What is conpal LAN Crypt for Android?

conpal LAN Crypt for Android enables users to work with their encrypted data remotely, by using their mobile devices, such as smartphones or tablets. With transparent file encryption on Windows / macOS, conpal LAN Crypt enables the secure exchange of confidential data within authorization groups in small, medium and large organizations. Numerous companies, business organizations and the public administration in Germany and worldwide are already relying on conpal LAN Crypt.

A Security Officer (SO) determines centrally, which files and storage locations should be protected by conpal LAN Crypt and defines which users are allowed to have access to specific data by setting one, or several encryption rules. As an example, the Security Office (SO) can ensure that all Word documents in a specific file storage path, are encrypted, by creating an encryption rule on the defined path e.g., "//Servername/Files/*.docx". As soon as this rule is transferred to the client computer via a policy file, created with the conpal LAN Crypt Administration console, all Word documents in this path will be encrypted from now on. Additionally, you can combine one or more encryption rules to one encryption profile. This applies to all files, independently of where the files are stored. You can access all conpal LAN Crypt encrypted files that are either stored locally, on a network storage or on a remote storage (e.g., cloud storage). A user can easily access the same conpal LAN Crypt encrypted files, that are also available on his workstation computer.

This release of **conpal LAN Crypt for Android** allows the user to open, edit and save encrypted files and access them per se and moreover extends the usual conpal LAN Crypt security infrastructure by using certificates (.p12 files) and policy files (.xml.bz2) on mobile devices. In addition, with this version you can now also encrypt and decrypt files with a very secure password (integrated conpal LAN Crypt 2Go).

conpal LAN Crypt 2Go

conpal LAN Crypt for Android now supports password-based encryption and decryption of files and is compatible with conpal LAN Crypt 2Go. This allows you to easily and securely exchange information with other people, such as your business partners or even external employees.

Sophos SafeGuard Enterprise encrypted files

With *conpal LAN Crypt for Android* you can also decrypt files that are encrypted with Sophos SafeGuard Enterprise. All you need for this is the corresponding key. For this to work, such keys must be exported from Sophos SafeGuard Enterprise and imported into conpal LAN Crypt Administration for Windows. More information is available at sgn-en.conpal.de. A step-by-step guide to migration is available via the Red Book "SafeGuard Enterprise: Migration file encryption in 5 steps".

Which versions are supported?

conpal LAN Crypt for Android supports Android 9 and later

conpal LAN Crypt for Android is available in German and English.

Supported encryption algorithms

Supported encryption algorithms for file encryption

conpal LAN Crypt for Android supports the following encryption algorithms:

- AES-256 Bit (XTS-Mode)
- AES-256 Bit (CBC-Mode)
- AES-128 Bit (XTS-Mode)
- AES-128 Bit (CBC-Mode)

Supported encryption algorithms for key wrapping

conpal LAN Crypt for Android supports the following encryption algorithms for key-wrapping:

- AES-256
- AES-192
- AES-128

Supported but not recommended: 3DES, 3DES TWO KEY

With key-wrapping (default setting), the transport key of the Security Officer data and the user profile data will be encrypted with a randomly generated session key using the selected algorithm (AES is used by default). This key in turn is RSA-encrypted using the public key from the certificate.

Note

- In comparison to conpal LAN Crypt for Windows, the algorithm "RC2" is not supported by *conpal LAN Crypt for Android*. If the Key-Wrapping for your policy file is set to this algorithm, the policy file cannot be used with *conpal LAN Crypt for Android*. In that case, you have to change the Key-Wrapping encryption algorithm and choose an algorithm that is supported (e.g., AES-128).

General preparations and setup

For security reasons, please always activate the screen lock on your Android device before using this app. You cannot run *conpal LAN Crypt for Android* without an activated screen lock. Never use an easy-to-guess password, such as "1234" or "password". Only with a strong password you can prevent unauthorized access to your confidential data, in case your device is lost or stolen. In general, conpal recommends to delete all App-Data on your Android device, if the device is not in use for a longer period of time, or if you exchange your device for a new one (see Delete App-Data).

