Manual

Cryptify Call application for Windows

Table of Contents

Scope

This document describes how to install, configure, maintain and operate the Cryptify Call application for Windows.

Target audience is end users of Cryptify Call.

Pre-requisites

A computer running Windows 11. Preferably the latest version of Windows 11 should be used.

Introduction

Cryptify Call voice and messaging encryption is approved by NCSC for HMG communication at level RESTRICTED/OFFICIAL, and by the NATO Communication and Information Agency (NCIA) at level NATO RESTRICTED.

Using Cryptify Call is as simple as making an ordinary phone call or SMS. Cryptify Call have a familiar user interface, and is using the ordinary phone numbers. The solution works in parallel with the ordinary functions of the phone enabling users to choose whether to make a secure or an ordinary call.

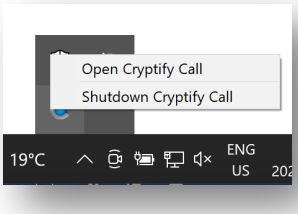
Cryptify Call is using *Cellular Data* service in existing mobile networks and complementing Wi-Fi infrastructures. Being able to use Wi-Fi in addition to the Cellular Data services ensures a cost-efficient solution that provides even better availability than regular mobile voice service.

Subject to authorization by the CMS of the respective organization, users can communicate with users belonging to other organizations in an end-to-end encrypted and authenticated manner.

Cryptify Call is built on reliable standards and protocols enabling multi-vendor interoperability. The comprehensive security of the solution is based on well-proven standard algorithms and protocols such as Advanced Encryption Standard (AES), MIKEY-SAKKE, and Secure Real-time Transport Protocol (SRTP).

IMPORTANT! To receive calls and messages the Cryptify Call application must be running. The application is designed to always run, it will not drain the battery and there is normally no reason to turn it off.

The application keeps running in the background, even if the main window is closed. To actually terminate the application, right-click the Cryptify Call icon in the Windows system tray select “Shutdown Cryptify Call”.



Note! When using Cryptify Call, please find a secluded place to talk. This might be obvious but can easily be forgotten.

Procedures

Installation and configuration

There are two main ways in which Windows devices are used in enterprises; administrators may have set up the devices with the Cryptify Call application, and other apps, before delivering them to end users, or end users may be able to install and updates app themselves.

Install Cryptify Call

If users are permitted to install, update or modify the apps on their Windows devices, they can install Cryptify Call application on the device by using the provided installer.

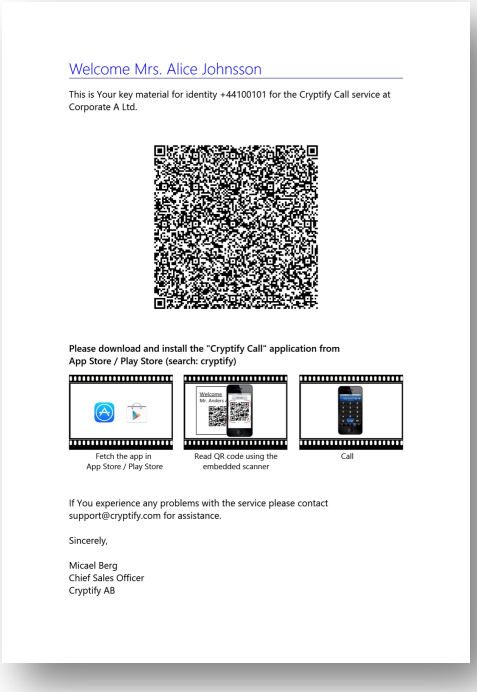
Otherwise, if the Cryptify Call app is not installed, users should ask their administrators to provision it for them.

Provisioning user credentials

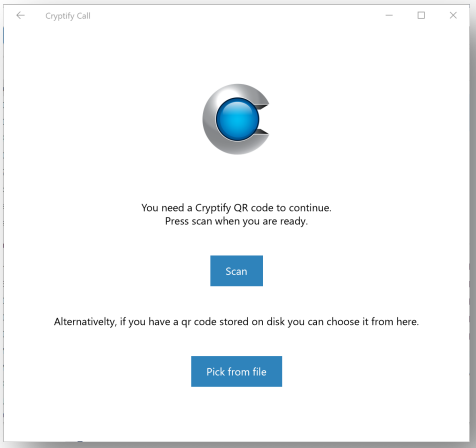
Users are enrolled through a controlled onboarding process managed by the CMS Operator or another designated trusted authority. As part of this process, users are issued the Cryptify Call App (CCA) and provided with an initiation letter containing their unique provisioning QR code.

It is essential that users verify the authenticity of the initiation letter and the QR code prior to scanning. The QR code must originate from the CMS Operator or another explicitly trusted and authorized party. Users must not scan QR codes received from unknown, unexpected, or unverified sources. Furthermore, the QR code must be treated as secret and disposed of in a secure manner after it has been scanned.

To provision the app, start the Cryptify Call app and use the embedded scanner to read the QR code provided in the initiation letter.



Alternatively, the app can be provisioned using a PDF-file containing the QR-code.



It is recommended that the initiation letter be destroyed once used in order to ensure the credentials don't get into the wrong hands.

Uninstallation

To uninstall the application, first perform the procedure *Manual key removal / replacement* (see page 29).

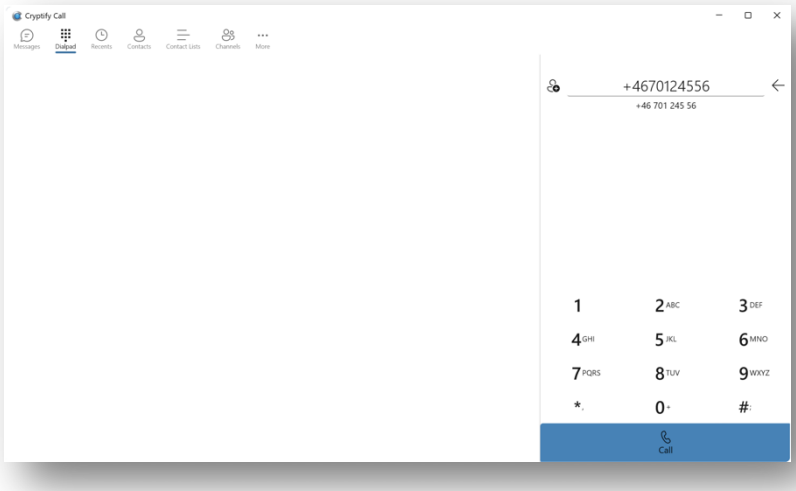
Then, in non-managed environments, the application can be uninstalled via system Settings → Apps & features → Cryptify Call → Uninstall.

Note that simply uninstalling the application does not remove the application user data (such as keys, messages or attachments).

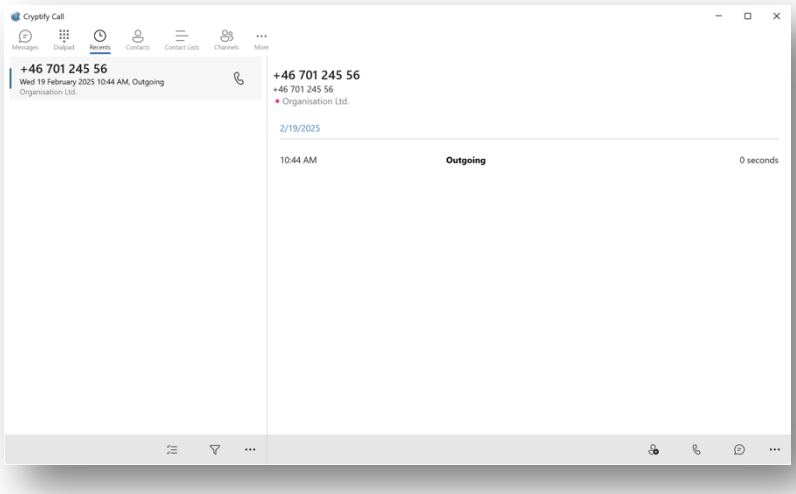
Make a secure call

Making a secure call is as easy as dialing the number of the person to call, and normally the number is the same as the mobile number for that person. The only requirement is that both parties use Cryptify Call.

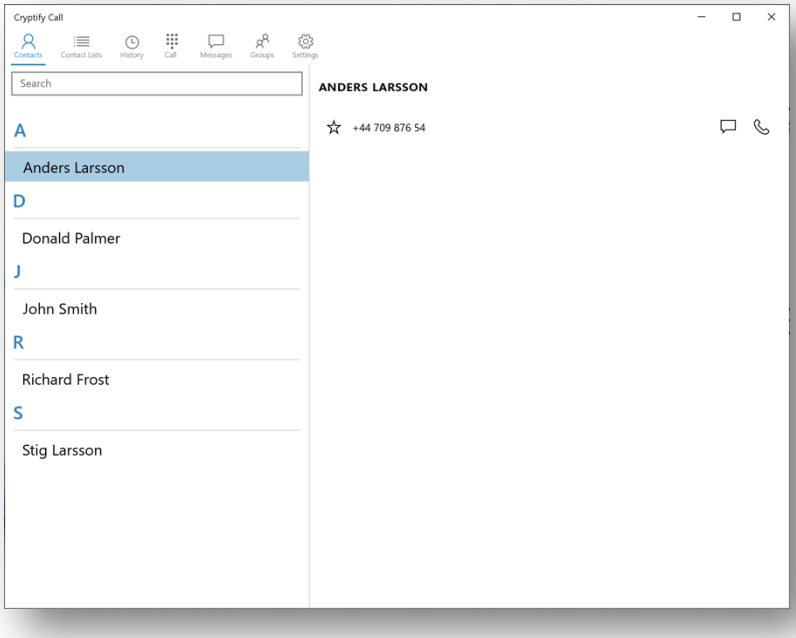
The number can be entered using the keypad.



