

Introduction to Mobile Device Management for Office 365

What is Mobile Device Management (MDM) for Office 365?

Mobile Device Management (MDM) for Office 365 helps secure and manage mobile devices like iPhones, iPads, Android phones, and Android tablets. The State of Delaware uses MDM for Office 365 to protect access to State of Delaware assets.

Why use MDM for Office 365?

Enrolling mobile devices in MDM helps protect the State's network and data while giving you the freedom to use your mobile device and Outlook apps. The Microsoft Outlook mobile app is now the required and supported mobile app to connect to your State of Delaware Exchange Online mailbox. (See Outlook Mobile App User Setup Guides iOS/Android on the website) You *must* enroll your mobile device(s) with MDM for Office 365 if you access your State of Delaware email-mailbox from a mobile device using Outlook mobile app.

The State of Delaware will be using the Microsoft Intune Company Portal app for mobile device enrollment into MDM for Office 365. Enrolling in MDM will require you to use a password or PIN on your mobile device. (To begin the enrollment process, see "Install MDM for your Mobile Device" on page 2 of this document.)

Privacy Concerns

Enrolling your personal device in MDM does not mean your private information is viewable by IT Administrators. Your private information remains for your eyes only.

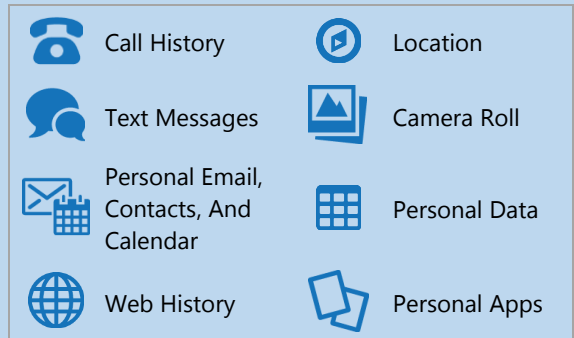
IT Administrators can **ONLY** perform the following security measures on a mobile device enrolled with MDM:

- Remotely reset the PIN or lock your phone if it is lost or stolen
- Selectively wipe company-related apps and data, without removing your personal apps and data
- Reset your phone to factory settings if it is lost or stolen

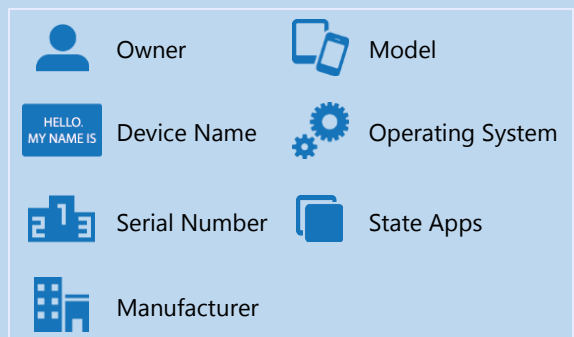
(Note: See MDM Policy vs Exchange Active Sync Comparison table on page 3.)

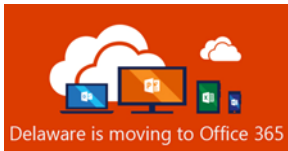
We care about your privacy

IT Administrators **cannot** see this information on your phone or tablet:



IT Administrators **can** see this information on your phone or tablet:



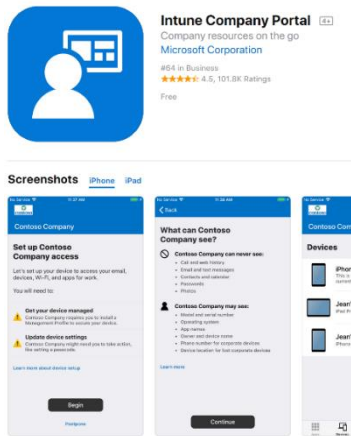


Install MDM for your Mobile Device

Install the Intune Company Portal app and enroll your device.

