

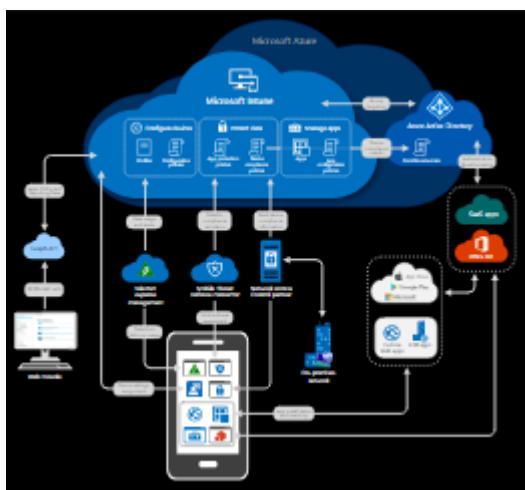
Microsoft intune

Intune- Microsoft Intune is a cloud-based enterprise mobility management tool that **aims** to help organizations manage the mobile devices employees use to **access** corporate data and applications, such as email.

- Manage the mobile devices and PCs your workforce uses to access company data.
- Manage the mobile apps your workforce uses.
- Protect your company information by helping to control the way your workforce accesses and shares it.
- Ensure devices and apps are compliant with company security requirements

How does Intune work?

Intune is the component of Microsoft's Enterprise Mobility + Security (EMS) suite that manages mobile devices and apps. It integrates closely with other EMS components like Azure Active Directory (Azure AD) for identity and access control and Azure Information Protection for data protection. When you use it with Office 365, you can enable your workforce to be productive on all their devices, while keeping your organization's information protected.



Intune app management explained

When we talk about app management, we are talking about:

- Assigning mobile apps to employees
- Configuring apps with standard settings that are used when the app runs
- Controlling how corporate data is used and shared in mobile apps
- Removing corporate data from mobile apps
- Updating apps
- Reporting on mobile app inventory
- Tracking mobile app usage

Before you start

To use Intune in the Azure portal, you must have an Intune admin and tenant account. [Sign up for an account](#) if you don't already have one.

quickstarts

The following quickstarts help you get you started with Intune and complete some common tasks, in a minimal amount of time.

Create a user

Users must have a user account to enroll in Intune device management. To create a new user:

The screenshot shows the Microsoft Intune 'All users' blade in the Azure portal. The left sidebar has 'Users' selected. The main area shows a list of users with one entry: 'Admin Team' (admin@contoso.onmicrosoft.com). A red box highlights the 'All users' link in the sidebar and the 'New user' button at the top right.

In Intune, choose Users > All users > New user.

1. In the Name box enter a name, such as *zeeshan jafri*.
2. In the User name box enter a user identifier, such as zeeshan@jafri.onmicrosoft.com.
3. Choose Show password and make a note of the generated password so that you can generate your own password.
4. Choose Create.

Assign a license to the user

After you've created a user, you must use the [Microsoft 365 admin center](#) to assign an Intune license to them. If you do not assign the user a license, they will be unable to enroll their device into Intune.

To assign an Intune license to a user:

1. Sign in to the [Microsoft 365 admin center](#) with the same credentials you used to sign in to Intune.
2. Choose Users > Active Users > and choose the user you just created.
3. Next to Product licenses select Edit.
4. Under Location, choose a location for the user.
5. Click On next to the Intune license (or another license that you have that includes Intune). The displayed [product name**](#) is used as the service plan in the Azure management
6. Choose Save > Close.

PRODUCTS	STATE	ENABLED SERVICES	ASSIGNMENT PATHS
Dynamics 365 Team Members	Active	10/11	Direct
Microsoft 365 Business	Active	29/30	Direct

Your your must have microsoft 365 business license.

Create a group

1. Once you've opened the Microsoft Intune pane, select Groups > New group.
2. In the Group type dropdown box, select Security.
3. In the Group name field, enter the name for the new group (for example, Contoso Testers).

4. Add a Description for the group.
5. Set the Membership type to Assigned.
6. Click Members and select one or more members for the group from the list

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with options like 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES'. The main area is titled 'Groups - All groups' under 'Microsoft Intune > Groups - All groups'. It shows a list of groups with the following columns: NAME, OBJECT ID, GROUP TYPE, MEMBERSHIP TYPE, EMAIL, and SOURCE. There are buttons for 'New group', 'Delete', 'Refresh', 'Columns', 'Add filters', and search fields for 'Search groups' and 'Add filters'.

