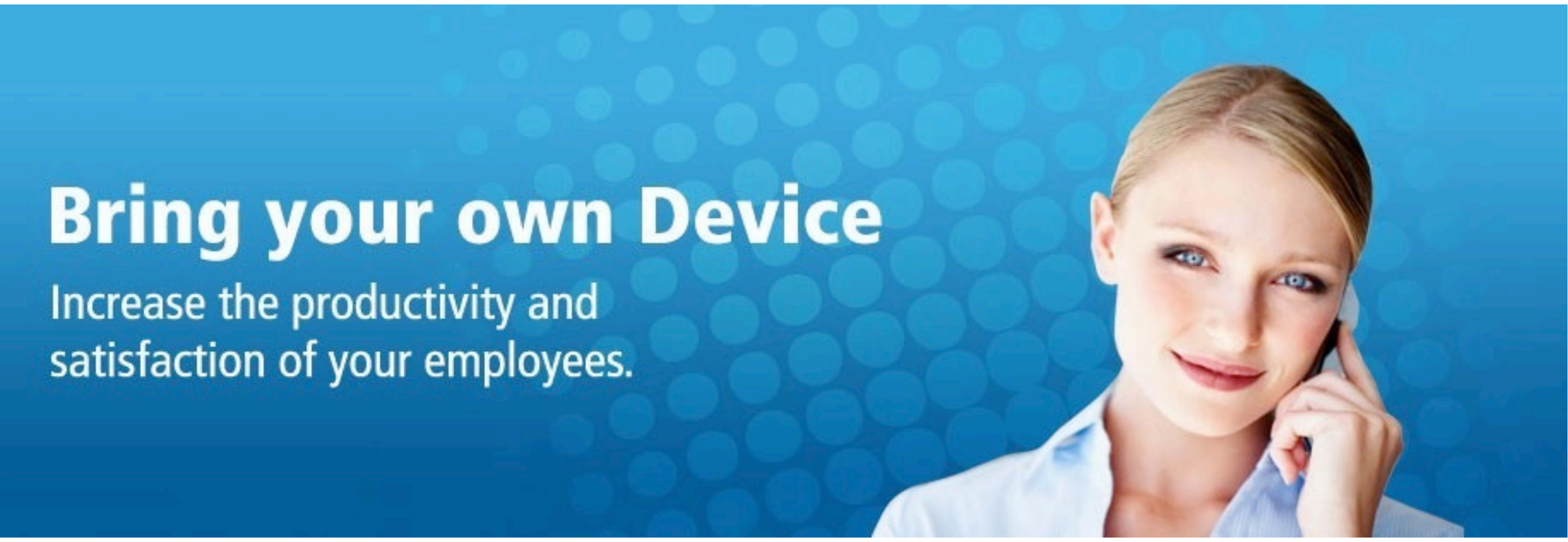
APPTEC360
Enterprise Mobility Management

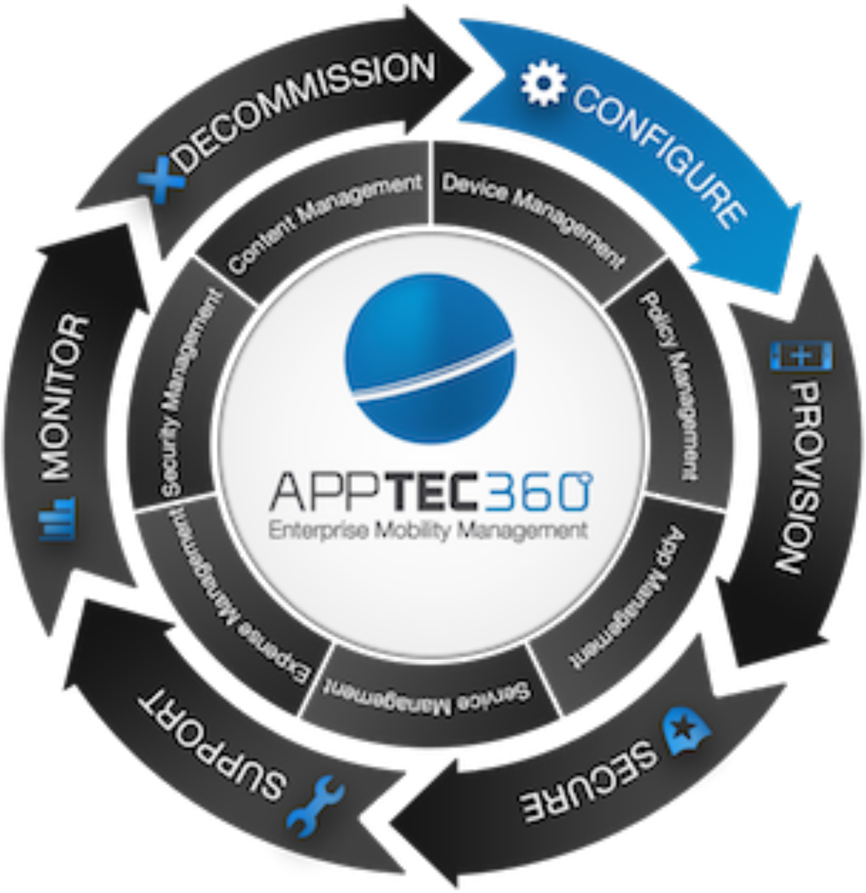
Frequently Asked Questions

„Enterprise Mobile Manager“


Bring your own Device
Increase the productivity and
satisfaction of your employees.

www.apptec360.com

Contents


CONFIGURE
PROVISION
SECURE
SUPPORT
MONITOR
DECOMMISSION
Device Management
Policy Management
App Management
Service Management
Expense Management
Security Management
Content Management
APPTEC360
Enterprise Mobility Management

Unable to connect the device to EMM Server

Symptoms

When a device is connected to Wi-Fi and has no cellular data connection, push notifications are not received.

Resolution

Apple

Devices using APNs need a direct connection to Apple's server. If a device is unable to connect using cellular data, it will attempt to use Wi-Fi where available. If there is a proxy server on the Wi-Fi network, the device will not be able to use APNs, because APNs require a direct and persistent connection from device to server.

