Manual

Cryptify Call application for iPhone

Table of Contents

Scope

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

Target audience is end users of Cryptify Call.

Introduction

Cryptify Call voice and messaging encryption for iOS 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).

Note! Cryptify Call is a Voice over IP (VoIP) solution and require an Internet connection to work, either Wi-Fi or Cellular Data. In case of travelling abroad, please make sure *Data Roaming* is enabled on the cellular service!

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 iOS 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 iOS devices, they can install Cryptify Call application on the device by opening the App Store app  , downloading and installing the Cryptify Call application by selecting "Cryptify Call" from the App Store search tab and clicking the install button.

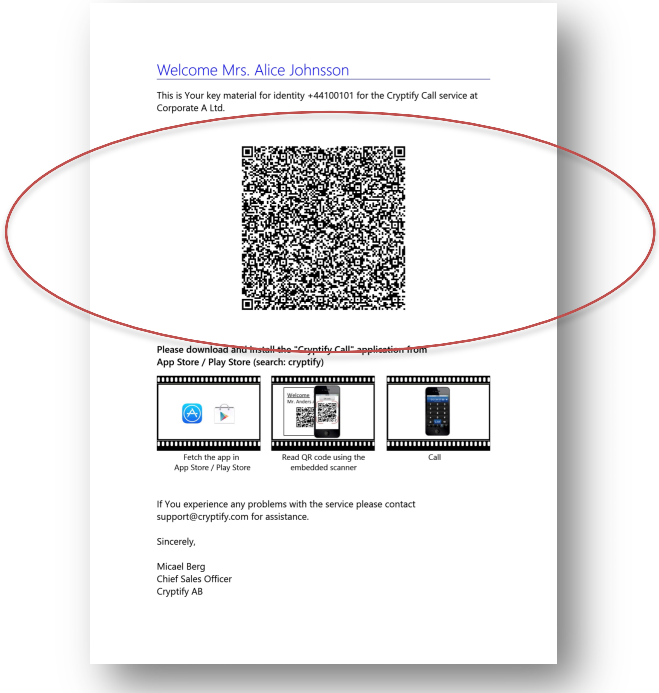
Otherwise, if the Cryptify Call app is not installed, users should ask their administrators to provision it for them.

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.



Welcome Mrs. Alice Johnsson

This is Your key material for identity +44100101 for the Cryptify Call service at Corporate A Ltd.

Please download and install the "Cryptify Call" application from App Store / Play Store (search: cryptify)

Fetch the app in App Store / Play Store

Read QR code using the embedded scanner

Call

If You experience any problems with the service please contact support@cryptify.com for assistance.

Sincerely,

Micael Berg
Chief Sales Officer
Cryptify AB

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

Permissions

During the provisioning the Cryptify Call will request permissions to use:

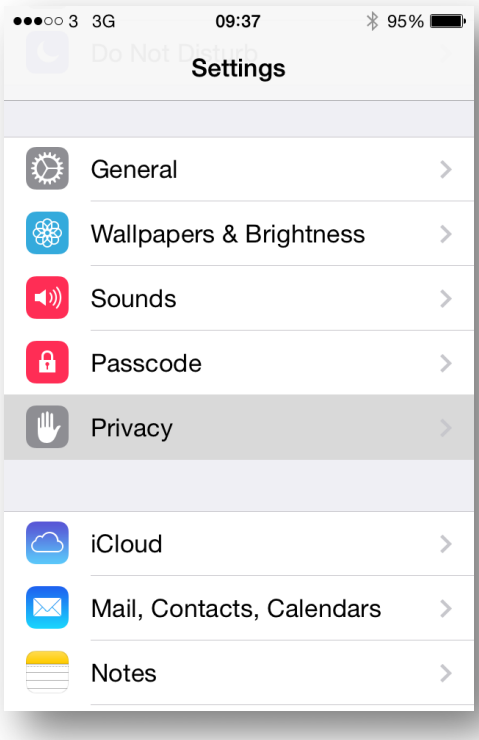
Camera
The camera is need to read the QR code as well as for video calls.

Microphone
The microphone is needed to record voice during calls.

Contacts
Cryptify Call uses the mobile phone number as contact and security identity. To be able to use the existing contact information please allow Cryptify Call access to the address book.

Cryptify only uses the contact information to show a name instead of a phone number and to allow users to easily call phone number in their address book. For the avoidance of doubt; Cryptify only uses the contact information locally on the device, and for no other purpose than what is declared above.

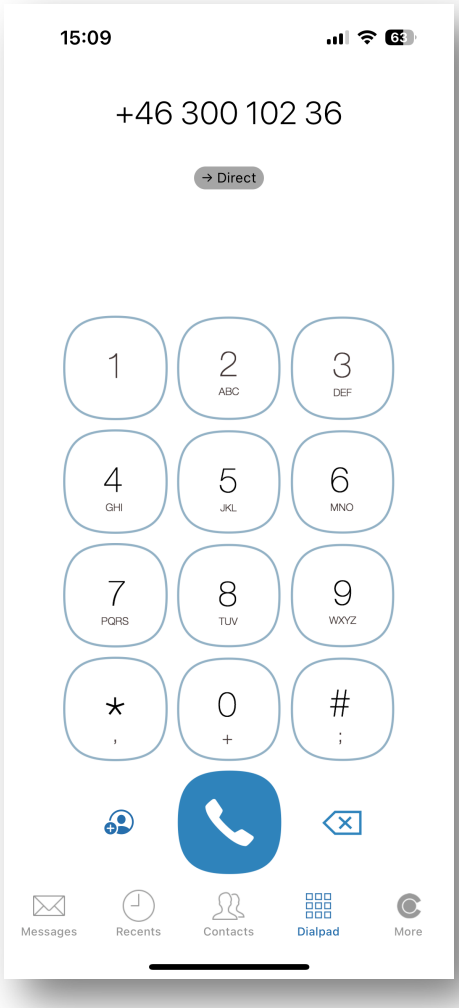
Permissions can be altered at a later stage in the *Privacy* menu in the *Settings* app. 



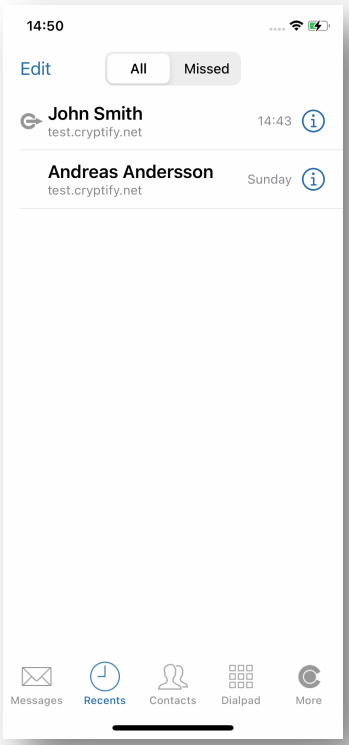
Make a secure call

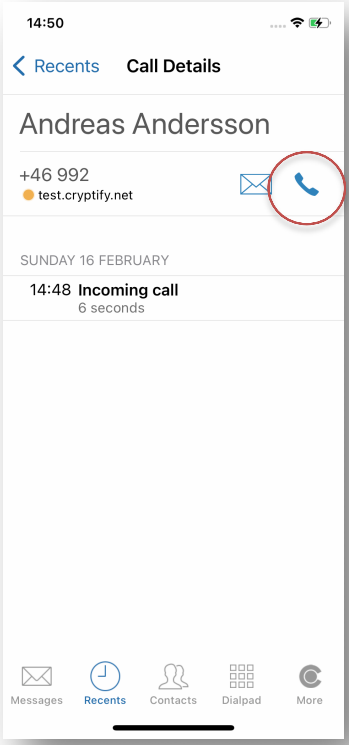
Making a secure call is as easy as dialing the number of the person to call, and normally the number is the same as the mobile number for that person. The only requirement is that both parties use Cryptify Call.

The number can be entered using the keypad.