The screenshot shows two overlapping dialogs. The left dialog is titled 'Group' and contains the following fields:

- * Group type: Security
- * Group name: Contoso Testers
- Group description: A group used for testers.
- * Membership type: Assigned
- Members: 0 members selected

The right dialog is titled 'Select members' and shows a list of users:

- Select member or invite an external user: Amanda Taylor, ataylor@contoso.onmicrosoft.com
- Selected members: Tyler Miller, tmiller@contoso.onmicrosoft.com (with a 'Remove' link)

At the bottom of the 'Group' dialog are 'Create' and 'Select' buttons.

Set up Windows automatic enrollment

For this example, you'll use MDM enrollment so that both corporate and bring-your-own-devices can be automatically enrolled. You will sign up for a free Azure Active Directory Premium subscription.

1. In Azure, choose Azure Active Directory > Mobility (MDM and MAM).
2. Select Get a free Premium trial to use this feature. Selecting this option will allow auto enrollment using the Azure Active Directory free Premium trial

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is open, with 'Azure Active Directory' selected and highlighted by a red box. Below it, 'Mobility (MDM and MAM)' is also highlighted by a red box. The main content area displays the 'Nod Publishers - Mobility (MDM and MAM)' page under 'Azure Active Directory'. At the top right, there is a message: 'Get a free Premium trial to use this feature' with a purple rocket icon, which is also highlighted by a red box. The page lists various management options: Users, Groups, Organizational relationships, Roles and administrators, Enterprise applications, Devices, App registrations, App registrations (Preview), Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), and Password reset. A single entry for 'Microsoft Intune' is shown under the 'NAME' column.

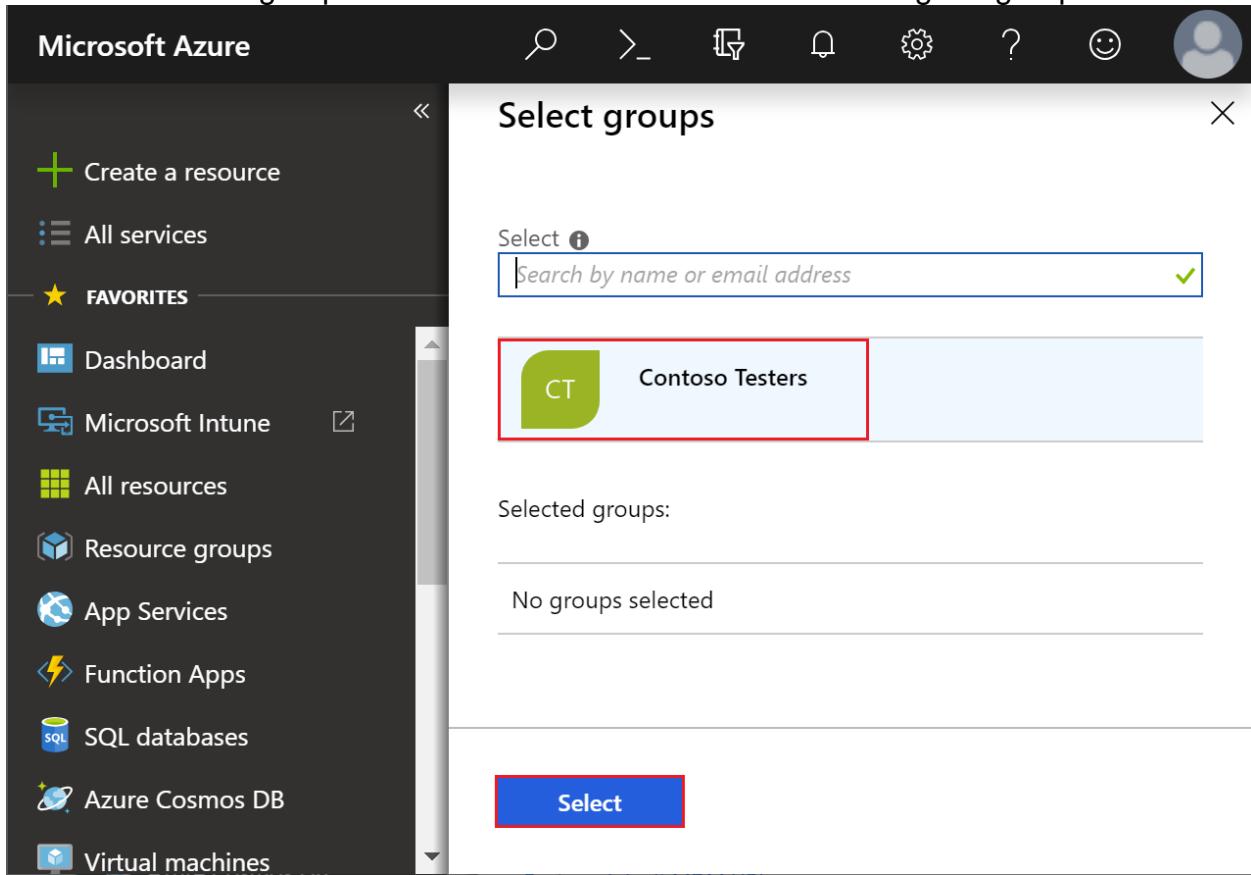
3. Select Microsoft Intune.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like 'Create a resource', 'All services', 'Dashboard', 'Microsoft Intune', 'All resources', 'Resource groups', and 'App Services'. The 'Microsoft Intune' icon is highlighted with a blue square. The main content area has a header 'Home > Nod Publishers - Mobility (MDM and MAM)'. Below the header, there's a search bar and a table titled 'Manage' with columns for 'NAME', 'Users', 'Groups', 'Organizational relationships', and 'Roles and administrators'. A row for 'Microsoft Intune' is selected and highlighted with a red box. The 'NAME' column shows the Microsoft Intune logo and the text 'Microsoft Intune'.

