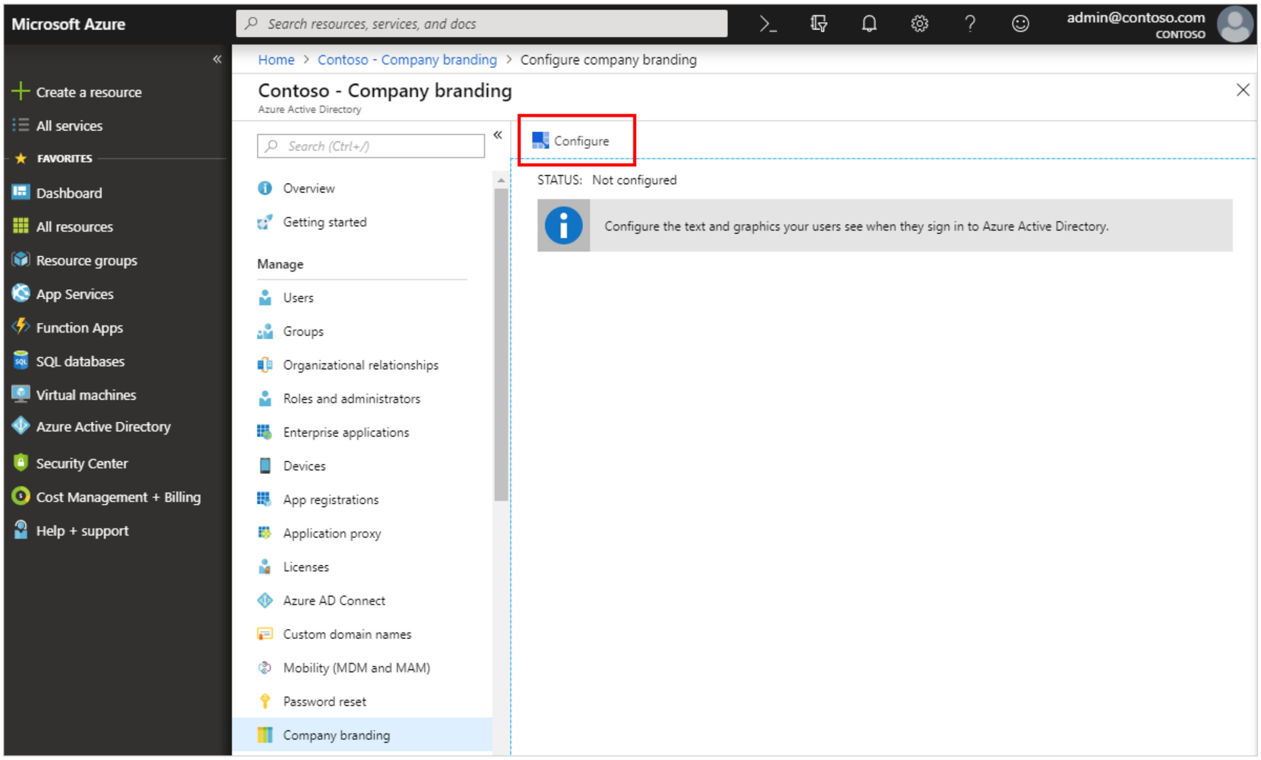
Customize your branding

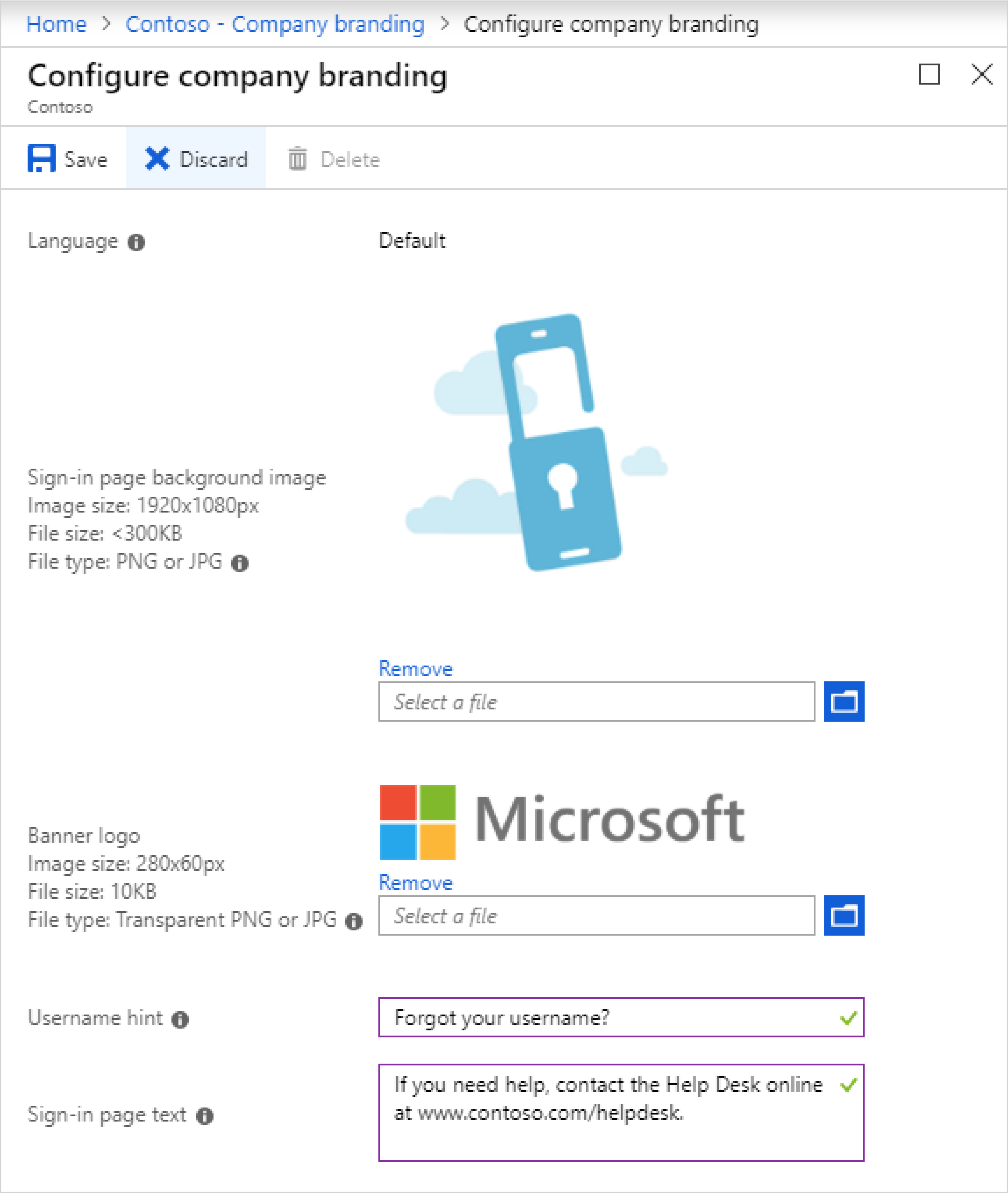
1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Company branding**, and then select **Configure**.



STATUS: Not configured

Configure the text and graphics your users see when they sign in to Azure Active Directory.

3. On the **Configure company branding** page, provide any or all of the following information.
   - **General settings**



Home > Contoso - Company branding > Configure company branding

Configure company branding

Contoso

Language: Default

Sign-in page background image
Image size: 1920x1080px
File size: <300KB
File type: PNG or JPG

Banner logo
Image size: 280x60px
File size: 10KB
File type: Transparent PNG or JPG

Username hint: Forgot your username?

Sign-in page text: If you need help, contact the Help Desk online at www.contoso.com/helpdesk.

- **Language.** The language is automatically set as your default and can't be changed.
- **Sign-in page background image.** Select a .png or .jpg image file to appear as the background for your sign-in pages.

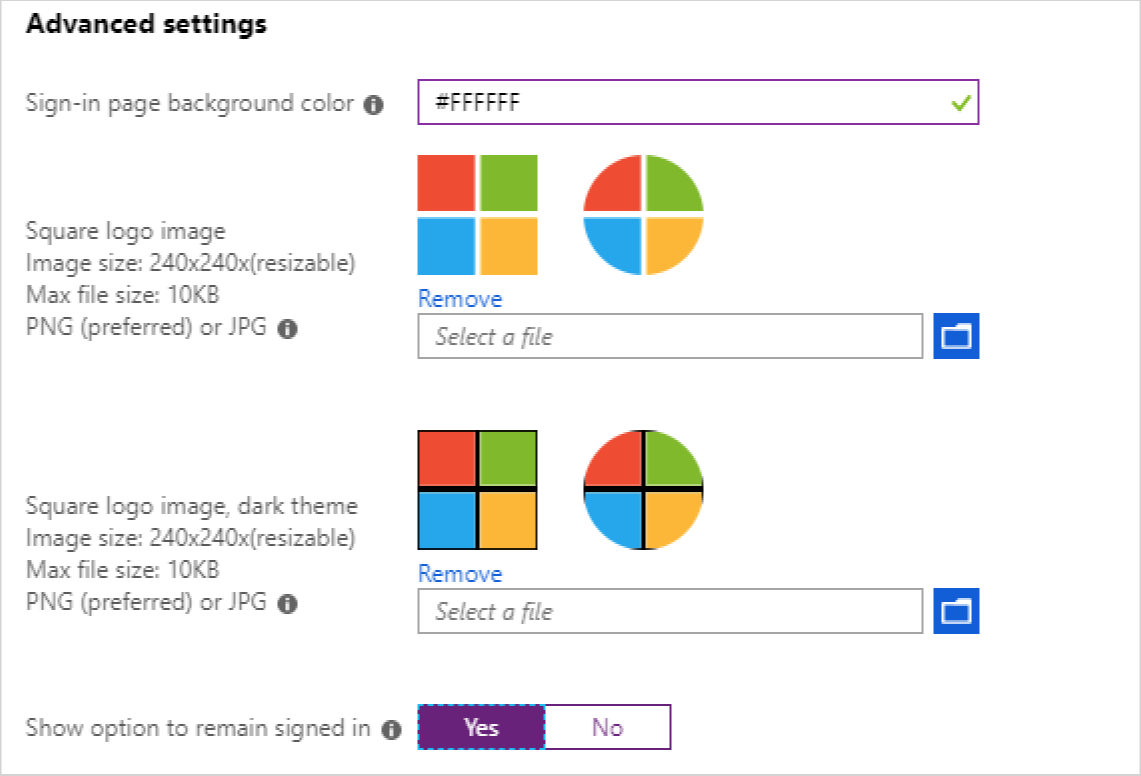
  The image can't be larger than 1920x1080 pixels in size and must have a file size of less than 300 KB.
- **Banner logo.** Select a .png or .jpg version of your logo to appear on the sign-in page after the user enters a username and on the **My Apps** portal page.

The image can't be taller than 36 pixels or wider than 245 pixels. We recommend using a transparent image since the background might not match your logo background. We also recommend not adding padding around the image or it might make your logo look small.