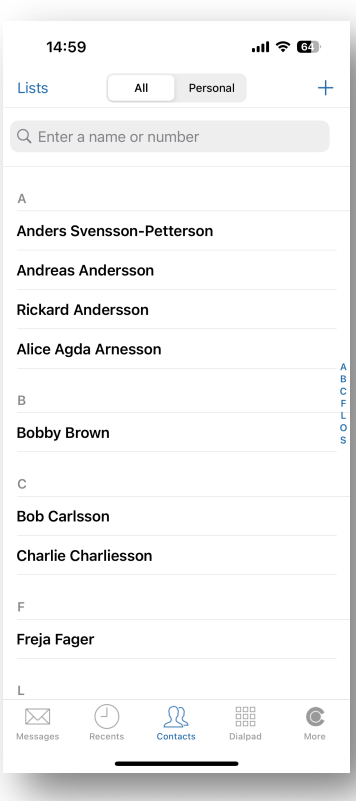


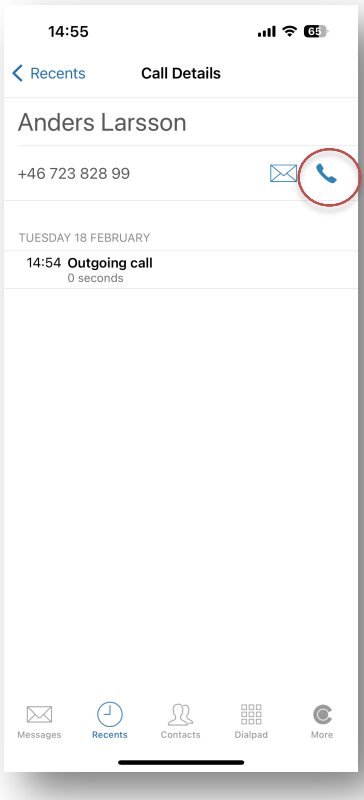
An alternative method to make a secure call is to use the *Recents view* where the call log is listed. A secure call can be initiated by tapping an entry in the list. Tapping the info-button opens the *Details view*, which offers a second way to initiate the call.





The application also has a Contacts tab, showing all contacts available to the app. Contacts are sourced from the contact book stored on the phone and from distributed contact lists as well as from the personal contact list. A secure call can be initiated from the *Details view* of a selected contact.

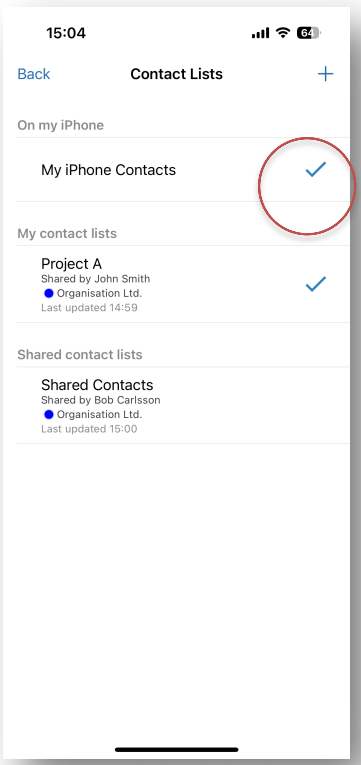


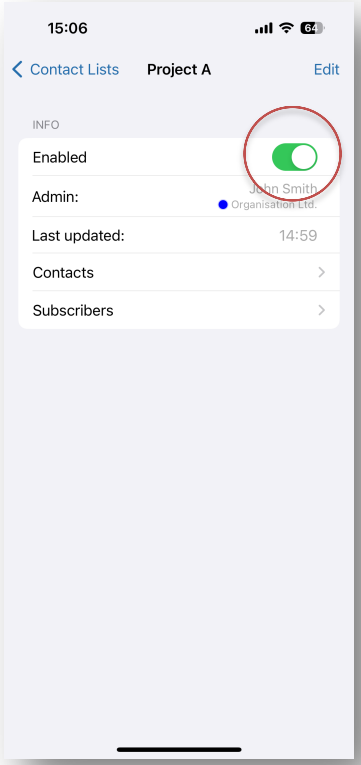


All available contact lists are shown under “Lists”. Lists that are enabled – that is, those lists that populate the “Contacts” tab and are used as a source of contact information – are marked with a checkmark. To enable or disable a list, tap the list and toggle the “Enabled” switch.

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

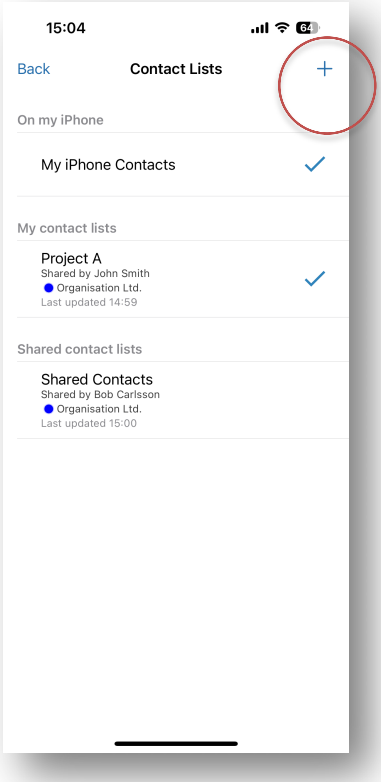
Only enable or import lists from trusted and verified sources. Importing or activating lists from untrusted or unknown sources may compromise the security of the application.

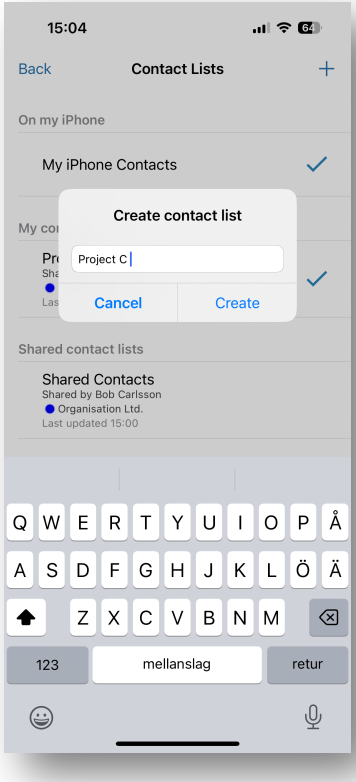




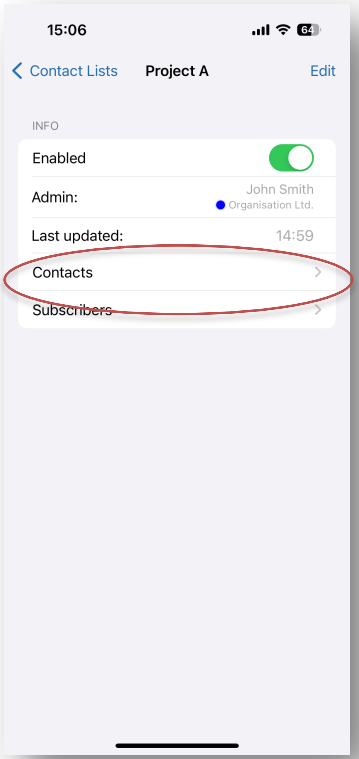
Creating and sharing contact lists

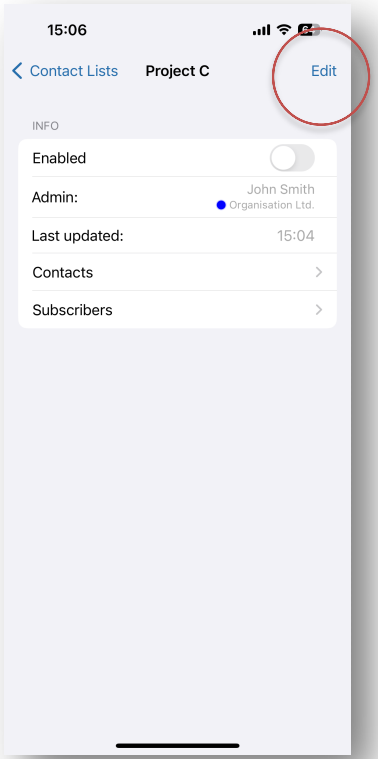
Contact lists can be created within the Cryptify Call app, and optionally shared with other users in a secure manner. To create a new contact list, tap the "+" button in the "Lists" view and enter a name for the contact list.