For APNs traffic to pass through a firewall, the following ports need to be open:

- TCP port 5223 (used by devices to communicate to the APNs servers)
- TCP port 2195 (used to send notifications to the APNs)
- TCP port 2196 (used by the APNs feedback service)
- TCP Port 443 (used as a fallback on Wi-Fi only, when devices are unable to communicate to APNs on port 5223)

The APNs servers use load balancing. iOS devices will not always connect to the same public IP address for notifications. The entire 17.0.0.0/8 address block is assigned to Apple, so the best way is to allow this range in the firewall settings.

Google Android

The ports to open are: 5228, 5229, and 5230. Generally Google Cloud Messaging uses port 5228 only, but sometimes it uses 5229 and 5230, too. GCM doesn't provide specific IPs, so you have to allow connections to all IP addresses contained in the IP blocks listed in Google's ASN of 15169.

AppTec EMM

The ports to open are: 443, 8080 and 8081. Port 80 is optional for redirecting http traffic to the console to https.

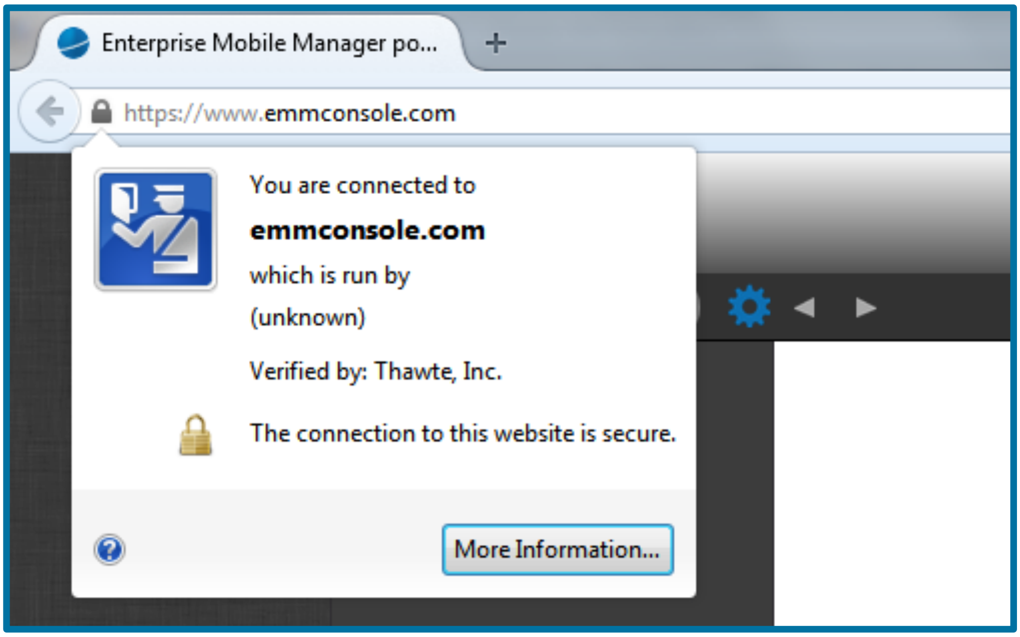
Unable to import AD into EMM Server in the Cloud

Resolution

The import of Active Directory into the EMM Server works only in the Virtual Appliance within the local environment. Generally, security settings don´t allow a connection to Active Directory from outside of a firewall.

How to extract the Intermediate Certificate from Firefox

1. Open the Web-interface of your EMM in Firefox.
2. Click on the little Lock on the left side of the URL bar.



You are connected to

emmconsole.com

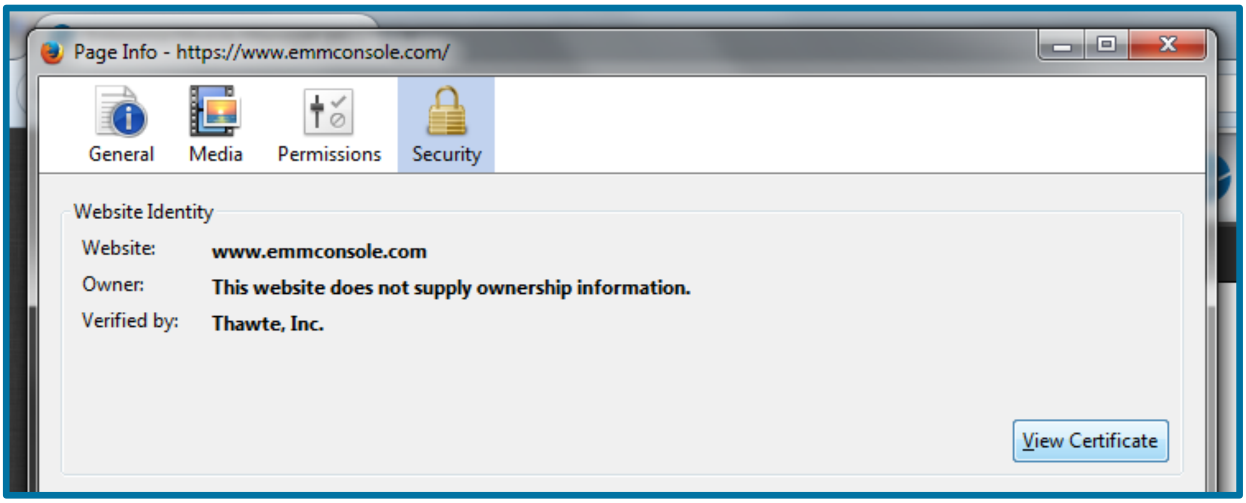
which is run by

(unknown)

Verified by: Thawte, Inc.

The connection to this website is secure.

3. In the Popup click on "More Information".
4. In the window that opens up choose the Security tab and click on "View Certificate".



