

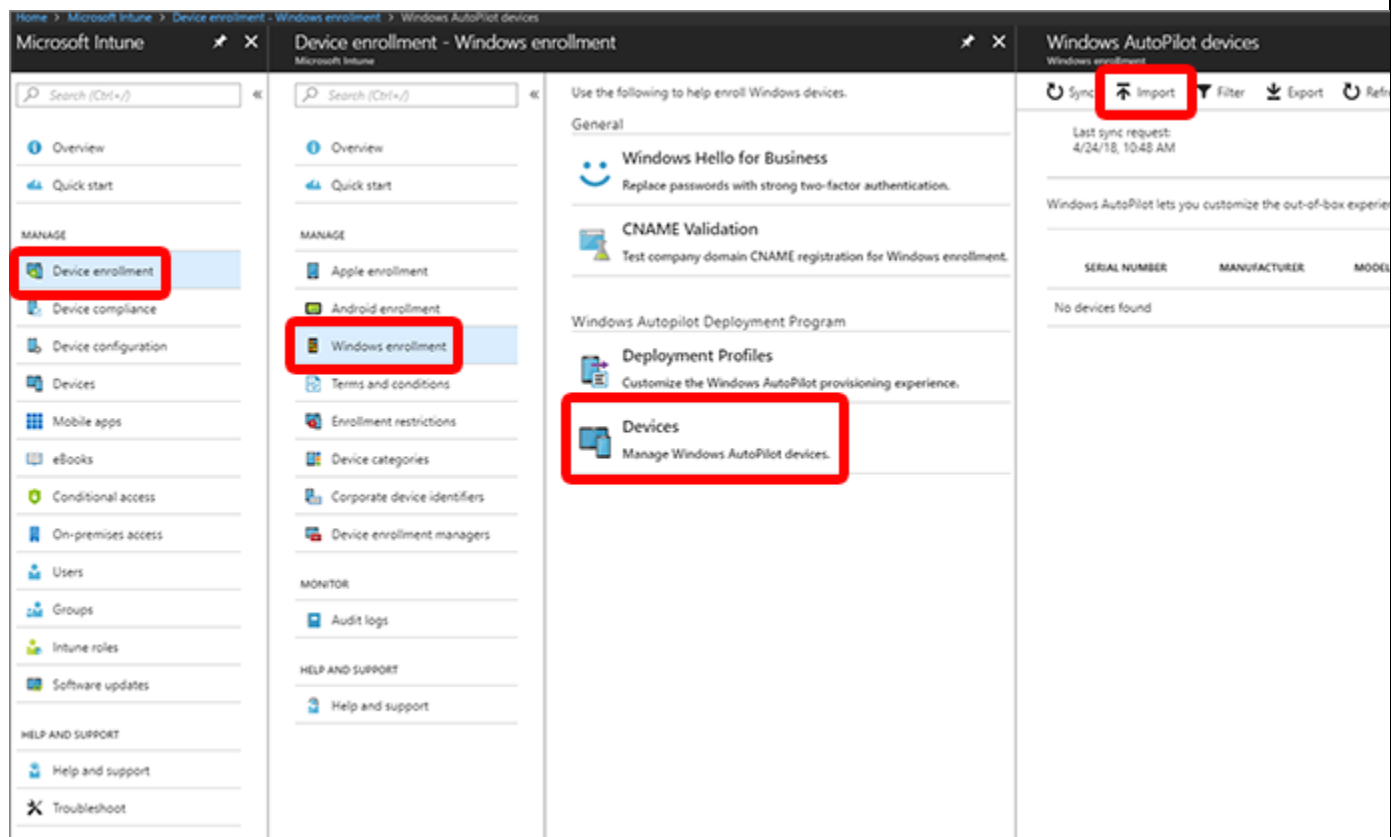
## Device Enrollment

### Steps

## Add devices

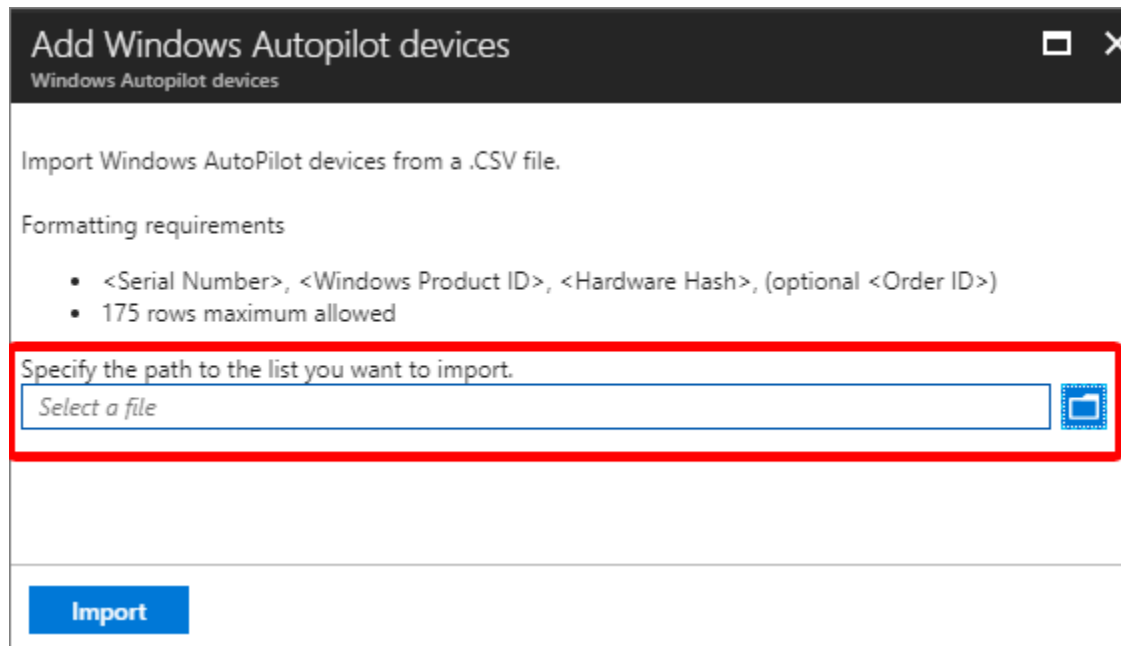
You can add Windows Autopilot devices by importing a CSV file with their information.