4. Select Some from the MDM user scope to use MDM auto-enrollment to manage enterprise data on your employees' Windows devices. MDM auto-enrollment will be configured for AAD joined devices and bring your own device scenarios.

The screenshot shows the 'Configure' page for Microsoft Intune. The left sidebar includes 'Create a resource', 'All services', 'Dashboard', 'Microsoft Intune' (which is expanded), 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', and 'Virtual networks'. The main area has a header 'Home > Nod Publishers - Mobility (MDM and MAM) > Configure'. It features a 'Configure' section for 'Microsoft Intune' with tabs for 'Save', 'Discard', and 'Delete'. Under 'MDM user scope', the 'None' button is unselected, 'Some' is selected (highlighted with a red box), and 'All' is unselected. The 'Groups' section shows a button to 'Select groups' followed by 'Contoso Testers'. There are also fields for 'MDM terms of use URL' (set to https://portal.manage.microsoft.com/TermsOfUse.aspx), 'MDM discovery URL' (set to https://enrollment.manage.microsoft.com/enrollmentserver/discover...), and 'MDM compliance URL' (set to https://portal.manage.microsoft.com/?portalAction=Compliance). A link 'Restore default MDM URLs' is available. The 'MAM User scope' section is similar, with 'None' unselected, 'Some' selected (highlighted with a red box), and 'All' unselected. The 'Groups' section here also shows a 'Select groups' button followed by 'Contoso Testers'.