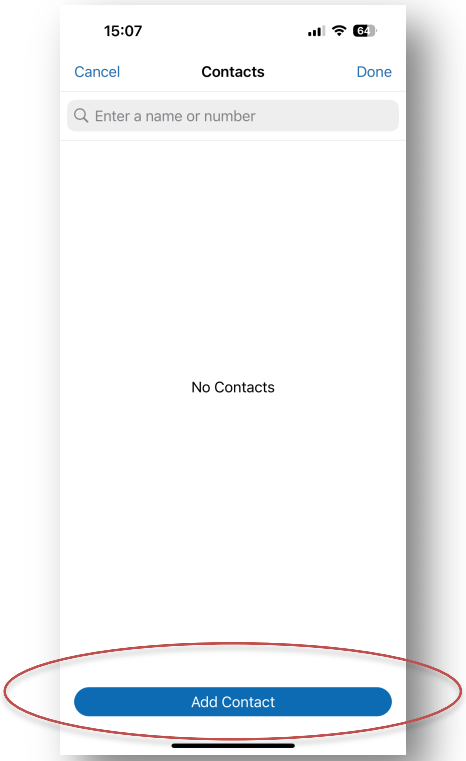


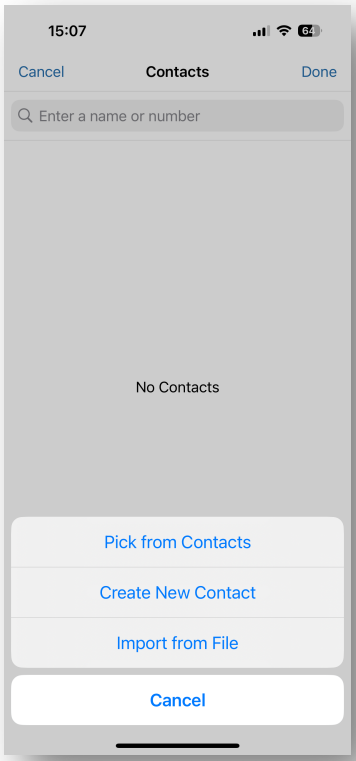
To modify the entries of the contact list, tap “Contacts” and then “Edit”.





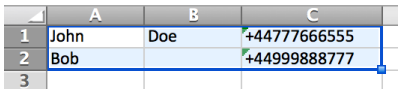
To add a new contact, tap “Add Contact” and select either “Pick from Contacts” to copy existing contacts from other contact sources – including the native phone book – or “Create New” to manually create a new contact list entry.



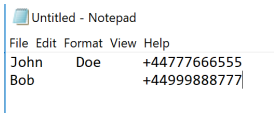


It is also possible to import contacts from a TSV (tab separated values) file by clicking the import button and selecting “Import from file”.

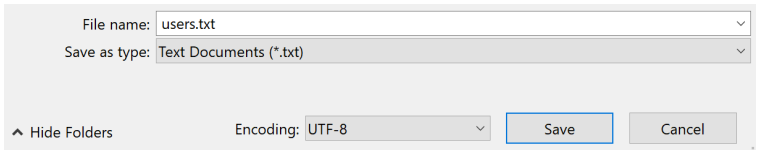
The file should have UTF-8 (or ASCII) encoding with three columns per line, specifying the first name, the last name and the phone number. It is easy to create such a file using Excel and Notepad (or TextEdit on macOS).



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

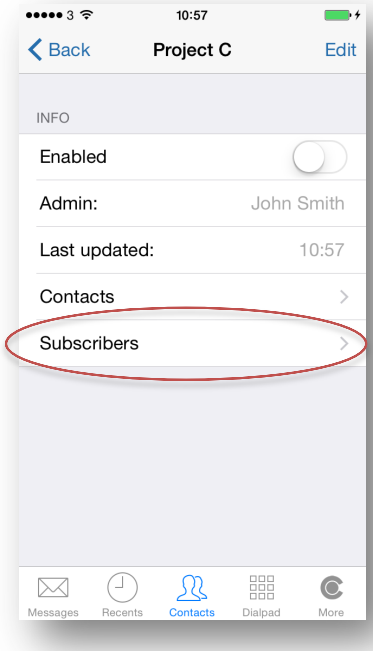


Step 2: Paste the result into a new document in Notepad. (If using TextEdit on macOS, select Format > Make Plain Text before pasting the data.)



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

Similarly, the list of subscribers – that is, those who will receive the contact list – is edited by tapping “Subscribers”. As before, only a contact list that is marked as “Enabled” is used as a contact list source, but even disabled lists are distributed to subscribers.



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.

The way the incoming call is displayed depends on whether Cryptify Call is active in the foreground or not.

Cryptify Call app active in the foreground

If the Cryptify Call app is open the incoming call will be displayed as

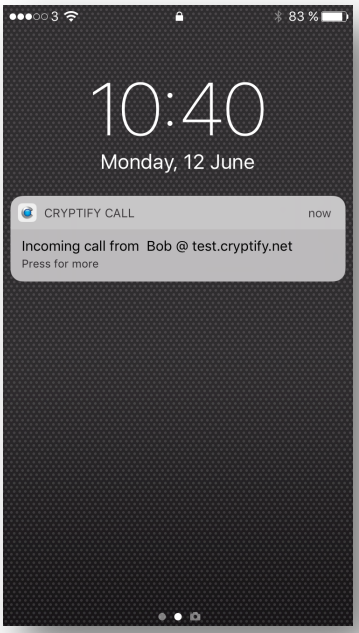
The call is accepted by clicking on the *accept button* to the right, or rejected by clicking on the *hang-up button* to the left.

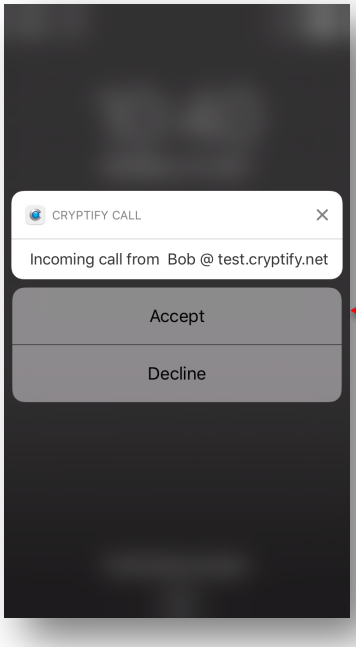
Locked or suspended device

In case the device is locked or suspended, incoming calls will be displayed using an iOS notification.

To accept the call, swipe left or Press on the notification itself and tap "Accept". To decline the call, tap "Decline" instead.

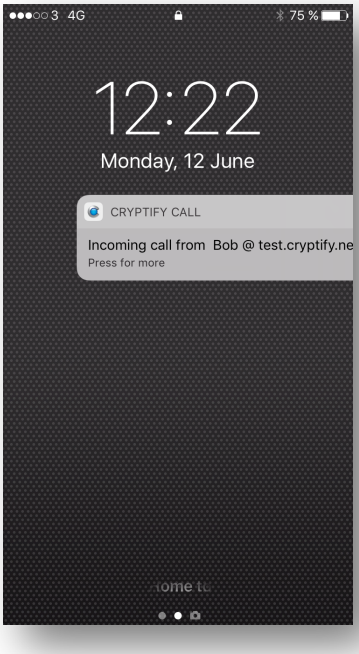
3D Touch





TAP

Alternately, swipe right on the notification to accept the call



SWIPE

(If the "unlock device" button is swiped the Cryptify Call must be opened manually to answer the call)

<u>Other app active</u>

If another app is active, or if the springboard is shown, the notification is displayed as:

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 add a third party to the call.

