Mobile Application Management

Assign Office 365 apps to Windows 10 devices with Microsoft Intune

1. Sign in to the Azure portal.
2. Select **All Services** > **Intune**. Intune is located in the **Monitoring + Management** section.
3. In the **Intune** pane, select **Client apps**.
4. In the **Client apps** workload pane, under **Manage**, select **Apps**.
5. Select **Add**.
6. In the **Add apps** pane, in the **App type** list, under **Office 365 Suite**, select **Windows 10**.
7. In the **Add App** pane, select **Configure App Suite**.
8. In the **Configure App Suite** pane, select the standard Office apps that you want to assign to devices.
   Additionally, you can install apps for the Microsoft Project Online desktop client and Microsoft Visio Pro for Office 365, if you own licenses for them.
9. Select **OK**.

Configure app information

1. In the **Add App** pane, select **App Suite Information**.
2. In the **App Suite Information** pane, do the following:
   - **Suite Name**: Enter the name of the app suite as it is displayed in the company portal. Make sure that all suite names that you use are unique. If the same app suite name exists twice, only one of the apps is displayed to users in the company portal.
   - **Suite Description**: Enter a description for the app suite. For example, you could list the apps you've selected to include.
   - **Publisher**: Microsoft appears as the publisher.
   - **Category**: Optionally, select one or more of the built-in app categories or a category that you created. This setting makes it easier for users to find the app suite when they browse the company portal.
   - **Display this as a featured app in the Company Portal**: Select this option to display the app suite prominently on the main page of the company portal when users browse for apps.
   - **Information URL**: Optionally, enter the URL of a website that contains information about this app. The URL is displayed to users in the company portal.
   - **Privacy URL**: Optionally, enter the URL of a website that contains privacy information for this app. The URL is displayed to users in the company portal.
   - **Developer**: Microsoft appears as the developer.

- **Owner**: Microsoft appears as the owner.
- **Notes**: Enter any notes that you want to associate with this app.
- **Logo**: The Office 365 logo is displayed with the app when users browse the company portal.
3. Select **OK**.

Configure app settings

In this step, configure installation options for the app suite. The settings apply to all apps that you added to the suite.

1. In the **Add App** pane, select **App Suite Settings**.
2. In the **App Suite Settings** pane, do the following:

- **Office version**: Choose whether you want to assign the 32-bit or 64-bit version of Office. You can install the 32-bit version on both 32-bit and 64-bit devices, but you can install the 64-bit version on 64-bit devices only.

- **Update Channel**: Choose how Office is updated on devices. For information about the various update channels, see Overview of update channels for Office 365 ProPlus. Choose **Semi-Annual.**

- After you choose a channel, you can optionally select **Specific** to install a specific version of Office for the selected channel on end user devices. Then, select the **Specific version** of Office to use.

- **Remove MSI from end-user devices** - Choose whether you want to remove pre-existing Office .MSI apps from end-user devices. The installation won't succeed if there are pre-existing .MSI apps on end-user devices. The apps to be uninstalled are not limited to the apps selected for installation in **Configure App Suite**, as it will remove all Office (MSI) apps from the end user device.

- **Automatically accept the app end user license agreement**: Select this option if you don't require end users to accept the license agreement. Intune then automatically accepts the agreement.

- **Use shared computer activation**: Select this option when multiple users share a computer.

- **Languages**: Office is automatically installed in any of the supported languages that are installed with Windows on the end-user's device. Select this option if you want to install additional languages with the app suite.

You can deploy additional languages for Office 365 Pro Plus apps managed through Intune. The list of available languages includes the **Type** of language pack (core, partial, and proofing). In the Azure portal, select **Microsoft Intune** > **Client apps** > **Apps** > **Add**. In the **App type** list of the **Add app** blade, select **Windows 10** under **Office 365 Suite**. Select **Languages** in the **App Suite Settings** blade.

When you're done, in the **Add App** pane, select **Add**. The app you've created is displayed in the apps list.

Add built-in apps to Microsoft Intune

Add a built-in app

To add a built-in app to your available apps in Microsoft Intune, do the following:

1. Sign in to the Azure portal.
2. To display the Microsoft Intune pane, select **More Services** > **Monitoring + Management** > **Intune**.
3. In the **Intune** pane, select **Client apps**.
4. In the **Client apps** pane, under **Manage**, select **Apps**.
5. Select **Add**.
6. In the **Add** app pane, in the **App type** list, select **Built-In app**.
7. Select **Select app**.
8. In the **Built-In app** pane, select the apps that you want to include.
9. In the **Add app** pane, select **Add**.