5. Choose Select groups > Contoso Testers > Select as the assigned group.



6. Select Some from the MAM Users scope to manage data on your workforce's devices.

7. Choose Select groups > Contoso Testers > Select as the assigned group.

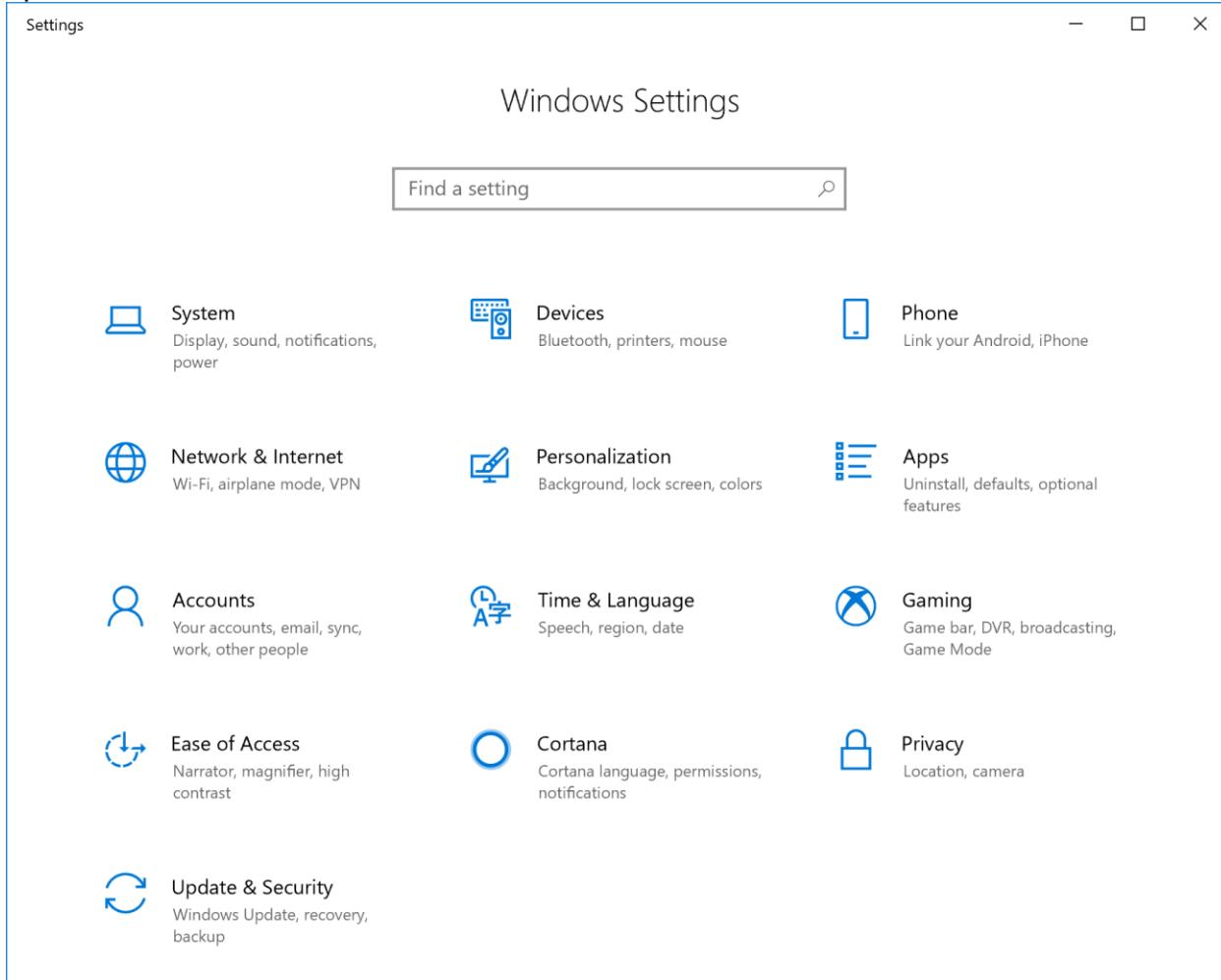
8. Use the default values for the remaining configuration values.

