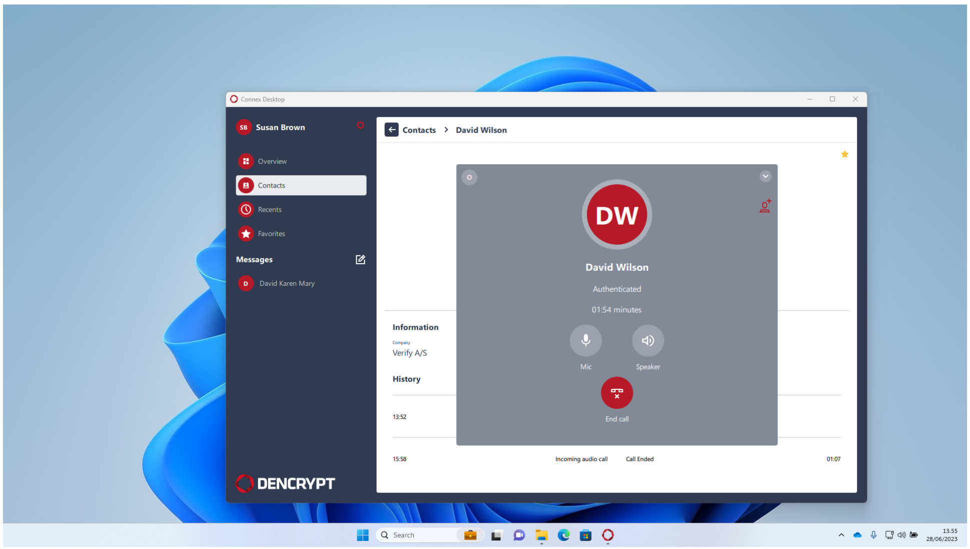
Dencrypt Communication Solution

Operational user guide

Dencrypt Connex for Windows/macOS

v. 1.5.0



April 26, 2024

Public

Contents

Version

This guide applies for:

- Dencrypt Connex v. 1.5.0 for Windows/macOS devices.

The version number can be verified from the Settings menu by tapping the ⚙-symbol in the top-left corner on the main screen. See Figure 44.

Support

Contact your local support for assistance and in case of security incidents.

Dencrypt support	
Phone	+45 72 11 79 11
Email	support@dencrypt.dk

1 Introduction

Dencrypt Connex is an application for making encrypted voice calls, videocalls and for the exchange of encrypted instant messages from:

- Windows laptops/desktops
- macOS laptops

It uses the patented Dynamic Encryption technology to apply state-of-the-art, end-to-end encryption between devices.

This guide is intended for end-users of the Dencrypt Connex application and provides instructions to operate and use the application securely.

The end-users of the Dencrypt Connex application shall have familiarized themselves with this document and received instructions from the system administrator prior to taking the product into use.

Dencrypt Connex support selected local languages. However, this guide and screenshots are shown in the English language.

Section 2 Section 3	Security instructions Getting started	**Essential**
Section 4 Section 5 Section 6 Section 7	Using Dencrypt Connex Making a secure call Sending a secure message Settings	User guidance
Appendix A	Dencrypt Communication Solution	For reference

Table 1: Reading Guide

2 Security instructions

These security instructions shall be read and understood before taking the Dencrypt Connex application into use.

2.1 General security measures

Some precautions must be observed to use the application in a secure way and to avoid disclosure of confidential information. Please observe the following before taking the application into use.

Organizational security policies Before taking Dencrypt Connex into use, the security policies and instructions for secure usage shall have been received and understood. Be aware of the classifications allowed to be exchanged using Dencrypt Connex .

Server system security The system administrator is responsible for the daily and secure operation of the Dencrypt Server System. In case of critical security incidents or unresolved vulnerabilities, the system administrator may prevent communication between specific users or may take the entire system out of operation until the issues have been resolved. In such cases, it may not be possible to establish secure communication at all or with specific users.

Secure delivery Dencrypt Connex shall only be received from a trusted location. For integrity validation, a SHA1 and MD5 checksum shall be provided with the Dencrypt Connex installation file. Dencrypt Connex shall only be installed if the checksum has been validated (3).

Device security The system security depends on a correct and secure operation of the laptop and the operating system, and there are no critical side-effects. Therefore, the Dencrypt Connex application and the operating system shall always be kept updated to the latest versions. In case of critical security incidents or unresolved vulnerabilities, the system administrator may prevent calls to a certain user or make the entire system unavailable until the issue has been resolved.

Benign applications The Dencrypt Connex application protects information during the data transmission and when stored on the device. It does not protect against malware intercepting audio, video, or text before encryption. Therefore, only benign apps shall be installed on the device. Be aware of applications, which make use of the microphone, perform screenshots, listen to the earpiece or speaker or capture keyboard strokes. Contact your system administrator for advice.

Single user device The phonebook is personal and dedicated to a specific end-user. Therefore, the device is personal and shall not be shared.

Prevent unauthorized access Protect your device against unauthorized access by always enabling a passcode or biometric login. In case of lost or stolen devices, contact your system administrator immediately.

2.2 Avoid acoustic coupling

It is not recommended to use encrypted voice or video calls in hotel rooms and like, which cannot be considered secure. Never exchange classified information through the Dencrypt Connex application when other unclassified telephones, radio transmitters, or similar are being used in immediate proximity.

Locations that are well suited to making calls may be public spaces where the caller's presence has not been pre-arranged. Using secure messaging is an alternative communication in areas where an acoustic coupling is possible.

2.3 Avoid screen exposure

Consider the surroundings when using Dencrypt Connex for secure video calls and messaging to ensure that the screen can not be observed by others. Be aware of the location of windows and cameras.

2.4 Other security recommendations

- **Avoid using wireless headsets** - The data connection from the device to the headset is not protected by Dencrypt Connex . Use wired headsets as an alternative.
- **Avoid using hands-free car systems** - The data connection from the device to the hands-free car system is not encrypted. Disable Bluetooth to avoid automatic connection and use wired headsets as an alternative.
- **Avoid using loudspeaker** - Use the Dencrypt Connex loudspeaker only with care and in locations that are protected from an acoustic coupling.
- **Don't take screenshots** – Screenshots are saved unencrypted on the devices and are not deleted when the app is closed.
- **Don't use copy/paste** – Don't use the copy/paste functionality during messaging.
- **Don't use voice recordings** – Voice recordings are saved unencrypted on the devices and are not deleted when the app is closed.
- **Avoid auto-correction and predictive text features** - Avoid using keyboards that include autocorrection or predictive text features. It is recommended to disable spell-checking and predictive text from the settings menu.
- **Avoid using apps with speech recognization** - Avoid using applications, that makes use of speech recognition features, such as speech-to-text applications.

3 Getting started

A few steps are required by the end-users to get started using Dencrypt Connex .