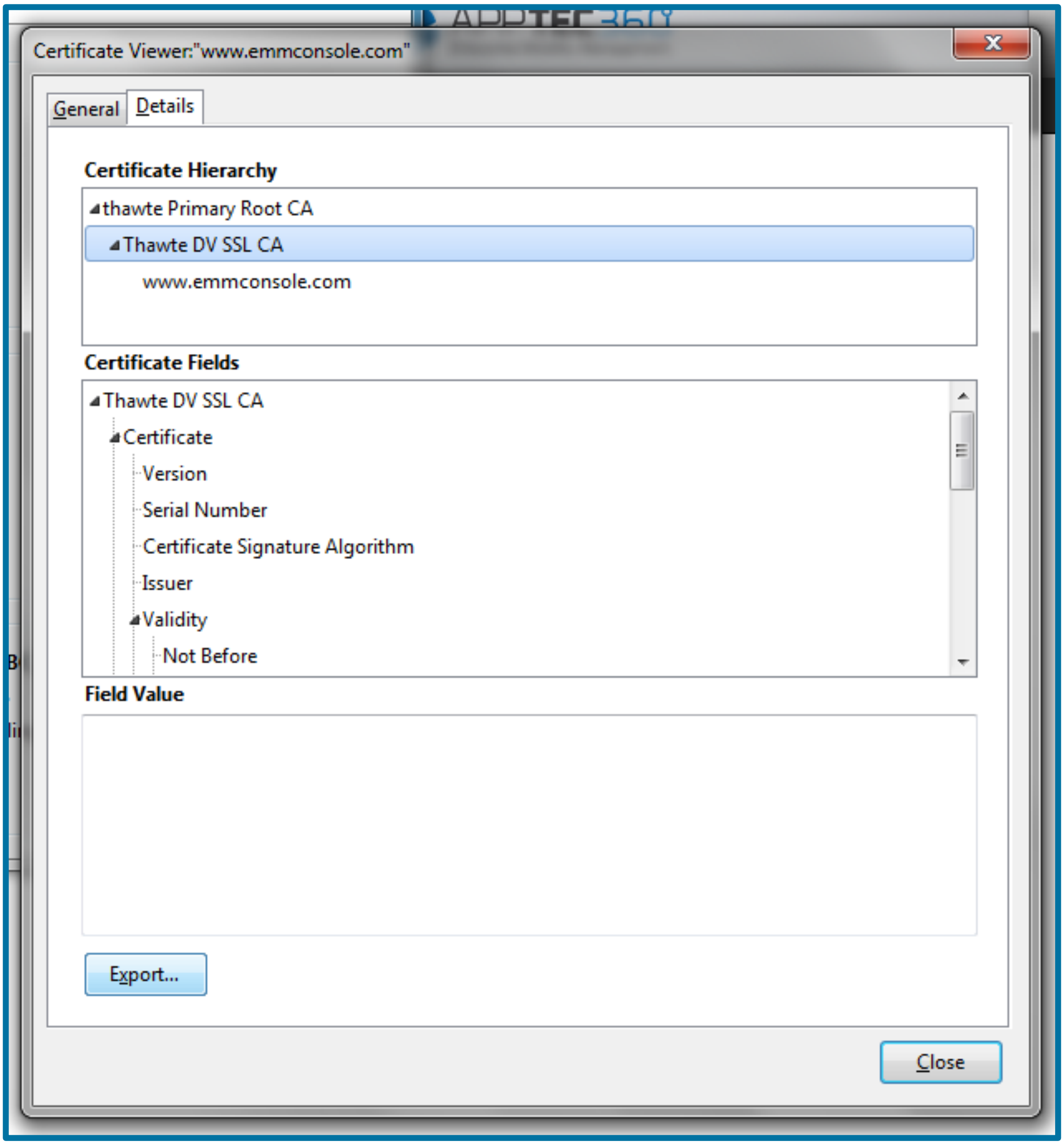
Website Identity

Website: www.emmconsole.com

Owner: This website does not supply ownership information.

Verified by: Thawte, Inc.

5. In the next window switch to the "Details" tab.



Certificate Viewer:"www.emmconsole.com"

Certificate Hierarchy

- thawte Primary Root CA
  - Thawte DV SSL CA
    - www.emmconsole.com

Certificate Fields

- Thawte DV SSL CA
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

Field Value

6. In the section "Certificate Hierarchy", select the certificate between the certificate of the appliance and the Root CA.

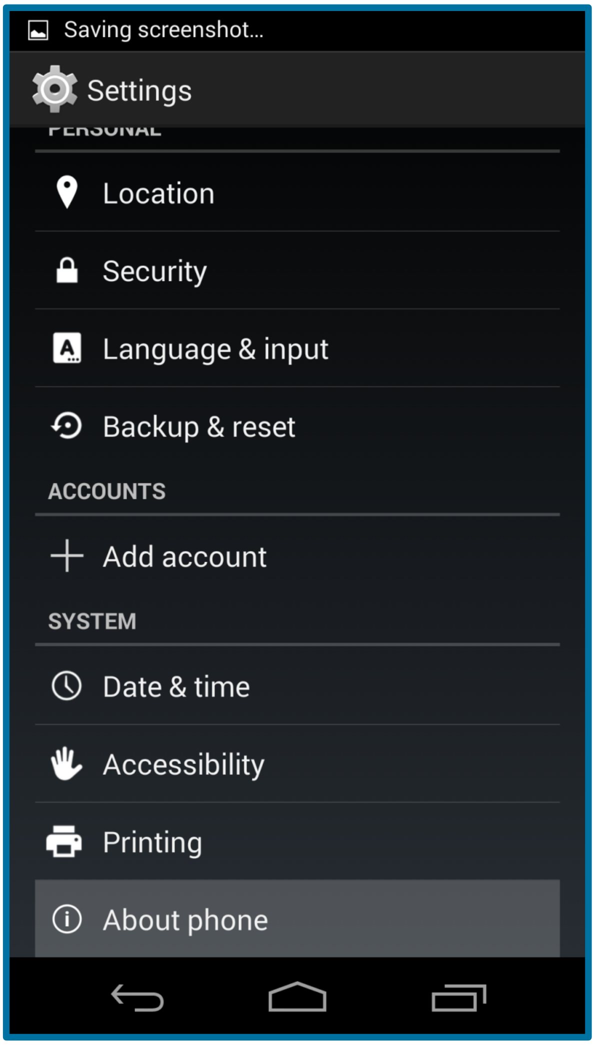
7. Click on "Export" on the bottom left and save the file.