9. Choose Save.

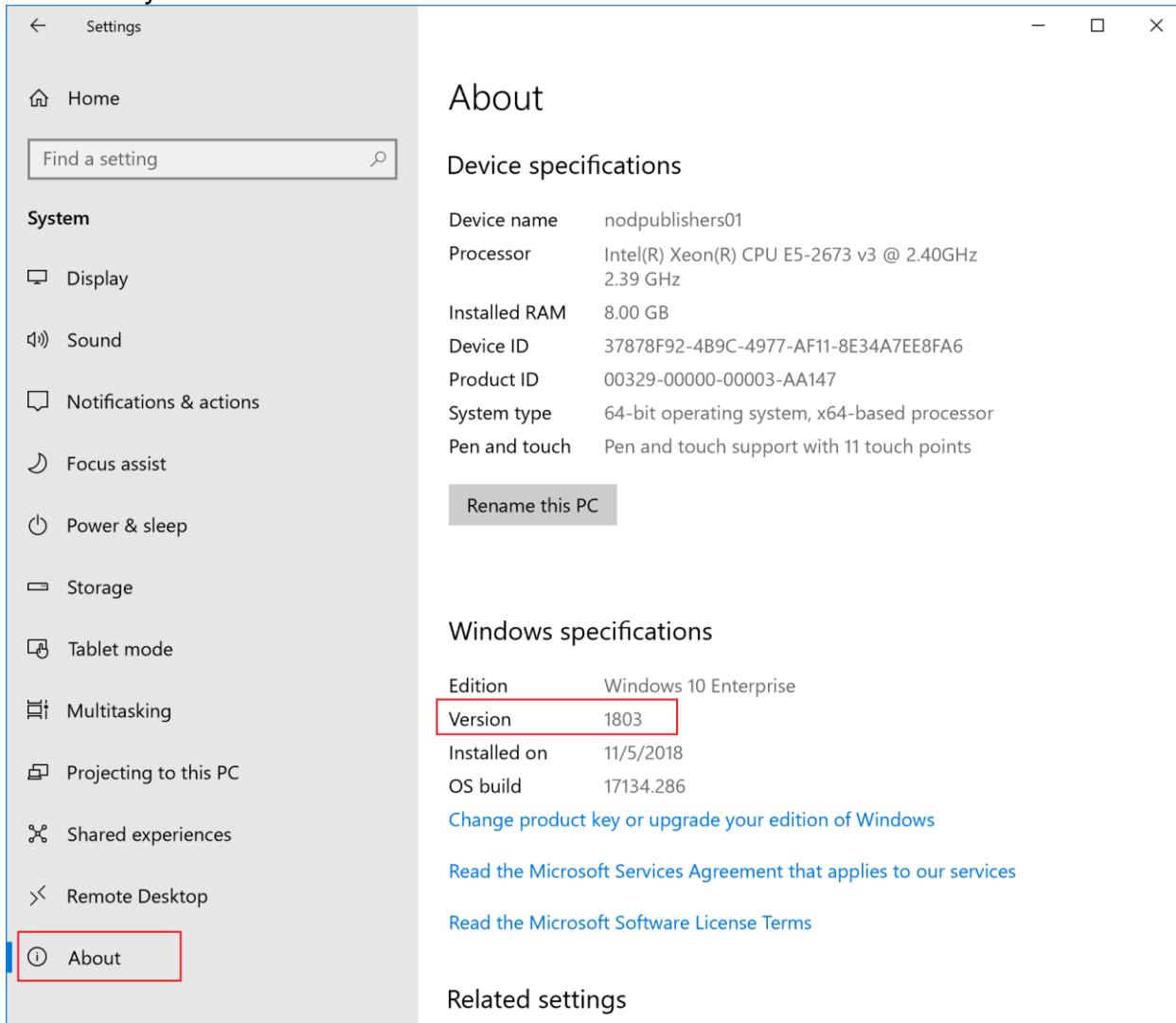
Confirm your Windows 10 Desktop version

Before enrolling your Windows 10 Desktop, you must confirm the version of Windows that you have installed.

1.Right-click the Windows Start icon and select Settings to display Windows Settings options.



2. Select System > About.



Tip

You can also type the phrase "About your PC" into the search bar, then select About your PC.

3. In the Settings window you will see a list of Windows specifications for your PC. Within this list, locate the Version.

4. Confirm that the Windows 10 Version is 1607 or higher.

Enroll Windows 10 Desktop

Windows Settings

 **System**Display, sound, notifications,
power**Devices**

Bluetooth, printers, mouse

**Phone**

Link your Android, iPhone

**Network & Internet**

Wi-Fi, airplane mode, VPN

**Personalization**

Background, lock screen, colors

**Apps**Uninstall, defaults, optional
features**Accounts**Your accounts, email, sync,
work, other people**Time & Language**