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

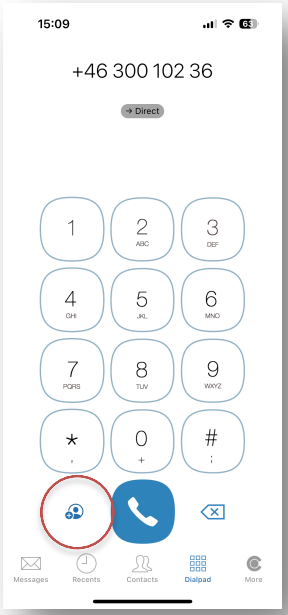
Multitasking

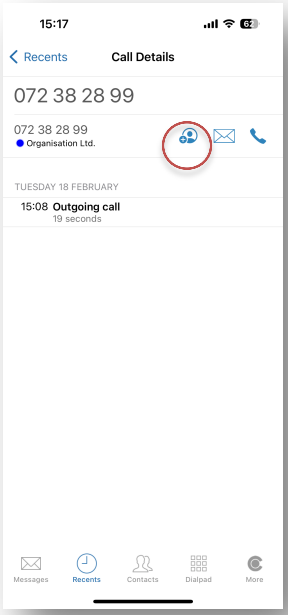
To access the rest of the app during a call, tap the “Hide” button to dismiss the call screen without ending the call. This makes it possible to use other parts of the app during an ongoing call.

A green banner on the top of the screen indicates that a call is active. To return to the call screen, simply tap the banner.

Adding personal contacts

A *personal contact* can be created by tapping the *Add personal contact* button for a phone number that is not already in a contact source, or by using the "+"-button in the Contacts tab.



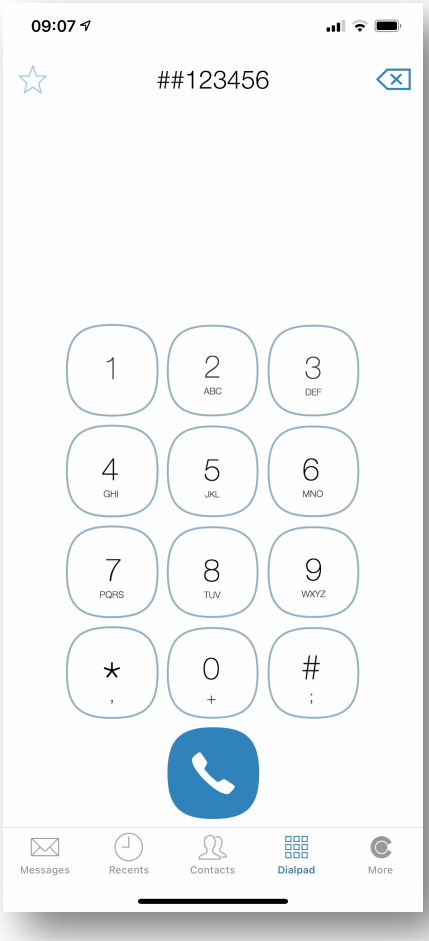


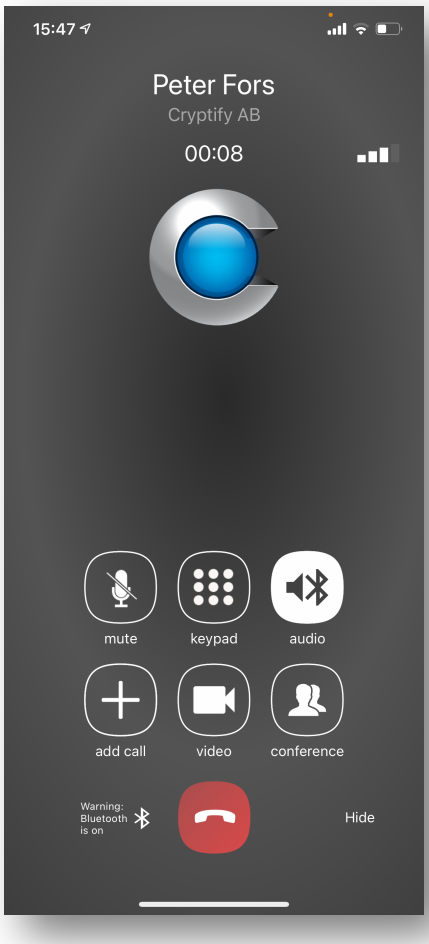
Conference calls

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

Dial in to a conference

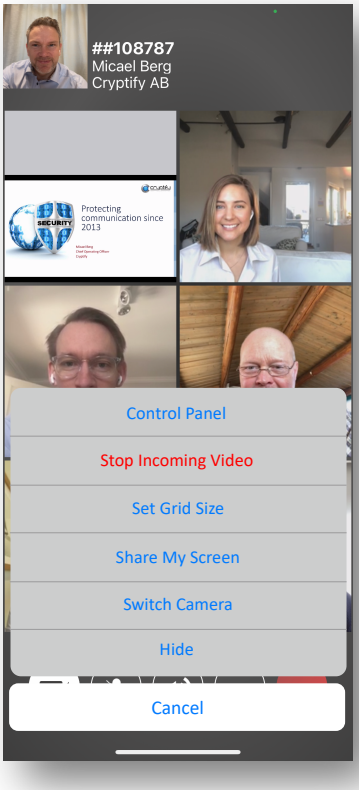
To dial in to a conference, simply dial the six-digit number given to you by the conference host on the dial pad, prefixed by "##". While you wait for the conference host to accept your participation, the call screen displays "Waiting for host" and an ordinary ring back tone is played in the speaker. 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 selecting “Share My Screen” from the *more* menu.

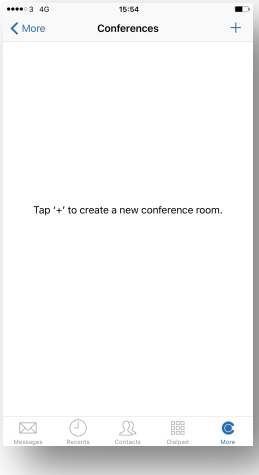


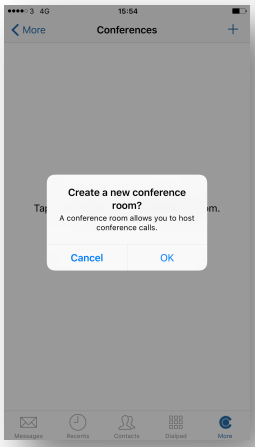
Shared content from other participants will be presented in their video tile. Pressing on a video tile will present that participant in in full screen.

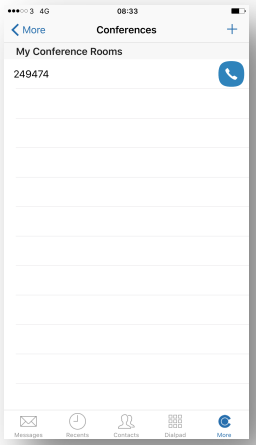
Hosting a conference

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 “More” 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.





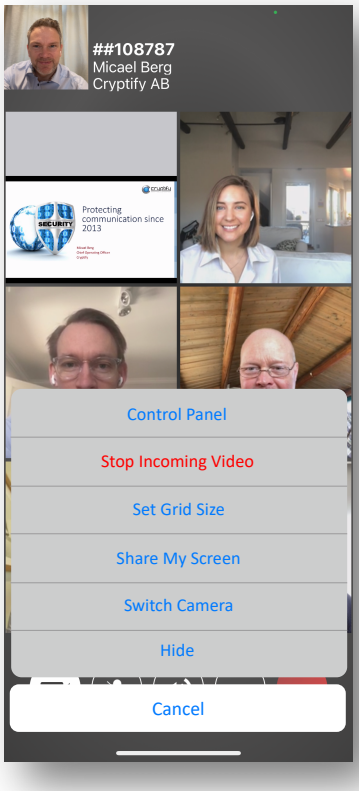


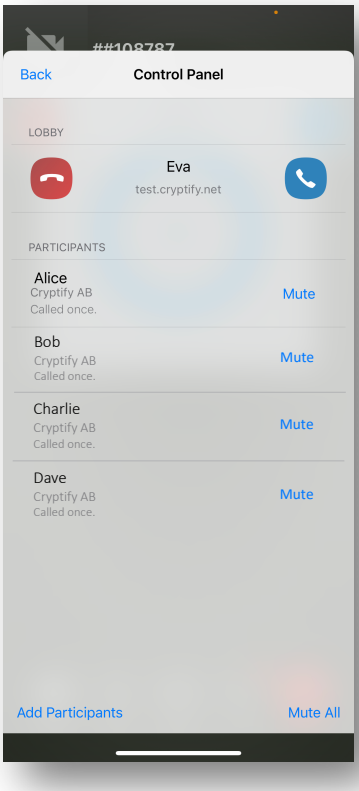
If desired, you can create multiple conference rooms and use them for different meetings, but you can only host one conference at a time. To remove a conference room, simply swipe right and tap “Remove”.

