Importing your Email or Personal Authentication certificate to Android Devices

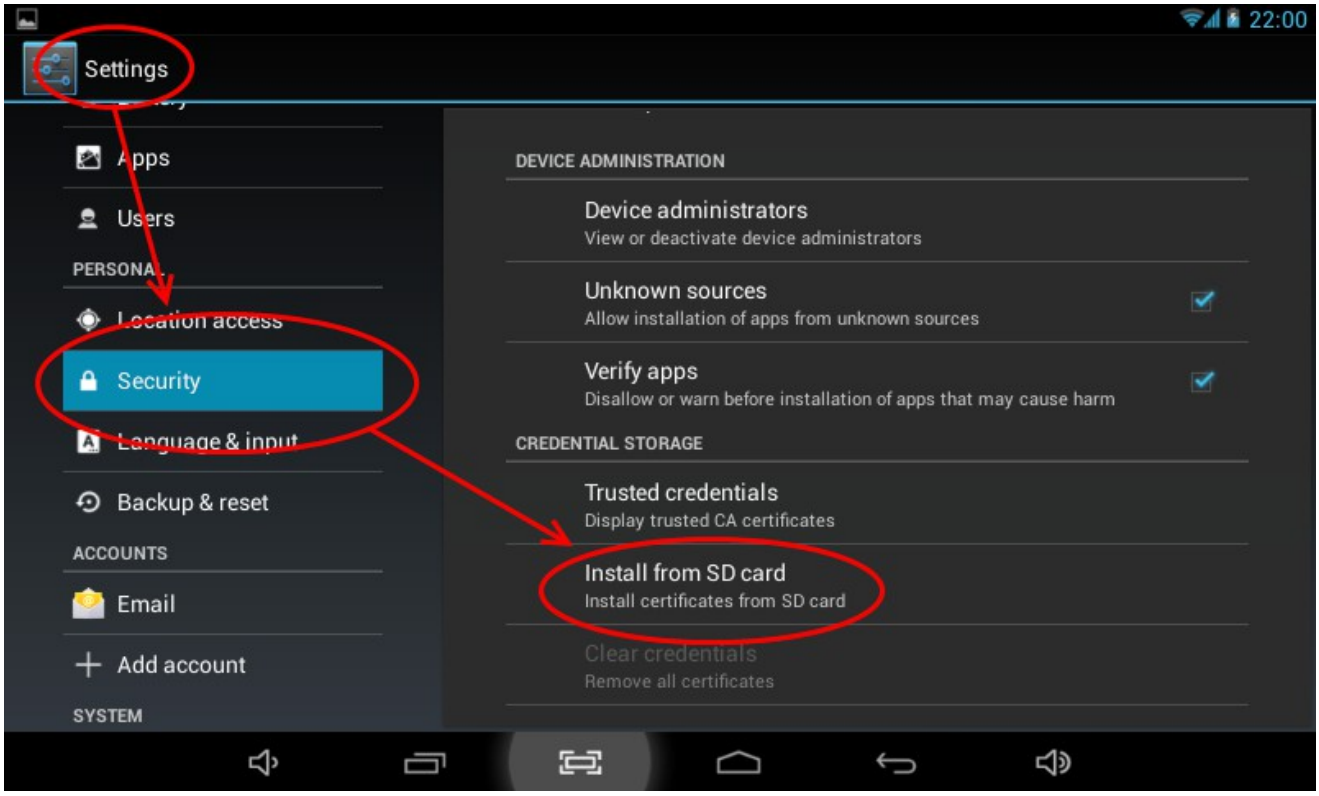
This document explains how you can import your CPAC/Email onto Android devices.

Background notes

- The native Android mail client does not support signing or encryption of emails. Signing and encryption is, however, supported by some 3rd party apps and by some manufacturer-specific mail clients such as the one found on Samsung Galaxy devices. For help in this area, see List of SMIME compatible Android clients and Android – Djigzo app. We will add more documents as support grows for SMIME on Android.
- If you originally downloaded your certificate to your desktop or laptop then you first need to export it using one of the browsers listed on the CPAC main page. When doing this, please make sure you export the private key and include all certificates in the certificate path if possible. You must also specify a strong password to protect the certificate file.
- Once exported from your computer, you need to transfer it to your Android device (for example, copy to a USB drive or upload then download from online storage or email it to your device). The example in this document shows installation of a certificate that has been transferred to an SD card.

