

# Device Configuration

---

## 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.
      8. **Encryption - Require**
  - **Cellular and connectivity:**
    - **Voice dialing (Samsung KNOX only): Block**

## Windows

---

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:
    - **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)**

### 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**

## 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.

## 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**

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

# iOS

---

## Configure iOS Updates 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.

## 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**.
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.

## Create a device feature 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 to add an **App**
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**.

## 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 to add an **App**.
4. Using the information in this topic, configure the apps and folders you want to appear on the page.

## Example

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 Add

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:

