Mobile device mailbox policies in Exchange 2016

**Exchange 2016**

Overview of mobile device mailbox policies

You can use mobile device mailbox policies to manage many different settings. These include the following:

* Require a password
* Specify the minimum password length
* Allow a numeric PIN or require special characters in the password
* Designate how long a device can be inactive before requiring the user to re-enter a password
* Wipe a device after a specific number of failed password attempts

|  |  |
| --- | --- |
| **Setting** | **Description** |
| Allow Bluetooth | This setting specifies whether a mobile device allows Bluetooth connections. The available options are Disable, HandsFree Only, and Allow. The default value is Allow. |
| Allow Browser | This setting specifies whether Pocket Internet Explorer is allowed on the mobile device. This setting doesn't affect third-party browsers installed on the mobile device. The default value is $true. |
| Allow Camera | This setting specifies whether the mobile device camera can be used. The default value is $true. |
| Allow Consumer EMail | This setting specifies whether the mobile device user can configure a personal email account (either POP3 or IMAP4) on the mobile device. The default value is $true. This setting doesn’t control access to email accounts that are using third-party mobile device email programs. |
| Allow Desktop Sync | This setting specifies whether the mobile device can synchronize with a computer through a cable, Bluetooth, or IrDA connection. The default value is $true. |
| Allow External Device Management | This setting specifies whether an external device management program is allowed to manage the mobile device. |
| Allow HTML Email | This setting specifies whether email synchronized to the mobile device can be in HTML format. If this setting is set to $false, all email is converted to plain text. |
| Allow Internet Sharing | This setting specifies whether the mobile device can be used as a modem for a desktop or a portable computer. The default value is $true. |
| AllowIrDA | This setting specifies whether infrared connections are allowed to and from the mobile device. |
| Allow Mobile OTA Update | This setting specifies whether the mobile device mailbox policy settings can be sent to the mobile device over a cellular data connection. The default value is $true. |
| Allow non-provisionable devices | This setting specifies whether mobile devices that may not support application of all policy settings are allowed to connect to Office 365 by using Exchange ActiveSync. Allowing non-provisionable mobile devices has security implications. For example, some non-provisionable devices may not be able to implement an organization’s password requirements. |
| Allow POPIMAPEmail | This setting specifies whether the user can configure a POP3 or an IMAP4 email account on the mobile device. The default value is $true. This setting doesn’t control access by third-party email programs. |
| Allow Remote Desktop | This setting specifies whether the mobile device can initiate a remote desktop connection. The default value is $true. |
| Allow simple password | This setting enables or disables the ability to use a simple password such as 1111 or 1234. The default value is $true. |
| Allow S/MIME encryption algorithm negotiation | This setting specifies whether the messaging application on the mobile device can negotiate the encryption algorithm if a recipient’s certificate doesn’t support the specified encryption algorithm. |
| Allow S/MIME software certificates | This setting specifies whether S/MIME software certificates are allowed on the mobile device. |
| Allow storage card | This setting specifies whether the mobile device can access information that's stored on a storage card. |
| Allow text messaging | This setting specifies whether text messaging is allowed from the mobile device. The default value is $true. |
| Allow unsigned applications | This setting specifies whether unsigned applications can be installed on the mobile device. The default value is $true. |
| Allow unsigned installation packages | This setting specifies whether an unsigned installation package can be run on the mobile device. The default value is $true. |
| Allow Wi-Fi | This setting specifies whether wireless Internet access is allowed on the mobile device. The default value is $true. |
| Alphanumeric password required | This setting requires that a password contains numeric and non-numeric characters. The default value is $true. |
| Approved Application List | This setting stores a list of approved applications that can be run on the mobile device. |
| Attachments enabled | This setting enables attachments to be downloaded to the mobile device. The default value is $true. |
| Device encryption enabled | This setting enables encryption on the mobile device. Not all mobile devices can enforce encryption. For more information, see the device and mobile operating system documentation. |
| Device policy refresh interval | This setting specifies how often the mobile device mailbox policy is sent from the server to the mobile device. |
| IRM enabled | This setting specifies whether Information Rights Management (IRM) is enabled on the mobile device. |
| Max attachment size | This setting controls the maximum size of attachments that can be downloaded to the mobile device. The default value is Unlimited. |
| Max calendar age filter | This setting specifies the maximum range of calendar days that can be synchronized to the mobile device. The following values are accepted:1. All
2. OneDay
3. ThreeDays
4. OneWeek
5. TwoWeeks
6. OneMonth
 |
| Max email age filter | This setting specifies the maximum number of days of email items to synchronize to the mobile device. The following values are accepted:1. All
2. OneDay
3. ThreeDays
4. OneWeek
5. TwoWeeks
6. OneMonth
 |
| Max email body truncation size | This setting specifies the maximum size at which email messages are truncated when synchronized to the mobile device. The value is in kilobytes (KB). |
| Max email HTML body truncation size | This setting specifies the maximum size at which HTML email messages are truncated when synchronized to the mobile device. The value is in kilobytes (KB). |
| Max inactivity time lock | This value specifies the length of time that the mobile device can be inactive before a password is required to reactivate it. You can enter any interval between 30 seconds and 1 hour. The default value is 15 minutes. |
| Max password failed attempts | This setting specifies the number of attempts a user can make to enter the correct password for the mobile device. You can enter any number from 4 through 16. The default value is 8. |
| Min password complex characters | This setting specifies the minimum number of complex characters required in the mobile device’s password. A complex character is a character that is not a letter. |
| Min password length | This setting specifies the minimum number of characters in the mobile device password. You can enter any number from 1 through 16. The default value is 4. |
| Password enabled | This setting enables the mobile device password. |
| Password expiration | This setting enables the administrator to configure a length of time after which a mobile device password must be changed. |
| Password history | This setting specifies the number of past passwords that can be stored in a user's mailbox. A user can't reuse a stored password. |
| Password recovery enabled | When this setting is enabled, the mobile device generates a recovery password that's sent to the server. If the user forgets their mobile device password, the recovery password can be used to unlock the mobile device and enable the user to create a new mobile device password. |
| Require device encryption | This setting specifies whether device encryption is required. If set to $true, the mobile device must be able to support and implement encryption to synchronize with the server. |
| Require encrypted S/MIME messages | This setting specifies whether S/MIME messages must be encrypted. The default value is $false. |
| Require encryption S/MIME algorithm | This setting specifies what required algorithm must be used when encrypting S/MIME messages. |
| Require manual synchronization while roaming | This setting specifies whether the mobile device must synchronize manually while roaming. Allowing automatic synchronization while roaming will frequently lead to larger-than-expected data costs for the mobile device data plan. |
| Require signed S/MIME algorithm | This setting specifies what required algorithm must be used when signing a message. |
| Require signed S/MIME messages | This setting specifies whether the mobile device must send signed S/MIME messages. |
| Require storage card encryption | This setting specifies whether the storage card must be encrypted. Not all mobile device operating systems support storage card encryption. For more information, see your mobile device and mobile operating system documentation. |
| Unapproved InROM application list | This setting specifies a list of applications that cannot be run in ROM. |