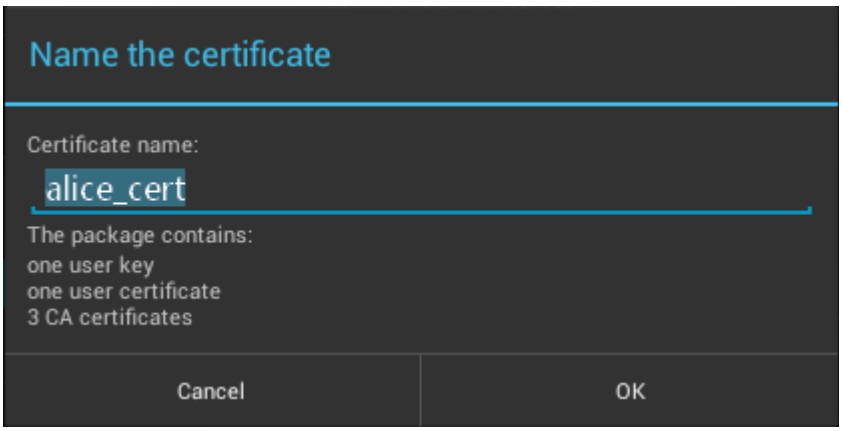
Import your certificate to Android

1. Tap **Settings** > **Security**. Under **'Credential Storage'** select **'Install from SD card'**.

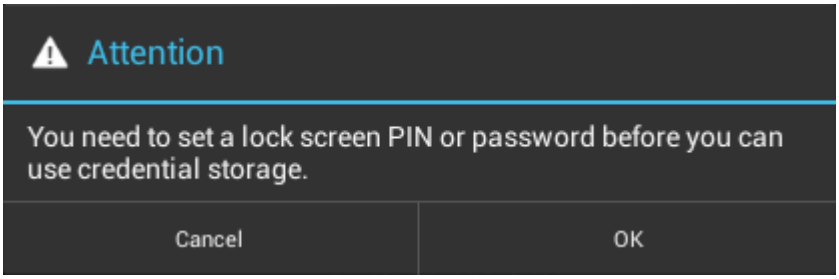


2. Enter the password you set up for the certificate when it was exported and click **'OK'**.

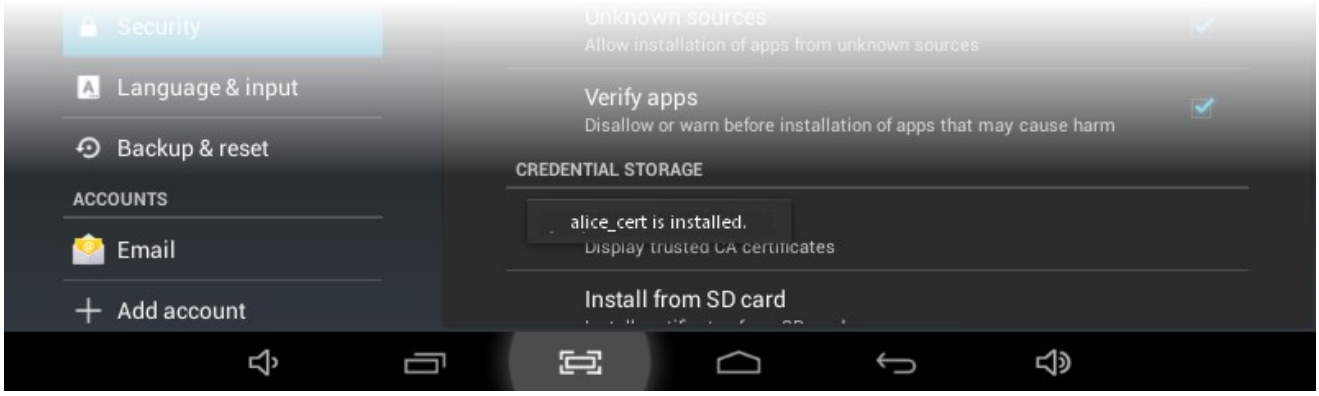
3. In the **'Name the certificate'** screen, enter a friendly name to identify the certificate and tap **OK**.



4. If you have not yet set a passcode or pattern to lock your home screen then you will be prompted to do so before proceeding. This is required before you can install your certificate and will be requested in future to access the Android certifcate store (Settings > Trusted Credentials). If you have already set a screen passcode this step will be skipped and the certificate will be installed.