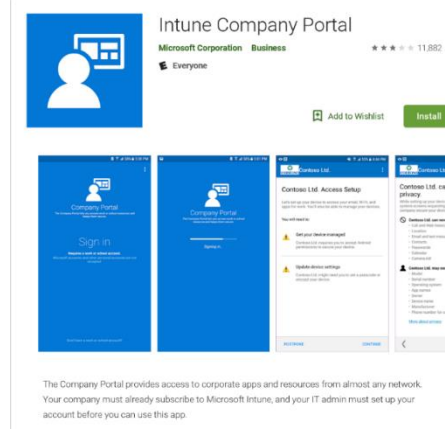
Download for iOS (Requires iOS 10.0 or later)


Open the App Store and search for "Intune Company Portal" app




Download for Android (Requires Android KitKat 4.4 or later)

Open the Play Store and search for "Intune Company Portal" app



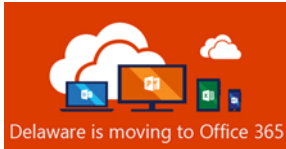
- 
1. Press **Home** → **App Store**
 2. **Search** → in the **Search** box, type **company portal** → **Microsoft Intune Company Portal**
 3. **GET** → **INSTALL**
 4. Press **Home** → **Comp Portal**
 5. Sign in to work → **Accept**
 6. **Begin** → **Continue** → **Continue** → **Enroll**
 7. **Install** → enter your passcode → **Install** → **Install** → **Trust** → **Done**
 8. **Open** → **Continue** → **Done**

- 
1. Press **Home** → **Play Store**
 2. **Search** → in the **Search** box, type **company portal** → **Intune Company Portal**
 3. **INSTALL**
 4. Press **Home** → **Company Portal**
 5. **Sign in** → sign in to work → **Accept**
 6. **Begin** → **Continue** → **Continue** → **Enroll**
 7. **Allow** → **Activate** → Select the Terms and Conditions Check Box → **Confirm**
 8. **Continue** → **Done**

Note The Android and iOS warnings you see simply verify that you want to enroll your device.

Additional Device Enrollment Instructions:
[iOS device enrollment instructions](#)

Additional Device Enrollment Instructions:
[Android device enrollment instructions](#)



MDM Policies vs. Exchange ActiveSync (EAS) Comparison Table

If you have been connecting to your on-premises Exchange mailbox using a mobile mail app, such as the native iOS/Android mail app, your mobile device has had an Exchange ActiveSync (EAS) policy applied to it. The EAS mobile policy is a set of security configurations, such as requiring a numeric passcode, which is applied to a collection of devices, typically defined by the type of mobile device (iOS and Android).

To be fully transparent, we have listed a comparison table so you can see the EAS policy settings we currently apply vs. new policy settings we will apply through MDM for Office 365. Additionally, MDM policies going forward allow us to standardize device inconsistencies that exist under old EAS.

	EAS Android	EAS iPhone		MDM Android	MDM iPhone
Password Required	Yes	Yes		Yes	Yes
Allow Simple Password	Yes	Yes		No	No
Alphanumeric Password Required	No	No		No	No
Minimum Password Length	4 digits	4 digits		4 digits	4 digits
Password Expiration	Never Expires	120 Days		120 Days	120 Days
Password History Remembered	None	1 Password		1 Password	1 Password
Max Password Failed Attempts	Unlimited	7		7	7
Require Encryption	No	No ¹		Yes	No ¹
Prevent Jail Broken Devices	Unavailable ²	Unavailable ²		Yes	Yes
¹ iOS is encrypted by default. ² Exchange ActiveSync policies are unable to prevent Jail Broken devices from connecting to mailboxes.					

Password Required: This setting enables the mobile device password

Allow Simple Password: This setting enables/disables the ability to use a simple password such as 1111 or 1234

Alphanumeric Password Required: This setting requires that a password contain numeric and non-numeric characters.

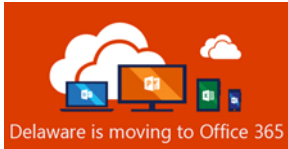
Minimum Password Length: This setting specifies the minimum number of characters in the mobile device password.

Password Expiration: The setting requires that the mobile password must be changed after a determined length of time.

Password History Remembered: This setting specifies the number of past passwords that are stored. A user cannot reuse a stored password.

Max Password Failed Attempts: This setting specifies the number of failed password attempts a user can make for the mobile device, before the mobile device is wiped.

Require Encryption: This setting specifies whether mobile device encryption is required.



Prevent Jail Broken Devices: This setting specifies whether jail broken or rooted mobile devices can connect to Office 365 resources, such as your cloud mailbox. A jail broken or rooted mobile device is the process of removing all restrictions imposed by the mobile device's operating system. It gives the user access to manipulate system settings that typically are not available to the end-user and not supported by the vendor.

Additional Resources

[iOS Enrollment Video](#)

[Android Enrollment Video](#)