How to copy the device log from Android devices

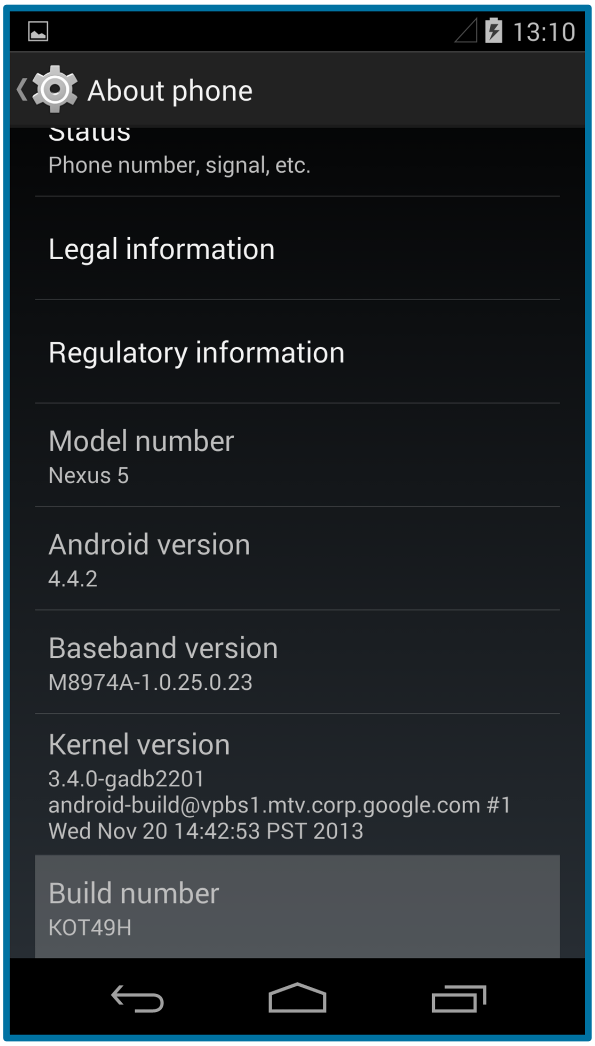
Note: Some menus on your device might look different from the screenshots (Google Nexus 5).

1. Extract the Folders "platform-tools" and "usb_driver" from the zip file.
   (e.g. drag and drop to the desktop).

2. Enable USB-Debugging
   a. Enable "Developer options".
      i. Go to "Settings" > "About phone".



ii. Scroll down to "Build number".



Status
Phone number, signal, etc.

Legal information

Regulatory information

Model number
Nexus 5

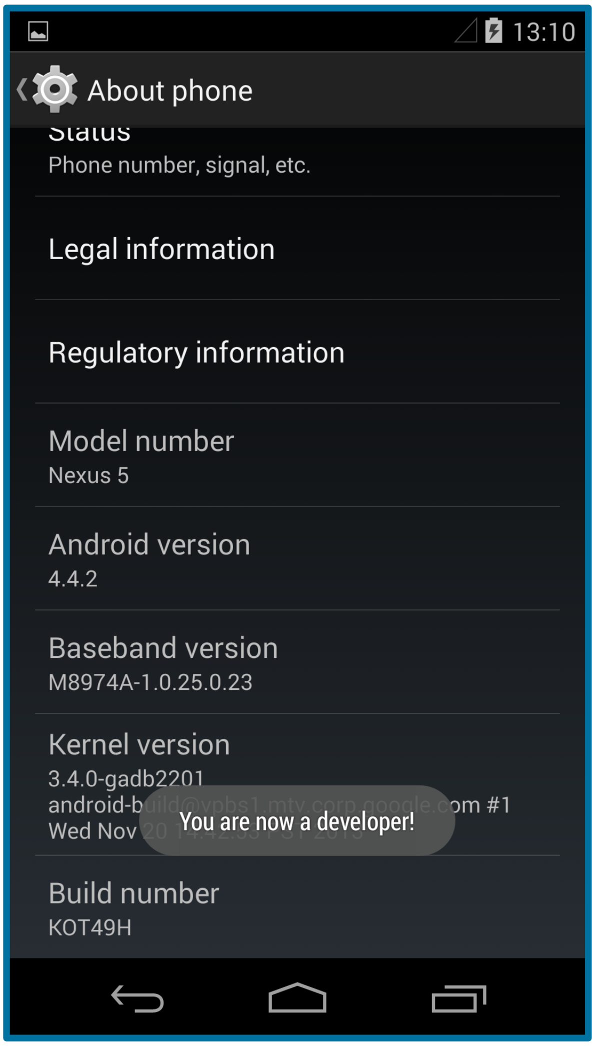
Android version
4.4.2

Baseband version
M8974A-1.0.25.0.23

Kernel version
3.4.0-gadb2201
android-build@vpbs1.mtv.corp.google.com #1
Wed Nov 20 14:42:53 PST 2013

Build number
KOT49H

iii. Press the entry multiple times, until you get a message telling you that you are a developer now.



Status
Phone number, signal, etc.

