

# ESET Tech Center

Kennisbank > Legacy > ESET Security Management Center > Mobile Device Management > Manage mobile devices using ESET Remote Administrator—FAQ (6.x)

---

## Manage mobile devices using ESET Remote Administrator—FAQ (6.x)

Ondersteuning | ESET Nederland - 2025-03-07 - Reacties (0) - Mobile Device Management

<https://support.eset.com/kb5773>

### Issue

---

Manage Android and Apple iOS mobile devices using ESET Remote Administrator

### Solution

---

#### 1. What device-types are supported?

You can manage the following mobile devices from ESET Remote Administrator:

**Android mobile devices running ESET Endpoint Security for Android version 2.x** can be managed using ESET Remote Administrator version 6.x and later. [Click here to read the ESET Endpoint Security for Android FAQ.](#)

**Mobile devices running Apple iOS 8 and later** can be managed using ESET Remote Administrator version 6.3 and later (this includes iPhones and iPads). However, given the nature of the Apple iOS operating system, remote management of these devices is limited and only recommended for company-managed devices. [Click here for more information.](#)

#### 2. How do I manage Android devices?

Prerequisites:

To manage Android mobile devices from ESET Remote Administrator, ESET Endpoint Security for Android must be purchased and installed on the device(s), and ESET Mobile Device Connector must be installed on the server. Use the following links to complete this process:

- [Purchase a license](#)
- [Instructions to install ESET Mobile Device Connector](#)
- [Instructions to install and manage ESET Endpoint Security for Android](#)

### 3. **How do I manage iOS devices?**

#### **Prerequisites:**

ESET Remote Administrator 6.3 or later

ESET Mobile Device Connector

Apple iTunes ID

Valid ESET license

Apple iOS device (iPhone or iPad) running iOS 8 or later

Using **ESET Mobile Device Management for Apple iOS**, you can enroll iOS mobile devices in ESET Remote Administrator 6.3 and set up a security profile for each device (or group of devices), all by using the standard Apple iOS MDM framework (for which you need a valid Apple ID). [Click here for instructions to enroll and manage Apple iOS devices.](#)

### 4. **I am running ERA 6.2—can I install the standalone ESET Mobile Device Connector?**

Yes, you can install the standalone ESET Mobile Device Connector; however, you must upgrade to ERA 6.3 to manage iOS devices from ERA.

### 5. **What Apple iOS settings can be managed from ESET Remote Administrator?**

Passcode	Description	Default Setting
Allow simple value	Simple values are ascending, descending or repeating character sequences	Enabled

<b>Require passcode</b>	Requires that a passcode be set and used to gain access to the device	Disabled
<b>Require alphanumeric value</b>	Requires passcodes to include at least one letter	Disabled
<b>Minimum passcode length</b>	Minimum number of passcode characters allowed	5
<b>Minimum number of complex characters</b>	Minimum number of non-alphanumeric characters allowed	1
<b>Maximum passcode age (1-730 days, or none)</b>	Days after which passcode must be changed	90
<b>Maximum Auto-Lock in minute(s)</b>	Device automatically locks after minutes elapse	1
<b>Passcode history (1-50 passcodes, or none)</b>	Number of unique passcodes before reuse	3
<b>Maximum grace period for device lock</b>	Maximum amount of time device can be locked without prompting for passcode on unlock	1 minute
<b>Maximum number of failed attempts</b>	Number of passcode entry attempts allowed before all data on device will be erased	6
<b>Restrictions—Device Functionality</b>		
<b>Allow installing apps</b>	—	Enabled
<b>Allow use of camera</b>	—	Enabled
<b>Allow FaceTime</b>	—	Enabled
<b>Allow Siri</b>	—	Enabled
<b>Allow Siri while device locked</b>	—	Enabled
<b>Allow Passbook notifications in Lock screen</b>	—	Enabled
<b>Show Control Center in Lock screen</b>	—	Enabled
<b>Show Notification Center in Lock screen</b>	—	Enabled
<b>Show Today view in Lock screen</b>	—	Enabled
<b>Allow voice dialing while device is locked</b>	—	Enabled
<b>Allow Handoff</b>	—	Enabled
<b>Allow screenshots and screen recording</b>	—	Enabled
<b>Allow in-app purchase</b>	—	Enabled

