Introducing 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. You must enroll your mobile device(s) with MDM for Office 365 if you access your State email through a mobile email application (not OWA).

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” found on the Office 365 website.)

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

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

We care about your privacy
IT Administrators cannot see this information on your phone or tablet:

- Call History
- Text Messages
- Personal Email, Contacts, And Calendar
- Web History

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

- Location
- Camera Roll
- Personal Data
- Personal Apps

- Owner
- Model
- Device Name
- Operating System
- Serial Number
- State Apps
- Manufacturer
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>EAS Android</th>
<th>EAS iPhone</th>
<th>MDM Android</th>
<th>MDM iPhone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Required</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow Simple Password</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Alphanumeric Password Required</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>4 digits</td>
<td>4 digits</td>
<td>4 digits</td>
<td>4 digits</td>
</tr>
<tr>
<td>Password Expiration</td>
<td>Never Expires</td>
<td>120 Days</td>
<td>120 Days</td>
<td>120 Days</td>
</tr>
<tr>
<td>Password History Remembered</td>
<td>None</td>
<td>1 Password</td>
<td>1 Password</td>
<td>1 Password</td>
</tr>
<tr>
<td>Max Password Failed Attempts</td>
<td>Unlimited</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Require Encryption</td>
<td>No</td>
<td>No¹</td>
<td>Yes</td>
<td>No¹</td>
</tr>
<tr>
<td>Prevent Jail Broken Devices</td>
<td>Unavailable²</td>
<td>Unavailable²</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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.