Legal information

Regulatory information

Model number
Nexus 5

Android version
4.4.2

Baseband version
M8974A-1.0.25.0.23

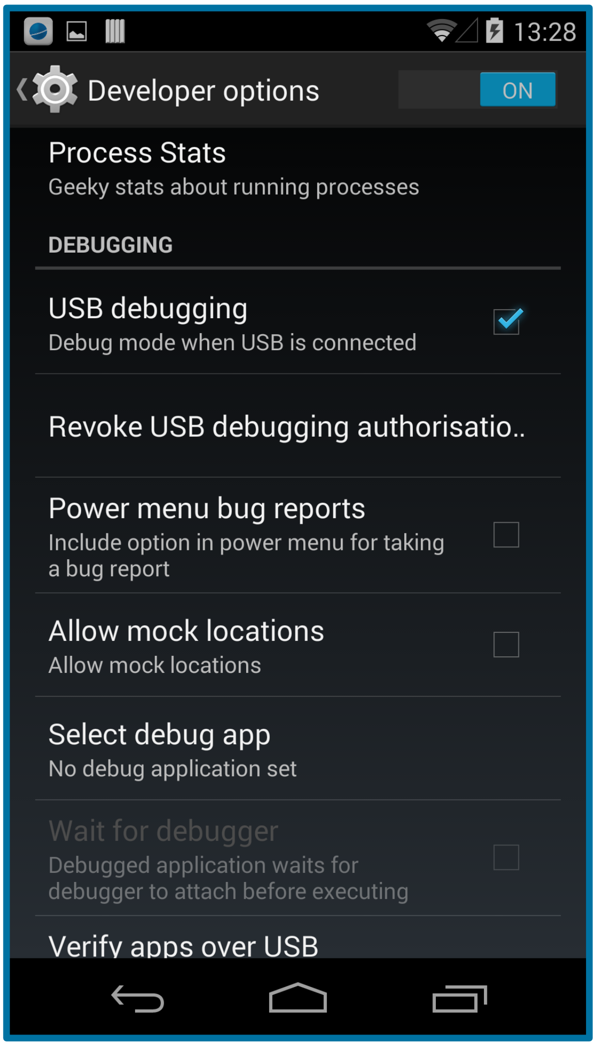
Kernel version
3.4.0-gadb2201
android-build@vpbs1.mtv.corp.google.com #1
Wed Nov 20 14:42:53 PST 2013

You are now a developer!

Build number
KOT49H

b. Go to "Settings" > "Developer options".

c. Enable "USB debugging".



13:28

Developer options ON

Process Stats
Geeky stats about running processes

DEBUGGING

USB debugging ☑
Debug mode when USB is connected

Revoke USB debugging authorisatio..

Power menu bug reports ☐
Include option in power menu for taking a bug report

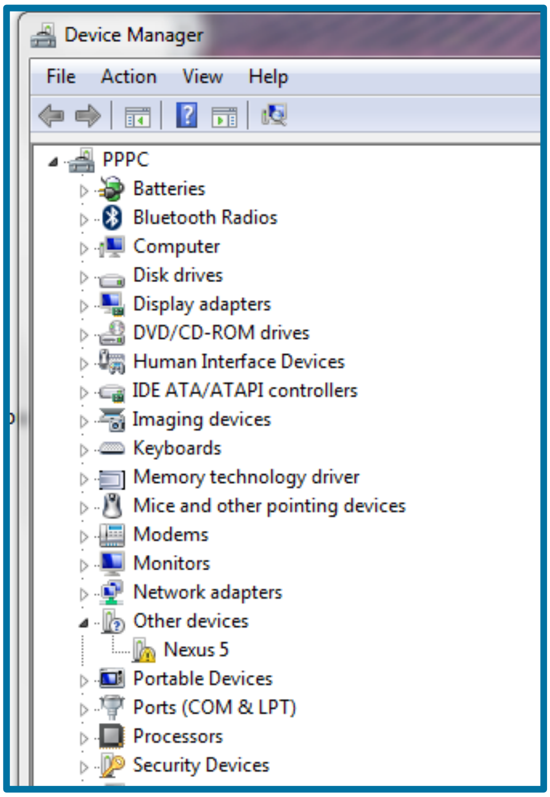
Allow mock locations ☐
Allow mock locations

Select debug app
No debug application set

Wait for debugger ☐
Debugged application waits for debugger to attach before executing

Verify apps over USB

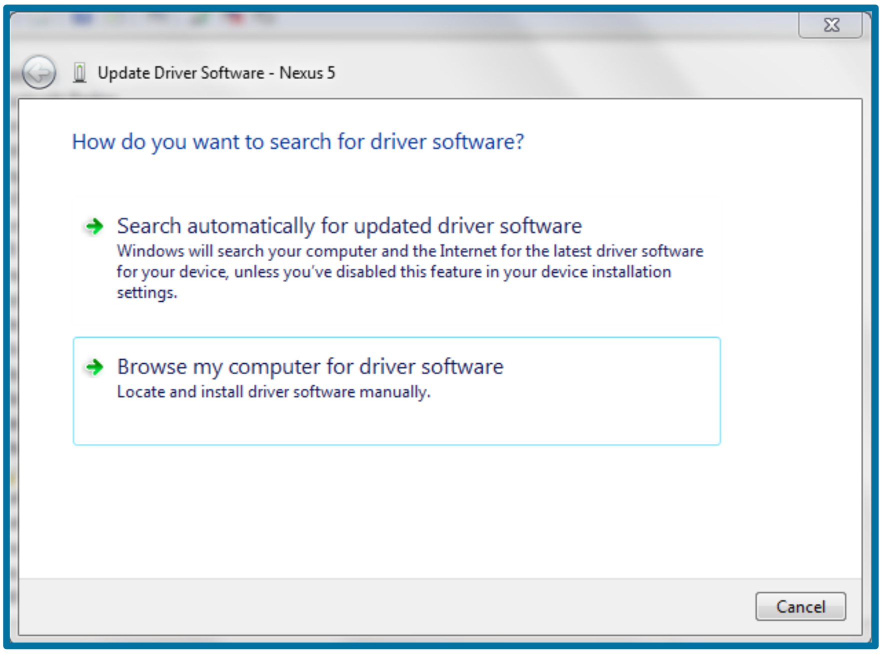
3. Make sure the device is unlocked while doing each step from now.
4. Connect the device to a computer.
5. Open the device manager.
6. If not already installed. Install the USB driver for your device.



- PPPC
  - Batteries
  - Bluetooth Radios
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Imaging devices
  - Keyboards
  - Memory technology driver
  - Mice and other pointing devices
  - Modems
  - Monitors
  - Network adapters
  - Other devices
    - Nexus 5
  - Portable Devices
  - Ports (COM & LPT)
  - Processors
  - Security Devices

a. In the device manager right click the device and select "Update driver Software".

b. Press "Browse my computer for driver software".



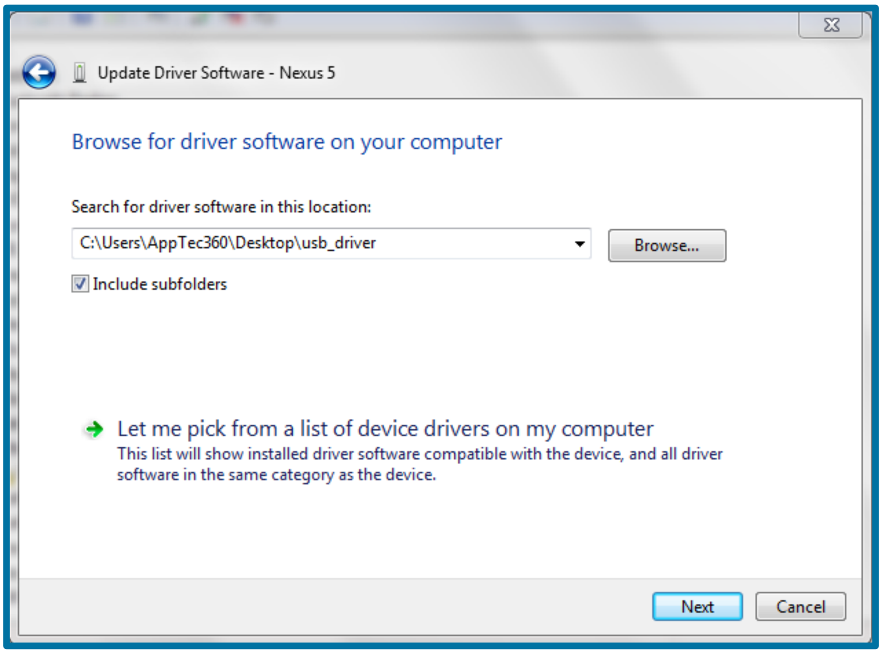
Update Driver Software - Nexus 5

How do you want to search for driver software?

Search automatically for updated driver software
Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.

Browse my computer for driver software
Locate and install driver software manually.

c. Select the folder with the device driver and press "Next".



Update Driver Software - Nexus 5

Browse for driver software on your computer

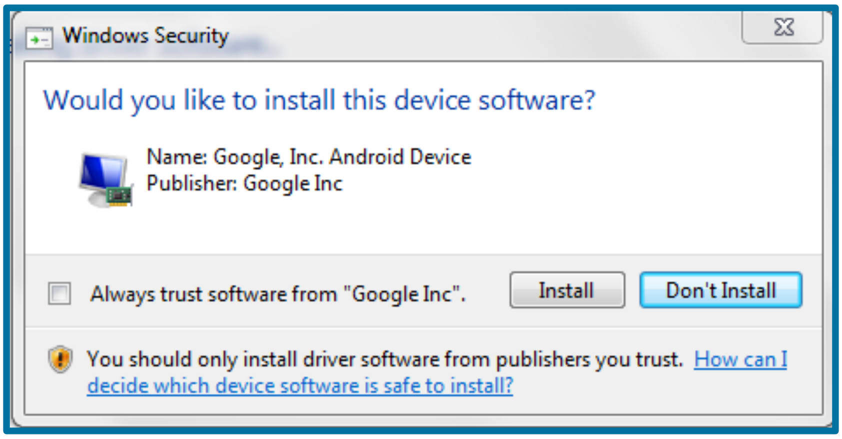
Search for driver software in this location:

C:\Users\AppTec360\Desktop\usb_driver

☑ Include subfolders

Let me pick from a list of device drivers on my computer
This list will show installed driver software compatible with the device, and all driver software in the same category as the device.

d. If a "Windows Security" windows pops up, check the name and publisher and if valid press "Install".



Windows Security

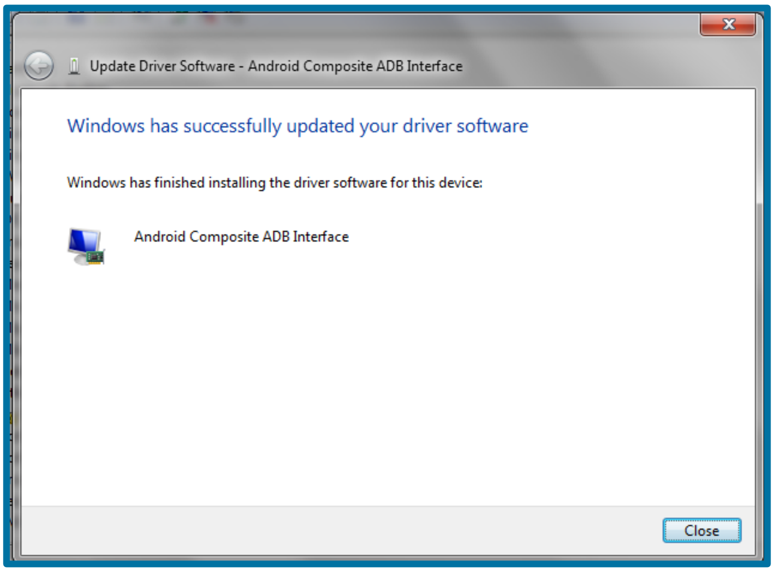
Would you like to install this device software?