1. Download, integrity check & installation.
2. Activation.
3. Configure audio devices.

3.1 Download, integrity check, and installation

Dencrypt Connex is available for download from `https://www.dencrypt.dk/downloads`. The download package consists of the following files:

For Windows:

- connex-desktop-<version>-installer-win.exe - Executable installation file
- connex-desktop-<version>-installer-win.exe.sha256 - SHA256 checksum

For macOS:

- connex-desktop-<version>-installer-osx.dmg - Executable installation file
- connex-desktop-<version>-installer-osx.dmg.sha256 - SHA256 checksum

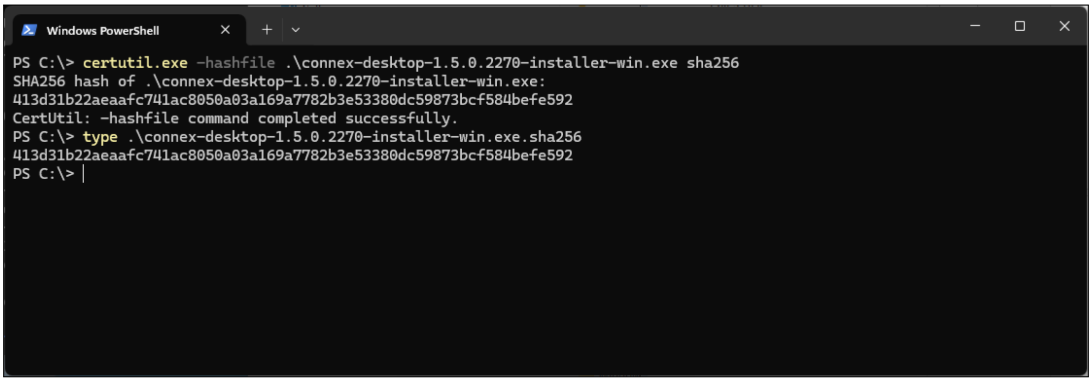
An integrity check shall be performed before running the executable installation file to validate that application has not been tampered with.

On Windows the checksum can be validated by:

1. Open a Windows command prompt in the directory where the installation file is located. (Press Windows start button + R and type cmd.)
2. Type: `certutil -hashfile connex-desktop-<version>-installer-win.exe sha256`
3. Type: `type connex-desktop-<version>-installer-win.exe.sha256`
4. Verify that the two outputs match exactly (figure 1)

On macOS the checksum can be validated by:

1. Open a Terminal in the folder where the installation file is located.
2. Type: `sha256 connex-desktop-<version>-installer-osx.dmg`
3. Type: `less connex-desktop-<version>-installer-osx.exe.sha256`
4. Verify that the two outputs match exactly.



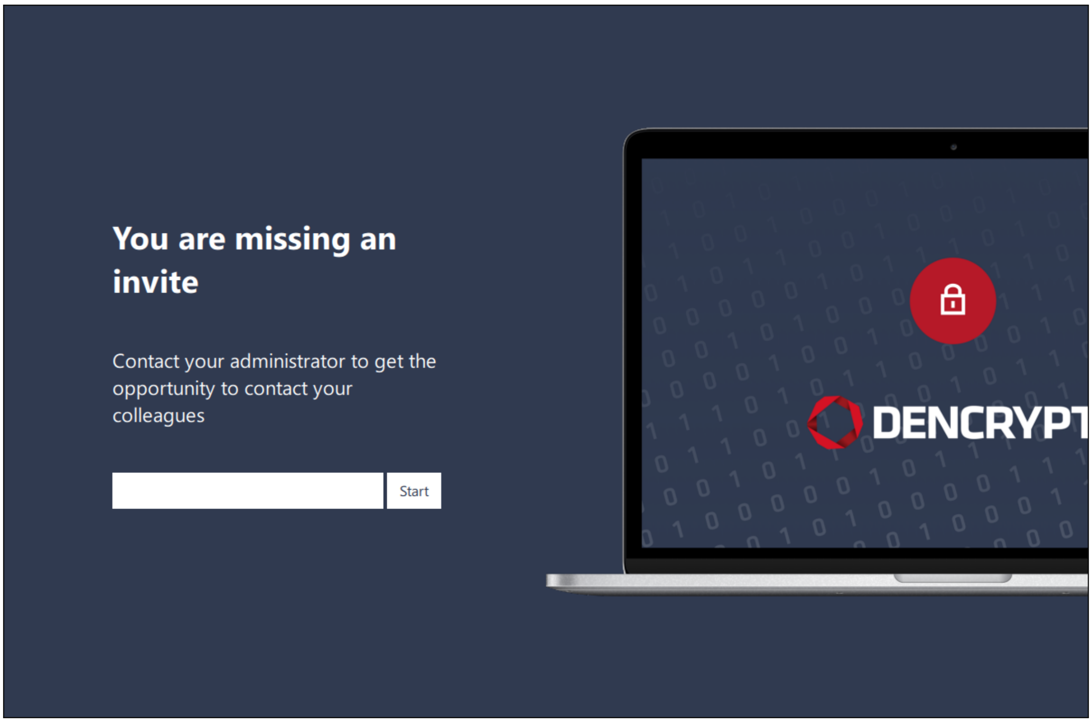
```
PS C:\> certutil.exe -hashfile .\connex-desktop-1.5.0.2270-installer-win.exe sha256
SHA256 hash of .\connex-desktop-1.5.0.2270-installer-win.exe:
413d31b22aeaafc741ac8050a03a169a7782b3e53380dc59873bcf584befe592
CertUtil: -hashfile command completed successfully.
PS C:\> type .\connex-desktop-1.5.0.2270-installer-win.exe.sha256
413d31b22aeaafc741ac8050a03a169a7782b3e53380dc59873bcf584befe592
PS C:\> |
```

Figure 1: Checksum (SHA256) validation of Dencrypt Connex installation file on Windows.

Once the executable installation file has been validated, the application is installed by running the installation file and following the instructions. Once the app is installed, it is launched by tapping the Dencrypt Connex icon. For quick access, a shortcut can be placed on the desktop or taskbar.

It is recommended to allow Dencrypt Connex to start automatically after login. Follow the instructions:

- Windows: https://support.microsoft.com/en-us/windows/add-an-app-to-run-automatically-at-startup-in-windows-10-150da165-dcd9-7230-517b-cf3c295d89dd
- macOS: https://support.apple.com/guide/mac-help/open-items-automatically-when-you-log-in-mh15189/mac

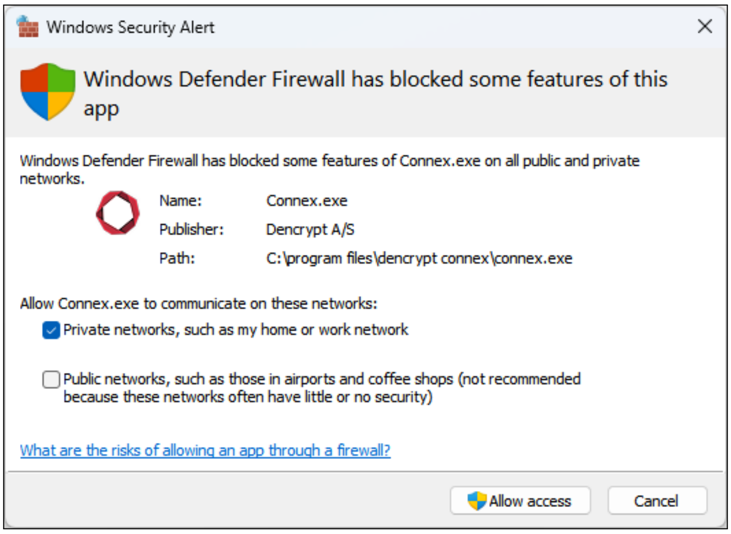


You are missing an invite

Contact your administrator to get the opportunity to contact your colleagues

Figure 2: Dencrypt Connex is ready for activation

The desktop firewall may ask for permission to establish an outgoing connection rule. Tap OK to accept.



