastructure
	Applicable to all users in an organization
Device ownership	Organization
Operating Systems	Windows 10, 8.1 and 7
Provisioning	Windows 10
	Domain join by IT and autojoin via Azure AD Connect
	Domain join by Windows Autopilot and autojoin via Azure AD Connect

Windows Enrollment Types

Two ways to get devices enrolled in Intune:

User-self enroll

- BYOD: Users enroll their personally owned devices
- MDM only enrollment
- Azure AD Join
- Autopilot

Administrator-based

- HYBRID Azure AD Join
- Co-management
- Device enrollment Manager (DEM) is a special service account
- Bulk enrollment
- Windows IoT core devices

User self-enroll

- BYOD:

Users enroll their personally owned devices by downloading and installing Company Portal App

- MDM only enrollment:

This method isn't recommended because it doesn't register the device into Azure Active Directory.

It also prevents the use of features such as Conditional Access.

- Azure AD Join

If Auto Enrollment is enabled, the device is automatically enrolled in Intune

- Autopilot

This method simplifies the out-of-box experience

Administrator-based enrollment

- Hybrid:

Lets administrators configure Active Directory group policy to automatically enroll devices that are hybrid Azure AD joined.

- Co-Management

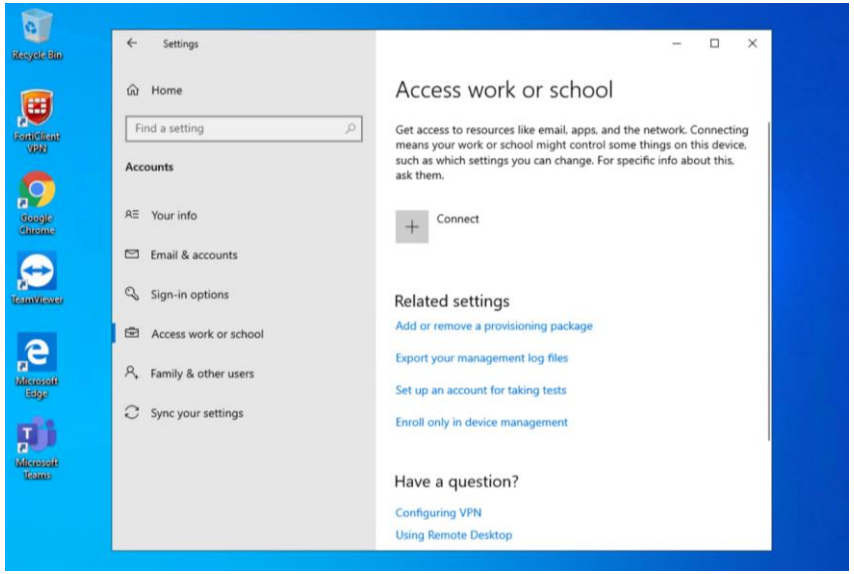
Lets administrators enroll their existing Configuration Manager managed devices into Intune to get the dual benefits of Intune and Configuration Manager.