An alternative method to make a secure call is to use the *History* tab, where the call log is listed. A secure call can be initiated by clicking one of the call buttons.



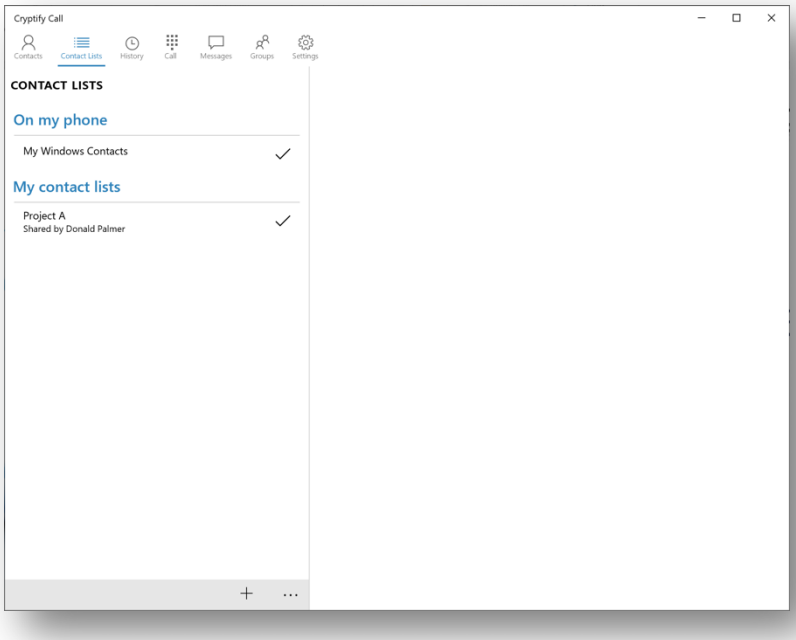
The application also has a Contacts tab, showing all contacts available to the app. Contacts are sourced from shared contact lists, centrally managed contact lists as well as from personal contacts.



All available contact lists are shown under the “Contact Lists” tab. Lists that are enabled – that is, those lists that are used as a source of contact information – are marked with a checkmark. To enable or disable a list, click the list and toggle the “Enabled” switch.

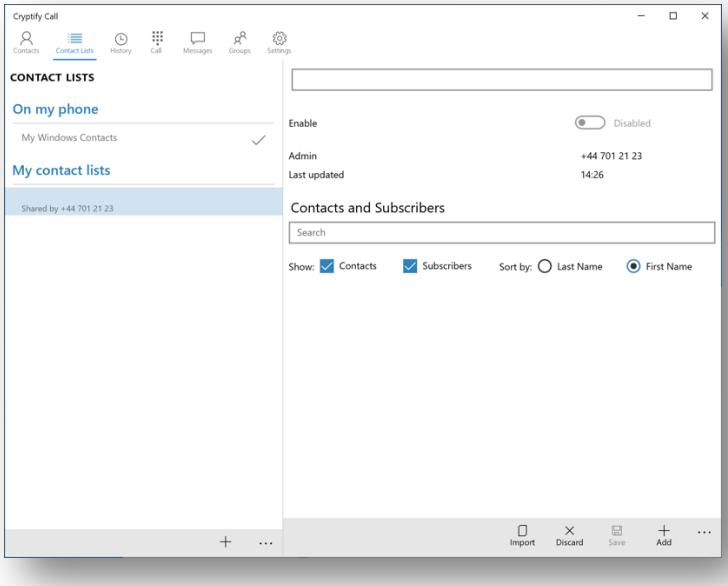
Shared contact lists are automatically kept up-to-date, and to unsubscribe from future updates you need to contact the admin of the list.

Only enable or import lists from trusted and verified sources. Importing or activating lists from untrusted or unknown sources may compromise the security of the application.



Creating and sharing contact lists

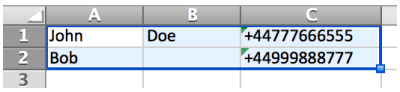
Contact lists can be created within the Cryptify Call app, and optionally shared with other users in a secure manner. To create a new contact list, click the "+" button and enter a name for the contact list.



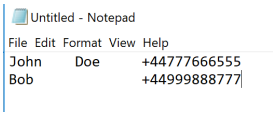
To add new entries to the contact list, click the "+" icon and then either select an existing entry (from the Windows contacts or another contact list) or create a new entry.

It is also possible to import contacts from a TSV (tab separated values) file by clicking the import button and selecting "Import". The file should have UTF-8 (or ASCII) encoding with three columns per line, specifying the first name, the last

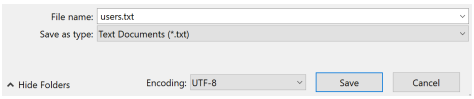
name and the phone number. It is easy to create such a file using Excel and Notepad (or TextEdit on macOS).



Step 1: Select a range of cells containing three columns and choose copy the cells using Edit > Copy (or control-C).



Step 2: Paste the result into a new document in Notepad. (If using TextEdit on macOS, select Format > Make Plain Text before pasting the data.)

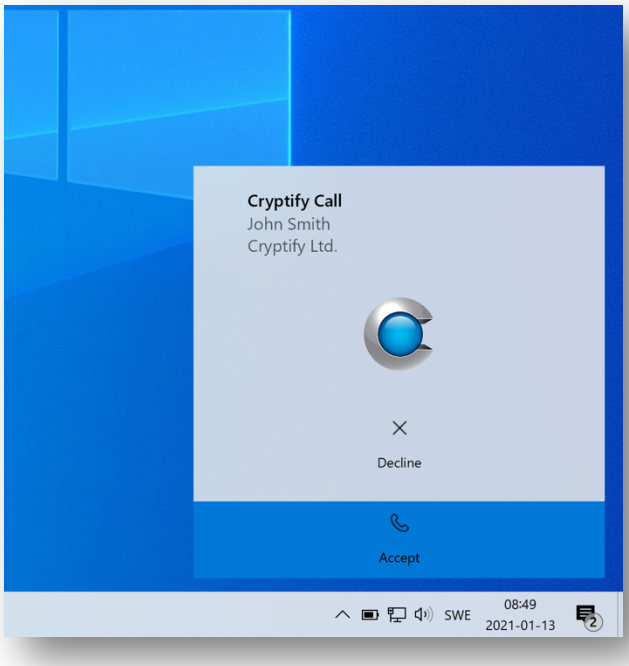


Step 3: Save the document, and make sure to select UTF-8 encoding.

Subscribers – that is, those who will receive the list – are added in a similar manner using “Create new subscriber”.

Answer an incoming secure call

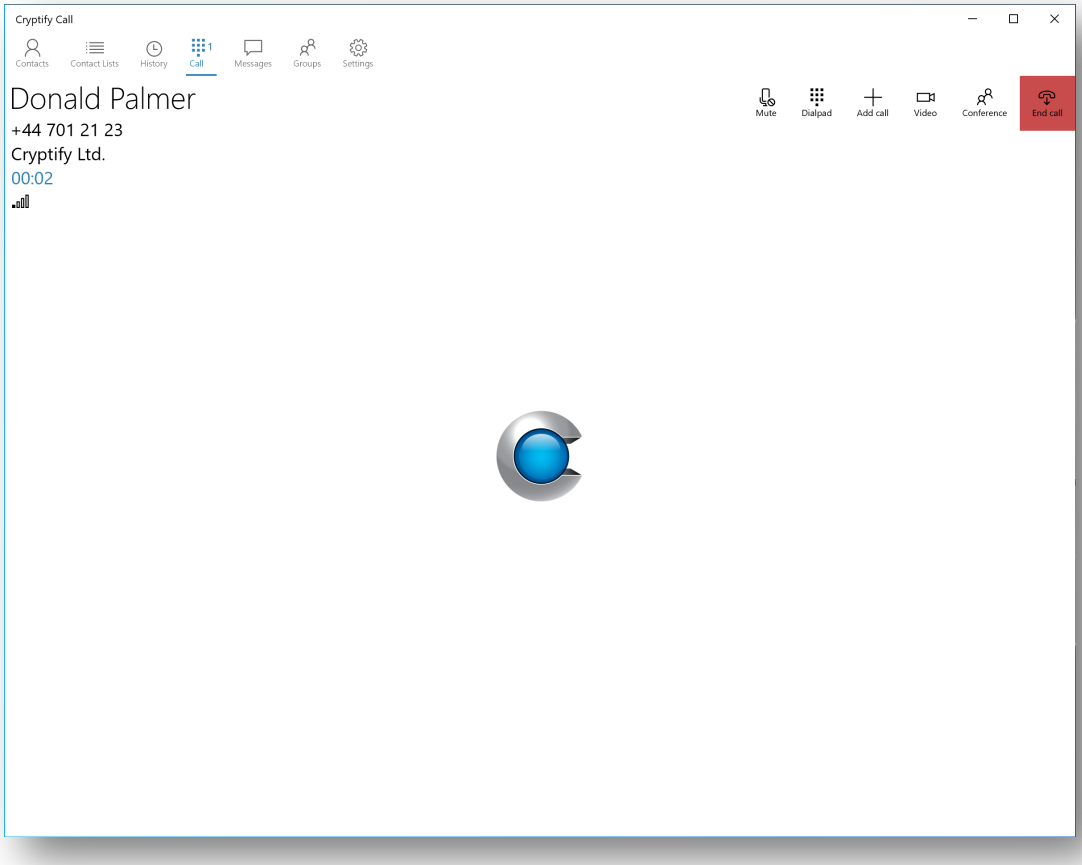
An incoming secure call will be displayed together with the number of the person who is calling and the Security Domain that person belongs to. If there is a contact available in the device for that number, the contact name is displayed instead of the number.