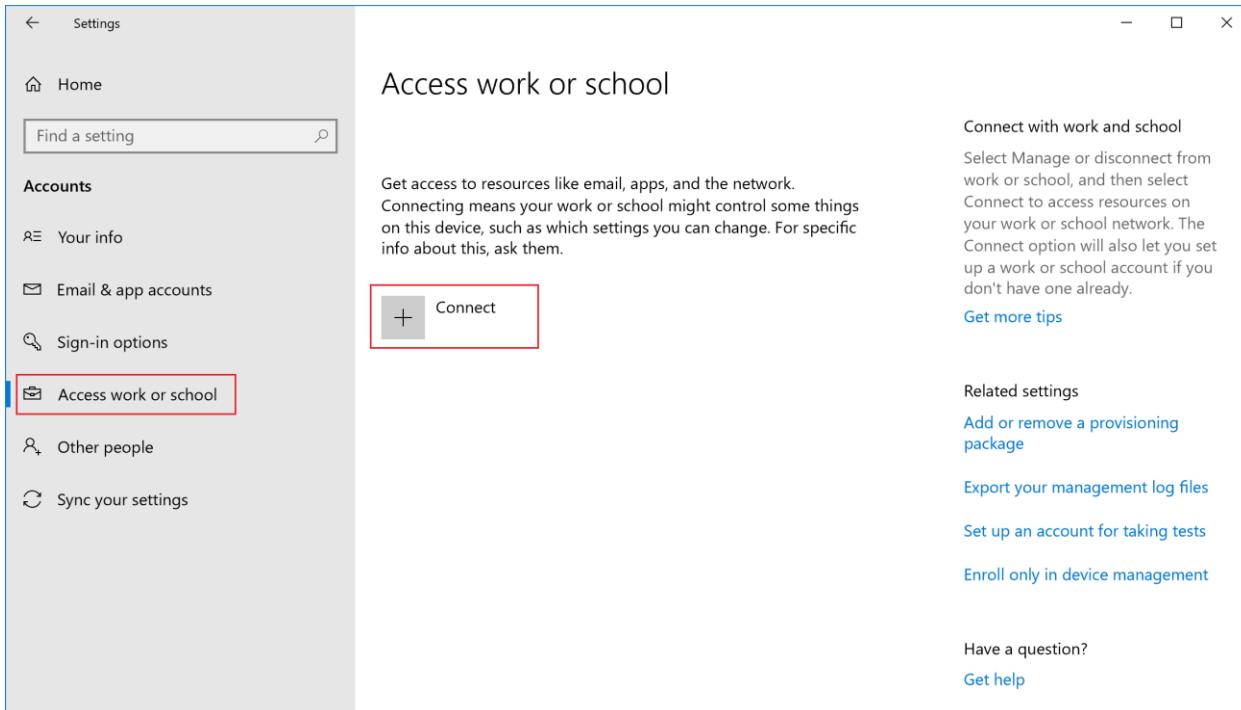
Speech, region, date

**Gaming**Game bar, DVR, broadcasting,
Game Mode**Ease of Access**Narrator, magnifier, high
contrast**Cortana**Cortana language, permissions,
notifications**Privacy**

Location, camera

**Update & Security**Windows Update, recovery,
backup

2. Select Access work or school > Connect.



3. Sign in to Intune with your work or school account, and then select Next. If you followed the [create a user and assign a license](#) quickstart, you can sign in with the user account that you created.

Note

If you setting up an ".onmicrosoft.com", the user account will have .onmicrosoft.com as part of the account address.

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

You'll see a message indicating that your company or school is registering your device.

4. When you see the You're all set! screen, select Done. You're done.

5. You will now see the added account as part of the Access work or school settings on your Windows Desktop.

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

Work or school account
emilyf@nodpublishers001.onmicrosoft.com

Related settings
[Add or remove a provisioning package](#)

Confirm your device enrollment in Intune

- 1.Sign in to [Intune](#) as a Global Administrator or an Intune Service Administrator.
- 2.Select Devices > All devices to view the enrolled devices in Intune.

Verify that you have an additional device enrolled within Intune.

Microsoft Azure

Devices Microsoft Intune

Tenant name: nodpublishers001.onmicrosoft.com
MDM authority: Microsoft Intune
Tenant location: ---
Account status: Active

Intune enrolled devices	
PLATFORM	DEVICES
Windows	1
Android	0
iOS	0
macOS	0
Windows Mobile	0
Total	1

Create a device compliance policy

For this quickstart, you'll use Intune to require your workforce's Android users to enter a password of a specific length before access is granted to information on their Android devices.

- 1.In Intune, select Device compliance > Policies > Create Policy.
- 2.Add Android compliance as the Name. Also, add a Description.
3. For Platform, select Android.
4. Select Settings > System Security to display the Android System Security blade.
5. Click Require next to Require a password to unlock mobile devices.
6. Select At least numeric next to Required password type.

Enter 6 next to Minimum password length.