- **Username hint.** Type the hint text that appears to users if they forget their username. This text must be Unicode, without links or code, and can't exceed 64 characters. If guests sign in to your app, we suggest not adding this hint.

- **Sign-in page text.** Type the text that appears on the bottom of the sign-in page. You can use this text to communicate additional information, such as the phone number to your help desk or a legal statement. This text must be Unicode and not exceed 256 characters. We also suggest not including links or HTML tags.

- **Advanced settings**



Advanced settings

Sign-in page background color: #FFFFFF ✓

Square logo image
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG

Remove

Select a file

Square logo image, dark theme
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG

Remove

Select a file

Show option to remain signed in: [✓ Yes] No

- **Sign-in page background color.** Specify the hexadecimal color (for example, white is #FFFFFF) that will appear in place of your background image in low-bandwidth connection situations. We recommend using the primary color of your banner logo or your organization color.

- **Square logo image.** Select a .png (preferred) or .jpg image of your organization's logo to appear to users during the setup process for new Windows 10 Enterprise devices. This image is only used for Windows authentication and appears only on tenants that are using [Windows Autopilot]() for deployment or for password entry pages in other Windows 10 experiences.

  The image can’t be larger than 240x240 pixels in size and must have a file size of less than 10 KB. We recommend using a transparent image since the background might not match your logo background. We also recommend not adding padding around the image or it might make your logo look small.

  - **Square logo image, dark theme.** Same as the square logo image above. This logo image takes the place of the square logo image when used with a dark background, such as with Windows 10 Azure AD joined screens during the out-of-box experience (OOBE). If your logo looks good on white, dark blue, and black backgrounds, you don’t need to add this image.

  - **Show option to remain signed in.** You can choose to let your users remain signed in to Azure AD until explicitly signing out. If you choose **No**, this option is hidden, and users must sign in each time the browser is closed and reopened.

4. After you've finished adding your branding, select **Save**.

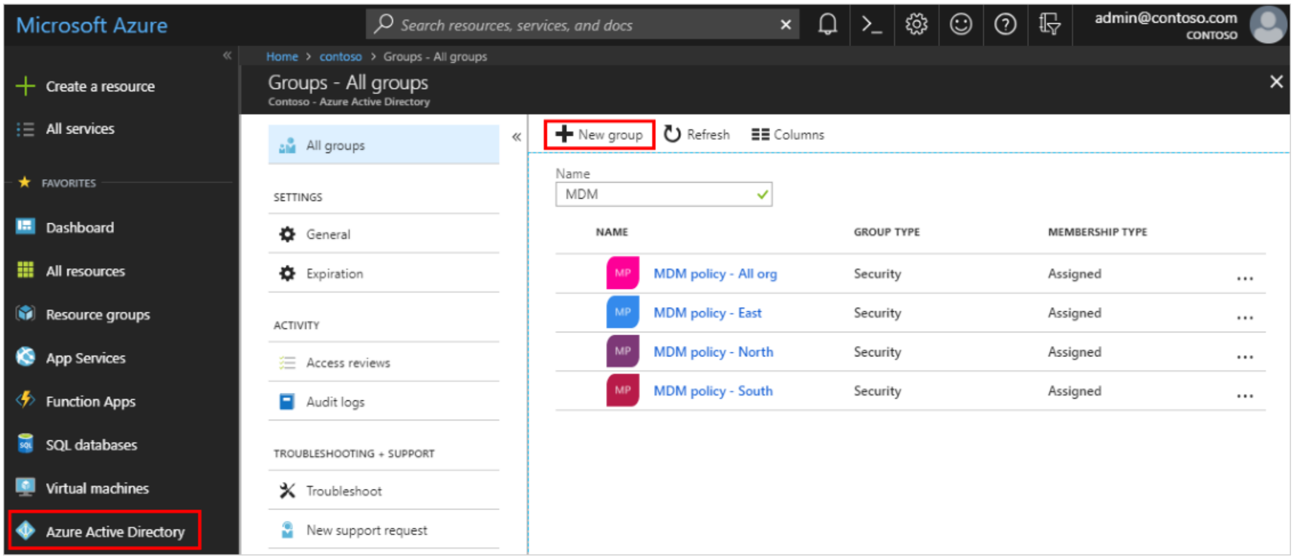
Create a basic group and add members

You can create a basic group and add your members at the same time.

To create a basic group and add members

1. Sign in to the [Azure portal]() using a Global administrator account for the directory.

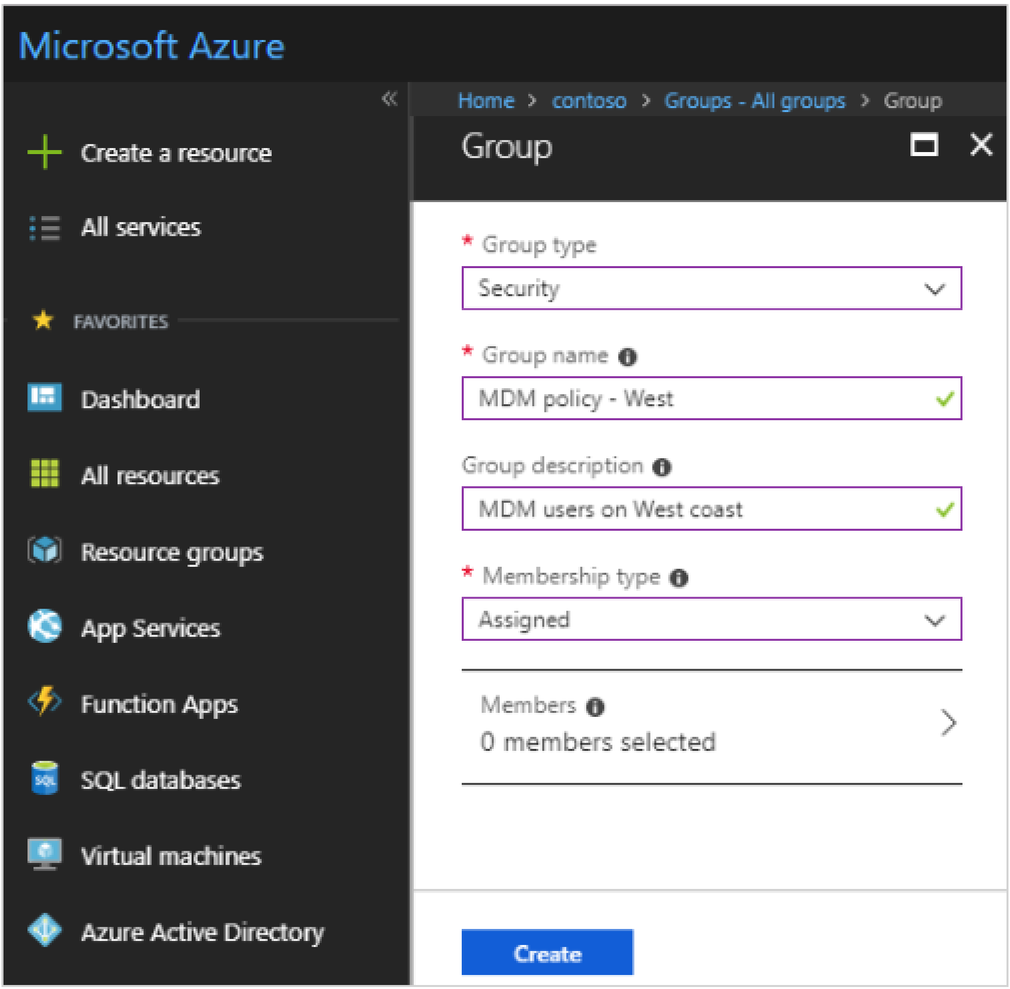
2. Select **Azure Active Directory**, **Groups**, and then select **New group**.



Name: MDM

NAME	GROUP TYPE	MEMBERSHIP TYPE
MDM policy - All org	Security	Assigned
MDM policy - East	Security	Assigned
MDM policy - North	Security	Assigned
MDM policy - South	Security	Assigned

3. In the **Group** page, fill out the required information.



* Group type: Security

* Group name: MDM policy - West

Group description: MDM users on West coast

* Membership type: Assigned

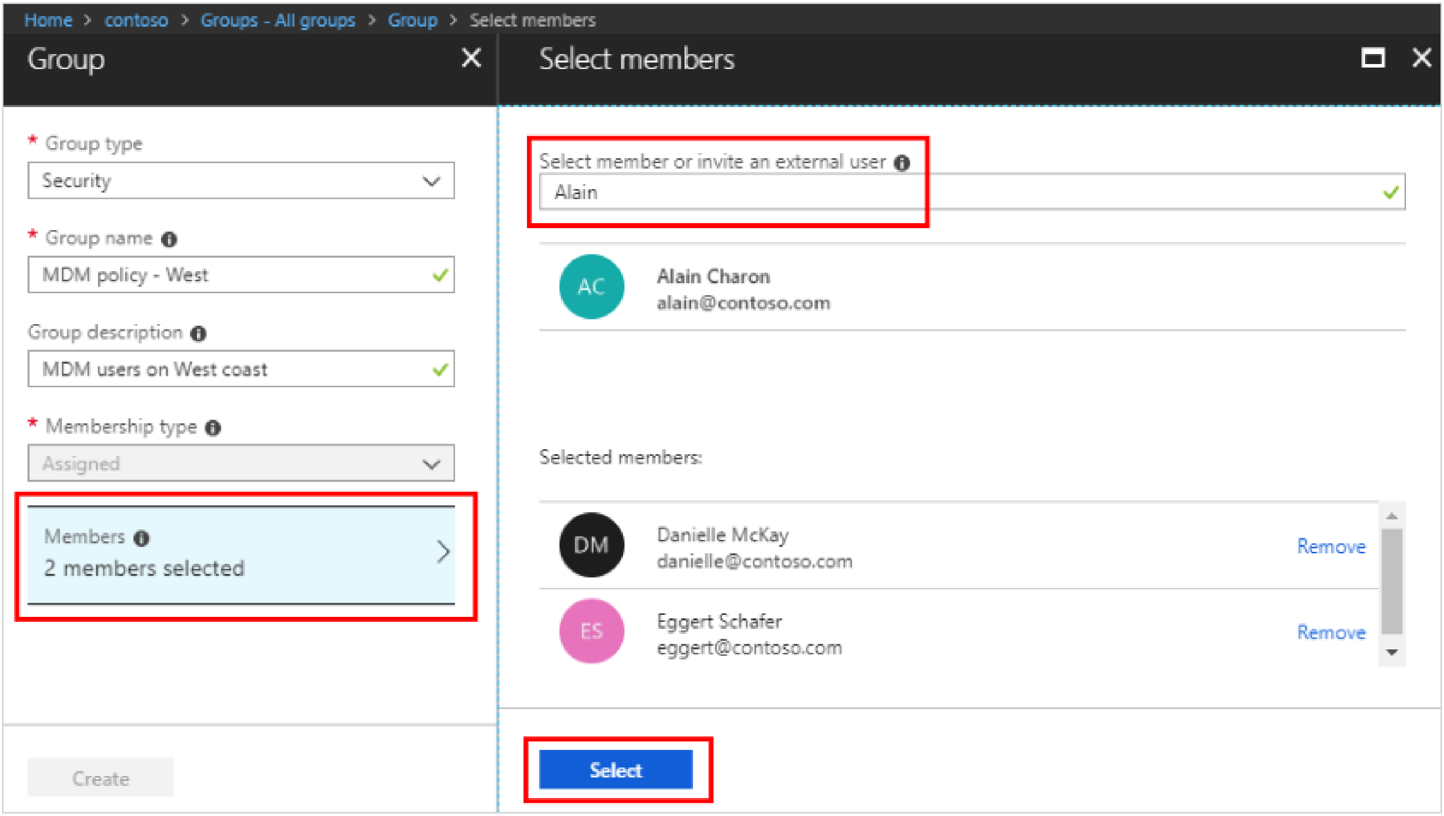
Members: 0 members selected

- **Group type (required).** Select **Security**
- **Group name (required).** Add a name for the group, something that you'll remember and that makes sense.
- **Group description.** Add an optional description to your group.
- **Membership type (required).** Select **Dynamic device**

4. Select **Create**.

   Your group is created and ready for you to add members.