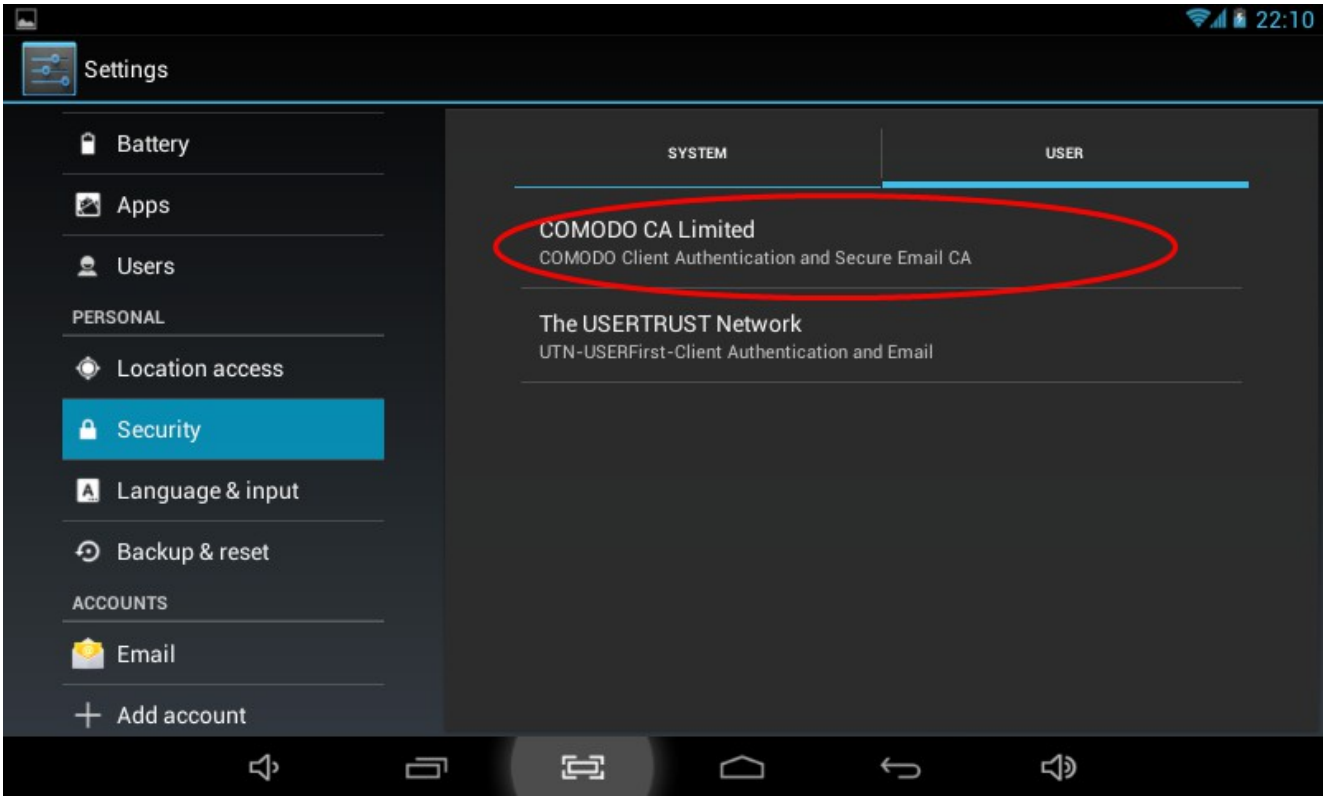


5. Click **OK**. The Certificate will be installed.



You can confirm tcertificate installation by viewing the User Certificates under Trusted Credentials.

- Open the Settings panel and tap **Security** > **Trusted Credentials**
- Tap the **User** tab. You will see the list of user authentication certificates installed on your Android device.


22:10
Settings
Battery
Apps
Users
PERSONAL
Location access
Security
Language & input
Backup & reset
ACCOUNTS
Email
Add account
SYSTEM
USER
COMODO CA Limited
COMODO Client Authentication and Secure Email CA
The USERTRUST Network
UTN-USERFirst-Client Authentication and Email

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, New Jersey 07013

United States

Tel : +1.888.266.6361

Tel : +1.703.581.9361

Email: sales@Comodo.com

Comodo CA Limited

3rd floor, Office Village Exchange Quay

Trafford Road, Salford, Manchester M5 3EQ

United Kingdom

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit **https://www.comodo.com**