Note

- If you deactivate the screen lock later, *conpal LAN Crypt for Android* deletes the certificate and the private key file from the certificate storage of your Android device.
- Rooted devices are not supported by *conpal LAN Crypt for Android*.

Providing the configuration data

Tap the **gear icon** at the bottom of the app to open the settings page, which allows you to provide the configuration data:

- Import your policy file
- Import your user certificate

Managing encryption keys

Managed keys and password-based keys can be both found within the settings. Managed keys originate exclusively from the given policy file, whereas password-based keys can be freely created, renamed and deleted inside the related settings. Renaming a key does not change the generated key used for encryption.

Note

- Password-based keys can also be created within the action of encrypting a file. These keys are then automatically added to the saved list of password-based keys.
- By successfully decrypting a file with a password-based key, the used key will also be automatically added to the saved list of password-based keys.

Policies

What are conpal LAN Crypt policy files?

A Security Officer (SO) determines centrally, which files and storage locations should be protected by conpal LAN Crypt and defines which users are allowed to have access to specific data, by setting one or several encryption rules. Each individual encryption rule consists of an encryption path, a key and an encryption algorithm. conpal LAN Crypt policy files contain all encryption rules, that the user requires, in order to be able to work with encrypted data. For the user to be able to use the policy file, he/she needs a certificate, which will be provided to him/her as a key file (.p12 file) by the conpal LAN Crypt Security Officer. The key file contains the certificate and the private key of the user. The access to the key file is secured by a password. The user will receive the password through his Security Officer

Before importing the policy file and the key file to the mobile device, both files have to be copied to a location that is accessible by the mobile device. This can be a private folder on OneDrive or a network share. Alternatively, you can copy the key file directly to the storage of the mobile device, by connecting it to the PC via USB or Bluetooth.

Import your policy file

Open the *conpal LAN Crypt for Android* App on your mobile device. Tap the **gear icon** at the bottom of the app to open the settings. Tap the **IMPORT** button on the **Import conpal LAN Crypt policy** screen and select the location that contains the policy file. Select the policy file. The policy file will be imported into your mobile device.

Import your user certificate

Open the *conpal LAN Crypt for Android* App on your mobile device. Tap the **gear icon** at the bottom of the app to open the settings. In the selection box, tap the **IMPORT** button on the **Import user Certificate screen**, and choose the location that contains the certificate key file (.p12 file). Tap the certificate key file (.p12), which will be indicated by a finger print icon. Into the dialog box, enter the password of your certificate, that you have received from your Security Officer. Once you have entered the correct password, the certificate and the corresponding private key will be saved to the storage of your Android device.

Note

- *conpal LAN Crypt for Android* also supports referencing multiple user certificates in the policy file. In order to be able to use the policy file, the user must have at least one of the certificates that have been issued to him and whose public key is used to encrypt the policy file, and of course he must also have imported it.

Display certificate details

Open the *conpal LAN Crypt for Android* App on your mobile device. Tap the **gear icon** at the bottom of the app to open the settings. There, tap on the **Certificate information** option. In the next dialog, you will see an overview of the certificates installed on the device. Tap on the desired certificate from which you want to obtain further information. You will then be shown the further details, such as the Serial number, validity period, Issuer, etc., of the certificate. You can also copy this information to the clipboard by tapping **COPY TO CLIPBOARD** further down in the sub-dialog. By tapping **OK** you close the dialog.

Rolling out policy files and certificates using MDM

In addition to the app, you can use a Mobile Device Management (MDM) solution to deploy the individual configuration (policy file and certificate) for the mobile devices in addition to the app itself. If you do not have a Mobile Device Management (MDM) solution at your disposal, the configuration data (policy file and certificate) must be imported by each user manually, as described above.

Note

- If *conpal LAN Crypt for Android* is rolled out via MDM, the security officer's public certificate (.cer), which was used to sign the policy file, can also be provided on the mobile device in addition to the policy and user certificate. In this case, policy files imported manually by the user are also checked by validating the signature of the Security Officer certificate.