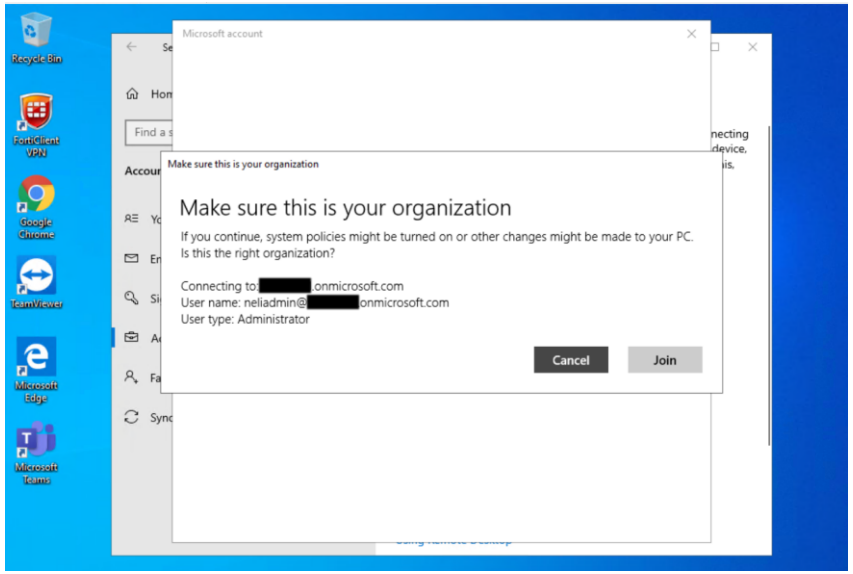
- DEM

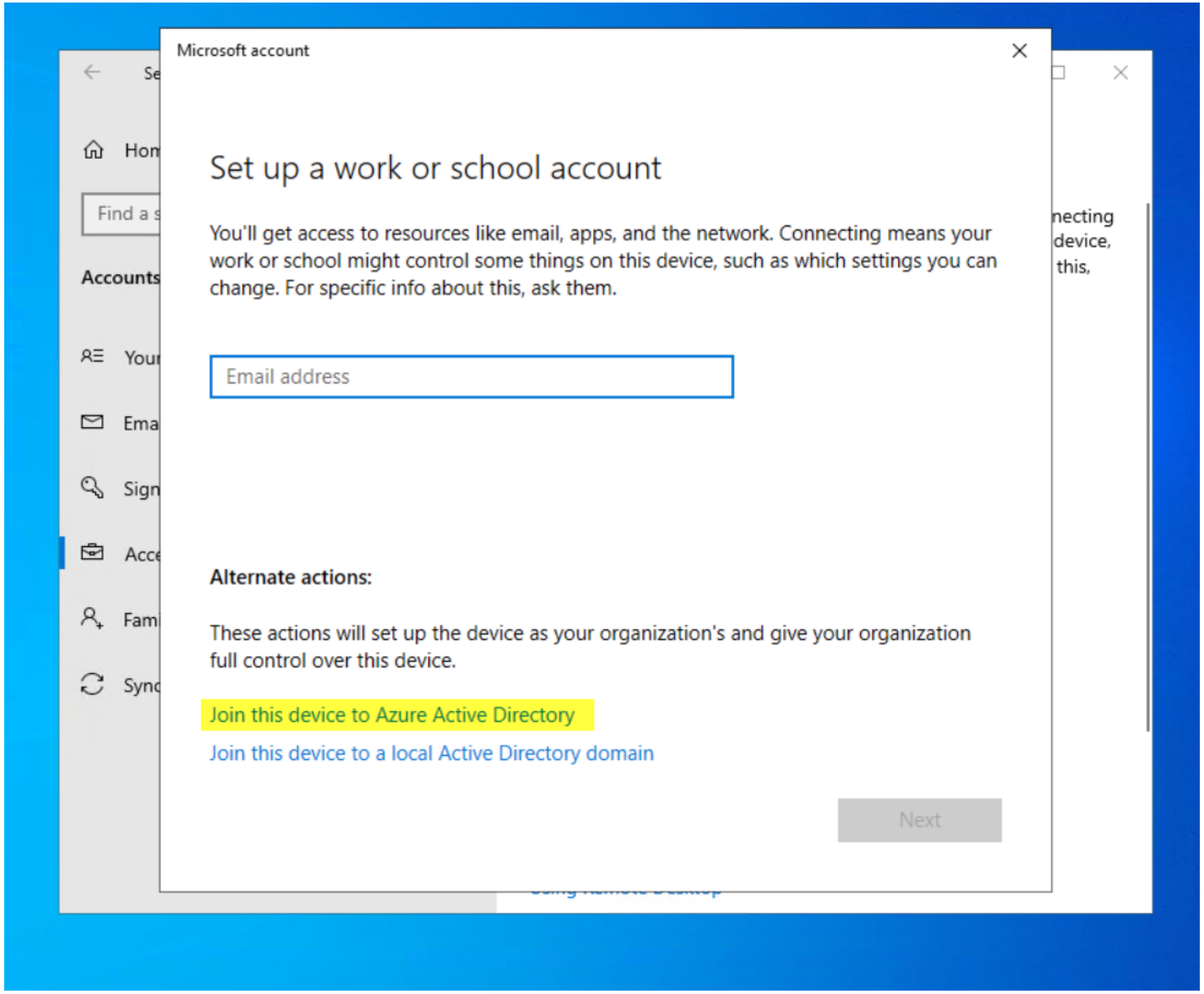
These types of devices are good for point-of-sale or utility apps, but not for users who need to access email or company resources. This method does not allow the use of features such as Conditional Access.

- Bulk Enroll & Windows IoT core devices

You create a provisioning package with the Windows Configuration Designer (WCD) app.


Settings
Home
Find a setting
Accounts
Your info
Email & accounts
Sign-in options
Access work or school
Family & other users
Sync your settings
Access work or school
Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.
Connect
Related settings
Add or remove a provisioning package
Export your management log files
Set up an account for taking tests
Enroll only in device management
Have a question?
Configuring VPN
Using Remote Desktop


Microsoft account
Make sure this is your organization
Make sure this is your organization
If you continue, system policies might be turned on or other changes might be made to your PC.
Is this the right organization?
Connecting to: [redacted].onmicrosoft.com
User name: neliadmin@[redacted]onmicrosoft.com
User type: Administrator
Cancel
Join


Microsoft account
Set up a work or school account
You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.
Email address
Alternate actions:
These actions will set up the device as your organization's and give your organization full control over this device.
Join this device to Azure Active Directory
Join this device to a local Active Directory domain
Next