To accept the call, simply tap the notification.

During a call

When a secure call is active the user is presented with relevant information about the ongoing call, and can optionally upgrade to either a conference or a video call.



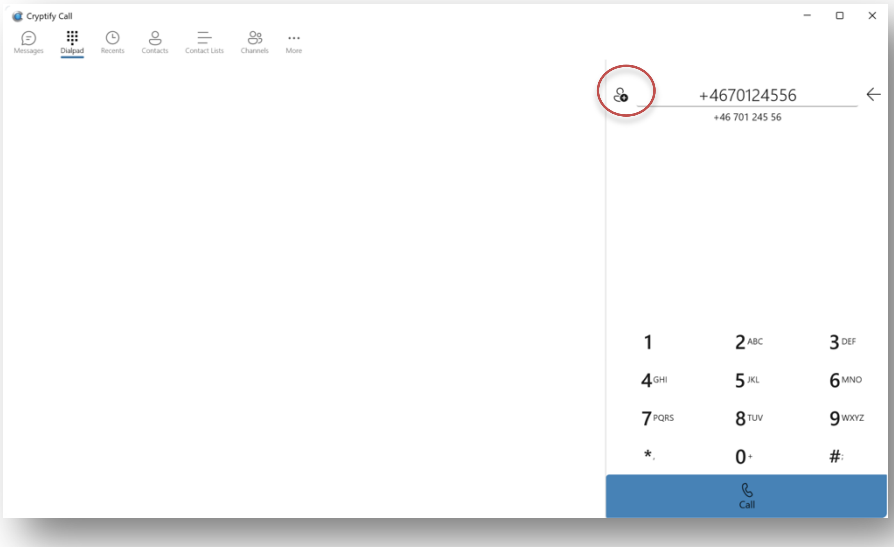
The Network Quality indicator shows the quality of the data connection, which might differ from the signal strength indicator provided by the phone. An example is cell congestions; where the signal strength might be excellent but no data can be transmitted over the cellular network.

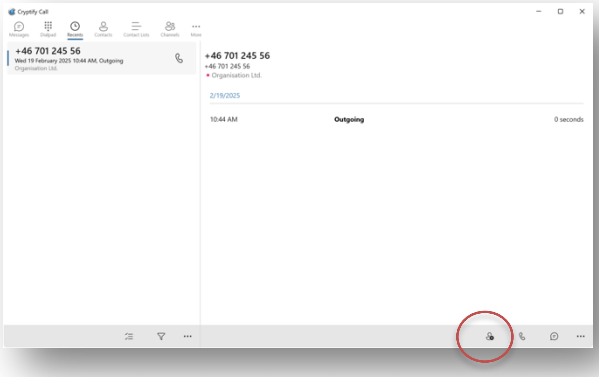
Video calls are automatically disabled when the other party, or an intermediate server, does not support video calls. Note that video calls have much higher bandwidth requirements and transfers much more data compared to audio calls.

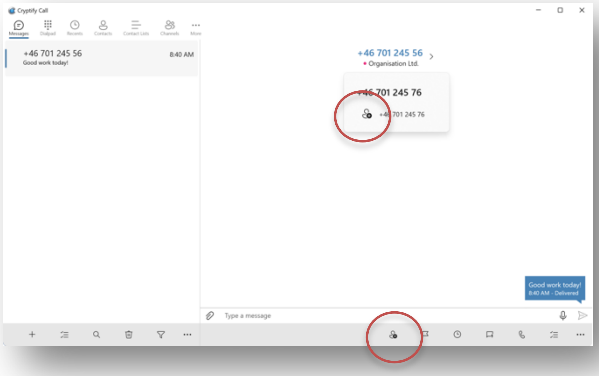
Personal contacts

Personal Contacts are displayed by clicking on “Personal Contacts” on the “Contact Lists” tab.

It is easy to create a new personal contact for a number that is not already in the contact book: simply click the button on the dial pad, the Call Details view or the conversation view.





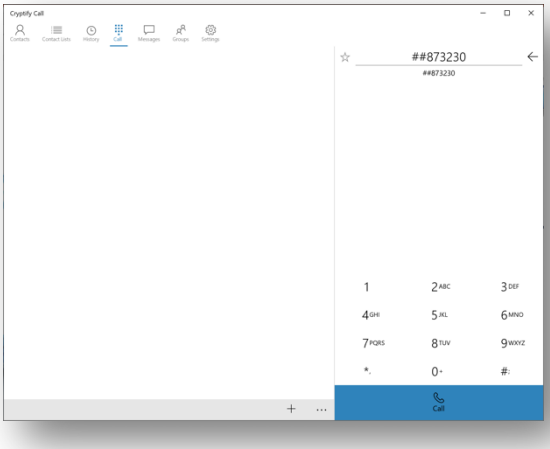


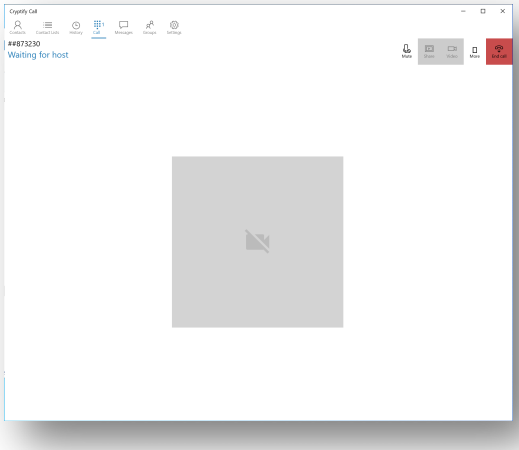
Conference

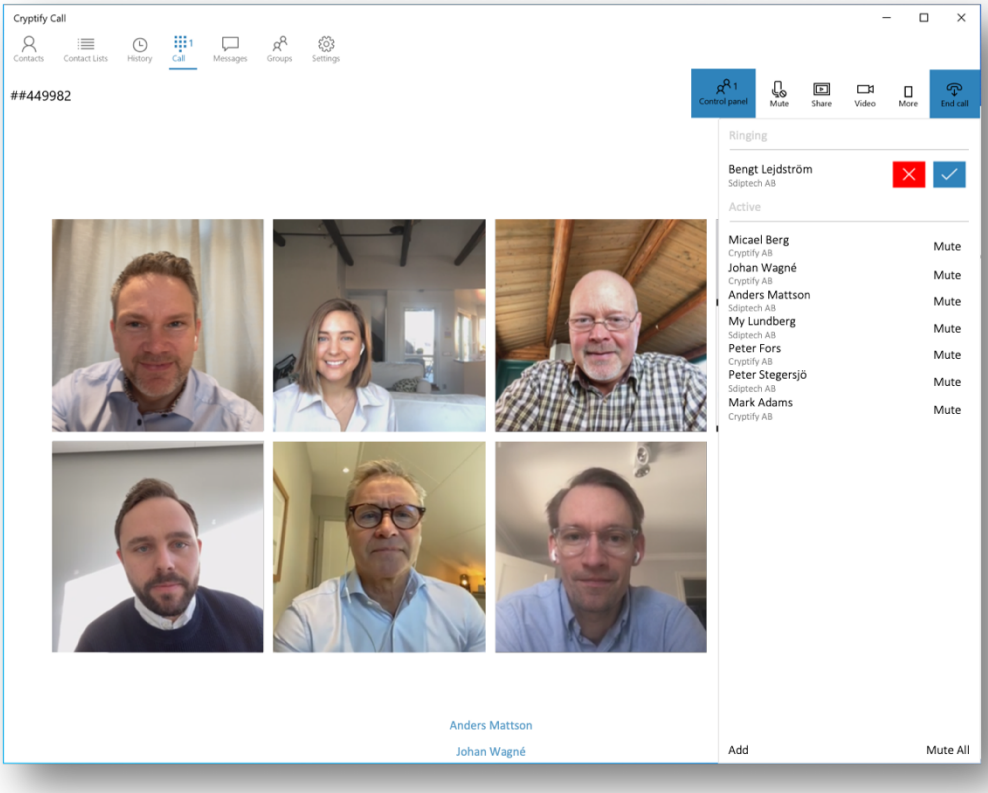
Cryptify Call supports secure, end-to-end encrypted conferences. Participating in a secure conference is just as easy as calling a regular conference bridge, and a *conference host* controls which callers are allowed to join the conference.