Configure app information

You can modify information about the built-in app. This information helps you to identify the app in Intune and helps users find the app in the company portal.

1. In the **Client apps - Apps** pane, select the built-in app that you want to modify.
   A pane for the built-in app is displayed.
2. Under **Manage**, select the **Properties** option.
3. To modify the built-in app information, select the **Configure** option.
4. In the **App information** pane, you can modify the following information:
   - **Name**: Enter the name of the built-in app as it is displayed in the company portal. Make sure all names that you use are unique. If the same app name exists twice, only one of the apps is displayed to users in the company portal.
   - **Description**: Enter a description for the app.
   - **Publisher**: Enter the name of the publisher of the app.
   - **Category**: Optionally, select one or more of the built-in app categories. Setting this option makes it easier for users to find the app when they browse the company portal.
   - **Display this as a featured app in the company portal**: Display the app prominently on the main page of the company portal when users browse for apps.
   - **Information URL**: Optionally, enter the URL of a website that contains information about this app. The URL is displayed to users in the company portal.
   - **Privacy URL**: Optionally, enter the URL of a website that contains privacy information for this app. The URL is displayed to users in the company portal.
   - **Developer**: Optionally, enter the name of the app developer.
   - **Owner**: Optionally, enter a name for the owner of this app (for example, *HR department*).

- **Notes**: Enter any notes that you want to associate with this app.
- **Upload Icon**: Upload an icon that is displayed with the app when users browse the company portal.

5. Select **OK**.
6. In the **Properties** pane, select **Save**.

Selectively wipe apps

Create a wipe request

1. Sign in to the [Azure portal](#).

2. Choose **All services**, type **Intune** in the filter textbox, and select **Intune**. The Intune pane opens, choose the **Client apps** pane.

3. On the **Client apps pane**, choose **App selective wipe**.

4. Choose **New wipe request**. The **New wipe request** pane opens.

5. Choose a user and then choose **Select** to select the user whose app data you want to wipe.

6. Next, choose **Device** from the **New wipe request** pane. This opens the **Select Device** pane that lists all the devices associated with the selected user, and also provides two columns, the device name, which is a friendly name defined by the user, and the device type, its device platform. Select the device you want to wipe.

7. You are now back on the **New wipe request** pane. Choose **OK** to make a wipe request.

The service creates and tracks a separate wipe request for each protected app on the device, and the user associated with the wipe request.

App protection policies

Create an app protection policy

1. In Intune portal, go to **Client apps** > **App protection policies**. This selection opens the **App protection policies** details, where you create new policies and edit existing policies.

2. Select **Create Policy**.

3. Specify a name for the policy, add a brief description, and select the platform type for your policy. You can create more than one policy for each platform.

4. Select **Apps** to open the **Apps** blade, where a list of available apps is displayed. Select one or more apps from the list that you want to associate with the policy that you're creating. Select at least one app to create a policy.

5. Once you've selected the apps, choose **Select** to save your selection.

6. On the **Add a policy** blade, select **Configure required settings** to open **Settings**.

    There are three categories of policy settings:

    - **Data relocation** - This group includes the data loss prevention (DLP) controls, like cut, copy, paste, and save-as restrictions. These settings determine how users interact with data in the apps.
    - **Access requirements** - This group contains the per-app PIN options that determine how the end user accesses the apps in a work context.
    - **Conditional launch** - This group holds settings like the minimum OS settings, jailbreak and rooted device detection, and offline grace periods.