Windows Security Alert

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of Connex.exe on all public and private networks.

Name: Connex.exe
Publisher: Dencrypt A/S
Path: C:\program files\dencrypt connex\connex.exe

Allow Connex.exe to communicate on these networks:

☑ Private networks, such as my home or work network

□ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

Figure 3: Accept inbound firewall rule.

3.2 Activation

Once installed, the Dencrypt Connex is unconfigured and shall be activated before it is taken into use. The system administrator is required to create a user account on the Dencrypt Server System and provide an activation link.

The activation link is time-limited and can only be used once, and it comes in the form of a weblink (URL) sent by email. The activation link may not be disclosed and shall be delivered in a secure way, i.e., by encrypted email connections.

Activation is started by tapping the Activate button or right-clicking to copy the hyperlink and paste it to the invitation field on Dencrypt Connex . Activating the link will start the provisioning process to configure the Dencrypt Connex with certificates and credentials to connect to the server system and download the phonebook. Only when the activation process has successfully completed the Dencrypt Connex is ready for use.

Activation process

Step 1: The system administrator creates a user account on the Dencrypt Server System and provides an invitation message containing the activation link to the end user.

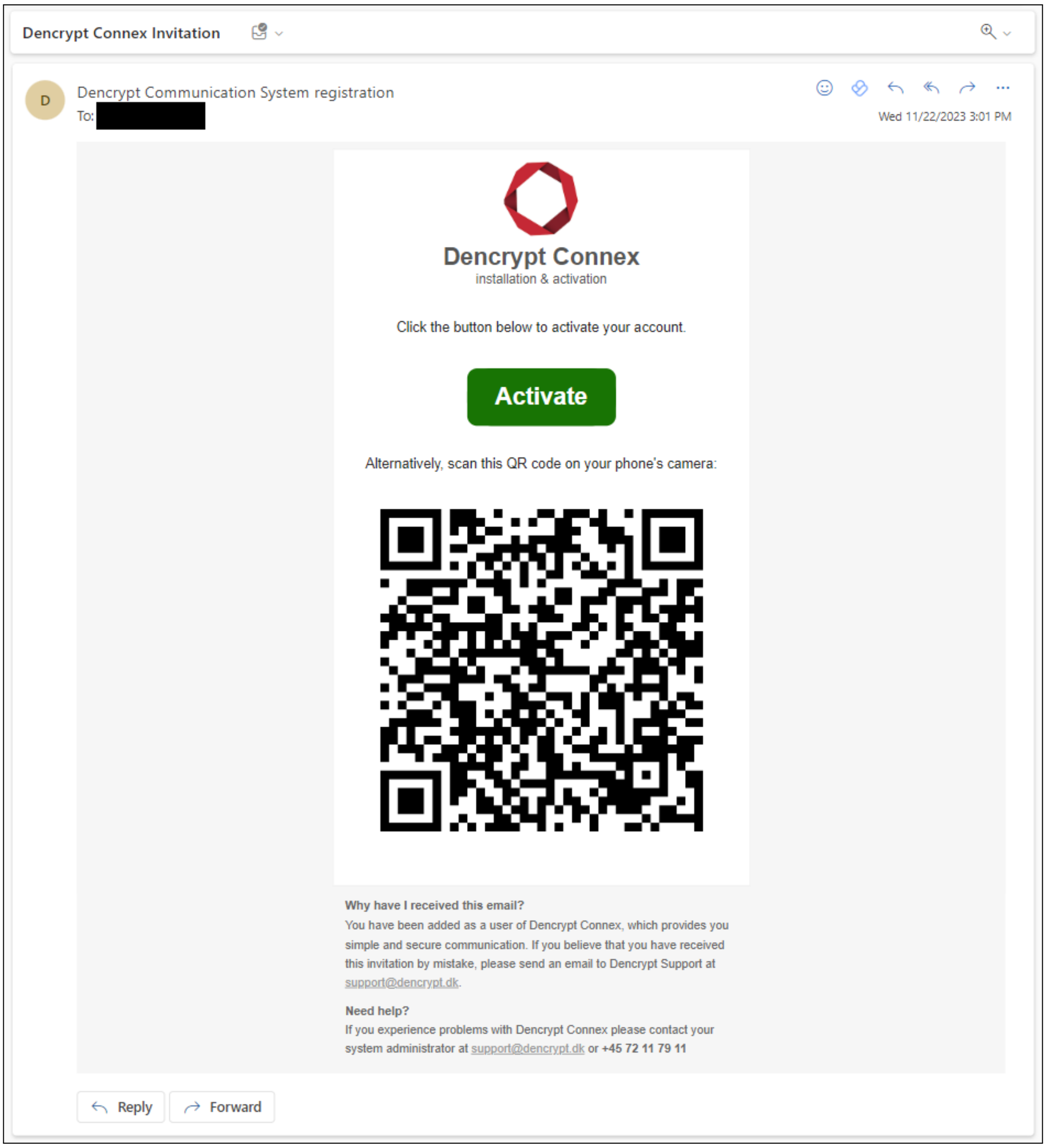
Step 2: The user activates the link by tapping the weblink or copy-/pasting the hyperlink to the invite field. The user may be prompted to open the link in the Dencrypt Connex .

Step 3: The Dencrypt Connex opens to configure the account. This may take 1-3 minutes. **Do not close the app during the activation.**

Step 4: Dencrypt Connex connects to the server system to download the phonebook.

Step 5: Tap Yes to configure audio device.

Step 6: Dencrypt Connex is now ready for use.



Dencrypt Connex Invitation

Dencrypt Communication System registration

To: [redacted]

Wed 11/22/2023 3:01 PM

Dencrypt Connex

installation & activation

Click the button below to activate your account.

Alternatively, scan this QR code on your phone's camera:

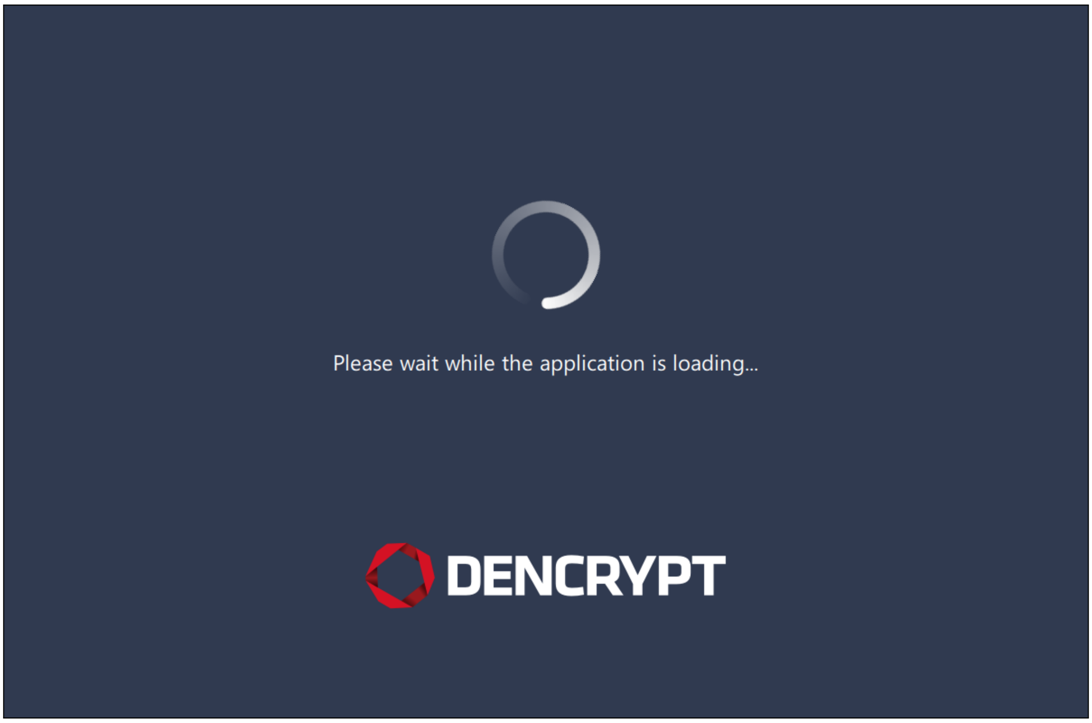
Why have I received this email?

You have been added as a user of Dencrypt Connex, which provides you simple and secure communication. If you believe that you have received this invitation by mistake, please send an email to Dencrypt Support at support@dencrypt.dk.

Need help?

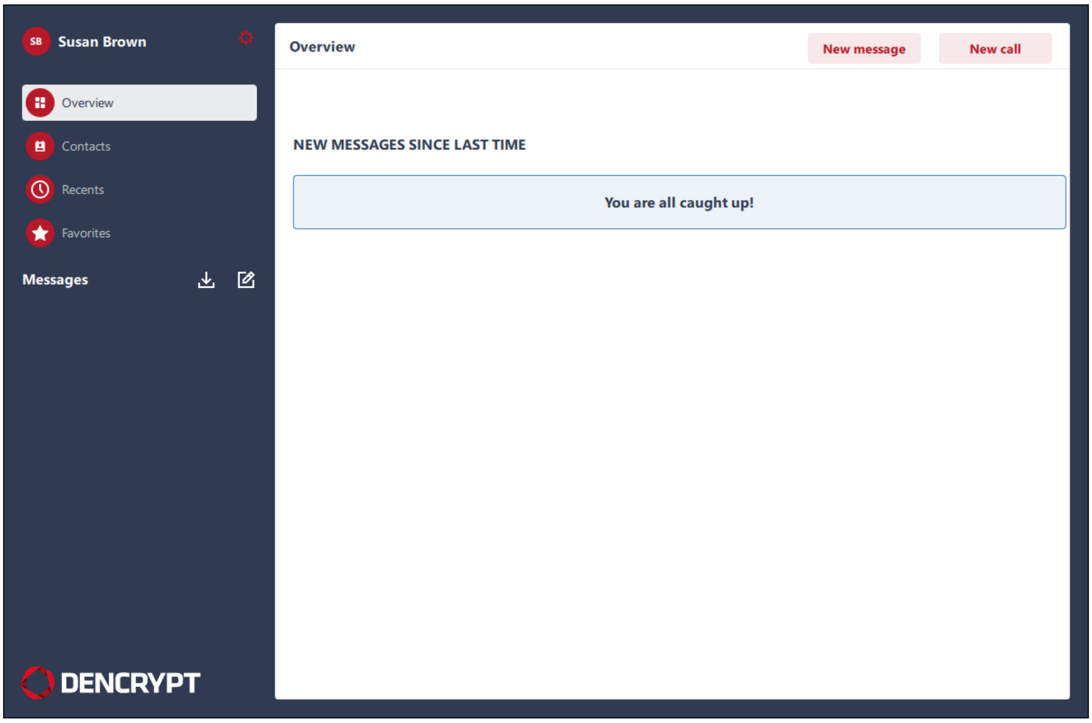
If you experience problems with Dencrypt Connex please contact your system administrator at support@dencrypt.dk or **+45 72 11 79 11**

Figure 4: Email invitation



Please wait while the application is loading...

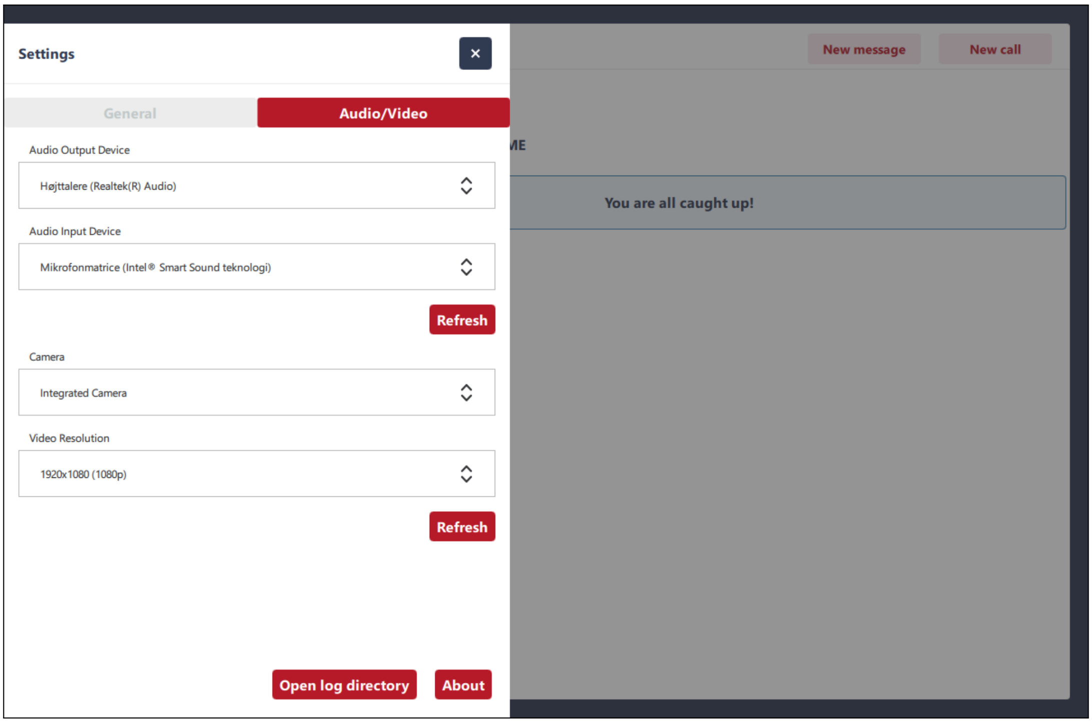
Figure 5: Activation in progress.



NEW MESSAGES SINCE LAST TIME

You are all caught up!

Figure 6: Activation completed



Audio Output Device
Højttalere (Realtek(R) Audio)

Audio Input Device
Mikrofonmatrice (Intel® Smart Sound teknologi)

Camera
Integrated Camera

Video Resolution
1920x1080 (1080p)

Figure 7: Configure audio devices.