The screenshot shows the Microsoft Intune Device Compliance - Policies blade. On the left, under 'Android compliance policy' (Android), there are three categories: Device Health (6 settings available), Device Properties (2 settings available), and System Security (10 settings available). The 'System Security' category is selected. On the right, under 'System Security' (Android), the 'Require a password to unlock mobile devices.' setting is configured. The 'Required password type' dropdown is set to 'At least numeric'. The 'Minimum password length' input field is set to '6', which is highlighted with a red border. Other configuration options include 'Maximum minutes of inactivity before password is required' (Not configured), 'Password expiration (days)' (41), and 'Number of previous passwords to prevent reuse' (5). Below these, sections for 'Encryption' (Require), 'Device Security' (Block), and 'Restricted apps' are shown. At the bottom, there are 'OK' buttons for both the left and right panes.

When done, click OK > OK > Create to create the policy.

Add the client app to Intune

An app can be included so that Intune can manage aspects of the app.

Use the following steps to add an app to Intune:

1. In [Intune](#), select Client apps > Apps > Add.
2. Select Windows 10 in the Office 365 Suite section of the App type dropdown box.
3. Select Configure App Suite to select the Office apps to be assigned to the Intune user.
4. Click OK to accept the default selected apps.
5. Select App Suite Information.
6. Enter Microsoft Office 365 app suite as the Suite Name.
7. Enter The Microsoft Office 365 app suite as the Suite Description.
8. Click Yes next to Display this as a featured app in the Company Portal.

Click OK.

The screenshot shows the Microsoft Azure Intune interface. On the left, there's a sidebar with various service icons like Dashboard, Microsoft Intune, Resource groups, etc. The main area has a breadcrumb trail: Home > Microsoft Intune > Client apps - Apps > Add app > App Suite Information. The central part is titled 'Add app' and shows 'App type' set to 'Windows 10'. Below it, there's a note about assigning Office 365 ProPlus apps to Windows 10 devices. Under 'Configure App Suite', it says '8 apps selected'. The 'App Suite Information' section is highlighted, showing 'Suite Name' as 'Microsoft Office 365 app suite' and 'Suite Description' as 'The Microsoft Office 365 app suite.'. There are also fields for 'Publisher' (Microsoft), 'Category' (Productivity), and 'Information URL' (with placeholder 'Enter a valid url'). At the bottom right, there are 'Yes' and 'No' buttons for 'Display this as a featured app in the Company Portal', and an 'OK' button.

Select App Suite Settings. In the Update Channel dropdown box, select Monthly > Click OK > Add.

Assign the app to a group

After you've added an app to Microsoft Intune, you can assign the app to groups of users or devices.

Use the following steps to assign an app to a group:

1. In [Intune](#), select Client apps > Apps.
2. Select the app that you want to assign to a group.
3. Click Assignments > Add group to display the Add group blade.
4. Select Available for enrolled devices in the Assignment type dropdown box.
5. Click Included Groups > Select groups to include > Testers.
6. Click Select > OK > OK > Save to assign the group.

You now have assigned the app to the Testers group.

Install the app on the enrolled device

You must install and use the Company Portal app to install the Contoso's To-Do app made available by Intune. Use the following steps to verify that the app is available to the user of the enrolled device.

1. Log in to your enrolled Windows 10 Desktop device.
Important
The device must be [enrolled with Intune](#). Also, you must sign in to the device using an account contained in the group you assigned to the app.
2. From the Start menu, open the Microsoft Store. Then, find the Company Portal app and install it.
3. Launch the Company Portal app.
4. Click the app that you added using Intune. In this quickstart you added the Microsoft Office 365 app suite app.
5. Click Install.

Create an app protection policy

Use the following steps to create an app protection policy:

1. In [Intune](#), select Client apps > App protection policies > Create Policy.
2. Enter the following details:
 - Name: *Windows 10 content protection*
 - Description: *Users associated with this policy will not be able to cut, copy, or paste any content between the assigned app and other non-managed apps on the device.*
 - Platform: *Windows 10*
 - Enrollment state: *With enrollment*
3. Select Protected apps to choose the apps that must adhere to this policy.
4. Click Add apps.
5. Under Recommended apps, select Word Mobile.
6. Click OK > OK.
7. Select Required settings to configure the app.
8. Click Allow Overrides to set the Windows Information Protection mode.
Selecting this option will block enterprise data from leaving the protected app.
9. Click OK > Create.

You'll now see the app protection policy in Intune.