5. Select the **Members** area from the **Group** page, and then begin searching for the members to add to your group from the **Select members** page.



Home > contoso > Groups - All groups > Group > Select members

Group

* Group type: Security

* Group name: MDM policy - West

Group description: MDM users on West coast

* Membership type: Assigned

Members: 2 members selected

Create

Select members

Select member or invite an external user: Alain

Alain Charon
alain@contoso.com

Selected members:

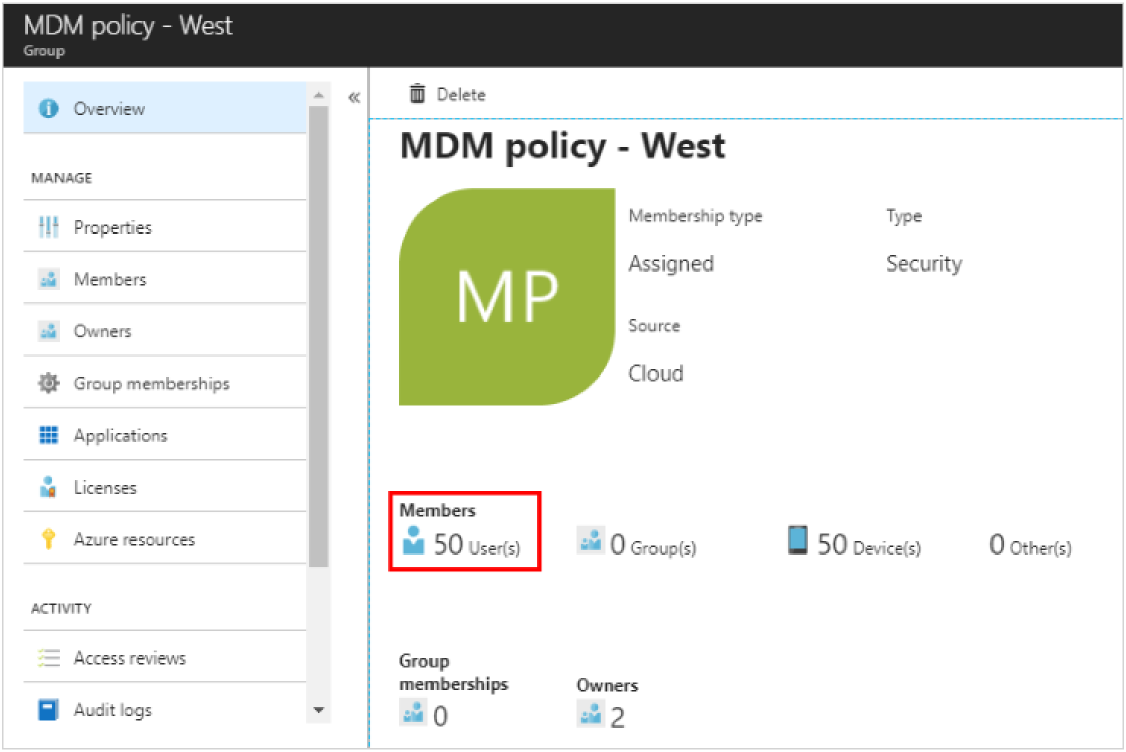
Danielle McKay danielle@contoso.com Remove

Eggert Schafer eggert@contoso.com Remove

Select

6. When you're done adding members, choose **Select**.

   The **Group Overview** page updates to show the number of members who are now added to the group.



MDM policy - West
Group

MDM policy - West

Membership type: Assigned

Type: Security

Source: Cloud

Members: 50 User(s) | 0 Group(s) | 50 Device(s) | 0 Other(s)

Group memberships: 0

Owners: 2

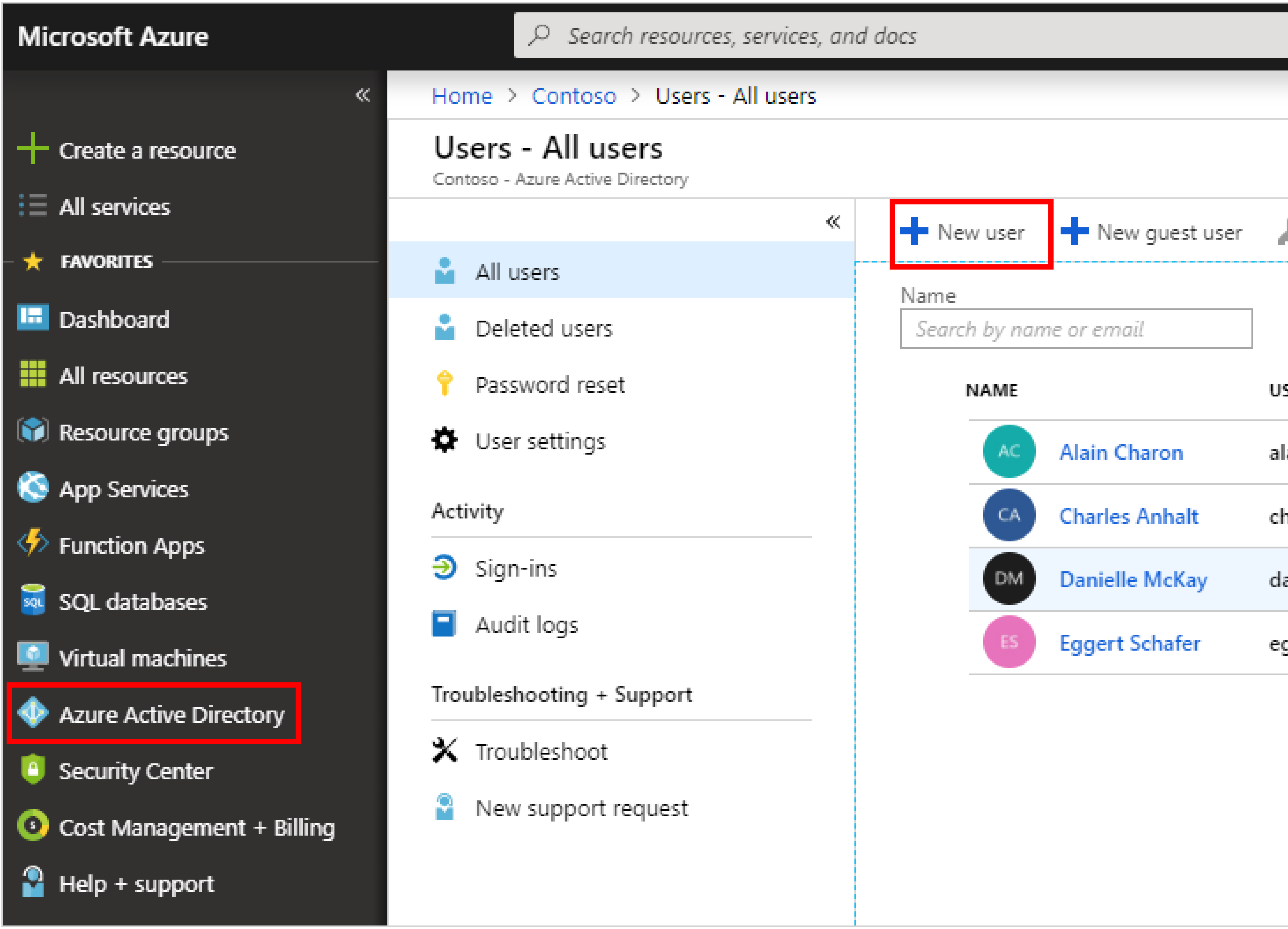
Add a new user

You can create a new user using the Azure Active Directory.

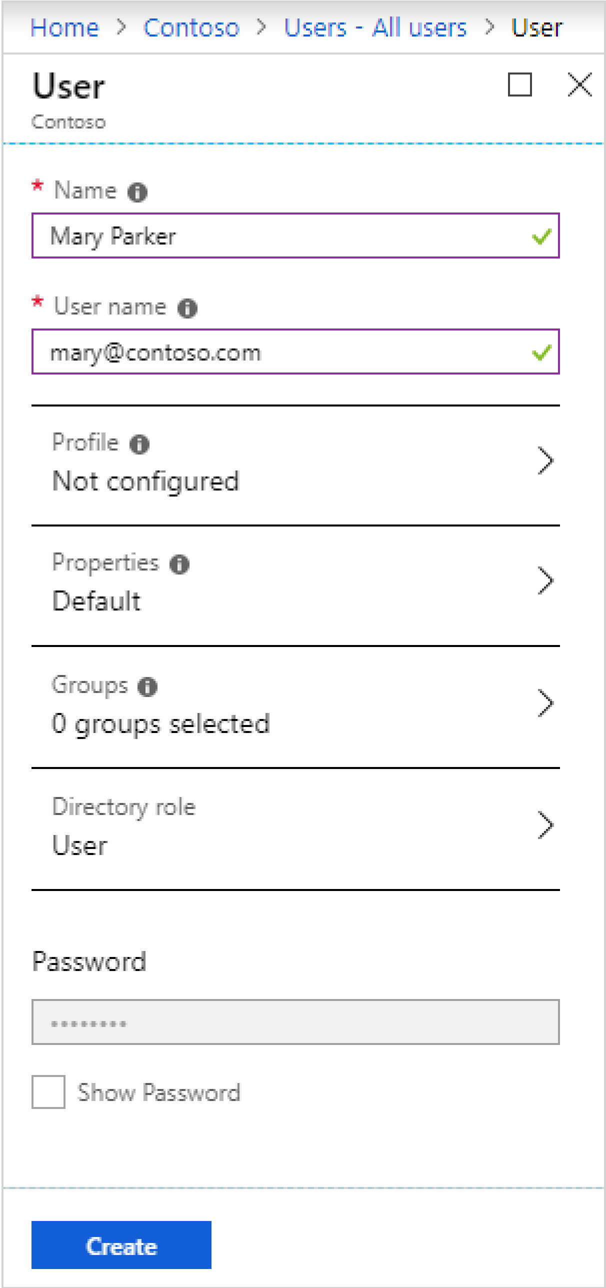
To add a new user

1. Sign in to the [Azure portal]() as a Global administrator or user administrator for the directory.

2. Select **Azure Active Directory**, select **Users**, and then select **New user**.



3. On the **User** page, fill out the required information.



User

Contoso

* Name: Mary Parker

* User name: mary@contoso.com

Profile: Not configured

Properties: Default

Groups: 0 groups selected

Directory role: User

Password: ••••••••

□ Show Password

- **Name (required).** The first and last name of the new user. For example, Mary Parker.
- **User name (required).** The user name of the new user. For example, mary@contoso.com.

