ESET Tech Center

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

Ondersteuning | ESET Nederland - 2017-11-24 - 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 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

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

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

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