Settings

Configuration data is a list of key+string tuples. Files must be provided as Base64-encoded strings, via URL, hosted on a HTTPS or SMB server. The following configuration keys are offered by conpal LAN Crypt:

Policy

policy_blob: Policy XML or XML.bz2 file as Base64-encoded **(STRING)**.

policy_url: URL to a policy XML or XML.bz2 file **(STRING)**.

User Certificate / P12 file

usercert_blob: Certificate PKCS-12 file as Base64-encoded **(STRING)**.

usercert_url: URL to a certificate PKCS-12 file **(STRING)**.

Security Officer Certificate

admcert_blob: Security Officer Certificate (.cer) file (DER encoded) as Base64-encoded **(STRING)**.

admcert_url: URL to a Security Officer Certificate (.cer) file (DER encoded) **(STRING)**.

Default Key

default_key_guid: GUID of the key that must be used for encryption of new files **(STRING)**.

Note

- If this key is set, the user is not allowed to change the encryption key (forced encryption key). However, he can always use a password-based key for encryption (which results in an encrypted copy of the original file).

Samba Credentials

smb_username: If one of the policy or user cert settings refers to a SMB location, the user name for the SMB connection can be configured with this key **(STRING)**.

Note

- If the value is not set, the user is asked to enter the user name.
- Due to security reasons, the password for the SMB connection has always to be entered by the user.

Certificate Validation

cert_validation: Enables the certificate validation. Validation is disabled if setting is missing **(BOOLEAN)**.

Note

- The validation is disabled if the setting is missing.

Compatibillity

microsoft_office_support: Enables editing of files in Microsoft Office. **(BOOLEAN)**.

Note

- Office support is disabled if the setting is missing. Requires "Allow management of all files" permission enabled in Microsoft Office App, too.

Rules

- Managed settings cannot be changed or overruled by the user.
- URLs must be hosted on HTTPS servers with a valid SSL certificate. You can verify this by entering the URL in a browser on the mobile device (e.g., Chrome, Safari). If the file can be shown, the URL will also work as configuration value.
- If both BLOB and URL are supported for a setting, the BLOB has priority.
- If the data BLOB or URL of a setting is invalid, an error is shown.
- When using URLs for SMB shares, username and passwords will be ignored (use smb_username instead) (smb://localfileserver/certificates/sepp.p12) format: smb:////
- There are no documented maximum lengths for configuration strings but size of the strings should not be bigger than a few kilobytes.

Deleting app data

Resetting *conpal LAN Crypt for Android*

In *conpal LAN Crypt for Android* select the option Delete App-Data in the app settings. This will delete all data stored in the *conpal LAN Crypt for Android* app, including the policy file, the user certificate and the private key. *conpal LAN Crypt for Android* will then be reset to factory defaults.

Open, edit, encrypt, decrypt and share files

conpal LAN Crypt for Android enables you to access files stored on the device itself (local memory and also data stored on the inserted SD card), on network shares or in the cloud (e.g., on OneDrive or Google Drive). File access via *conpal LAN Crypt for Android* can be done directly or via the "Storage Access Framework (SAF)" for Android. SAF allows to use remote access provided by other apps installed on the same device. For example, the conpal LAN Crypt app can access the user's data on OneDrive if the OneDrive app is installed. Similarly, access to Google Drive is then also provided if the associated app is installed on the mobile device, etc. To simplify the usability of *conpal LAN Crypt*

for Android, the integrated file browser has been extended by a menu. Tap on the folder icon in the lower left corner within the app to open the context menu. This allows you to quickly and directly access files that are stored on different storage locations.

Note

- You may need to log in to your OneDrive or Google Drive account first to access files there. This also applies to accessing files via a Windows share (SMB).

How to access encrypted data?