    To get you started, the policy settings have default values. If the default values meet your requirements, you don't have to make any changes.
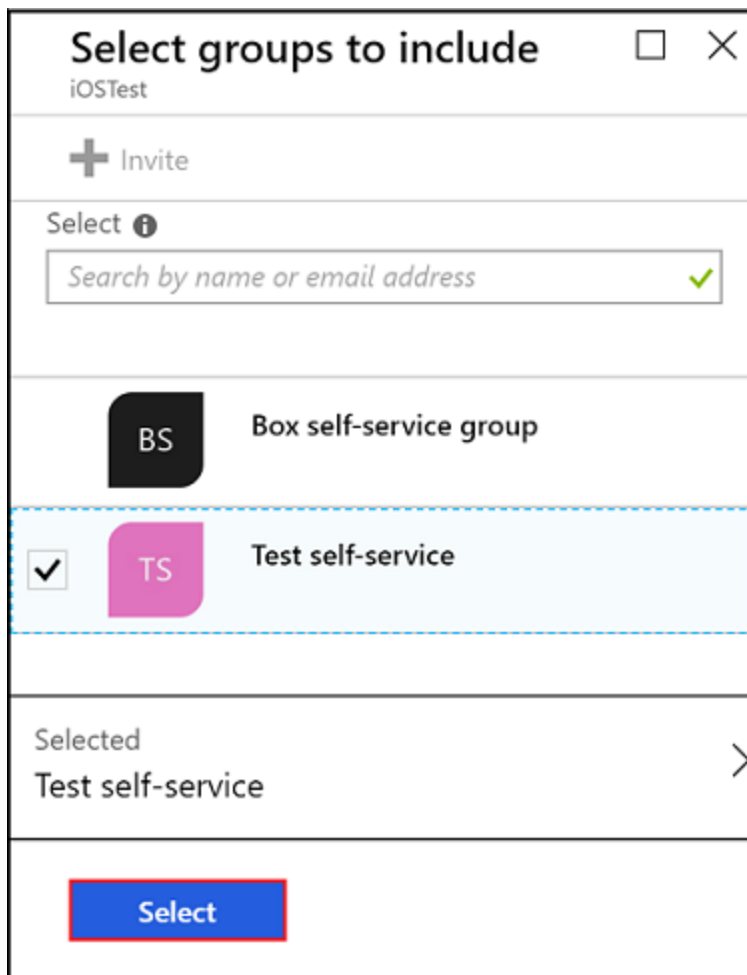
7. Select **OK** to save this configuration. You're now back in the **Add a policy** blade.

8. Select **Create** to create the policy and save your settings.

Deploy a policy to users

1. In the **App protection policies** pane, select a policy.

2. In the ***Intune App Protection** pane, select **Assignments** to open the **Intune App Protection - Assignments** pane. On the *Include* tab, select **Select groups to include**.
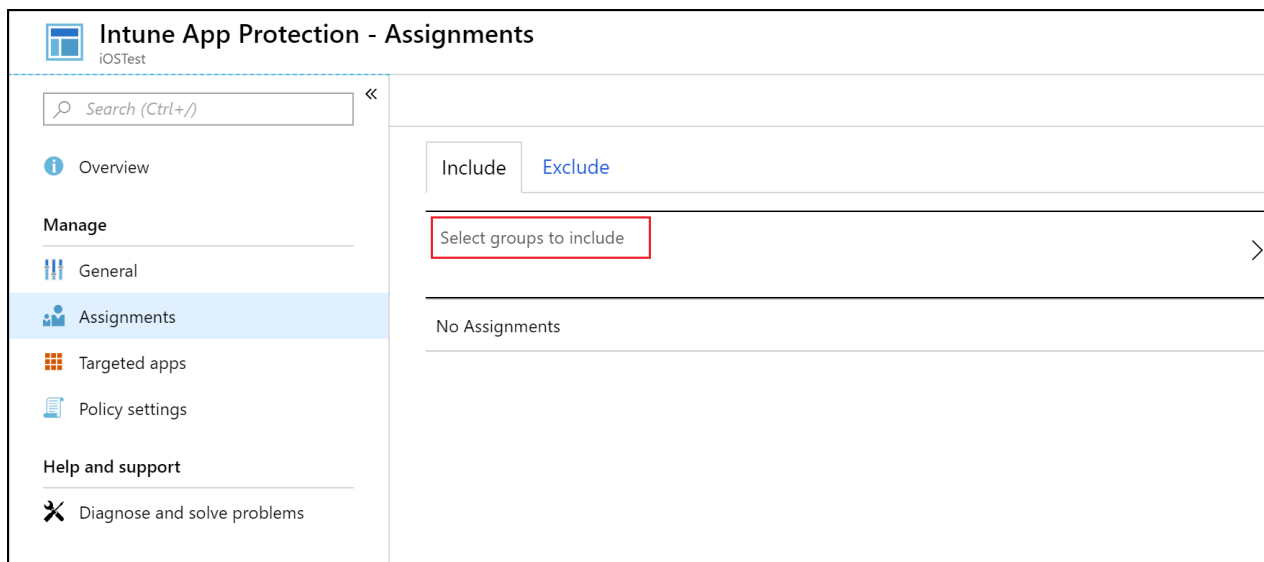
3. A list of all the security groups in your **Azure Active Directory** is displayed. Select the user groups that you want this policy to apply to, and then choose **Select**. Choosing **Select**, deploys the policy to users.