Assign the app protection policy

After you've created an app protection policy in Intune, you can assign to groups. Use the following steps to assign the app protection policy:

1. In [Intune](#), select Intune > Client apps > App protection policies.
2. Select the app protection policy you created earlier. In this quickstart, the policy is Windows 10 content protection.
3. Select Assignments.
4. Click Select groups to include in the Include tab.
5. Select Contoso Testers as the group to include.
6. Click Select > Save.

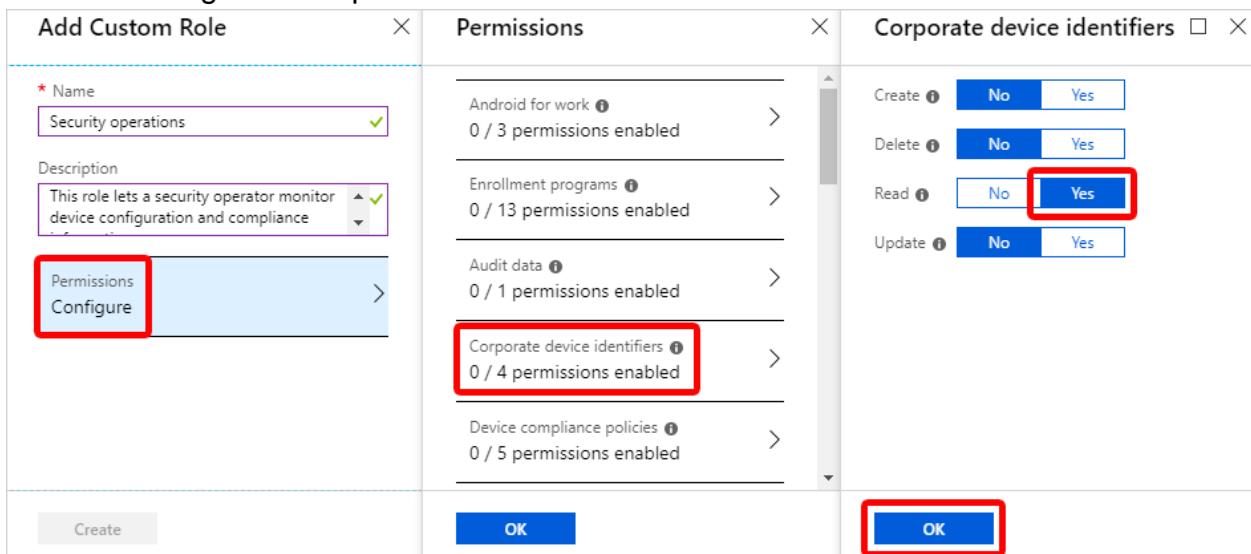
Create a custom role

When you create a custom role, you can set permissions for a wide range of actions. For the security operations role, we'll set a few Read permissions so that the operator can review a device's configurations and policies.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons under 'FAVORITES'. The main area has a title 'Microsoft Intune' and a sub-section 'Intune roles - All roles'. Below this, there's a navigation bar with 'Overview', 'Quick start', 'Manage', 'Monitor', 'Help and support', and 'Roles'. The 'Roles' item is highlighted with a red box. To the right, there's a list of roles with a search bar at the top. The first item, 'Policy and Profile manager', is highlighted with a red box. At the very top right of the main content area, there's an 'Add' button, which is also highlighted with a red box.

1. Under Add custom role, in the Name box, enter *Security operations*.
2. In the Description box, enter *This role lets a security operator monitor device configuration and compliance information*.

Choose Configure > Corporate device identifiers > Yes next to Read > OK.



3. Choose Device compliance policies > Yes next to Read > OK.
4. Choose Device configurations > Yes next to Read > OK.
5. Choose Organization > Yes next to Read > OK.
6. Choose OK > Create.

Assign the role to a group

Before your security operator can use the new permissions, you must assign the role to a group that contains the security user.

1. In Intune, choose Roles > All roles > Security operations.
2. Under Intune roles, choose Assignments > Assign.
3. In the Assignment name box, enter *Sec ops*.
4. Choose Member (Groups) > Add.
5. Choose the Contoso Testers group.
6. Choose Select > OK.
7. Choose Scope (Groups) > Select groups to include > Contoso Testers.
8. Choose Select > OK > OK.