As already described in part, files on a mobile device can be accessed in various ways. This can be done via a native file browser app, a proprietary app for cloud storage (such as OneDrive), or directly from an app. *conpal LAN Crypt for Android* contains its own integrated file browser. This means that (encrypted) files can now also be accessed directly via the dashboard, which are either stored on a local storage location, on a Windows share or on OneDrive cloud storage. You can also use the file browser to see the encryption information of the files displayed there. If a file is marked with a green key symbol, it means that the file is encrypted and that you have the necessary key to open and edit this file. A red key symbol, on the other hand, means that the file is encrypted by conpal LAN Crypt, but you do not have the key required to open or edit this file.

Open files, edit them and save them encrypted

To edit files, they can also be loaded directly from the *conpal LAN Crypt for Android* app via the integrated file browser using the respective context menu. You can then edit the files. When you save them, they will be automatically encrypted by *conpal LAN Crypt for Android*.

Note

- For editing Office documents, conpal recommends using the open source and free app "Collabora Office". This is based on LibreOffice, which is one of the best-known and most popular open-source office applications worldwide.

Users can thus browse, open, edit and save their files using a native file browser, via the integrated file browser, directly from an app, and via the *conpal LAN Crypt for Android* app. To open an encrypted file via the integrated file browser, tap the **folder icon** at the bottom left within the app. Then use the menu (OneDrive, Windows Share or Browse) to select the location where the file is stored.

Using the file browser, then select the path and there the encrypted file that you want to open via the conpal LAN Crypt app. Tap **OPEN** selection in the extended menu. the Open with dialog opens. Then select the app with which you want to open or edit this file. The previously selected file is then opened and decrypted on your mobile device via the app. You can then edit it and also save it again. The file is automatically encrypted during this process.

Note

- On the storage location itself, this file always remains encrypted. All encryption and decryption operations of *conpal LAN Crypt for Android* only take place within the protected data area of the app on the mobile Android device. Only *conpal LAN Crypt for Android* has access to this data area.

Display file encryption information

Each file has a key symbol indicating the status of the file:

- **green key:** The file is encrypted and can be accessed.
- **gray key:** The file is plain and can be accessed.
- **red key:** The file is encrypted and can not be accessed (the key is not available or the used encryption algorithm is not supported on mobile).

For more detailed information, you can display the encryption information for each file on your mobile device. To do this, open the *conpal LAN Crypt for Android* app for Android on your **mobile device. Then tap on the folder icon** at the bottom left within the app to open the file menu view. Select the appropriate location (OneDrive, Windows Share or Browse) where the file whose encryption information you want to view is located. Tap on the file and after that, tap on the **INFO** selection. The **Encryption Info** dialog now displays the following information about the previously selected file:

- **Encryption state:** Indicating if the file is encrypted or not.
- **Key name:** The name of the key used for encryption (only shown for encrypted files).
- **Key Id:** The GUID of the key used for encryption (only shown for encrypted files).
- **Key availability:** Indicating if the key is available in the policy (only shown for encrypted files).

Encrypt a file with a key from the policy file

To encrypt a file with a key from the policy file, open the *conpal LAN Crypt for Android* app on your mobile device. Then tap on the **folder icon** in the lower left corner within the app to open the file menu view. There, select the location (OneDrive, Windows Share or Browse) that contains the file you want to encrypt or perhaps share. Then select the file you want to encrypt by tapping on it. After that, tap the **ENCRYPT** selection in the advanced menu. Select the option for encryption with a stored key. Check the **Overwrite existing file option** if you want the original file to be encrypted and tap **OK**. The file will then be saved encrypted to the previously selected location. If you do not want to overwrite the original file, uncheck the Overwrite existing file option and tap OK. The Share dialog opens. From the list of apps displayed there, select the respective app with which you want to save or possibly share the encrypted file (e.g., Google Drive, Gmail etc.) and tap on it. The file will then be transferred to this app in encrypted form.

The **Nearby** option also allows you to share the encrypted file with a nearby device via Wi-Fi or Bluetooth.

Note:

- If no default encryption key was set up for you, you can change the encryption key from the list by tapping on another available key. In that case, the file will be encrypted using that key instead of the previously selected key.