  The domain part of the user name must use either the initial default domain name, <*yourdomainname*>.onmicrosoft.com, or a custom domain name, such as contoso.com.
- **Profile.** Optionally, you can add more information about the user. You can also add user information at a later time.
- **Groups.** Optionally, you can add the user to one or more existing groups. You can also add the user to groups at a later time.

- **Directory role.** Optionally, you can add the user to a directory role. You can assign the user to be a global administrator, or to one or more of the other administrator roles in Azure AD.

4. Copy the auto-generated password provided in the **Password** box. You'll need to give this password to the user for the initial sign-in process.

5. Select **Create**.

   The user is created and added to your Azure AD tenant.

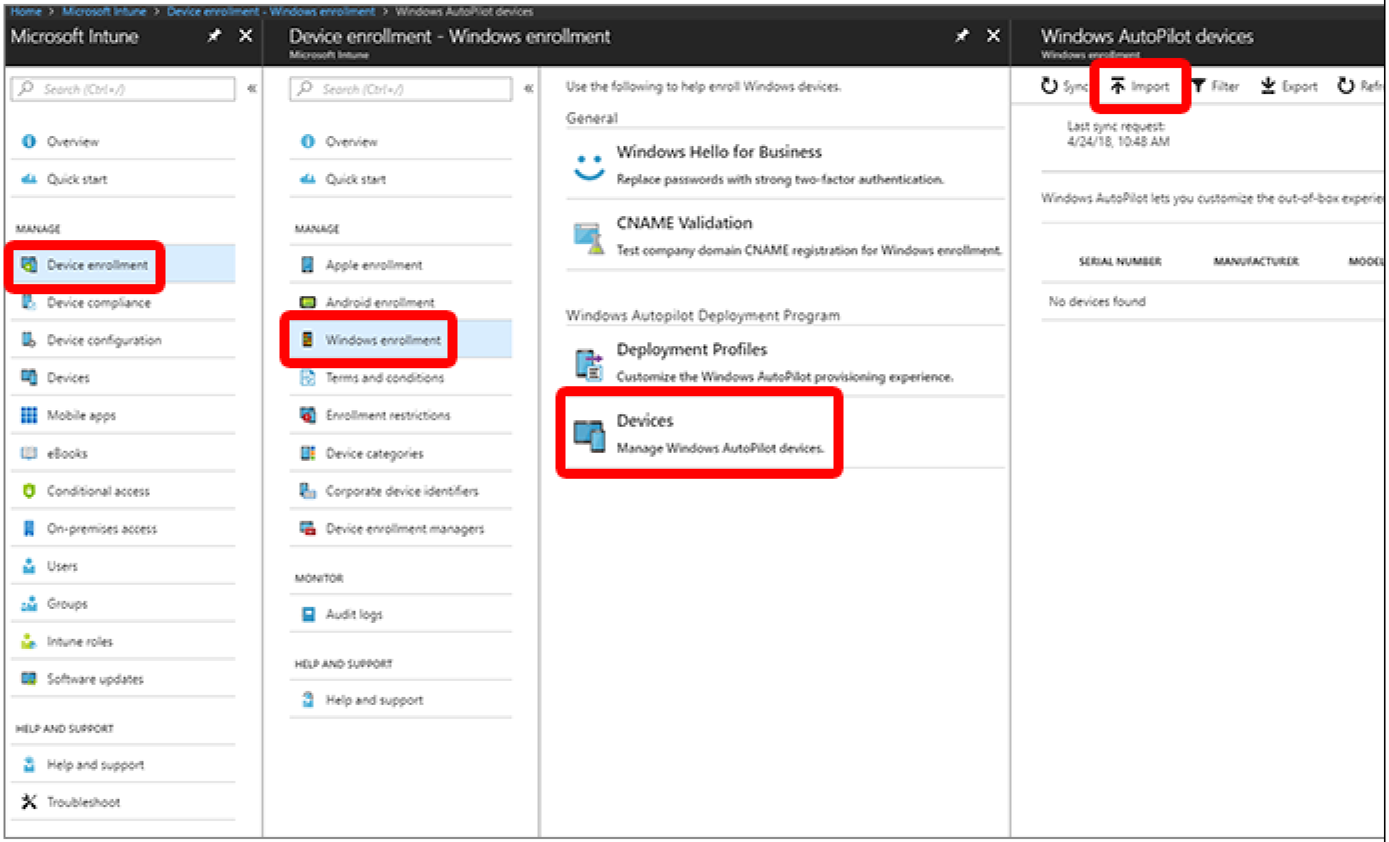
Device Enrollment

Steps

Add devices

You can add Windows Autopilot devices by importing a CSV file with their information.

1. In Intune in the Azure portal, choose **Device enrollment** > **Windows enrollment** > **Devices** > **Import**.



Use the following to help enroll Windows devices.

Replace passwords with strong two-factor authentication.

Test company domain CNAME registration for Windows enrollment.

Customize the Windows AutoPilot provisioning experience.

Manage Windows AutoPilot devices.

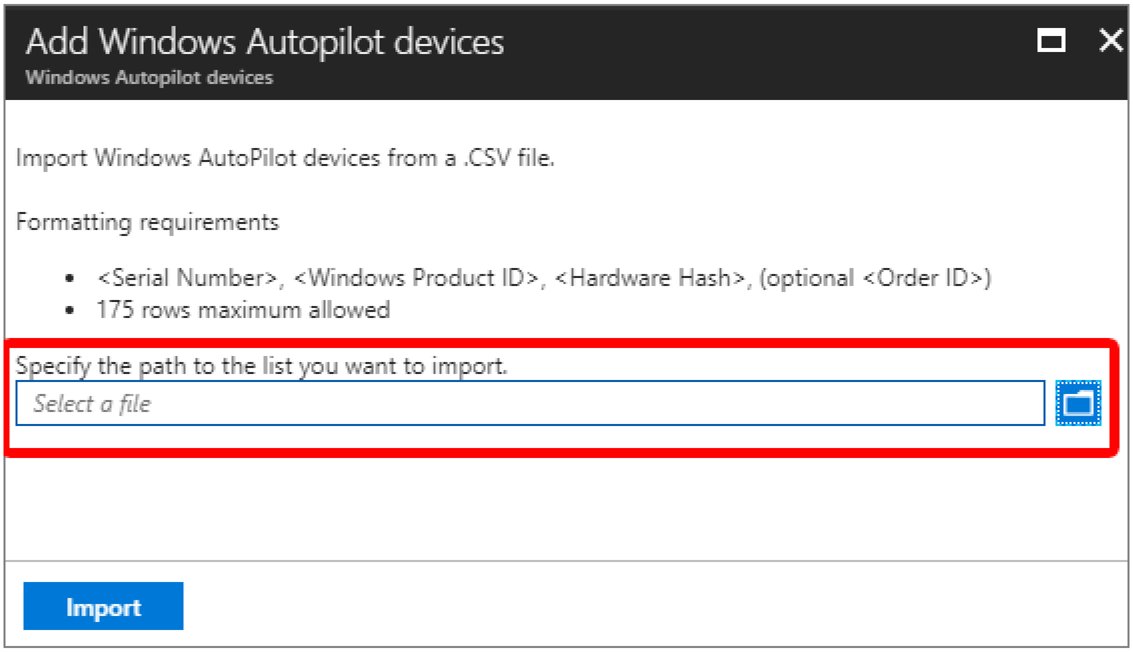
Last sync request:
4/24/18, 10:48 AM

Windows AutoPilot lets you customize the out-of-box experie

No devices found

2. Under **Add Windows Autopilot devices**, browse to a CSV file listing the devices that you want to add. The file should list the serial numbers, Windows product IDs, hardware hashes, and optional order IDs of the devices.

Steps



Add Windows Autopilot devices

Windows Autopilot devices

Import Windows AutoPilot devices from a .CSV file.

Formatting requirements

- <Serial Number>, <Windows Product ID>, <Hardware Hash>, (optional <Order ID>)
- 175 rows maximum allowed

Specify the path to the list you want to import.

Select a file

3. Choose **Import** to start importing the device information. Importing can take several minutes.

4. After import is complete, choose **Device enrollment** > **Windows enrollment** > **Windows Autopilot** > **Devices** > **Sync**. A message displays that the synchronization is in progress. The process might take a few minutes to complete, depending on how many devices are being synchronized.

5. Refresh the view to see the new devices.

Create an Autopilot device group

1. In Intune in the Azure portal, choose **Groups** > **New group**.

2. In the **Group** blade:
   a. For **Group type**, choose **Security**.
   b. Type a **Group name** and **Group description**.
   c. For **Membership type**, choose either **Assigned** or **Dynamic Device**.

3. If you chose **Assigned** for **Membership type** in the previous step, then in the **Group** blade, choose **Members** and add Autopilot devices to the group. Autopilot devices that aren't yet enrolled are devices where the name equals the serial number of the device.

4. If you chose **Dynamic Devices** for **Membership type** above, then in the **Group** blade, choose **Dynamic device members** and type any of the following code in the **Advanced rule** box.

Steps

- If you want to create a group that includes all of your Autopilot devices, type `(device.devicePhysicalIDs -any _ -contains "[ZTDId]")`
- If you want to create a group that includes all of your Autopilot devices with a specific order ID, type: `(device.devicePhysicalIds -any _ -eq "[OrderID]:179887111881")`
- If you want to create a group that includes all of your Autopilot devices with a specific Purchase Order ID, type: `(device.devicePhysicalIds -any _ -eq "[PurchaseOrderId]:76222342342")`

After adding the **Advanced rule** code, choose **Save**.

5. Choose **Create**.

Create an Autopilot deployment profile

Autopilot deployment profiles are used to configure the Autopilot devices.

1. In Intune in the Azure portal, choose **Device enrollment** > **Windows enrollment** > **Deployment Profiles** > **Create Profile**.

2. Type a **Name** and optional **Description**.

3. If you want all devices in the assigned groups to automatically convert to Autopilot, set **Convert all targeted devices to Autopilot** to **Yes**. All non-Autopilot devices in assigned groups will register with the Autopilot deployment service. Allow 48 hours for the registration to be processed. When the device is unenrolled and reset, Autopilot will enroll it. After a device is registered in this way, disabling this option or removing the profile assignment won't remove the device from the Autopilot deployment service. You must instead remove the device directly.

4. For **Deployment mode**, choose one of these two options:
   - **User-driven**: Devices with this profile are associated with the user enrolling the device. User credentials are required to enroll the device.
   - **Self-deploying (preview)**: (requires the most recent Windows 10 Insider Preview Build) Devices with this profile aren't associated with the user enrolling the device. User credentials aren't required to enroll the device.