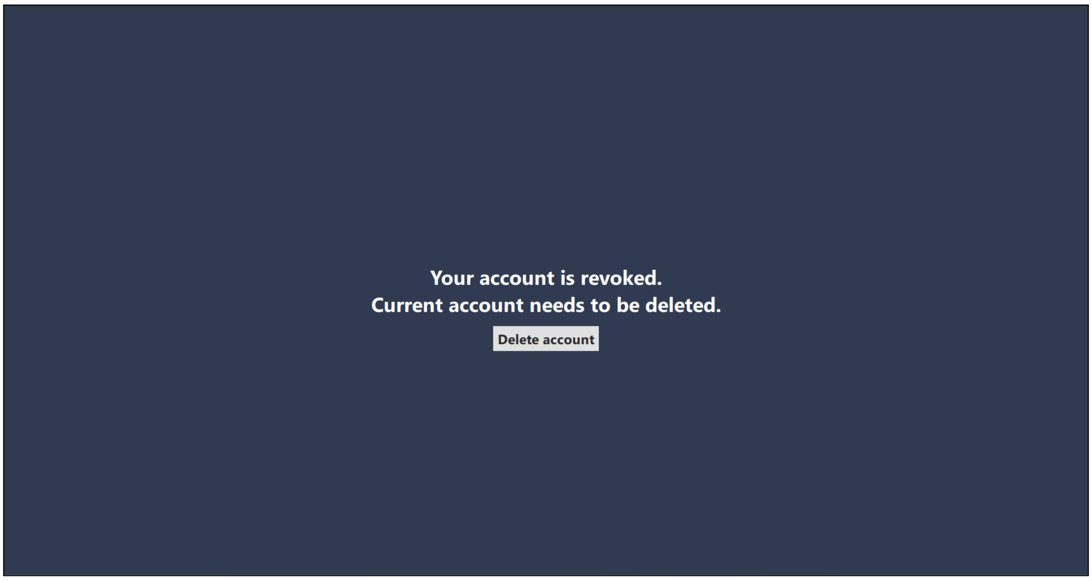
3.3 Revoked application

The system administrator may revoke the Dencrypt Connex access to the server system, which will result in a Security Issue message (Figure 8). This may happen if:

- The device has been reported lost or stolen, in which case the administrator will temporarily deactivate access.
- The account has been deleted, in which case access is permanently blocked.

In both cases, contact the system administrator to regain access to the services. The administrator may:

- Re-activate the device, in which messages and call history are preserved. This usually happens in case a lost device is found again.
- Send a new invitation to provision the Dencrypt Connex app again, in which messages and call history are **NOT** preserved. Before using the new invitation, the account should be deleted by pressing Delete account.



Your account is revoked.
Current account needs to be deleted.

Figure 8: Revoked access to the server system.

4 Using Dencrypt Connex

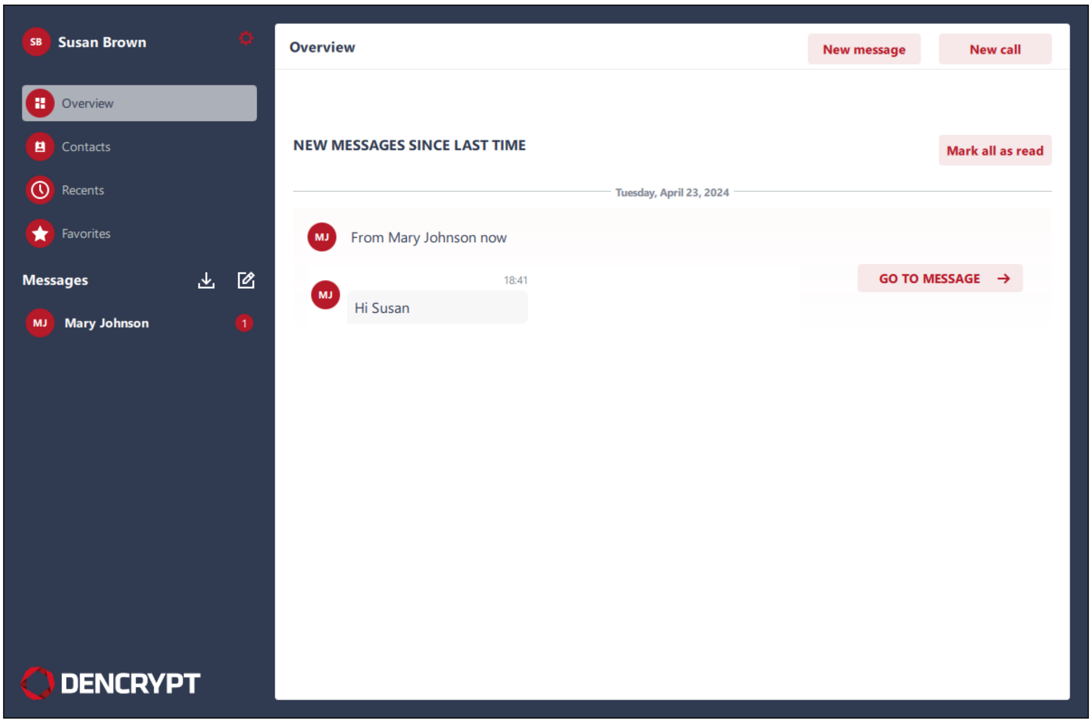
Dencrypt Connex offers two main functionalities:

- Secure voice/video communication
- Secure instant messaging of text and content (attachments).

The functionalities are accessible from the main screen. The icons in the menu bar at the left provide quick access to the following screens.

- Overview: List of new messages since the last login and quick access to:
  - New message to write a new message.
  - New call to place a secure voice/video call.
- Contacts: For accessing the phone book in alphabetic order.
- Recents: For accessing call history in descending order.
- Favorites: For accessing favorites in alphabetic order.
- Messages: Chat rooms are listed here.

Settings are accessed from the ⚙-icon in top-right corner of the menu bar.



From Mary Johnson now

Hi Susan

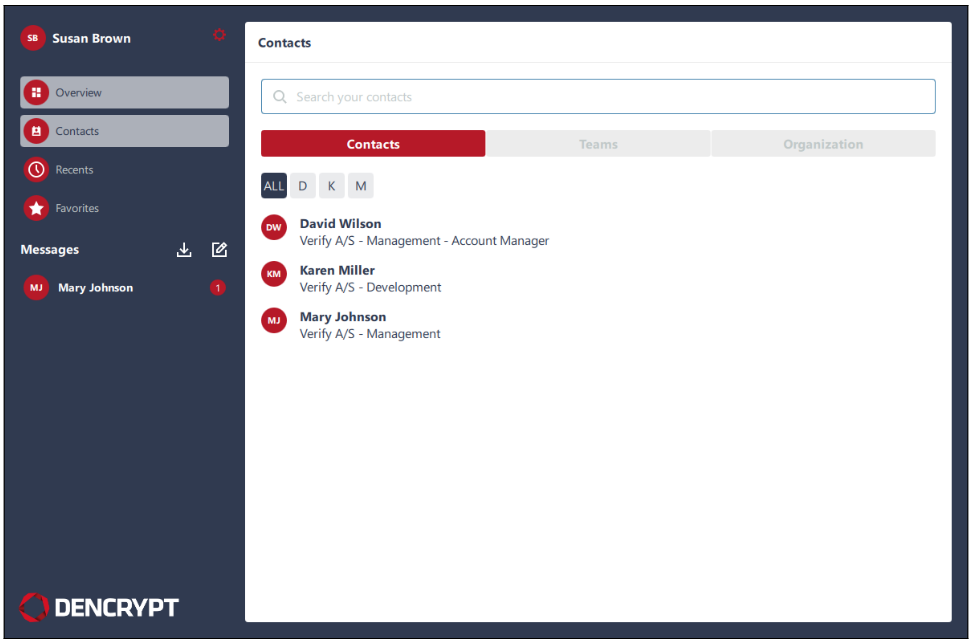
Figure 9: Overview screen

4.1 Contacts

The Contacts screen gives acccess to the phone book. Contacts are grouped in 3 categories - Contacts, Teams and Organization. The content of the phone book is centrally managed from the Dencrypt Control Center and is not editable from within the application.