Target app protection policies based on device management state

Browse to **Client apps** > **App protection policies** in the Intune console, and then select **Create Policy**. You can also edit an existing app protection policy.

To have the app protection policy apply to both managed and un-managed devices, confirm that **Target to all app types** is set to **Yes**, the default value.

If you want to granularly assign base on management state, set **Target to all app types** to **No**.

Add a policy   □   ✕

* Name

iOSAllApps   ✓

Description

Platform

iOS   ⌄

Target to all app types ⓘ

Yes   No

Apps
Select required apps   ❯

Settings
Configure required settings   ❯

Create

Create and deploy Windows Information Protection (WIP) app protection policy

To add a WIP app protection policy

1. Choose **All Services** > **Intune**.
2. Select **Client apps** on the **Microsoft Intune** blade.
3. Select **App protection policies** on the **Client apps** blade.
4. Select **Add a policy** to display the **Add a policy** blade.
5. Add the following values:
    - **Name:** Type a name (required) for your new policy.
    - **Description:** (Optional) Type a description.
    - **Platform:** Choose **Windows 10** as the supported platform for your app protection policy.
    - **Enrollment state:** Choose **Without enrollment** as the enrollment state for your policy.
6. Choose **Create**. The policy is created and appears in the table on the **App protection policies** blade.

To add recommended apps to your protected apps list

1. Select **Client apps** on the **Microsoft Intune** blade.
2. Select **App protection policies** on the **Client apps** blade.
3. On the **App protection policies** blade, choose the policy you want to modify. The **Intune App Protection** blade is displayed.
4. Choose **Protected apps** from the **Intune App Protection** blade. The **Protected apps** blade opens showing you all apps that are already included in the list for this app protection policy.
5. Select **Add apps**. The **Add apps** information shows you a filtered list of apps. The list at the top of the blade allows you to change the list filter.
6. Select each app that you want to allow access your corporate data.
7. Click **OK**. The **Protected apps** blade is updated showing all selected apps.
8. Click **Save**.

Add a Store app to your protected apps list

1. Select **Client apps** on the **Microsoft Intune** blade.
2. Select **App protection policies** on the **Client apps** blade.
3. On the **App protection policies** blade, choose the policy you want to modify. The **Intune App Protection** blade is displayed.
4. Choose **Protected apps** from the **Intune App Protection** blade. The **Protected apps** blade opens showing you all apps that are already included in the list for this app protection policy.

5. Select **Add apps**. The **Add apps** information shows you a filtered list of apps. The list at the top of the blade allows you to change the list filter.
6. From the list, select **Store apps**.
7. Enter values for **Name**, **Publisher**, **Product Name**, and **Action**. Be sure to set the **Action** value to **Allow**, so that the app will have access to your corporate data.
8. Click **OK**. The **Protected apps** blade is updated showing all selected apps.
9. Click **Save**.

Add a desktop app to your protected apps list

1. Select **Client apps** on the **Microsoft Intune** blade.
2. Select **App protection policies** on the **Client apps** blade.
3. On the **App protection policies** blade, choose the policy you want to modify. The **Intune App Protection** blade is displayed.
4. Choose **Protected apps** from the **Intune App Protection** blade. The **Protected apps** blade opens showing you all apps that are already included in the list for this app protection policy.
5. Select **Add apps**. The **Add apps** information shows you a filtered list of apps. The list at the top of the blade allows you to change the list filter.
6. From the list, select **Desktop apps**.
7. Enter values for **Name**, **Publisher**, **Product Name**, **File**, **Min Version**, **Max Version**, and **Action**. Be sure to set the **Action** value to **Allow**, so that the app will have access to your corporate data.
8. Click **OK**. The **Protected apps** blade is updated showing all selected apps.
9. Click **Save**.

Deploy your WIP app protection policy

After you created your WIP app protection policy, you need to deploy it to your organization using MAM.

1. On the **App policy** blade, choose your newly created app protection policy, choose **User groups** > **Add user group**.

    A list of user groups, made up of all the security groups in your Azure Active Directory, opens in the **Add user group** blade.

2. Choose the group you want your policy to apply to, then choose **Select** to deploy the policy.