Dial in to a conference

To dial in to a conference, simply dial the six-digit number given to you by the conference host on the dial pad, prefixed by "##". While you wait for the conference host to accept your participation, the call screen displays "*Waiting for host*" and an ordinary ring back tone is played in the speaker. Once accepted by the host, the ring back tone stops and the duration timer starts.

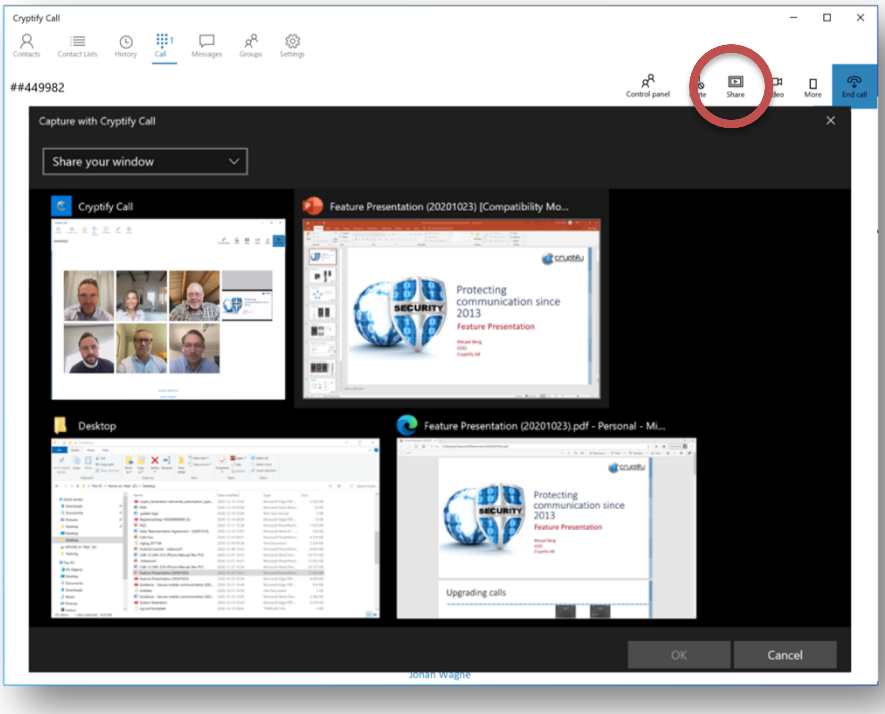




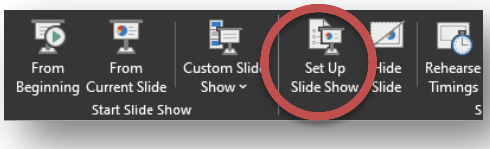


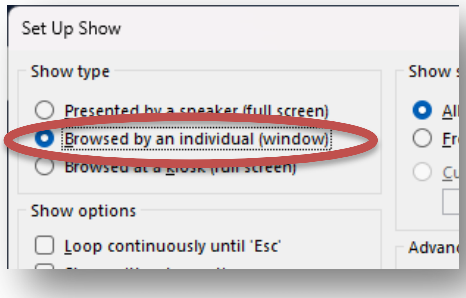
Screen sharing

Participants can share their screen during a conference by pressing the *Share* button.

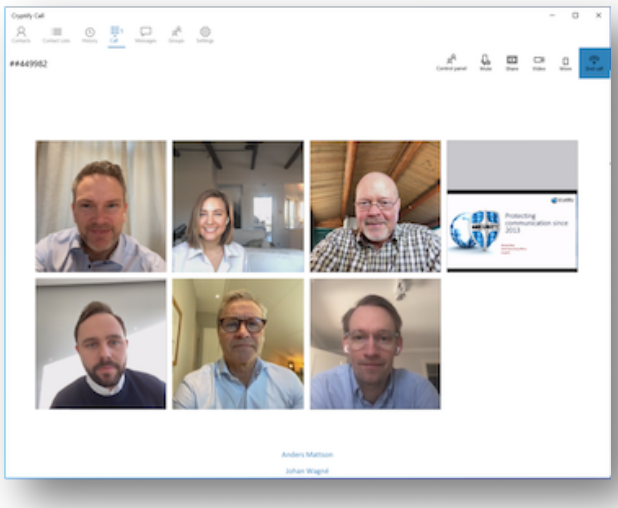


To share a PowerPoint presentation, please make sure you select “Share your display” to share your entire display. Alternatively, configure the PowerPoint presentation to be presented in a window by clicking “Setup Up Slide Show” on the “Slide Show” tab and selecting “Browsed by an individual (window)” as the “Show type”.





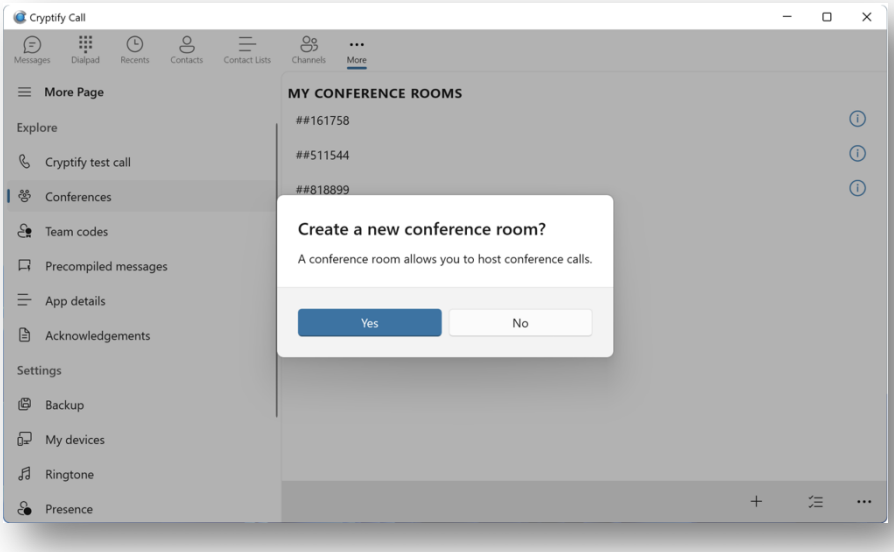
Shared content from other participants will be presented in their video tile. Pressing on a video tile will open a dedicated windows for that participant.



Hosting a conference

To host a conference, you must first create a *conference room*. A conference room is identified by a six-digit number, which the system automatically generates. Once a conference room has been created, it can be used indefinitely.

To create a conference room, select *Conferences* on the *Setting* tab, tap the "+" button and confirm the creation. A new conference room is then created and assigned a randomly selected number, which is used by participants to join the conference.



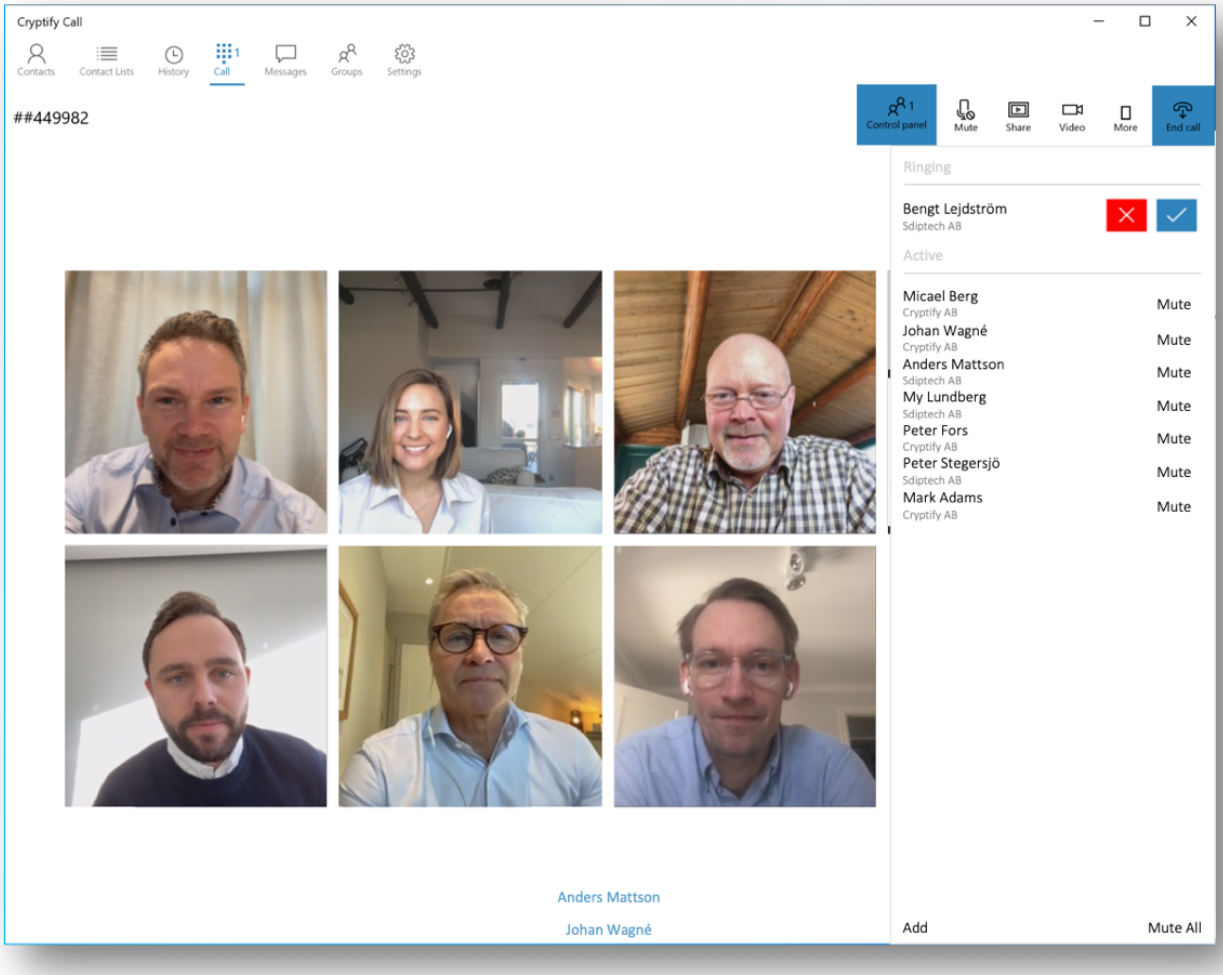
If desired, you can create multiple conference rooms and use them for different meetings, but you can only host one conference at a time.