5. In the **Join to Azure AD as** box, choose **Azure AD joined**.

6. Choose **Out-of-box experience (OOBE)**, configure the following options, and then choose **Save**:

Steps

- **Language (Region)***: Choose the language to use for the device. This option is only available if you chose **Self-deploying** for **Deployment mode**.
- **Automatically configure keyboard***: If a **Language (Region)** is selected, choose **Yes** to skip the keyboard selection page. This option is only available if you chose **Self-deploying** for **Deployment mode**.
- **End-user license agreement (EULA)**: (Windows 10, version 1709 or later) Choose if you want to show the EULA to users.
- **Privacy settings**: Choose if you want to show privacy settings to users.
- **Hide change account options (Windows Insider only)**: Choose **Hide** to prevent change account options from displaying on the company sign-in and domain error pages. This option requires company branding to be configured in Azure Active Directory.
- **User account type**: Choose the user's account type (**Administrator** or **Standard** user).
- **Apply computer name template (Windows Insider only)**: Choose **Yes** to create a template to use when naming a device during enrollment. Names must be 15 characters or less, and can have letters, numbers, and hyphens. Names can't be all numbers. Use the %SERIAL% macro to add a hardware-specific serial number. Or, use the %RAND:x% macro to add a random string of numbers, where x equals the number of digits to add.

7. Choose **Create** to create the profile. The Autopilot deployment profile is now available to assign to devices.

*Both **Language (Region)** and **Automatically configure keyboard** are only available if you chose **Self-deploying (preview)** for **Deployment mode** (requires the most recent Windows 10 Insider Preview Build).

Assign an Autopilot deployment profile to a device group

1. In Intune in the Azure portal, choose **Device enrollment** > **Windows enrollment** > **Deployment profiles** > choose a profile.
2. In the specific profile blade, choose **Assignments**.
3. Choose **Select groups**, then in the **Select groups** blade, choose the group(s) that you want to assign the profile to, then choose **Select**.

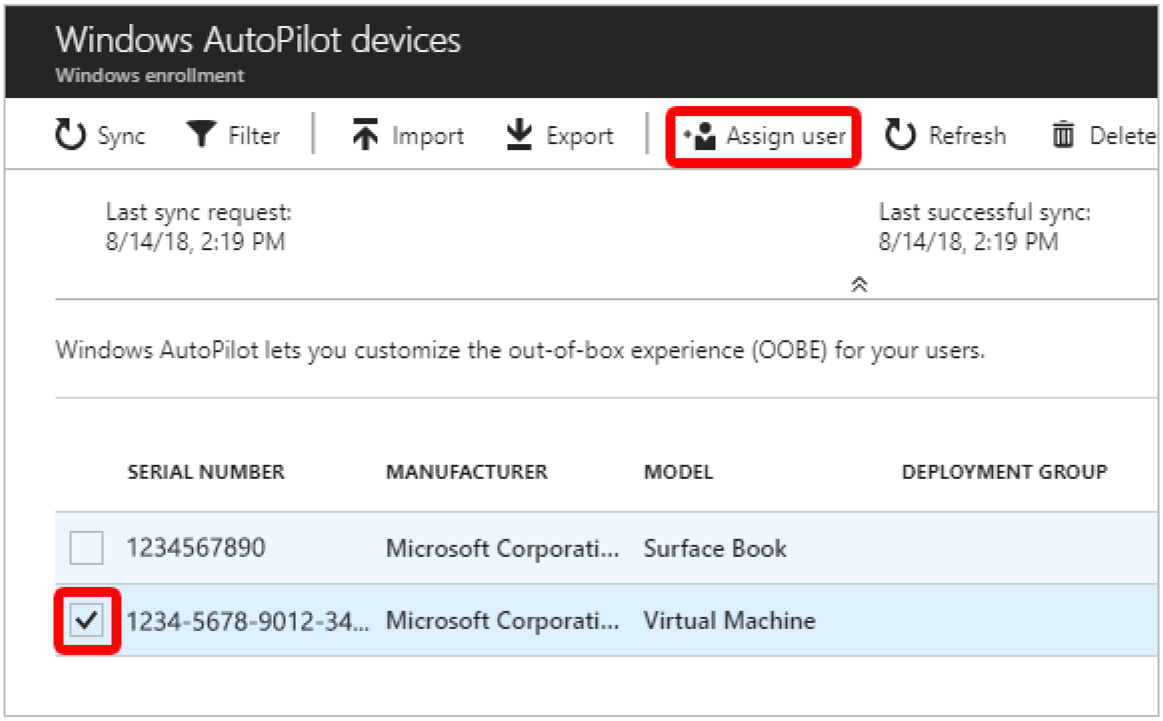
Steps

Assign a user to a specific Autopilot device

You can assign a user to a specific Autopilot device. This assignment pre-fills a user from Azure Active Directory in the company-branded sign-in page during Windows setup. It also lets you set a custom greeting name. It doesn't pre-fill or modify Windows sign-in. Only licensed Intune users can be assigned in this manner.

Prerequisites: Azure Active Directory Company Portal has been configured and the most recent Windows 10 Insider Preview Build.

1. In the Intune in the Azure portal, choose **Device enrollment** > **Windows enrollment** > **Devices** > choose the device > **Assign user**.



Last sync request:
8/14/18, 2:19 PM

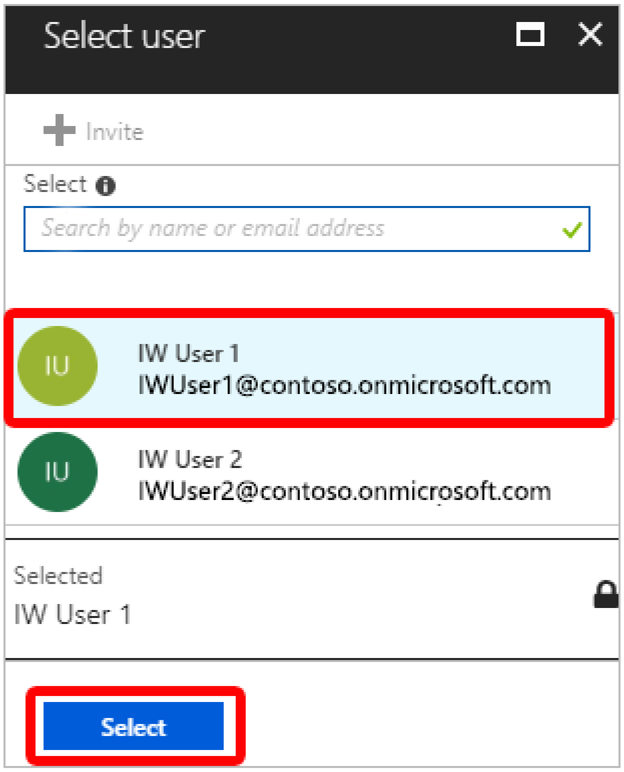
Last successful sync:
8/14/18, 2:19 PM

Windows AutoPilot lets you customize the out-of-box experience (OOBE) for your users.

	SERIAL NUMBER	MANUFACTURER	MODEL	DEPLOYMENT GROUP
□	1234567890	Microsoft Corporati...	Surface Book	
☑	1234-5678-9012-34...	Microsoft Corporati...	Virtual Machine	

2. Choose an Azure user licensed to use Intune and choose **Select**.

Steps



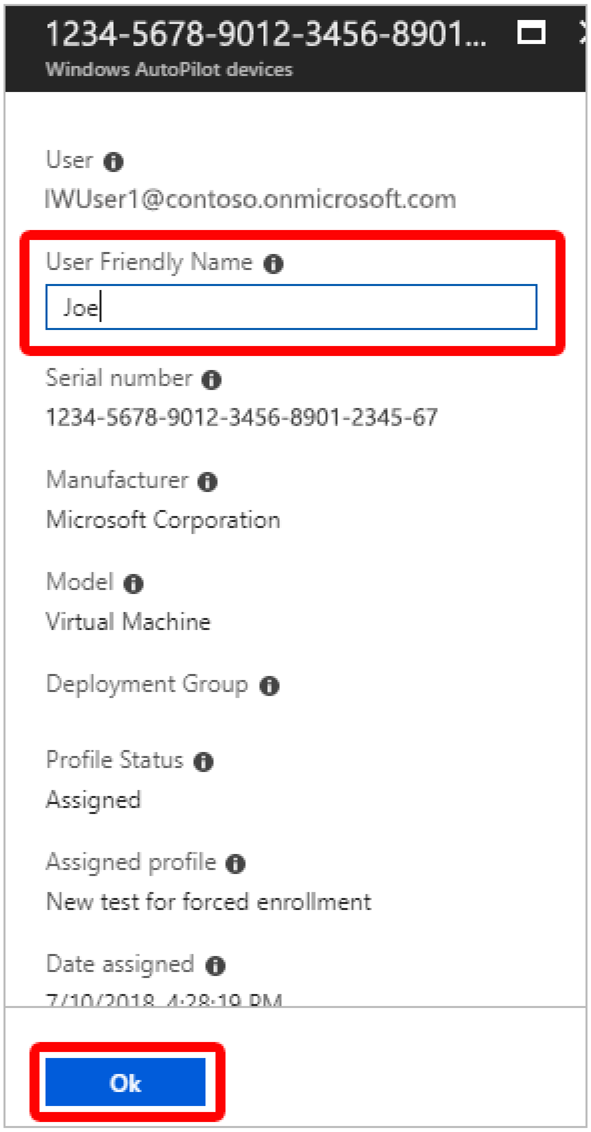
IW User 1
IWUser1@contoso.onmicrosoft.com

IW User 2
IWUser2@contoso.onmicrosoft.com

Selected
IW User 1

3. In the **User Friendly Name** box, type a friendly name or just accept the default. This string is the friendly name that displays when the user signs in during Windows setup.

Steps



1234-5678-9012-3456-8901...

Windows AutoPilot devices

User

IWUser1@contoso.onmicrosoft.com

User Friendly Name

Joe

Serial number

1234-5678-9012-3456-8901-2345-67

Manufacturer

Microsoft Corporation

Model

Virtual Machine

Deployment Group

Profile Status

Assigned

Assigned profile

New test for forced enrollment

Date assigned

7/10/2018 4:28:10 PM

4. Choose **Ok**.

Device Compliance Policies

Steps

Android

1. In the Azure portal, select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance** > **Policies** > **Create Policy**.
3. Enter a **Name** and **Description**.
4. For **Platform**, select **Android**.
5. Choose **Settings Configure**. Enter the **Device Health**, **Device Properties**, and **System Security** settings, as described in this article.

Device health

- **Rooted devices**: Choose **Block** to mark rooted (jailbroken) devices as not compliant. When you choose **Not configured** (default), this setting isn't evaluated for compliance or non-compliance.

- **Require the device to be at or under the Device Threat Level**: Use this setting to take the risk assessment from the Lookout MTP solution as a condition for compliance. When you choose **Not configured** (default), this setting isn't evaluated for compliance or non-compliance. To use this setting, choose the allowed threat level to be:
  - **Secured**: This option is the most secure, as the device can't have any threats. If the device is detected with any level of threats, it's evaluated as noncompliant.