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 Participants* function in the *Control Panel*.

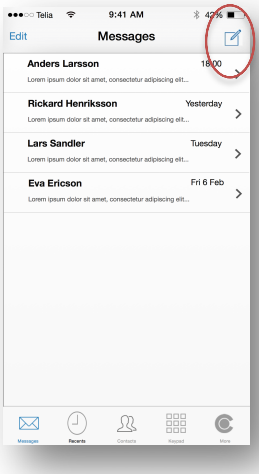
Accepting a caller into a conference is a one-way process, and it is not possible to force a caller to leave an ongoing conference. For this reason, users who have been accepted into the conference are also automatically accepted if they lose network connectivity and call into the conference again.

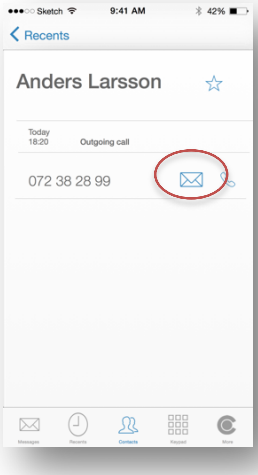
Note also that the entire conference is protected by a secret randomly generated by the conference host each time he or she (re-)enter the conference. If the conference host hangs up, the conference continues, but new participants cannot be accepted. Should the conference host dial in again, the conference will start anew after a brief interruption whilst rekeying.

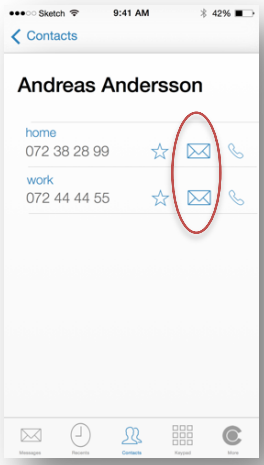
Best practice for allowing an external party, say, to participate only in the latter part of a conference is to maintain two conference rooms, and move to the second conference room when the external party should join.

Secure text messages

To start a new conversation please select *new message* icon on the top right corner in the Messages view, or from a Contact Details view.



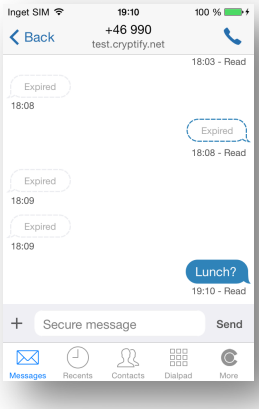


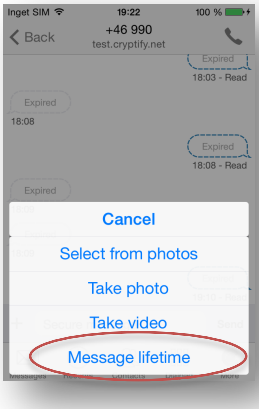


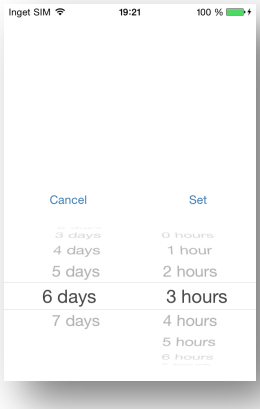
To post a new message in an existing conversation, open that conversation and select the input field to bring up the keyboard.

If supported by the server, images can be attached to a message by tapping the "+" button. Photos can optionally be resized before upload. Alternatively, a file can be copied from another app – such as from Mail – to a new conversation by tapping the "Share" button followed by "Copy to Cryptify Call". It is also possible to attach up to 30 seconds of video recorded in the app.

The administrator can limit for how long messages can be viewed in the app, in which case messages expire at a specific point in time. Note that messages may expire before the recipient has viewed them. The maximum lifetime cannot be increased, but it is possible to select a shorter message lifetime by tapping the "+"-button and selecting "Message lifetime".







Press the send button to send the message. A message that will expire is marked with a timer icon next to the message time stamp. To show when the message will expire, long press the message and select "Status".

To visit links, such as web addresses, embedded in messages, long press the message and tap “Links”.

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

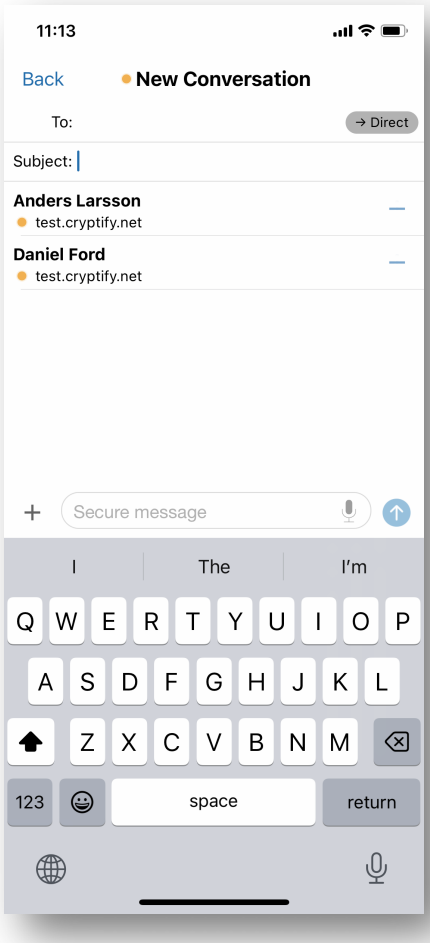
- *Sending* – the message is being uploaded to the server.
- *Sent* – the message has been transferred to the server.
- *Notified* – iOS recipients only. The recipient has been notified of the message.
- *Delivered* – the message has been delivered to the recipient.
- *Read* – the recipient has opened the conversation.
- *Failed* – sending the message failed; long press the message and select “Status” for more information or “Resend” to immediately try again.

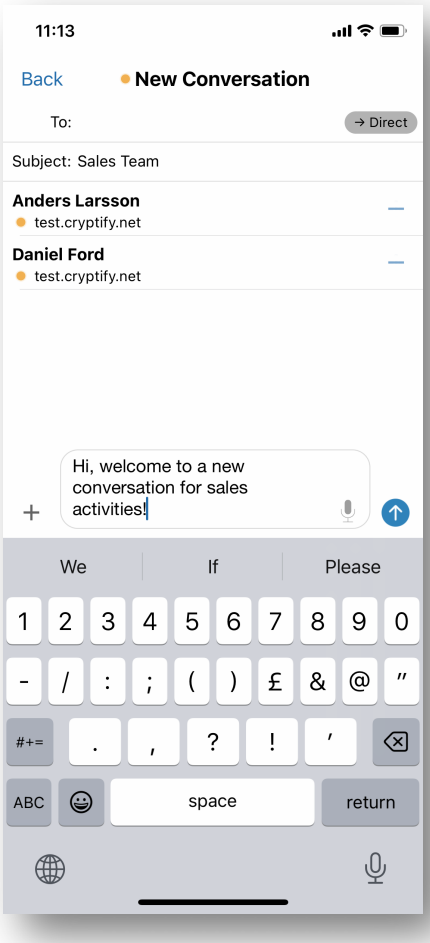
To show the sender’s compose time of an incoming message, long press the message and tap “Status”. If this timestamp differs more than 5 minutes from when the message was received, a warning icon is shown.