The conference room number is distributed to the participants, along with the date and time for the conference. As the conference room number plays no role

in the security of the conference, the number can be distributed to the participants in any form, for instance via email or by using a shared calendar.

When the conference should begin, the host simply dials the conference room number on the dial pad, prefixed by "##", or uses the call button in the list of conferences.

The host manages the conference using the *Control Panel*, where the host can admit, invite and mute participants.



In addition to participants dialing into the conference, the host can invite participants using the *Add* function in the *Control Panel*.

Accepting a caller into a conference is a one-way process, and it is not possible to force a caller to leave an ongoing conference. For this reason, users who have been accepted into the conference are also automatically accepted if they lose network connectivity and call into the conference again.

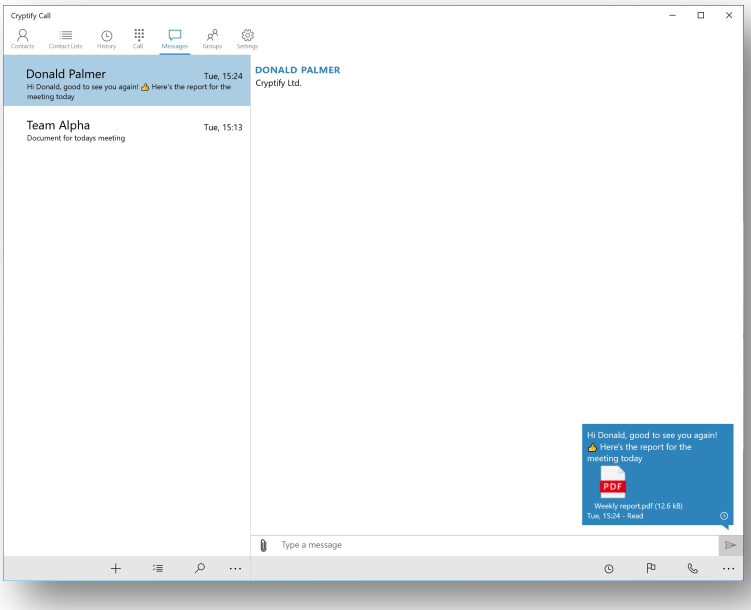
Note also that the entire conference is protected by a secret randomly generated by the conference host each time he or she (re-)enter the conference. If the conference host hangs up, the conference continues, but new participants cannot

be accepted. Should the conference host dial in again, the conference will start anew after a brief interruption whilst rekeying.

Best practice for allowing an external party, say, to participate only in the latter part of a conference is to maintain two conference rooms, and move to the second conference room when the external party should join.

Send a secure message

A conversation can be started from the *Messages* tab by clicking the new conversation button. A message can also be initiated by tapping the message button in the call history view or the contact details view.



To post a new message in an existing conversation, open that conversation and type the new message.

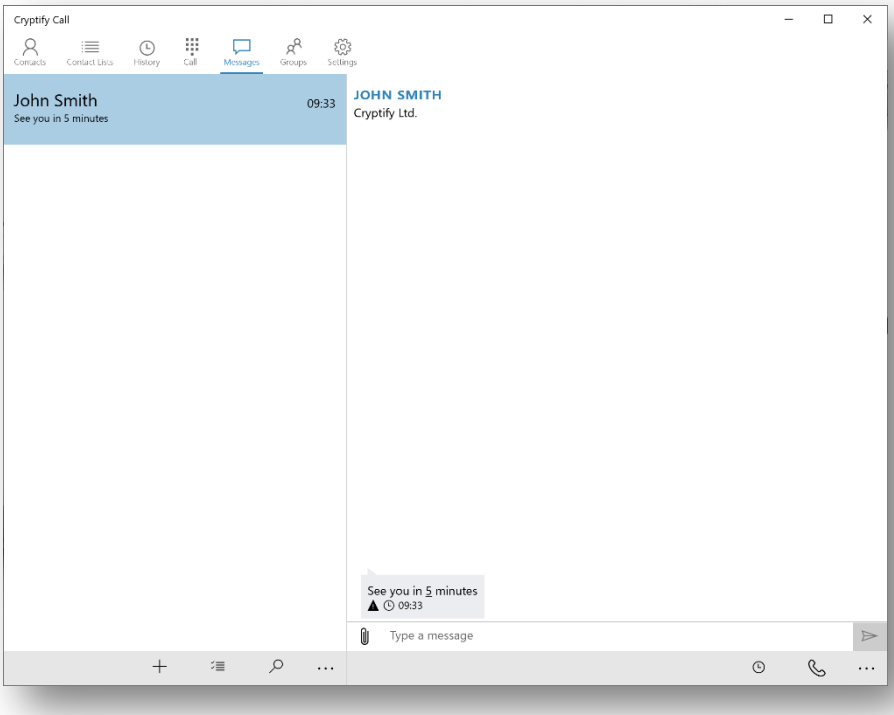
Files can be attached to a message by clicking the paperclip-button. Photos can optionally be resized before upload.

If configured by the management system, message expiry can be configured by clicking the clock.

The status of an outgoing message is displayed next to the timestamp:

- *Sending* – the message is being uploaded to the server.
- *Sent* – the message has been transferred to the server.
- *Notified* – iOS recipients only. The recipient has been notified of the message.
- *Delivered* – the message has been delivered to the recipient.
- *Read* – the recipient has opened the conversation.

- *Failed* – sending the message failed; right click the message and select "Status" for more information or "Resend" to immediately try again.

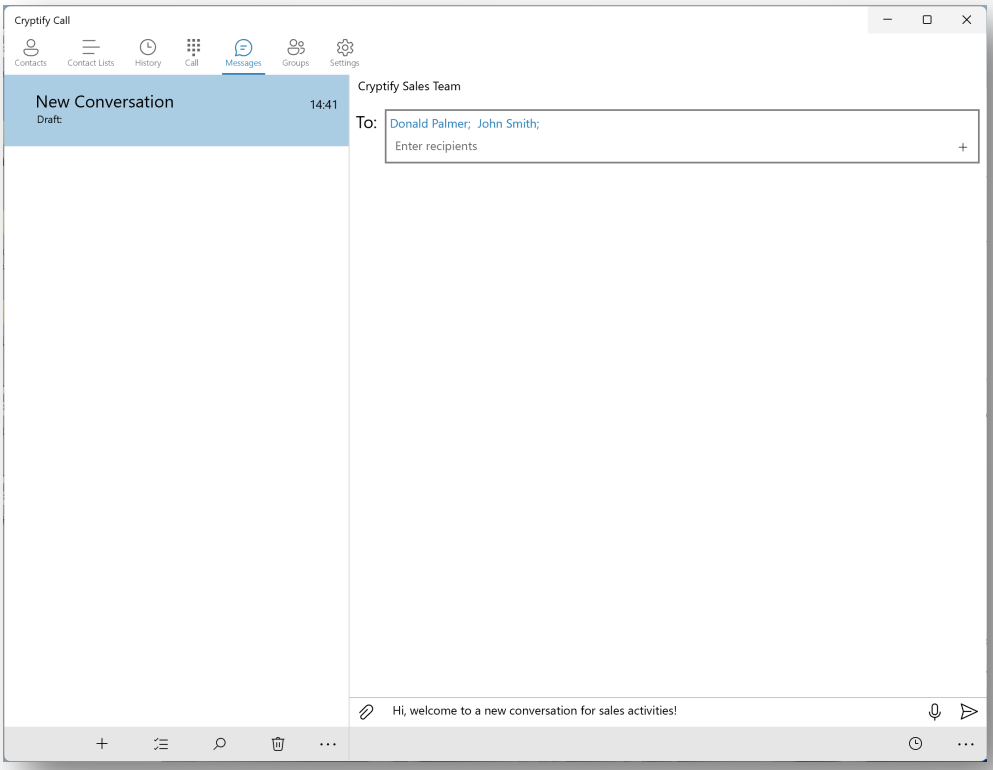


To show the sender's compose time of an incoming message, right click the message and tap *Status*. If this timestamp differs more than 5 minutes from when the message was received, a warning icon is shown.