- **Google Play Services is configured**: **Require** that the Google Play services app is installed and enabled.

- **Up-to-date security provider**: **Require** that an up-to-date security provider can protect a device from known vulnerabilities.

- **Threat scan on apps**: **Require** that the Android **Verify Apps** feature is enabled.

- **SafetyNet device attestation**: Enter the level of SafetyNet attestation that must be met:
  - **Check basic integrity & certified devices**

System security settings

Password

Steps

- **Require a password to unlock mobile devices**: **Require** users to enter a password before they can access their device.
- **Minimum password length**: 8
- **Required password type**: **At least alphanumeric with symbols**
- **Maximum minutes of inactivity before password is required**: 10
- **Password expiration (days)**: 60
- **Number of previous passwords to prevent reuse**: 5

Encryption

- **Encryption of data storage on a device** (Android 4.0 and above, or KNOX 4.0 and above): Choose **Require** to encrypt data storage on your devices.

Device Security

- **Block apps from unknown sources**: Choose to **block** devices with "Security > Unknown Sources" enabled sources (supported on Android 4.0 – Android 7.x; not supported by Android 8.0 and later).
- **Company portal app runtime integrity**: Choose **Require** to confirm the Company Portal app meets all the following requirements:
  - Has the default runtime environment installed
  - Is properly signed
  - Isn't in debug-mode
  - Is installed from a known source
- **Block USB debugging on device** (Android 4.2 or later): Choose **Block** to prevent devices from using the USB debugging feature.

When done, select **OK** > **OK** to save your changes.

iOS

1. In the Azure portal, select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance** > **Policies** > **Create Policy**.

Steps

3. Enter a **Name** and **Description**.
4. For **Platform**, select **iOS**. Choose **Settings Configure**, and enter the **Email**, **Device Health**, **Device Properties**, and **System Security** settings. When you're done, select **OK**, and **Create**.

Device health

- **Jailbroken devices**: Block
- **Require the device to be at or under the Device Threat Level** (iOS 8.0 and newer): Choose the maximum threat level to mark devices as noncompliant. Devices that exceed this threat level get marked as noncompliant:
  - **Secured**: This option is the most secure, as the device can't have any threats. If the device is detected as having any level of threats, it is evaluated as noncompliant.

System security

Password

- **Require a password to unlock mobile devices**: **Require** users to enter a password before they can access their device.

- **Simple passwords**: Set to **Block** so users can't create simple passwords, such as **1234** or **1111**.

- **Minimum password length**: 6

- **Required password type**: **Numeric**

- **Maximum minutes of inactivity before password is required**: 10

- **Password expiration (days)**: 60

- **Number of previous passwords to prevent reuse**: 5

Windows:

1. In the Azure portal, select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance** > **Policies** > **Create Policy**.
3. Enter a **Name** and **Description**.

Steps

4. For **Platform**, select **Windows Phone 8.1**, **Windows 8.1 and later**, or **Windows 10 and later**. Choose **Settings Configure**, and enter the **Device Health**, **Device Properties**, and **System Security** settings. When you're done, select **OK**, and **Create**.

System security

Password

Require a password to unlock mobile devices: **Require** users to enter a password before they can access their device.

Simple passwords: Set to **Block** so users can't create simple passwords, such as **1234** or **1111**.

Minimum password length: 8

Password type: **Alphanumeric**

Number of non-alphanumeric characters in password: If **Required password type** is set to **Alphanumeric**, this setting specifies the minimum number of character sets that the password must contain. The four character sets are:

Lowercase letters

Uppercase letters

Symbols

Numbers

Maximum minutes of inactivity before password is required: 15

Password expiration (days): 90

Number of previous passwords to prevent reuse: 5

Encryption

Require encryption on mobile device: **Require**

Steps

Windows 10 and later policy settings

Device health

Require BitLocker: Yes

Require Secure Boot to be enabled on the device: Yes

Device properties

Minimum OS version: `Microsoft Windows [Version 10.0.17134.1]`

Encryption of data storage on a device: Choose **Require** to encrypt data storage on your devices.

Device Security

Antivirus: When set to **Require**, you can check compliance using antivirus solutions that are registered with Windows Security Center, such as Symantec and Windows Defender.

AntiSpyware: When set to **Require**, you can check compliance using antispyware solutions that are registered with Windows Security Center, such as Symantec and Windows Defender.

Windows Defender ATP

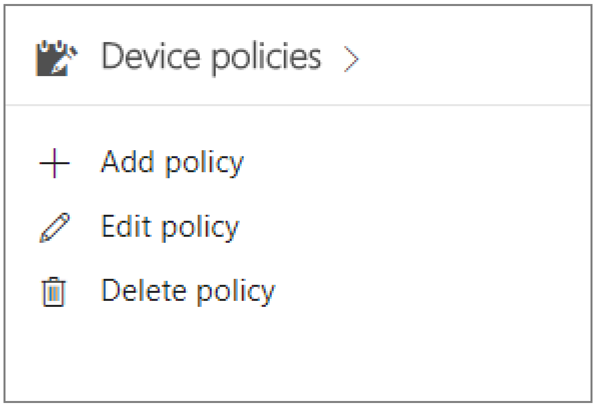
Require the device to be at or under the machine risk score: Use this setting to take the risk assessment from your defense threat services as a condition for compliance. Choose the maximum allowed threat level:

Medium: The device is evaluated as compliant if existing threats on the device are low or medium level. If the device is detected to have high-level threats, it is determined to be noncompliant.

Set device protection settings for Windows 10 PCs

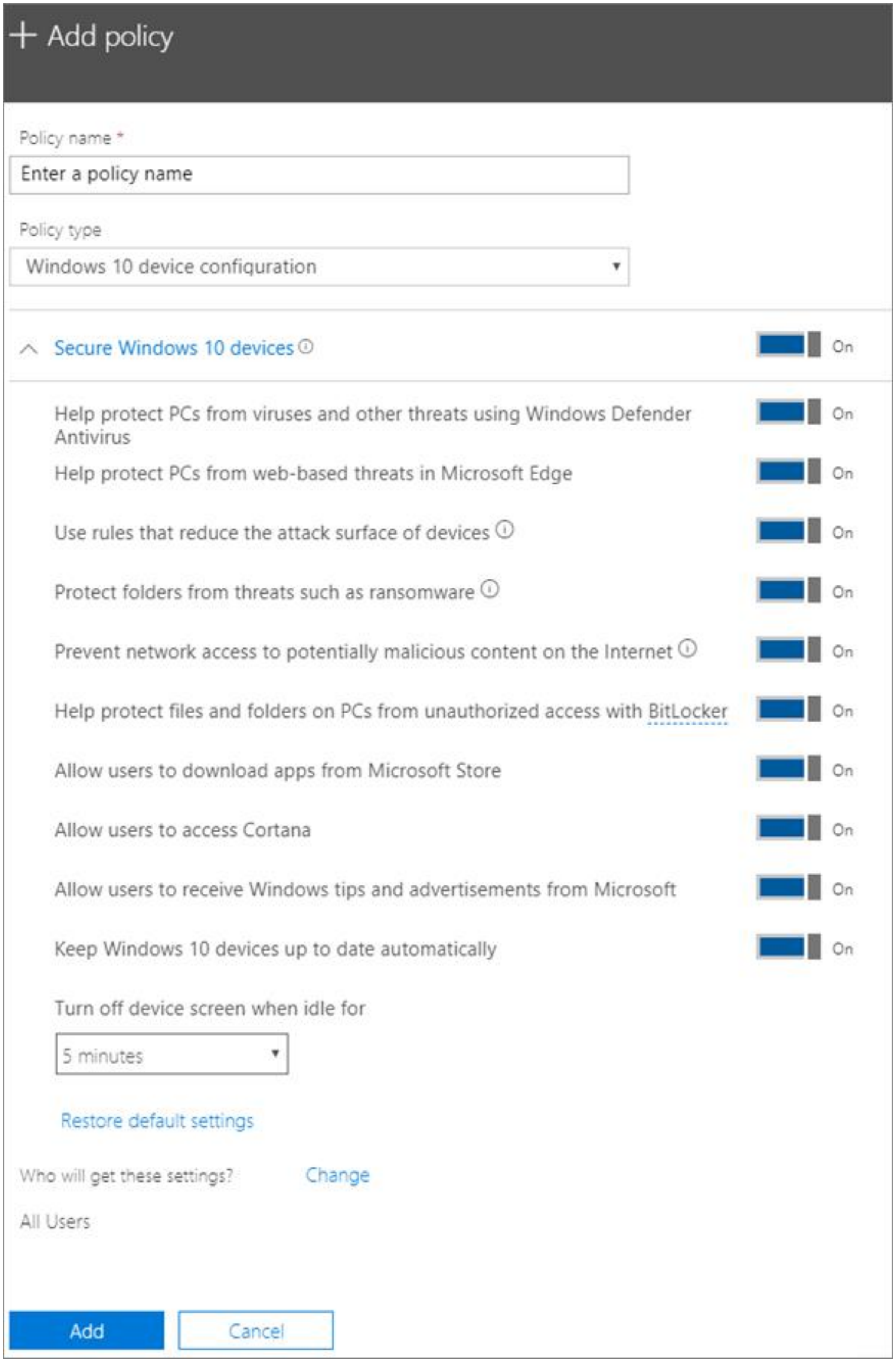
Secure Windows 10 devices

1. Sign in to Microsoft 365 Business with global admin credentials.
2. in the admin center, on the **Device policies** card, choose **Add policy**.



3. On the **Add policy** pane, enter a unique name for this policy.
4. Under **Policy type**, choose **Windows 10 Device Configuration**.
5. Expand **Secure Windows 10 Devices** > configure the settings how you would like.

   You can always use the **Reset default settings** link to return to the default setting.



+ Add policy

Policy name *

Enter a policy name

Policy type

Windows 10 device configuration

Secure Windows 10 devices — On

Help protect PCs from viruses and other threats using Windows Defender Antivirus	On
Help protect PCs from web-based threats in Microsoft Edge	On
Use rules that reduce the attack surface of devices	On
Protect folders from threats such as ransomware	On
Prevent network access to potentially malicious content on the Internet	On
Help protect files and folders on PCs from unauthorized access with BitLocker	On
Allow users to download apps from Microsoft Store	On
Allow users to access Cortana	On
Allow users to receive Windows tips and advertisements from Microsoft	On
Keep Windows 10 devices up to date automatically	On

Turn off device screen when idle for

5 minutes

Who will get these settings?

All Users

6. Next decide **Who will get these settings?** If you don't want to use the default **All users** security group, Choose **Change**, search for the security group who will get these settings > **Select**.