subsubsectionContacts

Contacts are listed in alphabetic order sorted by the first name per default and can be searched from the Search field. Filtering can be done with either the Alphabet selector or the Search field. The Alphabet selector will filter contacts based on the first letter in their firstname while Search will match all occurrences in the full contact name. Selecting a contact will open the Contact details (figure 12) and allow the user to start a secure voice call, secure video call, or send a secure message. The Contact details screen also displays the call history.

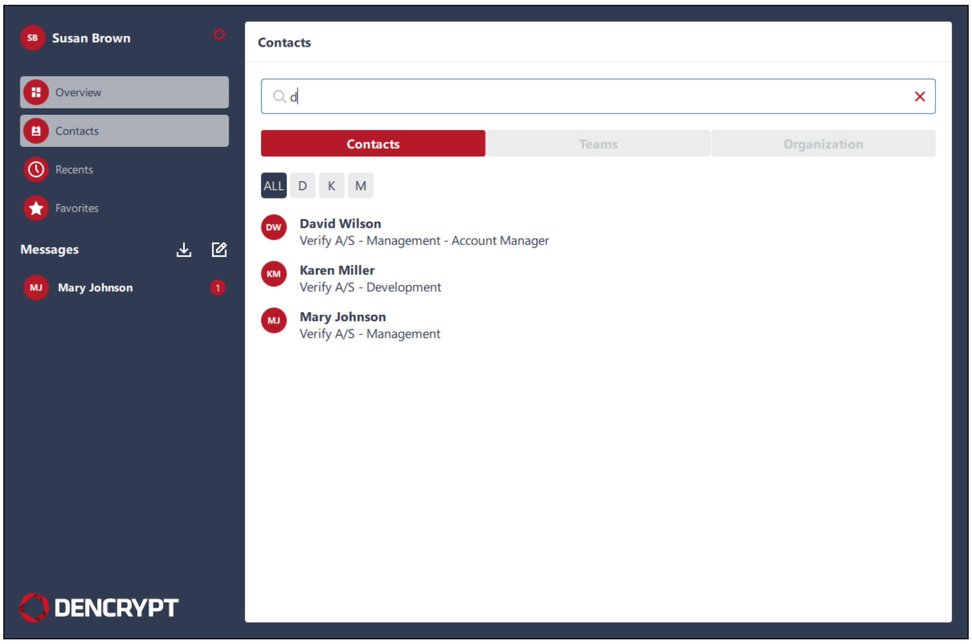


DW David Wilson
Verify A/S - Management - Account Manager

KM Karen Miller
Verify A/S - Development

MJ Mary Johnson
Verify A/S - Management

Figure 10: Contacts.

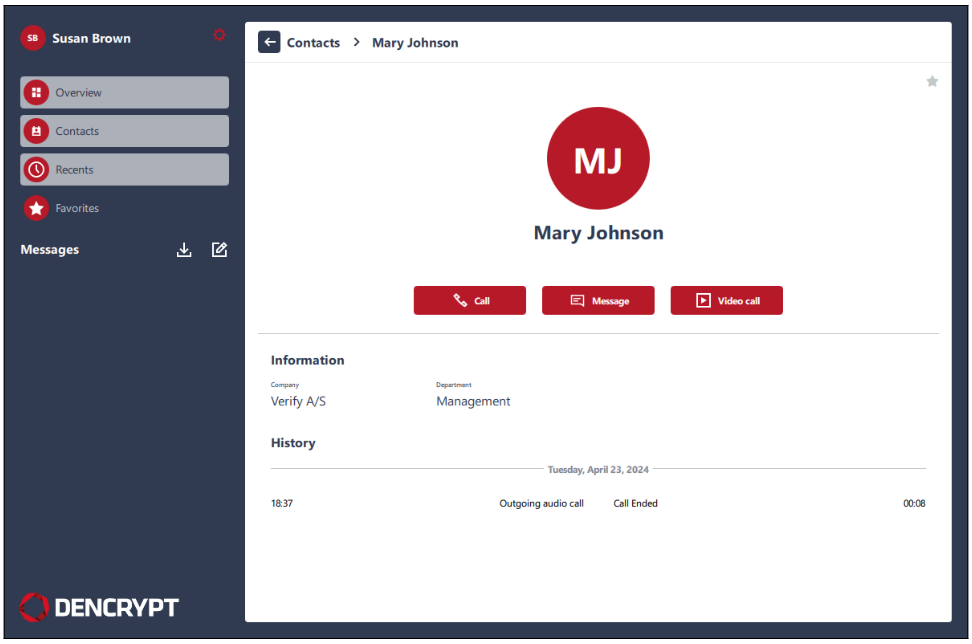


DW David Wilson
Verify A/S - Management - Account Manager

KM Karen Miller
Verify A/S - Development

MJ Mary Johnson
Verify A/S - Management

Figure 11: Contact search.