<b>Require iTunes Store password for all purchases</b>	—	Disabled
<b>Restrictions—iCloud</b>		
<b>Allow backup</b>	—	Enabled
<b>Allow backup of enterprise books</b>	—	Enabled
<b>Allow iCloud documents and data sync</b>	—	Enabled
<b>Allow iCloud keychain</b>	—	Enabled
<b>Allow managed apps to store data in iCloud</b>	—	Enabled
<b>Allow notes and highlights sync for enterprise books</b>	—	Enabled
<b>Allow iCloud photo sharing</b>	—	Enabled
<b>Allow iCloud photo library</b>	—	Enabled
<b>Allow My Photo Stream (disallowing can cause data loss)</b>	—	Enabled
<b>Allow automatic sync while roaming</b>	—	Enabled
<b>Restrictions—Security and Privacy</b>		
<b>Allow diagnostic data to be sent to Apple</b>	—	Enabled
<b>Allow user to accept untrusted TLS certificates</b>	—	Enabled
<b>Force encrypted backups</b>	—	Disabled
<b>Force limited ad tracking</b>	—	Disabled
<b>Allow automatic updates to certificate trust settings</b>	—	Enabled
<b>Allow documents from managed sources in unmanaged destinations</b>	—	Enabled
<b>Allow documents from unmanaged sources in managed destinations</b>	—	Enabled
<b>Require passcode on first AirPlay pairing</b>	—	Disabled
<b>Allow Touch ID to unlock device</b>	—	Enabled
<b>Treat AirDrop as unmanaged destination</b>	—	Disabled
<b>Restrictions—Applications</b>		
<b>Allow use of Safari</b>	—	Enabled
<b>Enable AutoFill</b>	—	Enabled
<b>Force fraud warning</b>	—	Disabled
<b>Enable JavaScript</b>	—	Enabled

<b>Block pop-ups</b>	—	Disabled
<b>Accept cookies</b>	Controls when Safari accepts cookies	<b>Always</b> selected by default
<b>Allow playback of explicit music, podcasts &amp; iTunes U media</b>	—	Enabled
<b>Allow explicit sexual content in iBooks Store</b>	—	Enabled
<b>Other</b>		
<b>Certificate list</b>	—	Set manually by user
<b>AirPrint printers</b>	—	Set manually by user
<b>Access Point Name (APN) settings</b>	—	Set manually by user
<b>Wi-Fi connections list</b>	—	Set manually by user
<b>VPN connections list</b>	—	Set manually by user
<b>Mail Accounts</b>	—	Set manually by user
<b>Exchange ActiveSync Accounts</b>	—	Set manually by user
<b>Contacts Accounts</b>	—	Set manually by user
<b>LDAP Accounts</b>	—	Set manually by user
<b>Calendar Accounts</b>	—	Set manually by user
<b>Subscribed Calendar Accounts</b>	—	Set manually by user

## 6. What are the advantages of ESET Mobile Device Management for Apple iOS?

- Ability to manage security of iOS devices from ESET Remote Administrator 6
- Manage key security aspects of iOS: passcode settings, autolock time, device restrictions for camera usage, settings for iCloud usage
- Anti-theft: remotely wipe all device data if a device is lost or stolen (including emails, contacts)
- Ability to push Exchange account, Wi-Fi account, VPN settings and other related settings in batches to iOS devices

- [Enrollment with Apple DEP.](#)

7. **How is ESET Mobile Device Management for Apple iOS licensed?**

Each device running ESET Mobile Device Management for Apple iOS will consume a seat. You can use your ESET Endpoint Security for Android license to manage iOS devices from ESET Remote Administrator 6.3 and later.

8. **How often do mobile devices check in with ESET Mobile Device Connector?**

By default, ESET Mobile Device Connector proactively pings devices to retrieve information. Otherwise, the connection is made according to need. For example, when updated policies or tasks are sent from ESET Remote Administrator. ESET Endpoint Security for Android connects to ESET Mobile Device Connector according to need, such as when virus definitions are updated or changes in protection status are distributed. In addition, some periodic logs are sent to ESET Mobile Device Connector on a daily basis.

iOS devices only connect to ERA once every 12 hours, unless a policy change or mobile task has been made from ERA. When no change is requested, an iOS device will not report its status.

9. **Will the existing policy settings remain on the device after the owner deletes the profile?**

Most of the settings (passcode and device settings, for example) will remain disabled; applications that were restricted will reappear on the device and be functional again.

10. **If an admin enforces the passcode setting, what happens if the end user does not input a passcode?**

When the passcode setting has been enforced by the admin, the end user will have sixty minutes to input a passcode. After sixty minutes, the end user will not be able to use the device until a passcode has been set.

11. **If a restriction is set on the device, what happens on the**

**device?**

The app or feature will not be available on the device. For example, if you disable “allow installing application,” the App Store app will be removed from the device.

Tags

ERA 6.x

MDM