7. Finally, choose **Done** to save the policy, and assign it to devices.

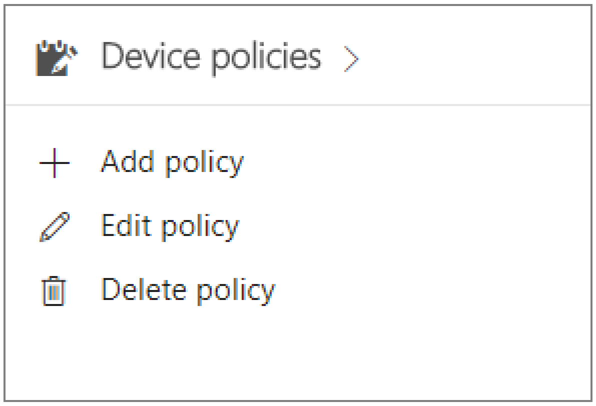
Set application protection settings for Windows 10 devices

Create an app management policy for Windows 10

If your users have personal Windows 10 devices on which they perform work tasks, you can protect your data on those devices as well.

1. Sign in to [Microsoft 365 Business]() with global admin credentials. Choose the **Admin** tile to go to the admin center.

2. On the **Device policies** card of the admin portal, choose **Add policy**.



3. On the **Add policy** pane, enter a unique name for this policy.

4. Under **Policy type**, choose **Application Management for Windows 10**.

5. Under ** Device type **, choose either **Personal** or **Company Owned**.

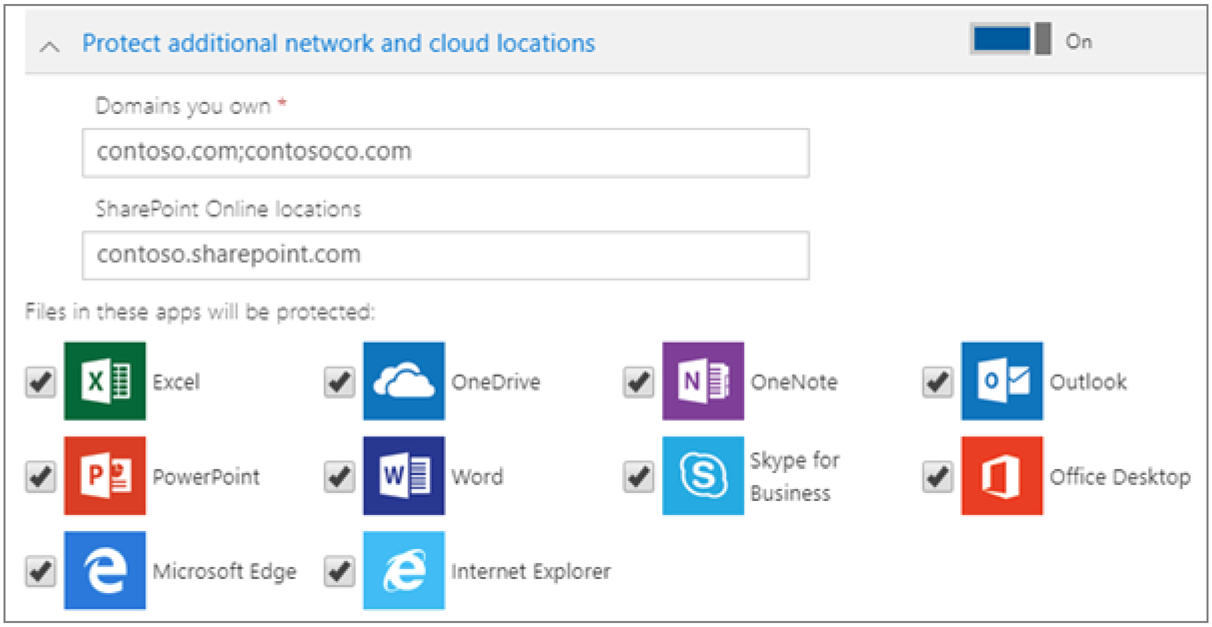
6. The **Encrypt work files** is turned on automatically.

7. Set **Prevent users from copying company data to personal files and force them to save work files to OneDrive for Business** to **On** if you don't want the users to save work files on their PC.

8. Expand **Manage how users access Office files on devices** > configure the settings how you would like. The **Manage how users access Office devices on mobile devices** is **Off** by default, but it is recommended that you turn it **On** and accept the default values. See Available settings for more information.

   You can always use the **Reset default settings** link to return to the default setting.

9. Expand **Protect additional network and cloud locations** if you want to add additional domains or SharePoint Online locations to make sure that files in all the listed apps will be protected. If you need to enter more than one item for either field, use a semicolon (;) between the items.



Protect additional network and cloud locations — On

Domains you own *

contoso.com;contosoco.com

SharePoint Online locations

contoso.sharepoint.com

Files in these apps will be protected:

☑ Excel ☑ OneDrive ☑ OneNote ☑ Outlook

☑ PowerPoint ☑ Word ☑ Skype for Business ☑ Office Desktop

☑ Microsoft Edge ☑ Internet Explorer

10. Next decide **Who will get these settings?** If you don't want to use the default **All Users** security group, choose **Change**, choose the security groups who will get these settings > **Select**.

11. Finally, choose **Add** to save the policy, and assign it to devices.

Device Configuration Profiles

Steps

Android

1. In the Azure portal, select **All Services**, and search for **Microsoft Intune**.
2. In **Microsoft Intune**, select **Device configuration**, and select **Profiles**. Then select **Create Profile**.
3. Enter the following properties:
   - **Name**: Enter a descriptive name for the new profile.
   - **Description**: Enter a description for the profile. (This is optional, but recommended.)
   - **Platform**: Select the platform type:
     - **Android**
   - **Profile type**: **Device Restrictions**
     - **General: Block Factory Reset**
     - **Password:**
       1. **Password: Require**
       2. **Minimum password length** – 8
       3. **Maximum minutes of inactivity until screen locks** - 15
       4. **Number of sign-in failures before wiping device** - 10
       5. **Password expiration (days)** - 60
       6. **Required password type**: **At least alphanumeric**
       7. **Fingerprint unlock (Samsung Knox only)** - Allows the use of a fingerprint to unlock supported devices.

Steps

8. **Encryption - Require**

- **Cellular and connectivity:**
    - **Voice dialing (Samsung KNOX only): Block**

Windows

4. In the Azure portal, select **All Services**, and search for **Microsoft Intune**.
5. In **Microsoft Intune**, select **Device configuration**, and select **Profiles**. Then select **Create Profile**.
6. Enter the following properties:

- **Name**: Enter a descriptive name for the new profile.
- **Description**: Enter a description for the profile. (This is optional, but recommended.)
- **Platform**: Select the platform type:
    - **Windows 10 and later**
- **Profile type**: **Device Restrictions**
- **General**
    - **Manual unenrollment – Block**
    - **Phone reset – Block**
    - **Device name modification – Block**
    - **Automatic redeployment - Allow**
- **Personalization**
    - **Desktop background picture URL (Desktop only)**

Integrate Windows Hello for Business with Microsoft Intune

Steps

Create a Windows Hello for Business policy

1. In the Azure portal, choose **All Services** > **Monitoring + Management** > **Intune**.
2. On the Intune pane, choose **Device enrollment**, and then choose **Windows enrollment** > **Windows Hello for Business**.
3. On the pane that opens, choose the **Default** settings.
4. On the **All Users** pane, click **Properties** and then enter a **Name** and optional **Description** for the Windows Hello for Business settings.
5. On the **All Users** pane, click **Settings** and then choose from the following options for **Configure Windows Hello for Business**: **Enabled**
    - **Use a Trusted Platform Module (TPM)**: **Required** (default). Only devices with an accessible TPM can provision Windows Hello for Business.
    - **Minimum PIN length/Maximum PIN length**: 10
        - **Lowercase letters in PIN/Uppercase letters in PIN/Special characters in PIN**: **Allowed**
    - **PIN expiration (days)**. 65
    - **Allow biometric authentication**: **Yes**.
    - **Allow phone sign-in**: **Yes**

Windows 10 Update Rings

Steps

Create and assign update rings

1. Sign in to the Azure portal.
2. Select **All services**, filter on **Intune**, and then select **Microsoft Intune**.
3. Select **Software updates** > **Windows 10 Update Rings** > **Create**.
4. Enter a name, a description (optional), and then choose **Configure**.
5. In **Settings**, enter the following information:
   - **Servicing channel**: Set the channel from which the device receives Windows updates.
   - **Microsoft product updates**: Choose to scan for app updates from Microsoft Update.
   - **Automatic update behavior**: **Auto install and restart at scheduled time**
   - **Restart checks**: Enabled by default.
6. When done, select **OK**. In **Create Update Ring**, select **Create**.

The new update ring is displayed in the list of update rings.

1. To assign the ring, in the list of update rings, select a ring, and then on the <*ring name*> tab, choose **Assignments**.
2. On the next tab, choose **Select groups to include**, and then choose the groups to which you want to assign this ring.
3. Once you are done, choose **Select** to complete the assignment.

iOS update policies

Steps

Configure the policy

1. Sign in to the Azure portal.
2. Select **All services**, filter on **Intune**, and select **Microsoft Intune**.
3. Select **Software updates** > **Update policies for iOS** > **Create**.
4. Enter a name and description for the policy.
5. Select **Settings**.

   Enter the details for when iOS devices aren't forced to install the latest updates. These settings create a restricted timeframe. You can configure the **Days** of the week, the **Time zone**, the **Start time**, the **End time**, and whether to **Delay visibility of software update (days)** to enter users. You can select a delay range of software updates from 1 to 90 days. To opt-out of setting a software update delay, enter 0. These update settings will apply only to supervised iOS devices.

6. Select **OK** to save your changes. Select **Create** to create the policy.

Change the restricted times for the policy

1. In **Software updates**, select **Update policies for iOS**.
2. Choose an existing policy > **Properties**.
3. Update the restricted time:
   a. Choose the days of the week
   b. Choose the time zone that this policy is applied
   c. Enter the start and end time for the blacklisted hours

Assign the policy to users

Existing policies are assigned to groups, users, or devices. When assigned, the policy is applied.

1. In **Software updates**, select **Update policies for iOS**.
2. Choose an existing policy > **Assignments**.

Steps

3. Select the Azure Active Directory groups, users, or devices to include or exclude from this policy.
4. Choose **Save** to deploy the policy to your groups.

Configure identity protection settings

Steps

Create a device profile with identity protection settings

1. Sign in to the Azure portal.

2. Select **All services**, filter on **Intune**, and select **Microsoft Intune**.

3. Select **Device configuration** > **Profiles** > **Create profile**.

4. Enter a **Name** and **Description** for the identity protection profile.

5. From the **Platform** drop-down list, select **Windows 10 and later**. Windows Hello for Business is only supported on devices running Windows 10 and later.

6. From the **Profile type** drop-down list, choose **Identity protection**.

7. On the Windows Hello for Business pane, choose from the following options for Configure Windows Hello for Business: **Enabled**.

- **Minimum PIN length/Maximum PIN length**. 10

- **Lowercase letters in PIN/Uppercase letters in PIN/Special characters in PIN**: **Allowed**.

- **PIN expiration (days)**. 60

- **Enable PIN recovery**: **Enable**.

- **Use a Trusted Platform Module (TPM)**: **Enable**.