Encrypt and share as password-protected file (conpal LAN Crypt 2Go)

To encrypt and share a file with a password-based key, open the *conpal LAN Crypt for Android* app on your mobile device. Then tap on the **folder icon** in the lower left corner within the app to open the file menu view. There, select the location (OneDrive, Windows Share or Browse) that contains the file you want to encrypt or perhaps share. Then select the file you want to encrypt by tapping on it. After that, tap the **ENCRYPT** selection in the advanced menu. Select the option for encryption with a password-based key. Now you can either select a previously used password or create a new password for encryption. By creating a new password in this way, the password will automatically be saved on device and can be used to further encrypt and decrypt files. Password-based keys can also be found and edited in the settings menu.

The Share dialog opens. From the list of apps displayed there, select the respective app you want to save or possibly share the encrypted file (e.g., Google Drive, Gmail, etc.) with and tap on it. The file is then transferred to this app in encrypted form and can be processed, saved, or shared with others (e.g., Gmail) depending on the functionality (e.g., native file browser or Google Drive, etc.).

The **Nearby** option also allows you to share the encrypted file with a nearby device via Wi-Fi or Bluetooth.

Note:

- The encryption requires a secure password! This must be at least 8 characters long and contain upper- and lower-case letters, numbers and special characters.
- The name given to the encryption password does not have any impact on the key used for encryption. The actual key value for encryption is generated separately.
- Unlike the in-place encryption using a key from the police file, the encryption with a password-based key will not manipulate the original file and will instead create an encrypted copy of the file to then share.

Decrypt and share a file

To decrypt a file, open the *conpal LAN Crypt for Android* app on your mobile device. Then tap on the **folder icon** at the bottom left within the app to open the file menu view. There, select the location (OneDrive, Windows Share or Browse) where the file you want to decrypt or perhaps share is stored. Then select the file you want to decrypt by tapping on it. After that, tap on the **DECRYPT** selection in the advanced menu. If the file is a password-protected file, an additional dialog may be displayed at this point. In this case, enter the required password in the Enter password field.

The **Share** dialog opens. From the list of apps displayed there, select the respective app with which you want to save or possibly share the decrypted file (e.g., Google Drive, Gmail, etc.) and tap on it. The file is then transferred to this app in decrypted form and can be processed, saved, or shared with others (e.g., Gmail) depending on the functionality (e.g., native file browser or Google Drive, etc.).

The **Nearby** option also allows you to share the decrypted file with a nearby device via Wi-Fi or Bluetooth.

Note:

- If you choose the same location, another dialog will ask you if you want to replace the existing file.
- By successfully decrypting a file with a password-based key, the used key will automatically be added to the saved list of password-based keys. The list of password-based keys can be found and edited in the settings.

Logging

conpal LAN Crypt for Android has a Verbose Logging feature. **The usage of this feature is only intended for error analysis and should only be activated if you encounter any errors or problems with the *conpal LAN Crypt for Android* app.**

Verbose logging

The **Verbose Logging** feature can be activated or deactivated at any time in the settings of the *conpal LAN Crypt for Android* app. To activate **Verbose Logging**, open *conpal LAN Crypt for Android* on your device. Tap the **gear icon** at the bottom of the app to open the settings. Activate the Verbose Logging by moving the slider, for the **Verbose Logging**, to the right. The logging feature will be displayed as activated (red color). Take the necessary steps to reproduce the error, to create the log files.

Note:

- In no case will the log files reveal sensitive information!

Send logs

By using the **Send Logs** feature, you can send the log files, for analysis purposes, to the conpal support team by e-mail. To send the log files, tap the **share icon**, that appears to the right of **Send Logs**. Then select the app you use for your email communication. The log file will be attached as a compressed file (.zip) and sent to the team at support@conpal.de. To disable the **Verbose Logging** feature, move the slide button back to the left.

Technical support

To access technical support for conpal products do the following:

All maintenance contract customers can access further information and/or knowledge base items at the following link support.conpal.de. As a maintenance contract customer, send an email to technical support using the support@conpal.de email address and let us know the exact version number, operating system and patch level of your conpal software and, if applicable, a detailed description of any error messages you receive or applicable knowledge base items.