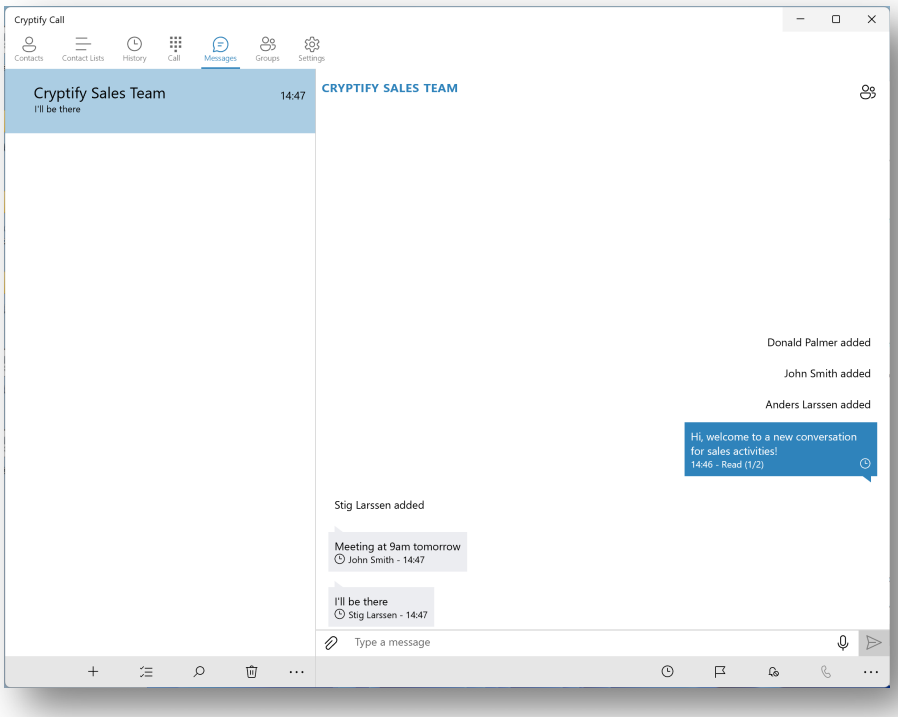
Groups

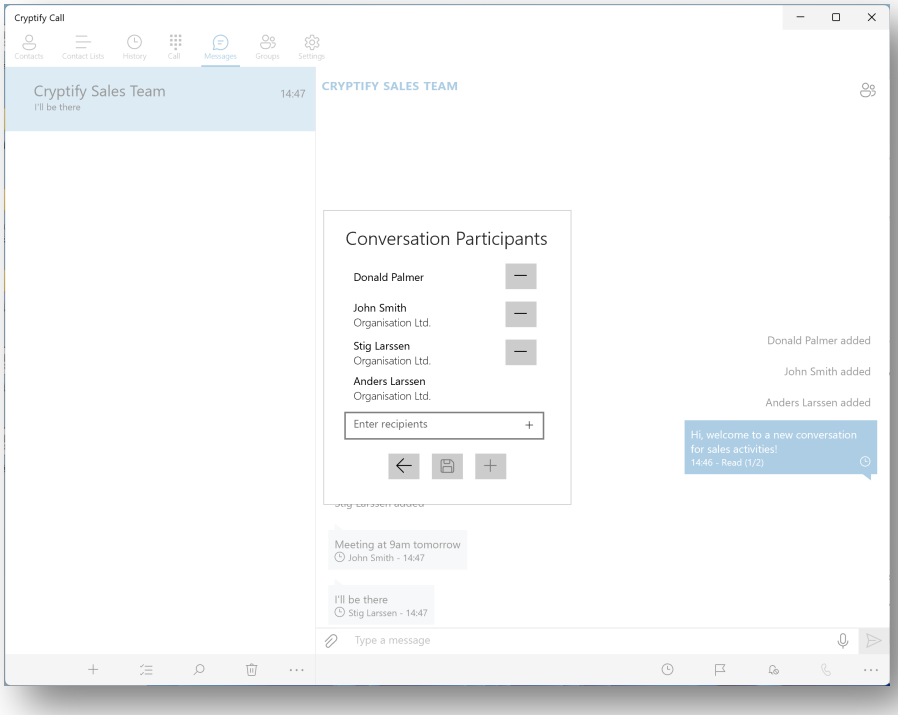
Setting up a group conversation is as easy as sending a regular text message. The *instant group conversations* replace the *managed groups* concept found in older versions of Cryptify Call.

To start a new *instant group conversation* simply click the new conversation button and add the recipients. If more than one recipient is added an *instant group conversation* is created and a *Subject* field is presented.



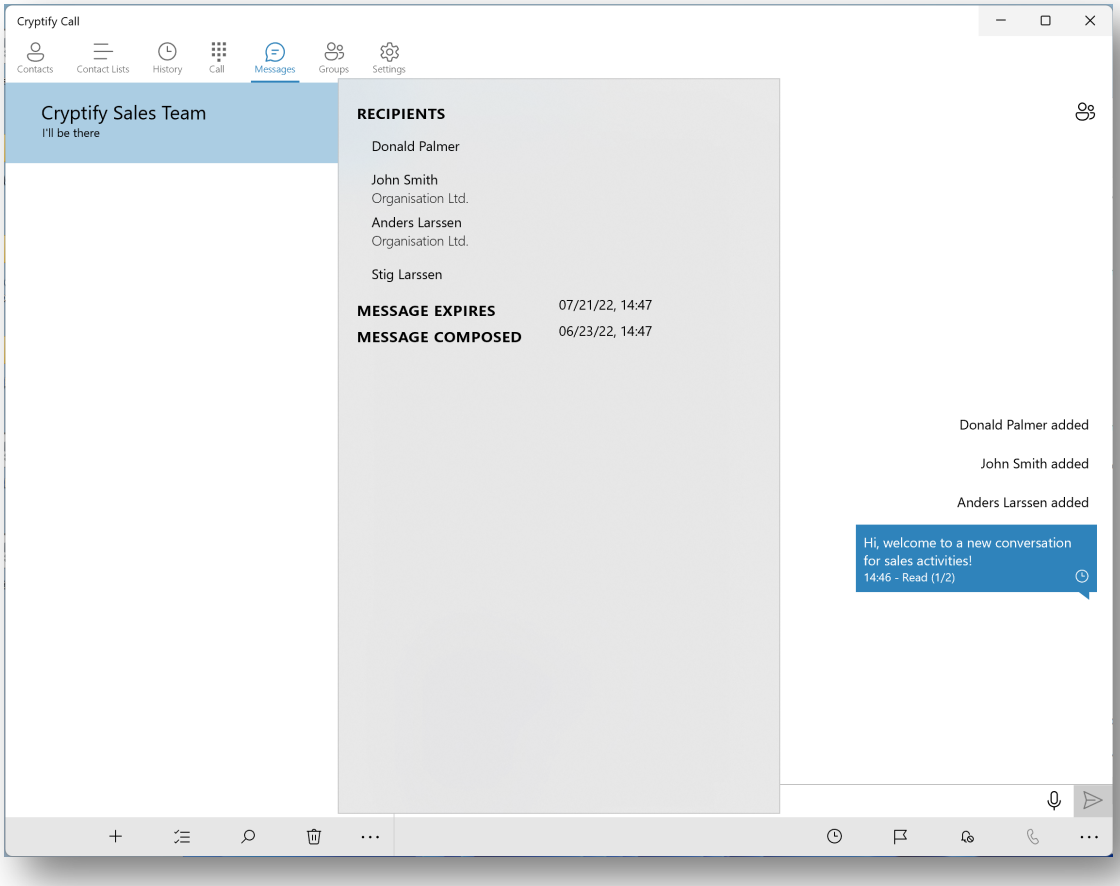
To add and remove recipients from the group conversation select the group icon in the top right corner.





Each received message is marked with the identity of the sender as well as a timestamp of when the message was received. The history of added and removed are presented in the conversation.

To view the delivery status a posted message, right click on the message to bring up a pop over menu and select *Status*



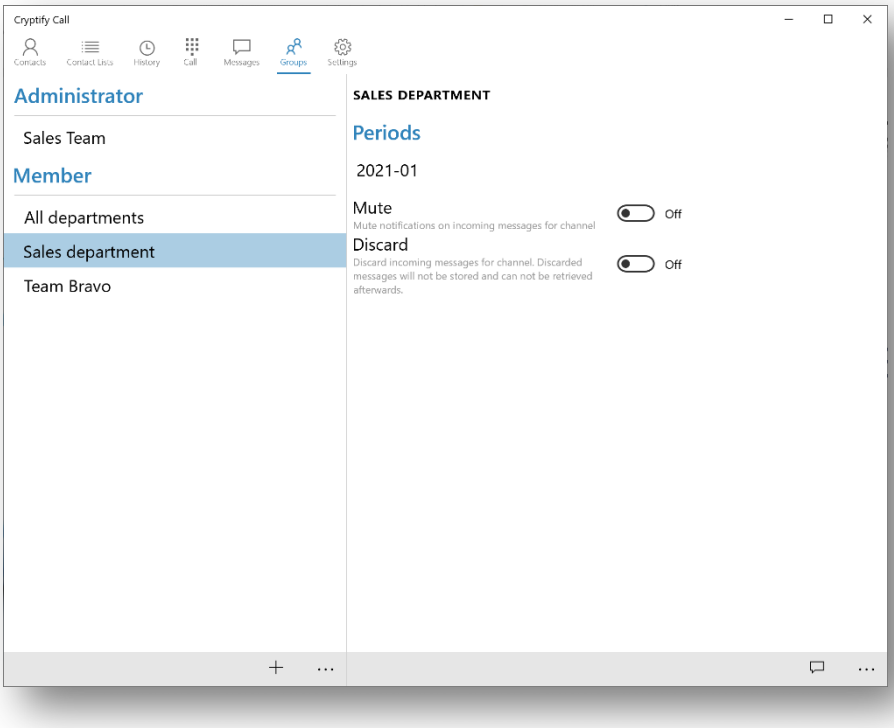
Channels

In addition to Groups, Cryptify Call also supports so called *Channels*, which are message groups that are centrally managed by the CMS operator. Channels are particularly well suited for large groups, such as everyone in an organization, and there is no extra step where the user accepts or declines membership.