Groups

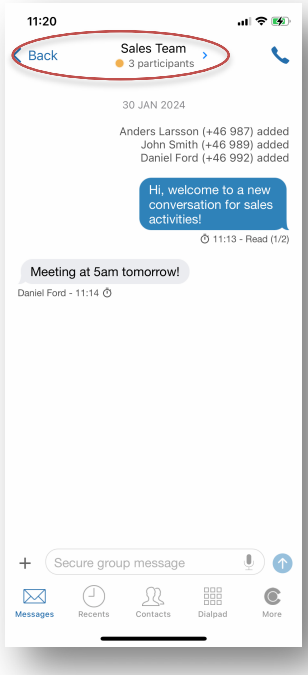
Setting up a group conversation is as easy as sending a regular text message. The *instant group conversations* replace the *managed groups* concept found in older versions of Cryptify Call.

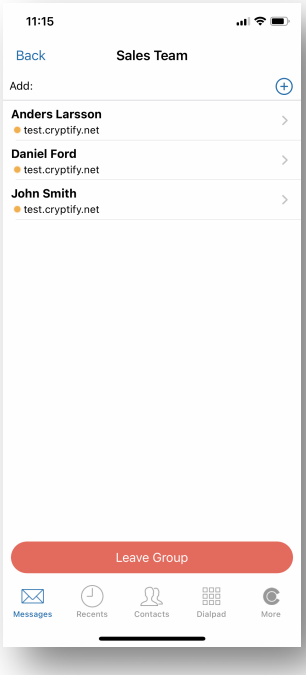
To start a new *instant group conversation* simply select *new message* icon on the top right corner in the Messages view and add the recipients. If more than one recipient is added an *instant group conversation* is created and a *Subject* field is presented.





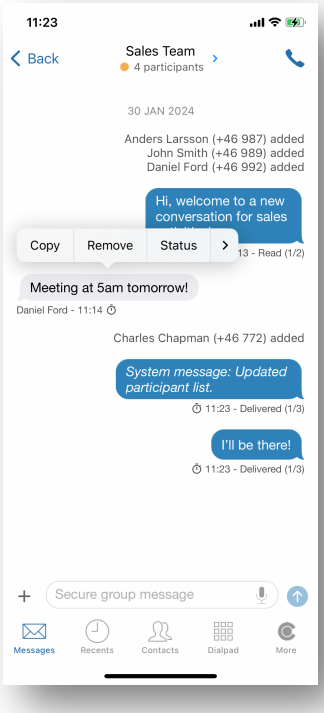
To add and remove recipients from the group conversation press the group name.

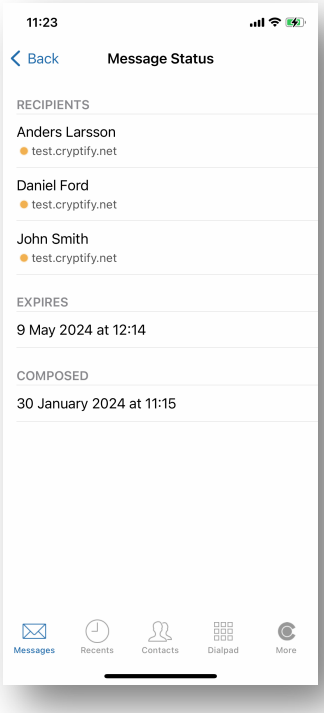




Each received message is marked with the identity of the sender as well as a timestamp of when the message was received. The history of added and removed are presented in the conversation.

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

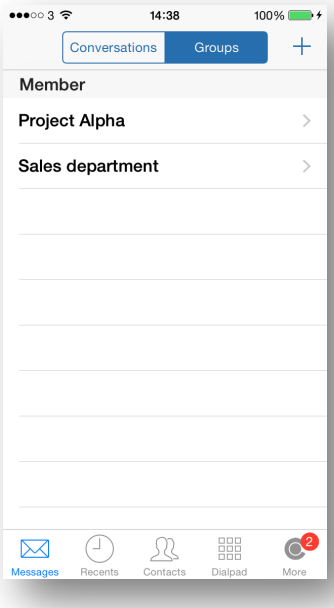


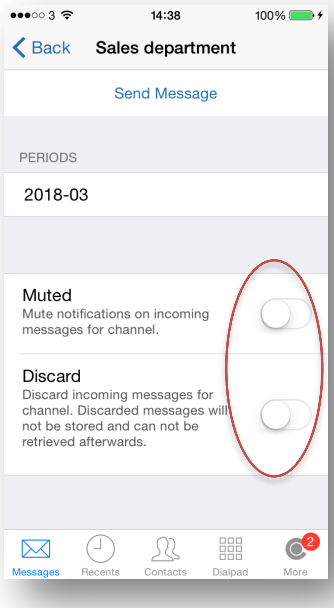


Channels

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.

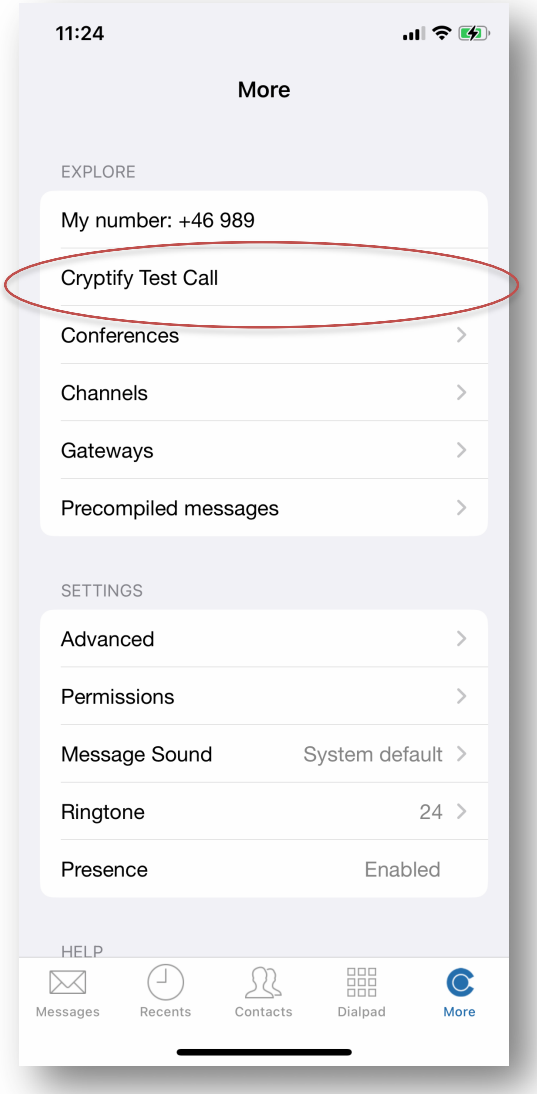
If a device is to be offline for an extended period of time, it is recommended to configure any high traffic channels to discard incoming traffic. Otherwise, once the device goes online, the app may become unresponsive while it decrypts the messages that have been queued up.

The channel settings are also visible under More > Channel settings.

Cryptify Test Call

A user can make a Cryptify Test Call to verify the call quality.

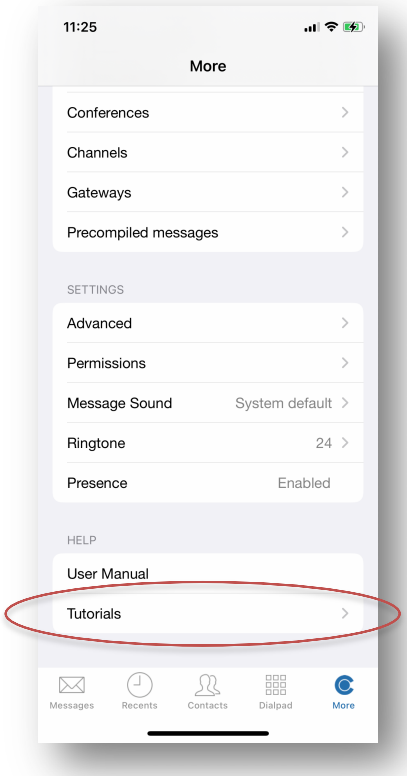
In the *More view* select *Cryptify Test Call* and follow the audio instructions.



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.