MJ

Mary Johnson

Information

Company
Verify A/S

Department
Management

History

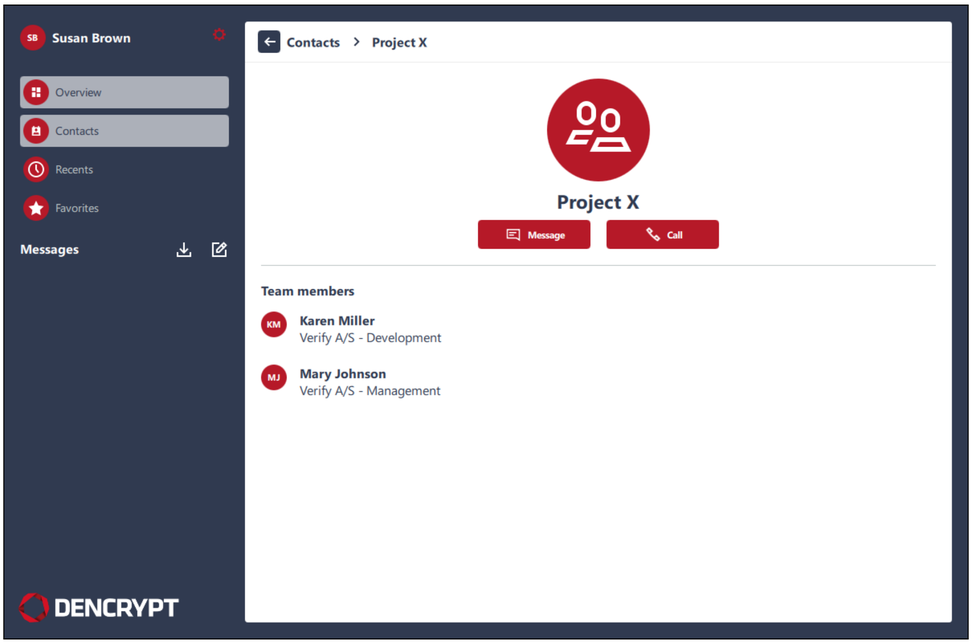
Tuesday, April 23, 2024

18:37 Outgoing audio call Call Ended 00:08

Figure 12: Contact details

4.1.1 Teams

Team rooms are persistent chat rooms defined by the system administrator. The Teams section lists the team rooms of which the user is a member of (figure 13). Filtering can be done with either the Alphabet selector or the Search field. The Alphabet selector will filter teams based on the first letter in the team name while Search will match all occurrences in the full team name. Tapping a team room will list the members of the team room (figure 14). Tap the Message button to open the chat room to exchange messages with the team. Filtering



Project X

Team members

KM Karen Miller
Verify A/S - Development

MJ Mary Johnson
Verify A/S - Management

Figure 13: Team View

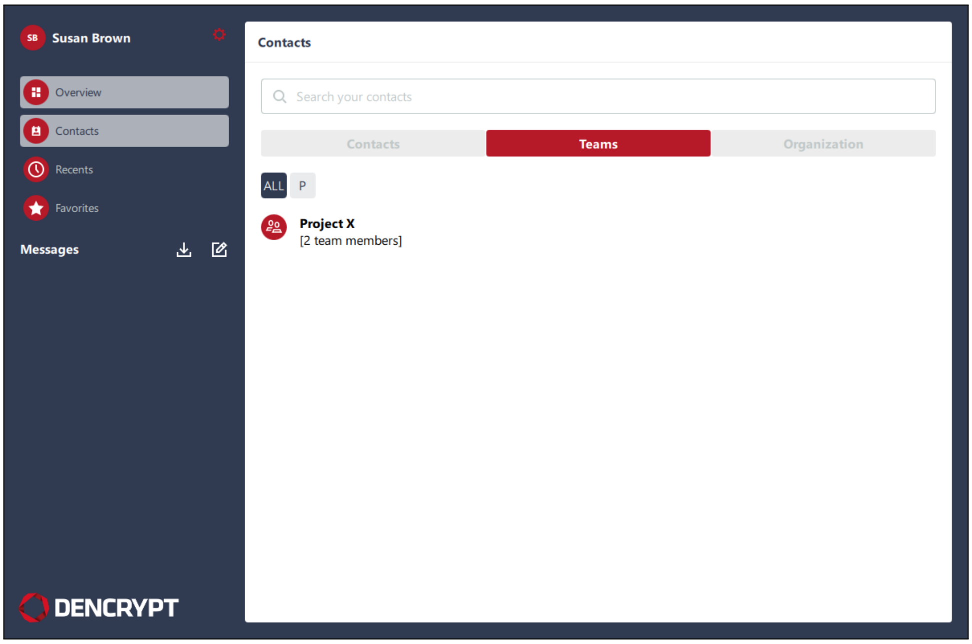


Figure 14: Team details.

4.1.2 Organisation

The Organsization is often used for navigating large phonebooks. The view structures the contacts by two levels: By organization and department (Figure 15). Filtering can be done for both with either the Alphabet selector or the Search field. The Alphabet selector will filter entries based on the first letter in their name while Search will match all occurrences in the full name. By tapping a contact, the contact details appear (figure 12).