Name: Google, Inc. Android Device
Publisher: Google Inc

□ Always trust software from "Google Inc".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

e. If everything went fine you should see this window:



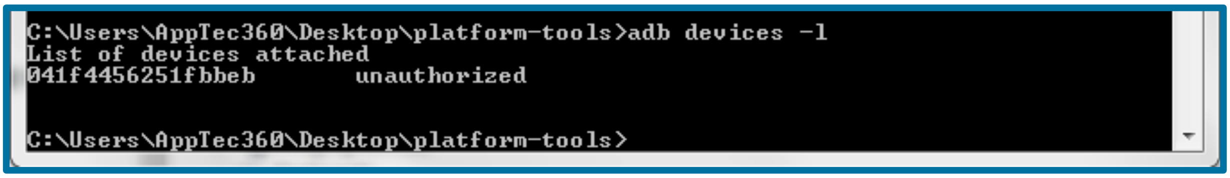
Update Driver Software - Android Composite ADB Interface

Windows has successfully updated your driver software

Windows has finished installing the driver software for this device:

Android Composite ADB Interface

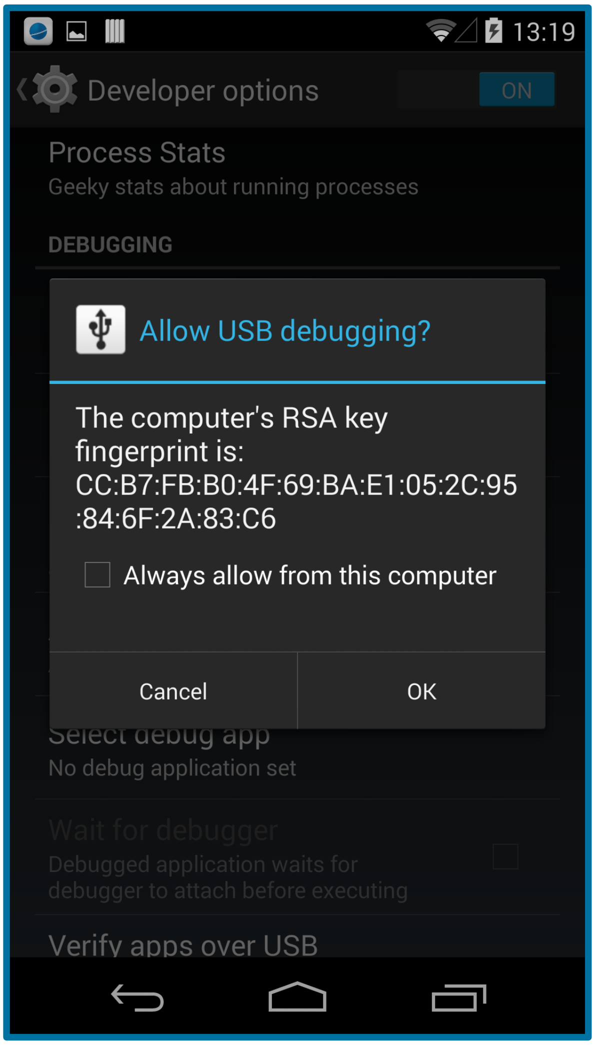
7. Open a command prompt (⊞+R to open run, type in cmd and press enter) and navigate into the "platform-tools" folder.
8. Run "adb devices –l" to get a list of connected devices.



```
C:\Users\AppTec360\Desktop\platform-tools>adb devices -l
List of devices attached
041f4456251fbbeb        unauthorized

C:\Users\AppTec360\Desktop\platform-tools>
```

9. When the device asks if you want to allow USB debugging confirm with "OK"



Process Stats

Geeky stats about running processes

DEBUGGING

Allow USB debugging?

The computer's RSA key fingerprint is: CC:B7:FB:B0:4F:69:BA:E1:05:2C:95:84:6F:2A:83:C6

□ Always allow from this computer

Select debug app

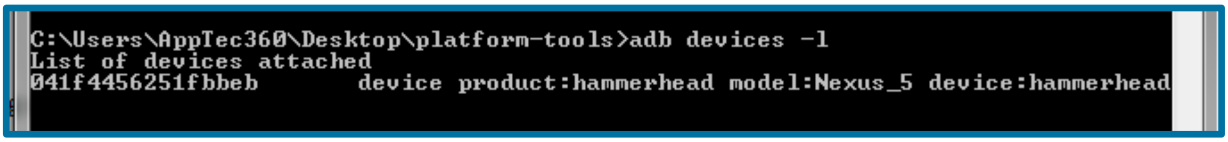
No debug application set

Wait for debugger

Debugged application waits for debugger to attach before executing

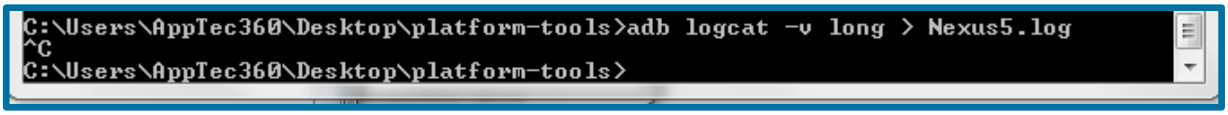
Verify apps over USB

10. Rerun "adb devices –l". Now the device should show up in the list together with some information about it.



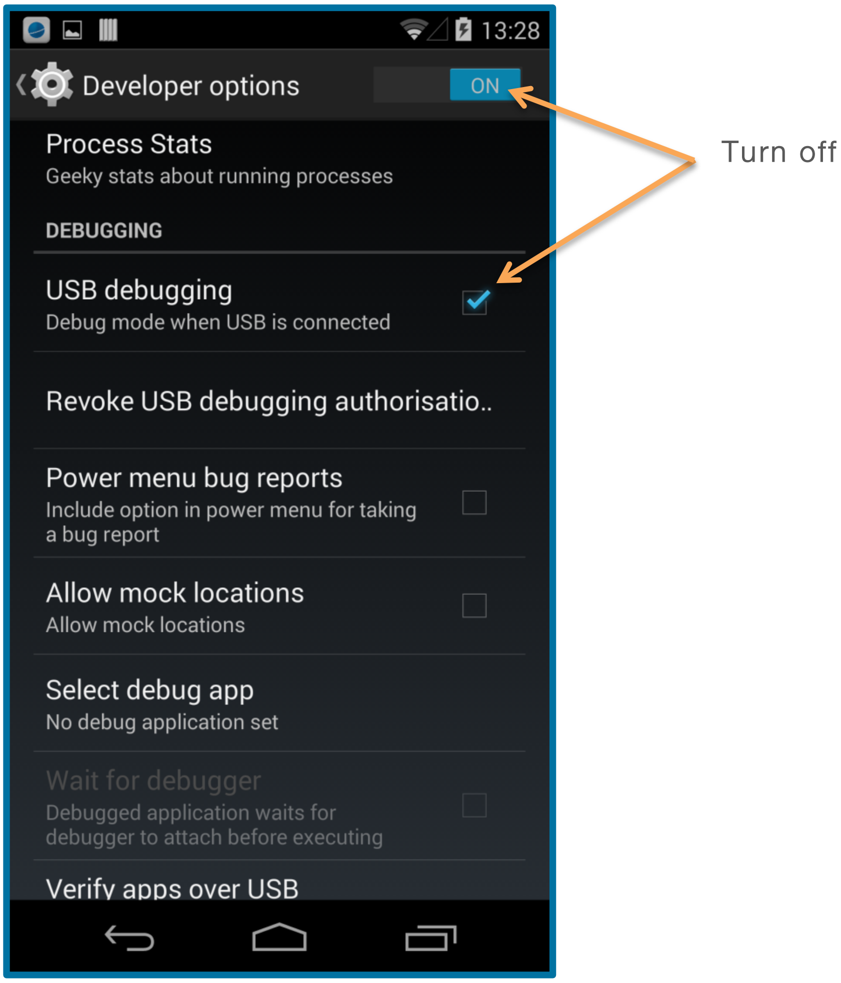
```
C:\Users\AppTec360\Desktop\platform-tools>adb devices -l
List of devices attached
041f4456251fbbeb       device product:hammerhead model:Nexus_5 device:hammerhead
```