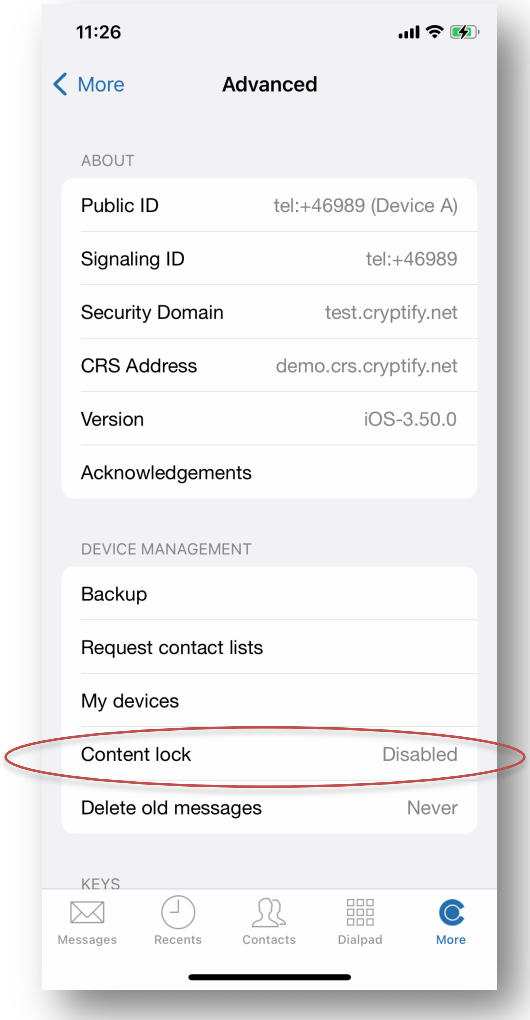
Tutorials and manual

Under the “More” tab you will find the user manual – this document – along with a set of in-app tutorials that highlight new features or help you discover new ways to use Cryptify Call.



The Advanced menu and message PIN lock

In the *More view* select *Advanced* to display detailed information of the Cryptify Call application. Messages, contacts and call history 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.



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.

Application Update

To guarantee full functionality and security within the application it is important that users keep Cryptify Call up to date.
Updates are handled by iOS and the App Store. If users are permitted to update their apps, they will receive notifications from the App Store when a new version is available.  When the AppStore indicates that an update is available, the user should open the AppStore app, select the update tab, and click the update button for Cryptify Call if shown.

Otherwise, administrators for the local system may ask to update the apps when these updates are available on behalf of their users.

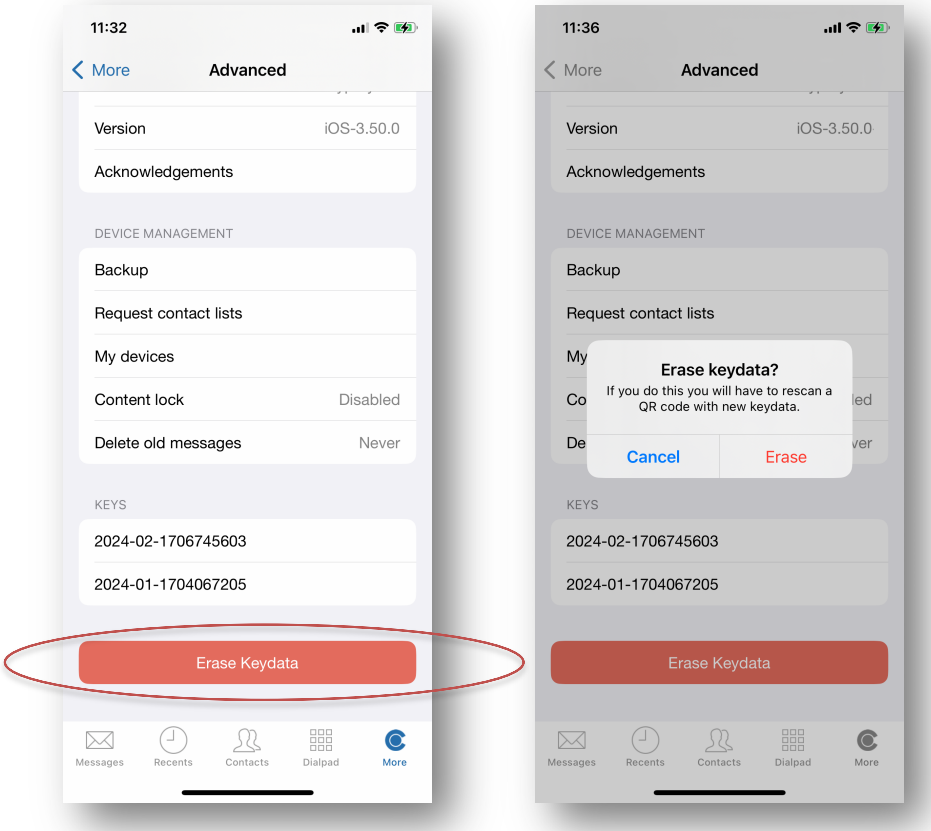
Add, Delete and Modify a contact

Please use the *Contacts* app  provided by iOS.

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 *More* tab select *Erase keydata* and press the *Erase* 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 contacts!

New keys must be received by the user in the form of a QR code, see Provisioning user credentials above.

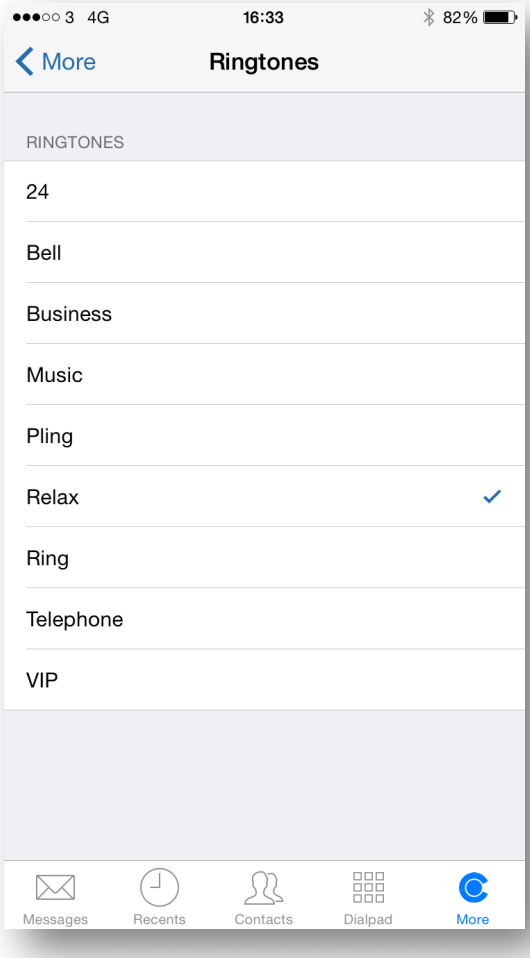
Configuration

Application specific configuration

Parameters that can be configured by the users are presented in the *More* tab.

Ringtone
This is the ringtone played during incoming calls.

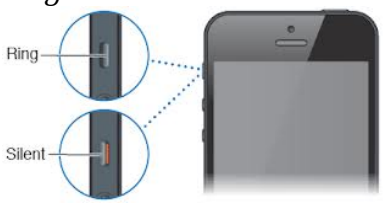
The user can select from a list of different ring tones.



Message Sound
The notification sound played when an incoming message is received can be selected from a list of custom notification sounds, set to the default system notification sound or muted.

Related configuration

Mute
Please use the physical mute switch on the side of the phone to toggle between *Ring* and *Silent*.



Vibration
Please use the switch *Vibrate on Ring* in the *Sounds* menu in *Settings*.

Volume
Please use the physical buttons to adjust the volume. Please notice that *Ringer* volume and *audio/media* volume are handled separately by iOS.
Go to the Springboard (no app open) to adjust the *Ringer* volume.
The *audio/media* volume can be adjusted during a call.

Passcode Lock and timer
When a call is received and the phone is on locked mode, there is an inactivity timer determining if the passcode is required, before access to the application is allowed.