- **Allow biometric authentication**: **Enable**

Steps

Click **OK** to save your profile. The profile is created and appears in the **Device configuration - Profiles** list.

iOS or macOS device feature settings

Steps

Create a device profile

1. Sign in to the Azure portal.
2. Select **All services**, filter on **Intune**, and then select **Microsoft Intune**.
3. Select **Device configuration** > **Profiles** > **Create profile**.
4. Enter the following properties:
   - **Name**: Enter a descriptive name for the new profile.
   - **Description**: Enter a description for the profile
   - **Platform**: **iOS**
   - **Profile type**: Select **Device features**.
   - **Settings**: **Home screen layout settings for iOS**

Add items to the dock

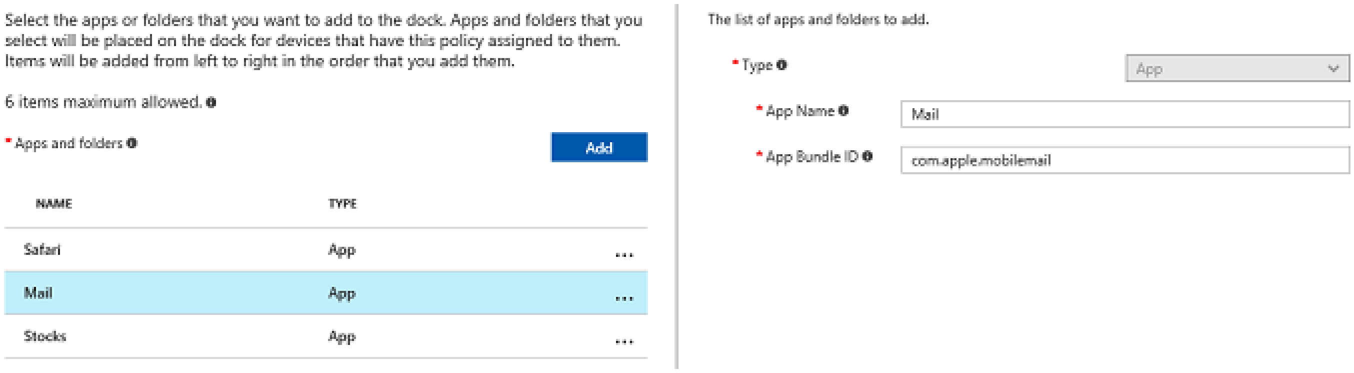
On the **Dock** pane, you can add up to six items or folders to the dock of the iOS screen. However, many devices support fewer items; for example, iPhone devices support up to four items. In this case, only the first four items you configured are displayed on the device.

1. Choose **Add** to add an item to the dock.
2. On the **Add Row** pane, choose whether you want to add an **App**, or a **Folder**.
3. Using the information in this topic, configure the apps and folders you want to appear in the dock.
4. Continue to add items. When you are finished, click **OK** on each pane until you return to the **Create Profile** pane. Choose **Create**.

Steps

Example

In this example, you've configured the dock screen to show only the Safari, Mail, and Stocks apps. In the following image, the Mail app is selected to illustrate its properties:



Select the apps or folders that you want to add to the dock. Apps and folders that you select will be placed on the dock for devices that have this policy assigned to them. Items will be added from left to right in the order that you add them.

6 items maximum allowed.

* Apps and folders

Add

NAME	TYPE	
Safari	App	...
Mail	App	...
Stocks	App	...

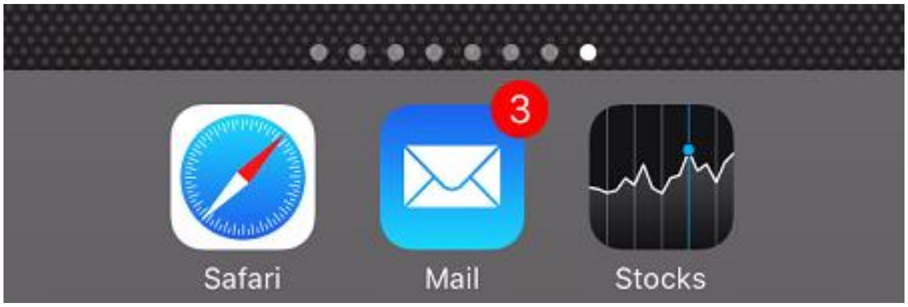
The list of apps and folders to add.

* Type: App

* App Name: Mail

* App Bundle ID: com.apple.mobilemail

When you assign the policy to an iPhone, the result is a dock that looks similar to this screenshot:



Add Home screen pages

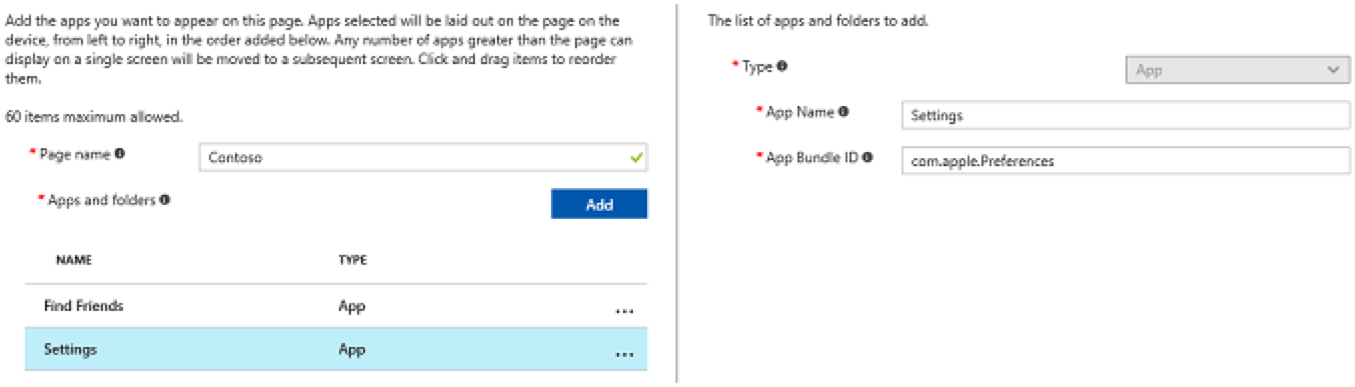
Add the pages you want to appear on the home screen, and the apps that appear on each page. Apps that you add to a page are arranged from left to right, in the order they are specified in the list. If you add more apps than can fit on a page, the apps are moved to a subsequent page.

1. On the **Pages** pane, choose **Add**.
2. On the **Add Row** pane, enter a **Page name**. This name is used for your reference in the Azure portal, and *is not displayed* on the iOS device.
3. Choose **Add**, then choose whether you want to add an **App**, or a **Folder** to the page.
4. Using the information in this topic, configure the apps and folders you want to appear on the page.

Example

Steps

In this example, you've configured a new page named **Contoso**. The page shows only the Find Friends, and Settings apps. In the following image, the Settings app is selected to illustrate its properties:



Add the apps you want to appear on this page. Apps selected will be laid out on the page on the device, from left to right, in the order added below. Any number of apps greater than the page can display on a single screen will be moved to a subsequent screen. Click and drag items to reorder them.

60 items maximum allowed.

* Page name: Contoso

* Apps and folders

NAME	TYPE	
Find Friends	App	...
Settings	App	...

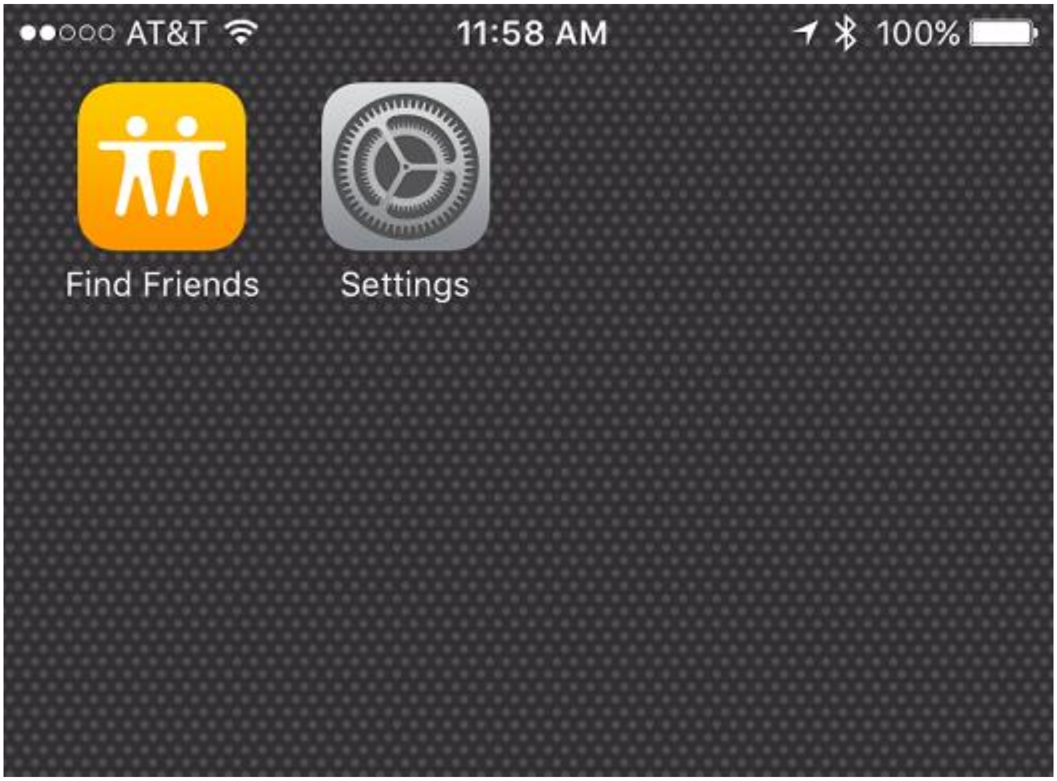
The list of apps and folders to add.

* Type: App

* App Name: Settings

* App Bundle ID: com.apple.Preferences

When you assign the policy to an iPhone, the result is a page that looks similar to this screenshot:



How to add an app to the list

1. Enter the **App Name**. This name is used for your reference in the Azure portal, and *is not displayed* on the iOS device.

Steps

2. Enter the **App Bundle ID** of the app you want to display. See **Bundle ID reference for built-in iOS apps** later in this topic for help.
3. Click **OK**, then continue to add items, up to a maximum of **6** for the device dock, and **60** for a device page.
4. When you are finished, click **OK**.

How to add a folder to the list

Apps that you add to a page in a folder are arranged from left to right, in the order they are specified in the list. If you add more apps than can fit on a page, the apps are moved to a subsequent page.

1. Enter the **Folder name**. This name is displayed to users on their device.
2. Choose **Add** to create a page in the folder. You can add up to 20 pages.
3. On the **Add Row** pane, enter a name for the page. This name is used for your reference in the Azure portal, and *is not displayed* on the iOS device.
4. Enter the **App Name**. This name is used for your reference in the Azure portal, and *is not displayed* on the iOS device.
5. Enter the **App Bundle ID** of the app you want to display. See **How to add an app to the list** for help.
6. Choose **Add**. You can add up to 60 items.
7. When you are finished, click **OK**.