11. Run "adb logcat -v long > Device.log". Wait 10 Seconds, and then stop the command by pressing CTRL+C.



```
C:\Users\AppTec360\Desktop\platform-tools>adb logcat -v long > Nexus5.log
^C
C:\Users\AppTec360\Desktop\platform-tools>
```

12. The Log file should be in the "platform-tools" folder.
13. (Optional) Disable "USB debugging" and "Developer options" in the Settings



Developer options ON

Process Stats
Geeky stats about running processes

DEBUGGING

USB debugging ☑
Debug mode when USB is connected

Revoke USB debugging authorisatio..

Power menu bug reports ☐
Include option in power menu for taking a bug report

Allow mock locations ☐
Allow mock locations

Select debug app
No debug application set

Wait for debugger ☐
Debugged application waits for debugger to attach before executing

Verify apps over USB

General Questions

How to get an APNS Certificate

To create an APNS Certificate you need an Apple-ID. It's recommended not to use a personalized Apple-ID, please use an Apple-ID used for your corporation.

If you own an Apple-ID, press "General Settings" and follow the steps in "iOS-Configuration".

What happens if I change my APNS Certificate or don't renew it annually?

The devices don't get any configuration from the AppTec MDM Server anymore and have to be enrolled again.

How do I move users between groups?

You have two options:

1. You just drag and drop a user from one group to another.

2. While you have selected a user, press the gear icon, choose "Edit User" and select the new group in "Usergroup".

How do I move devices between users?

Drag and drop the device from user to another.

Is it possible to change setting per device?

In the Enterprise Mobile Manager you can change settings per group or/and device. That settings made on device level have a higher priority than settings on group level. If group settings get overwritten in the device settings, a blue square shows up on the left side of that setting. You can reset the setting back to the group setting by pressing this blue area.

Is it possible to buy new SMS-Credits?

Yes, please contact our sales department for further requests.

Is it possible to switch between black- and whitelisting on group level or is this reserved to global settings?

At the moment this is only available as a global setting. At the moment you have to choose between the two methods, but it's possible to black- or whitelist Apps on group level.

While enrolling a device I get an error saying "Network Connection Failure"

Please make sure that you've opened the necessary ports in you firewall configuration. For further information see the architectural diagram.

What kind of certificate is needed to run the virtual appliance?

You need an official certificate signed by a trusted certificate authority. It's possible to use wildcard certificates. You cannot use a self-signed certificate because they are not accepted by Apple and Android devices.

While enrolling an iOS device the certificate in the certificate installation shows up as "Not Verified".

Please check if the certificate uploaded in step 2 of the appliance configuration is correct. Also check if you have uploaded the right intermediate certificate. If you upload new certificates don't forget to save the changes by pressing "Configure Appliance" in step 5.

What do you use the username and password for that show up in step 3 of the configuration?

This is the account for the license manager. You can use it as login for the console to manage the licenses on multi-client appliances and to export the configuration for backup and maintenance purposes.

While enrolling an Android device I get an error in the app that says "Exception:java.security.cert.CertPathValidatorException: Trust anchor for certification path not found"

Please check if the certificate uploaded in step 2 of the appliance configuration is correct. Also check if you have uploaded the right intermediate certificate. If you upload new certificates don't forget to save the changes by pressing "Configure Appliance" in step 5.

I can't login as root user in the OS of the virtual machine

You can't login to the appliance as root user. To work with root permissions you need to use the "sudo" command line utility.

If I install GoolePlayStore Apps via the Console but the GooglePlaystore is disabled in the SysApp Restrictions settings, will the apps still be updated automatically?

The updates will be installed automatically if the automatic updates were activated prior restricting the GooglePlayStore. There is no Interface available to us to get the apps to automatically update.

CONTACT

Questions? Simply contact us at:

support@apptec360.com

DISCLAIMER

The information provided in this document does not warrant or assume any legal liability or responsibility for the accuracy and completeness. This document is meant to provide a general structure on the discussed issue. Thus it is not meant to document specific licensing terms. Please refer to your license agreements, available product licensing information and other sources provided by respective software vendor to review valid terms and conditions for license compliance reconciliation.

This documentation is protected by copyright. All rights reserved by AppTec GmbH. Any other usage, in particular, dissemination to third parties, storage within a data system, distribution, editing, speech, presentation, and performance are prohibited. This applies for the document in parts and as a whole. This document is subject to changes.

Reprints, even of excerpts, are only permitted after written consent of AppTec GmbH. The software described in this documentation is continuously developed, which may result in differences between the documentation and the actual software. This documentation is not exhaustive and does not claim to cover the complete functionality of the software.