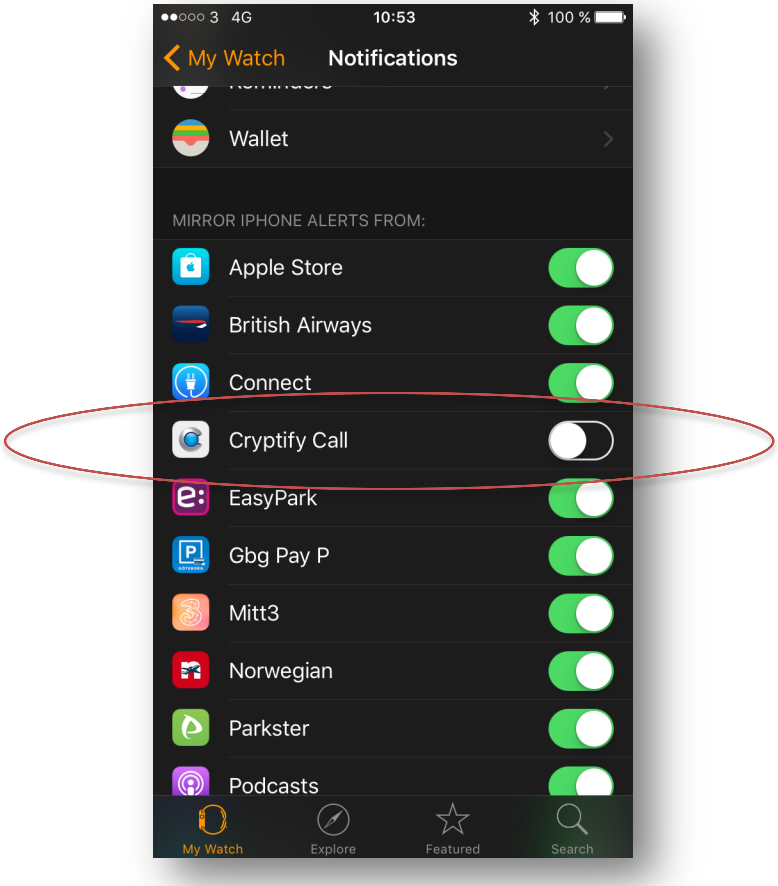
To modify the passcode timer, please select the *Face ID & Passcode* menu in *Settings*.

The timer is managed in *Require Passcode* setting.

Apple Watch

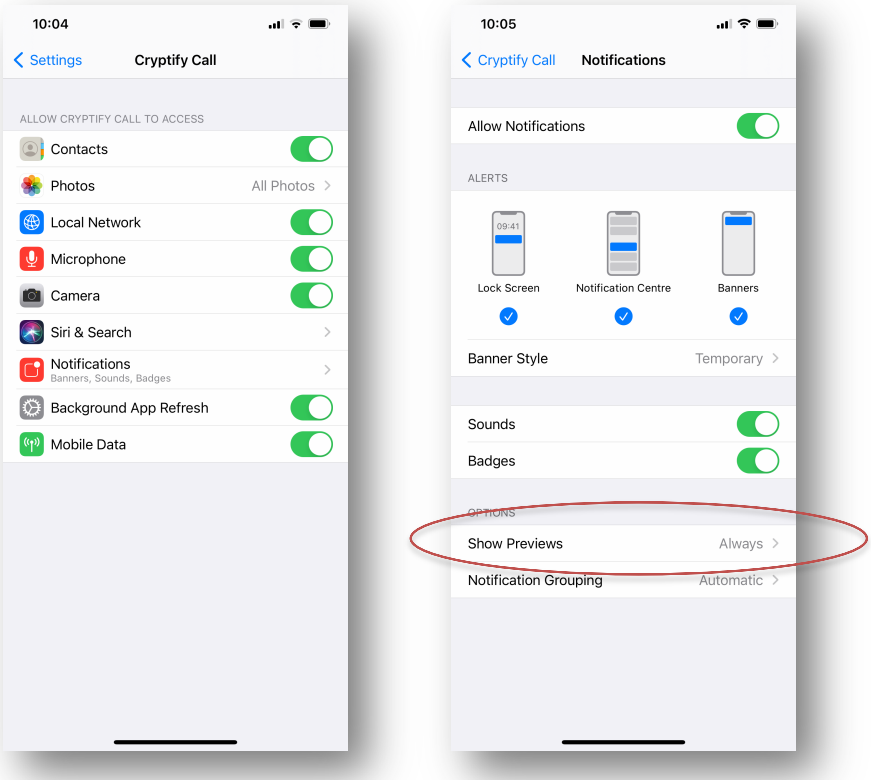
By default notifications are forwarded to the Apple Watch when the iPhone is locked, and hence the iPhone will not ring on incoming calls, nor will a notification be displayed on the lock screen.

To enforce that incoming Cryptify Call calls are displayed and ringing on the iPhone please disable notification alerts for Cryptify Call to the Apple Watch by toggling off for Cryptify Call in the notifications menu in the Apple Watch app.



Default settings for Cryptify Call

Please verify that your settings are as presented below



Please notice that it's possible to decide if content of notifications should be presented when the device is locked. Default setting varies depending on unlock method, e.g. using Face ID default setting is "When Unlocked" and for PIN is "Always". If "When Unlocked" is selected notifications for incoming calls and messages will only state "notification" until the device is unlocked. Please select "Always" to see the full content of the notification.

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.

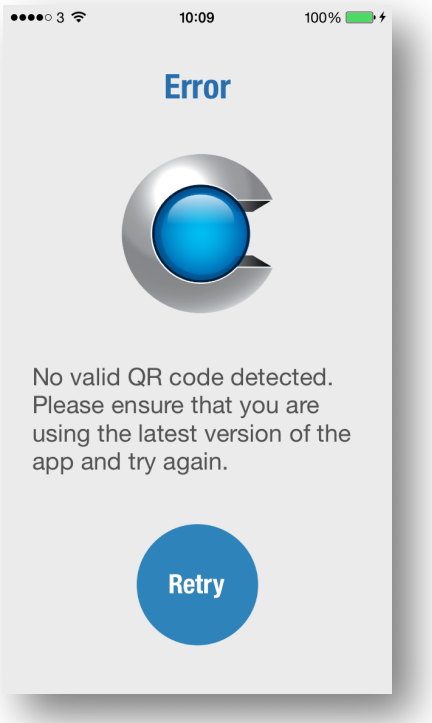
Unsuccessful messaging

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.

FAQ

Q: Why do I get a failure when scanning a QR code?



A: Failure to scan a QR code can be subcategorized into the following subcategories

1. Video quality problem
   Symptom: The app is unable to detect the QR code and keeps on recording
   Description: if the captured video feed does not have high enough quality it will not be possible to decode images containing the QR code.
   Remedy: This is normally due to a malfunctioning camera or distorted paper copy of the QR code.
2. QR code not created by a Cryptify Management System
   Symptom: Error message stating, "No valid QR code detected"
   Description: the Cryptify Call app will only accept a QR code that is created by a Cryptify Management System
   Remedy: Please request a QR code from your system administrator
3. Obsolete app version
   Symptom: Error message stating, "No valid QR code detected"
   Description: In case the system administrator enables mandatory policies only Cryptify Call version compliant with such policies will accept the QR code.
   Remedy: Please update to the latest version of the Cryptify Call app in the App Store.

Q: Why doesn't my app get the monthly update?

A: Failure to get monthly update can be subcategorized into the following subcategories

1. Network problem
   Symptom: A "No network" warning in the "More" tab
   Description: The app must be able to connect to the Cryptify Rendezvous Server in order to download new updates and to use the Cryptify Call service.
   Remedy: Please acquire network connectivity in order for the device to connect to the Cryptify Rendezvous Server
2. Obsolete app version
   Symptom: Key for the period is not listed under More->Advanced. Keys for September 2017 will have the syntax "2017-09-NNNNNNNNNN"
   Description: In case the system administrator enables mandatory policies only Cryptify Call version compliant with such policies will accept the update.
   Remedy: Please update to the latest version of the Cryptify Call app in the App Store.
3. Changed update key
   Symptom: Key for the period is not listed under More->Advanced. Keys for September 2017 will have the syntax "2017-09-NNNNNNNNNN"

Description: In case the system administrator has deleted the account or performed a “re-key” operation the existing update key stored is no longer valid.
Remedy: Please request a QR code from your system administrator