1. In [Intune in the Azure portal](#), choose **Device enrollment** > **Windows enrollment** > **Devices** > **Import**.



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

**Import**

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**.

## Edit an Autopilot deployment profile

After you've created an Autopilot deployment profile, you can edit certain parts of the deployment profile.

## Steps

1. In [Intune in the Azure portal](#), choose **Device enrollment**.
2. Under **Windows enrollment**, in the **Windows Autopilot** section, choose **Deployment Profiles**.
3. Select the profile you would like to edit.
4. Click **Properties** on the left to change the name or description of the deployment profile. Click **Save** after you make changes.
5. Click **Settings** to make changes to the OOB settings. Click **Save** after you make changes.

## 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**.

Windows AutoPilot devices

Windows enrollment

Sync Filter Import Export Assign user Refresh Delete

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

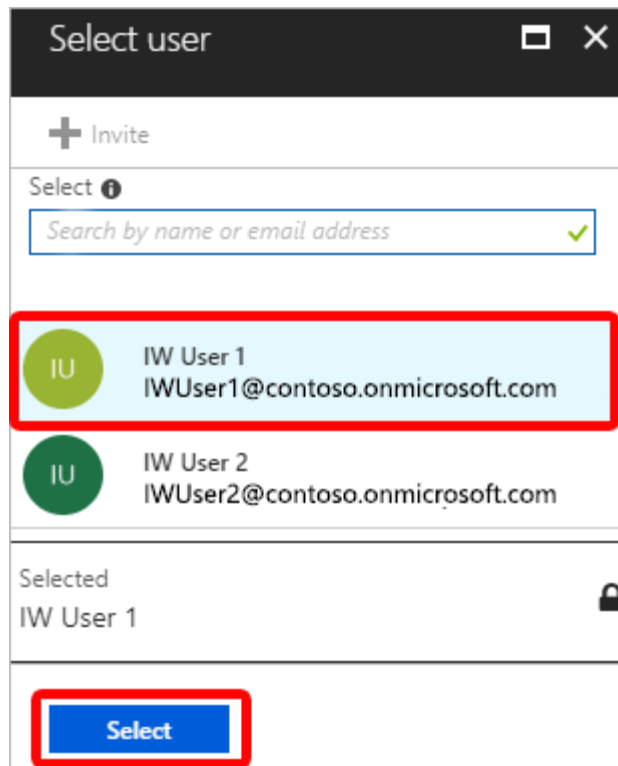
Last successful sync: 8/14/18, 2:19 PM

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

SERIAL NUMBER	MANUFACTURER	MODEL	DEPLOYMENT GROUP
<input type="checkbox"/> 1234567890	Microsoft Corporati...	Surface Book	
<input checked="" type="checkbox"/> 1234-5678-9012-34...	Microsoft Corporati...	Virtual Machine	

## Steps

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



The screenshot shows a 'Select user' dialog box. At the top, there is a search bar with the placeholder text 'Search by name or email address'. Below the search bar, two users are listed: 'IW User 1' with email 'IWUser1@contoso.onmicrosoft.com' and 'IW User 2' with email 'IWUser2@contoso.onmicrosoft.com'. The first user is highlighted with a red box. Below the list, the 'Selected' section shows 'IW User 1'. At the bottom, a blue 'Select' button is highlighted with a red box.

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 ⓘ

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

**Ok**

4. Choose **Ok**.

## Delete Autopilot devices

You can delete Windows Autopilot devices that aren't enrolled.

1. If the devices are enrolled in Intune, you must first [delete them from the Azure Active Directory portal](#).
2. In the [Intune in the Azure portal](#), choose **Device enrollment** > **Windows enrollment** > **Devices**.

## Steps

3. Under **Windows Autopilot devices**, choose the devices you want to delete, and then choose **Delete**.
4. Confirm the deletion by choosing **Yes**. It can take a few minutes to delete.

## 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.



## Steps

- **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

- **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

## Steps

- **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**.
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

## Steps

## 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**.
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

## Steps

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

### Encryption

**Require encryption on mobile device:** Require

## 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

## Steps

**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.

## 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**

## Steps

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.
  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**

## Steps

- **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.