Channels are shown in the list of Groups under "Member" and work just as regular message groups. However, as channels supports thousands of users, it is for performance reasons not possible to see when a particular user has received or read a message.

By default, and just as for regular text or group text messages, each incoming message to a channel renders a notification. It is, however, possible to *mute* a channel, which prevents notifications on incoming messages to that channel. Only the notification is blocked, ensuring that the messages can be read if they are decrypted within 14 days (unless prevented by message expiry).

It is also possible to configure that incoming messages to a channel should be discarded immediately when received, without ever being decrypted or notified. Discarded messages are permanently deleted and cannot be retrieved at a later time.

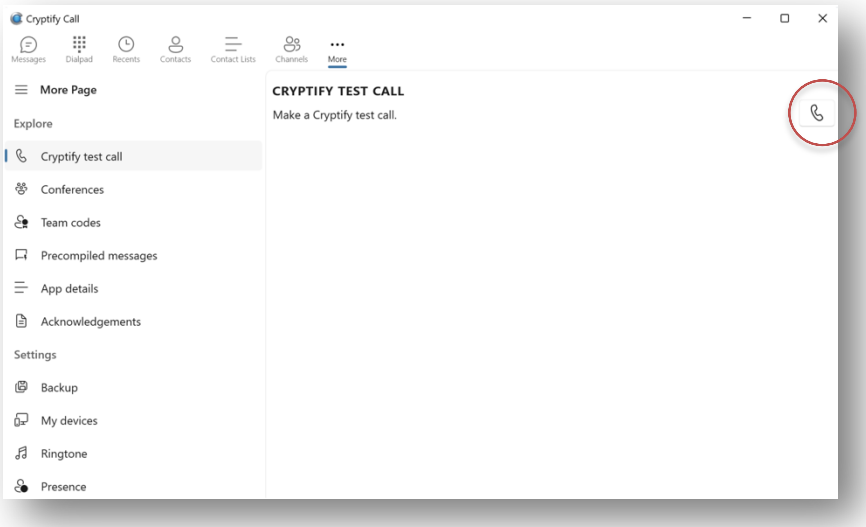


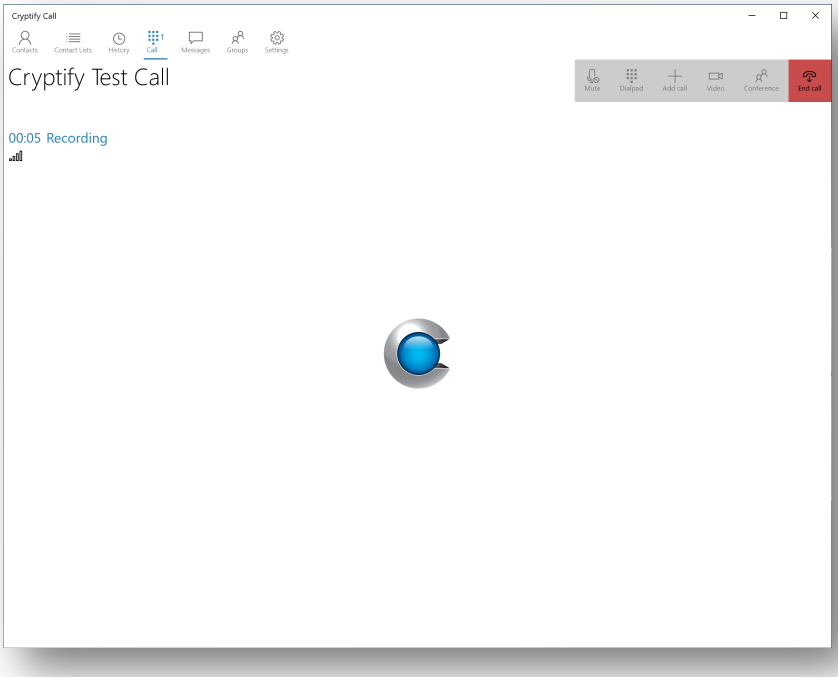
If a device is to be offline for an extended period of time, it is recommended to configure any high traffic channels to discard incoming traffic. Otherwise, once the device goes online, the app may become unresponsive while it decrypts the messages that have been queued up.

The channel settings are also visible under Settings in the command bar.

Test Call

A user can make a *test call* to verify the call quality: select “Settings” on the “More” tab, select *Cryptify test call* and click on the call button.





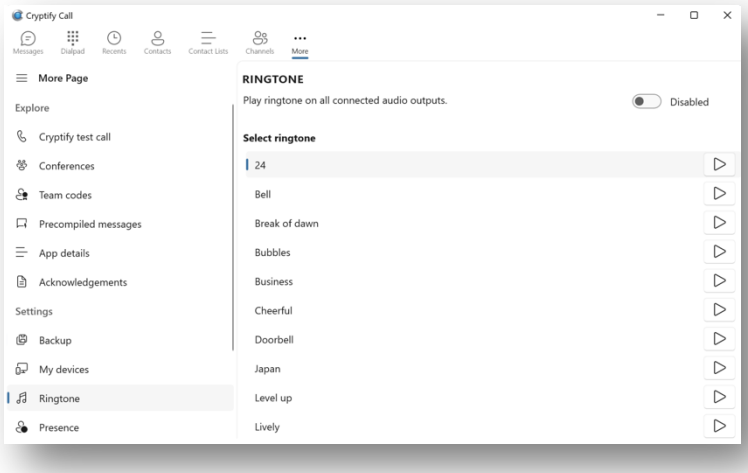
During a Cryptify Test Call the quality of the network as well as connected audio peripherals, e.g. attached conference phone or headsets, are tested.

Configuration

Setting

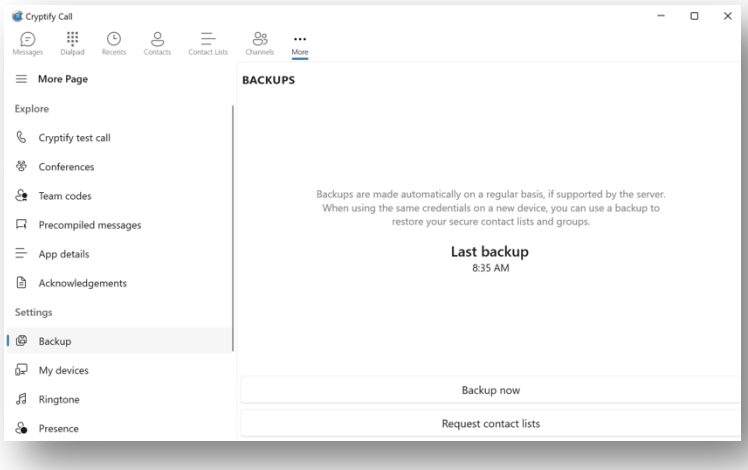
Ringtone

The user can select from a list of different ring tones.



Backup

The app will automatically create a backup and deposit on the CRS. The backup is protected with a key derived from the update key, i.e. as long as the update key is unchanged the backup can be used to restore settings on a new device.

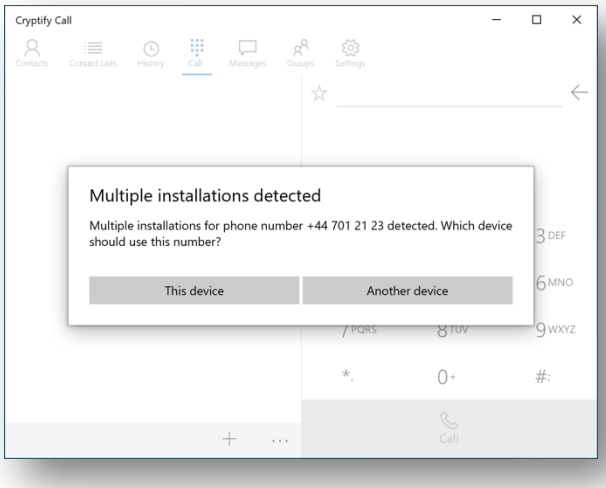


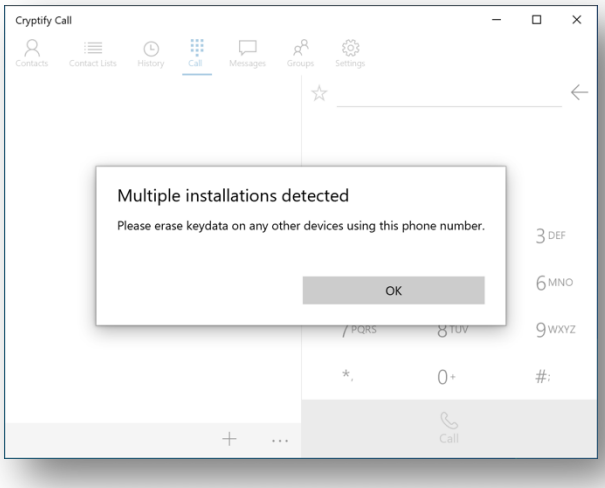
The backup contains the following data:

- Contact lists
- Group memberships

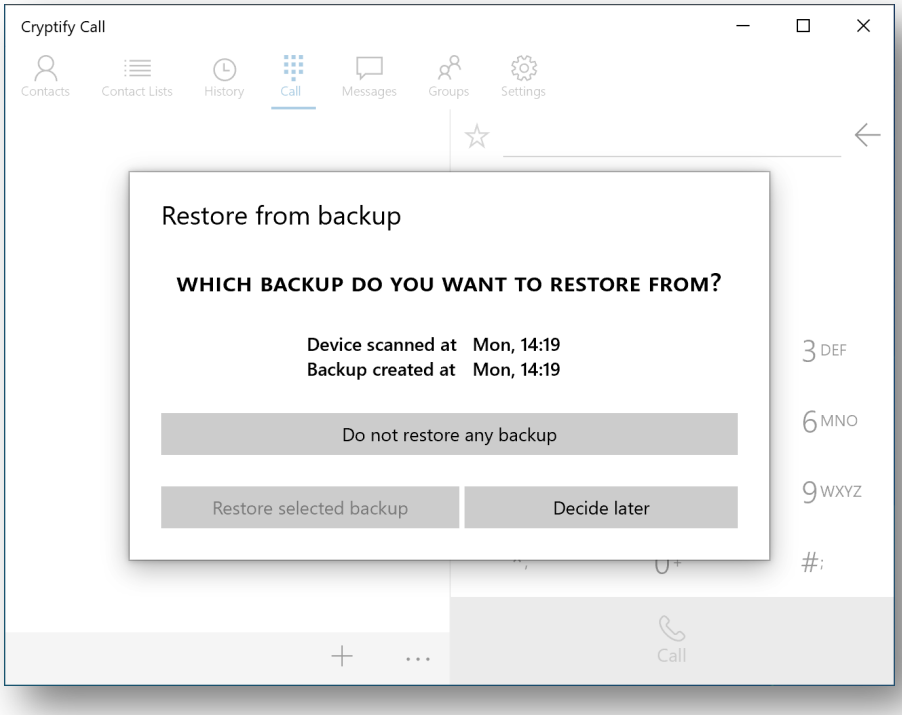
Restore

If the same QR code is scanned on separate device, e.g. when switching to a newer device, the app will detect that multiple installations are found for the phone number and will prompt the user decide whether to proceed with this phone number and hence assume ownership, or cancel the operation.





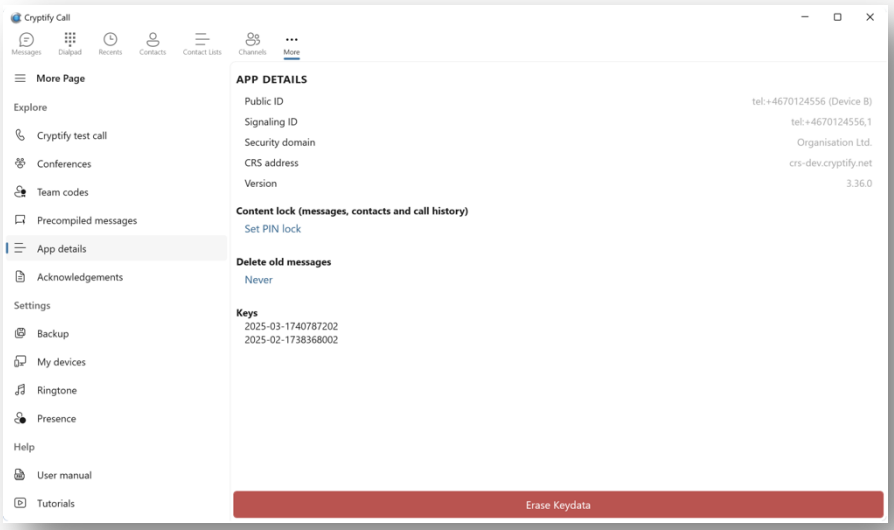
If continuing, available backups will be presented and the user can select to restore.



However, if the update key is changed between the backup and newly scanned QR code the restore operation will fail as the app cannot decrypt the content.

App details

The *App details* view on the *Settings* tab shows detailed information of the Cryptify Call application.



Name	Description
Public ID	This is the users public cryptographic identity
Security Domain	This is the identity of the Cryptify Management System (CMS) that has issued the cryptographic keys for the user
CRS Address	This is the Fully Qualified Domain Name (FQDN), or IP address of the Cryptify Rendezvous Server (CRS) serving the user
Keys	Valid keys are listed. There could be two keys during the grace period. Syntax is YYYY-MM-XXXXXXXXX, where YYYY-MM is the year and month the key is valid

NB! *Erase Keydata* will prompt the user to erase all content and settings for the Cryptify Call application! The app will not be usable until a new QR code has been scanned.

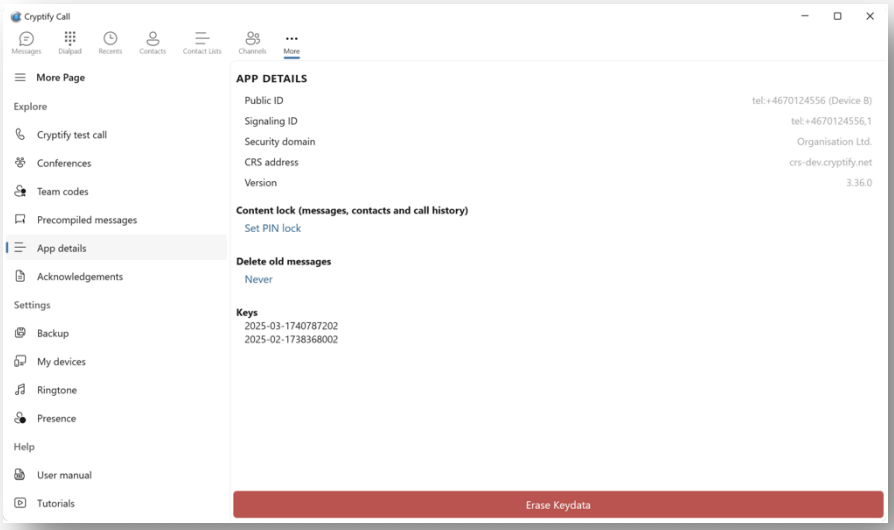
PIN lock

The message tab can be locked with a PIN code by tapping “Lock” and entering a 4 digit PIN code. If the PIN code is forgotten, the message tab can be unlocked with a PUK code available in the Cryptify Management System.

Manual key removal / replacement

This procedure is in case the keys should be deleted from the device, or if the CMS administrator decides to perform a manual key replacement. Normally keys are updated automatically without any user intervention.

In the *App details* view on the Settings tab, click *Erase Keydata* and press the *OK* button.



NB! Erase keydata will prompt the user to erase all content and settings for the Cryptify Call application, including stored messages, call history, and stored favorites!

Once the key data has been erased, new keys must be received by the user in the form of a QR code, see above.

Troubleshooting

Reason Codes

Unsuccessful call establishment

Reason Code	Description
Not Found	There is no match for the called number. Either the called number does not have a Cryptify Call subscription, or the called number belongs to another Cryptify Call domain not connected to callers' domain. To request another Cryptify Call domain to be connected / approved, please contact Your local Cryptify Call support.
Not Available	The called number is currently not connected to the system, e.g. when the phone is powered off, or in airplane mode, or if the called party have manually terminated the Cryptify Call application.
Busy	The called party declined the call, or is currently occupied by another call, either an ordinary call or a secure Cryptify Call.
Communication Failure	This could be caused by an incompatible software version. Please make sure Your and called party's Cryptify Call applications are up-to-date. If this happens repeatedly please contact Your local Cryptify Call support.
Authentication Failure	Cryptographic failure. Please contact Your local Cryptify Call support!
No Answer	The called party has not answered the call within one minute.

Dropped call

Reason Code	Description
Network Failure	No audio received the last 30 seconds. The network problem could be either you, or the other party. This problem is normally triggered when going out of cellular coverage, e.g. a building, underground, etc.

Unsuccessful messaging

Reason Code	Description
Failed, user not found	There is no match for the recipient number. Either the recipient number does not have a Cryptify Call subscription, or that number belongs to another Cryptify Call domain not connected to callers' domain.

	To request another Cryptify Call domain to be connected / approved, please contact Your local Cryptify Call support.
Failed, bad network	Several failed attempts to send the message. This is caused by unstable network connection. If You are using Wi-Fi, please disable Wi-Fi and try again. If this happens repeatedly please contact Your local Cryptify Call support.
Failed to authenticate	Cryptographic failure. Please contact Your local Cryptify Call support!
Failed, invalid	This could be caused by an incompatible software version. Please make sure Your and called party's Cryptify Call applications are up-to-date. If this happens repeatedly please contact Your local Cryptify Call support.
Failed, no support	This could be caused by an incompatible software version. Please make sure Your and called party's Cryptify Call applications are up-to-date. If this happens repeatedly please contact Your local Cryptify Call support.