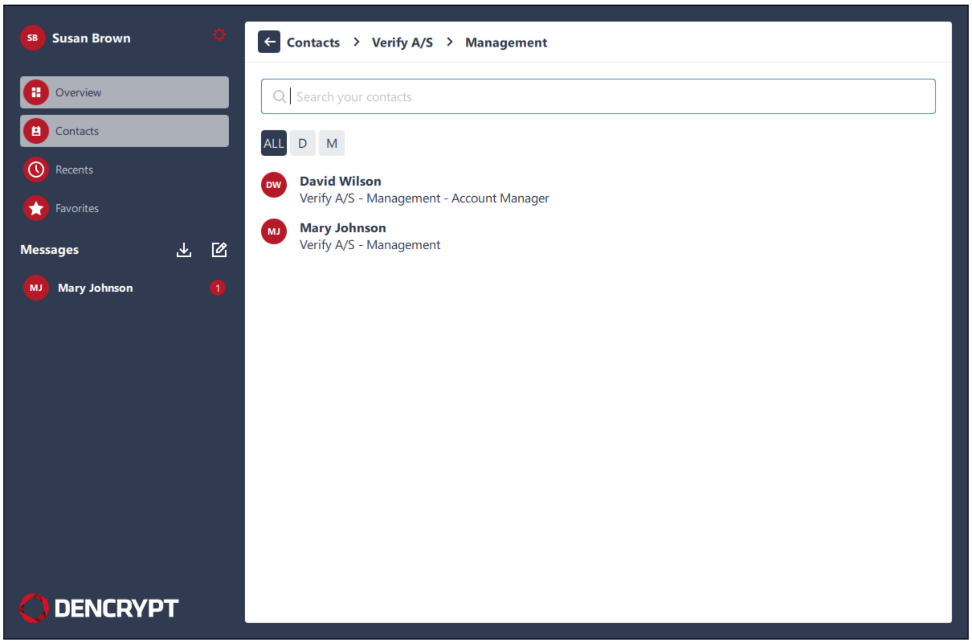


Figure 15: Organisation View

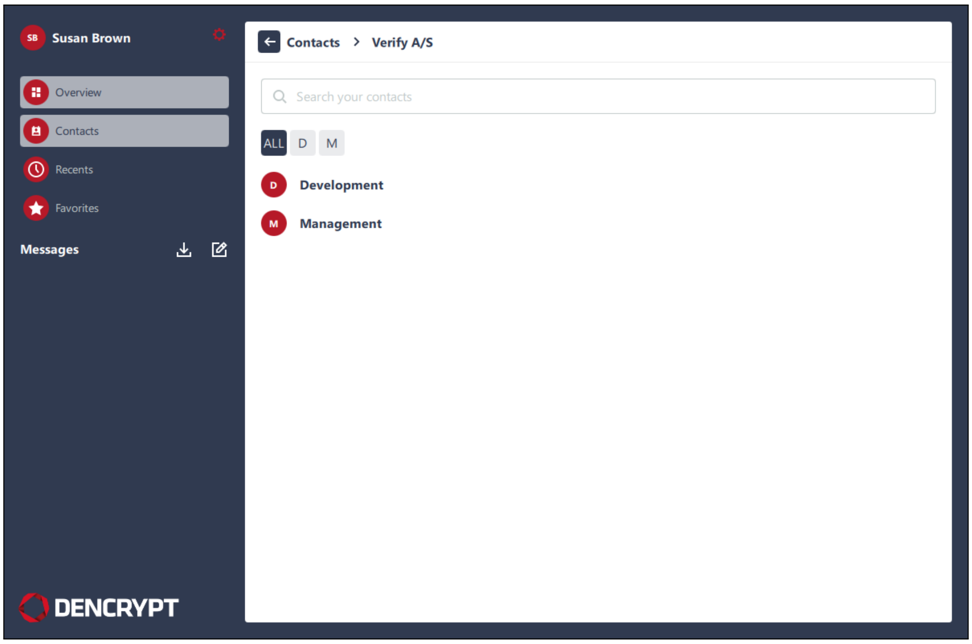


Figure 16: Departments View

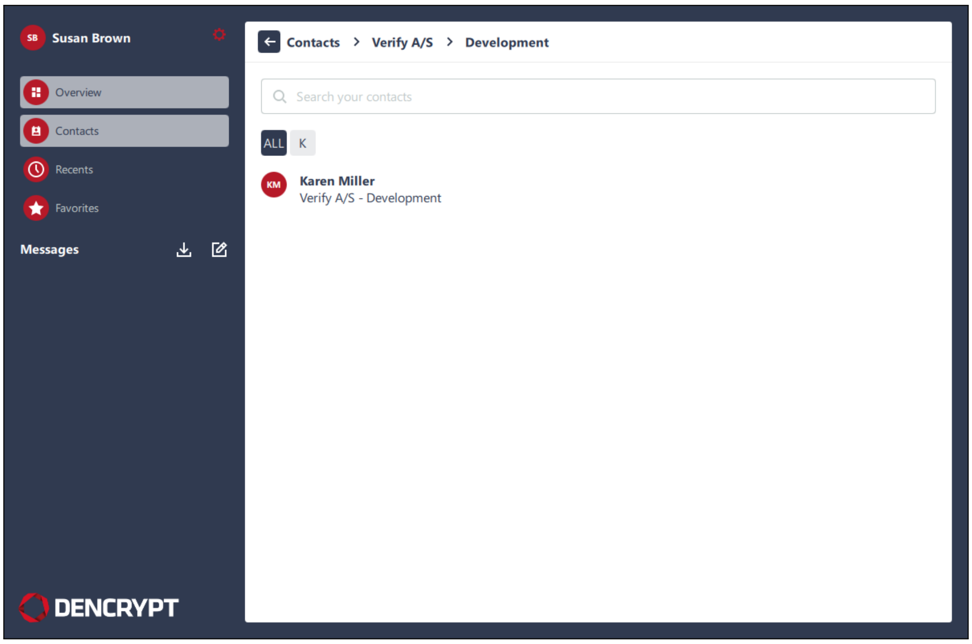
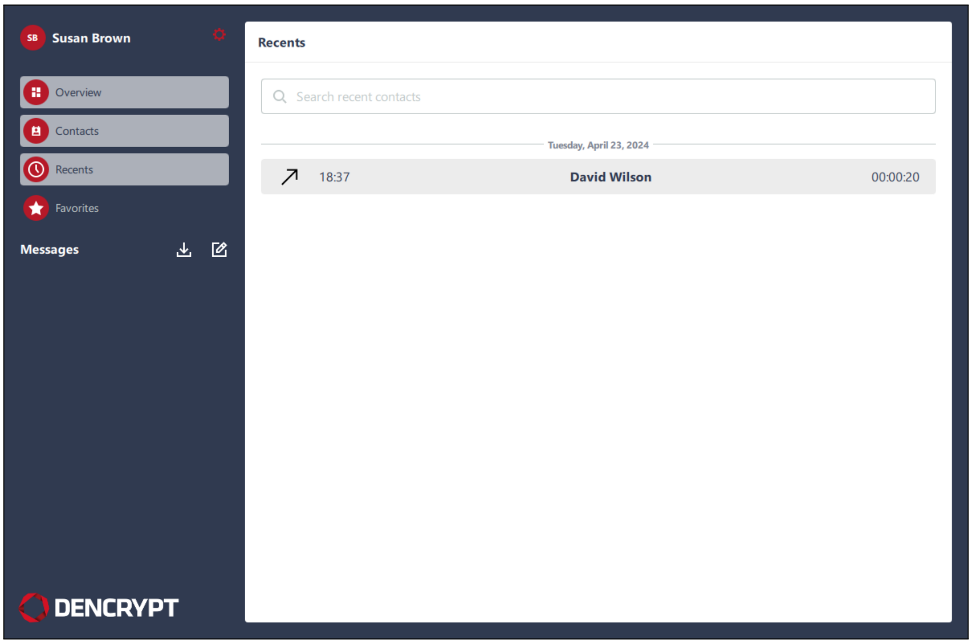


Figure 17: Department contacts

4.2 Recents

The Recents view lists recents calls in descending order. Selecting a contact will open the Contact details (figure 12) and allow the user to start a secure voice call, secure video call, or send a secure message.

The Search field can be used to filter the list. Search text will match all occurrences in the full contact name.



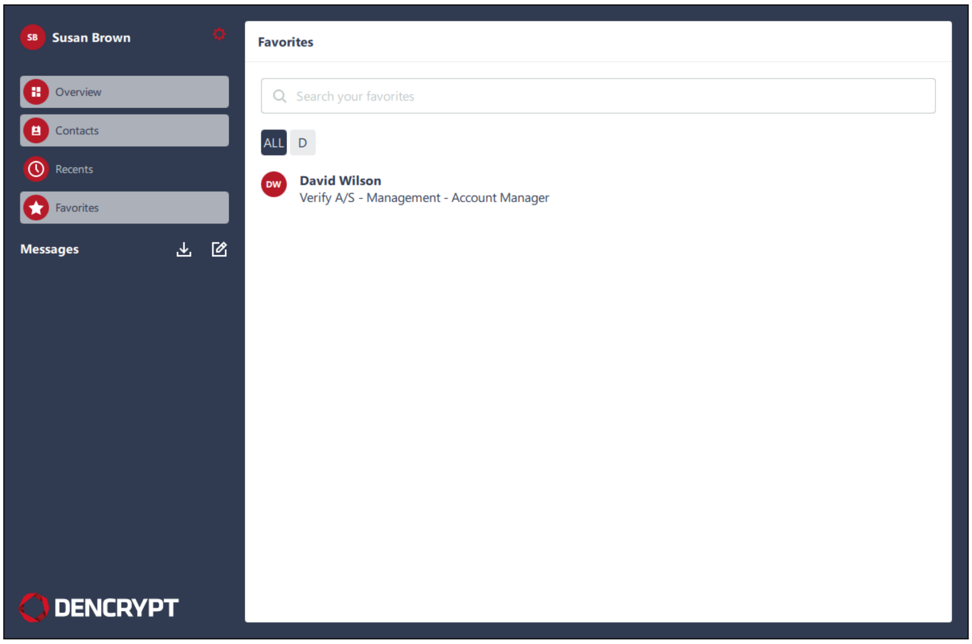
Tuesday, April 23, 2024

18:37 David Wilson 00:00:20

Figure 18: Recents

4.3 Favorites

The Favorites view lists favorite contacts for quick access. The list can filtered with either the Alphabet selector or the Search field. The Alphabet selector will filter favorites based on the first letter in their firstname while Search will match all occurrences in the full name. Selecting a contact will open the Contact details (figure 12) and allow the user to start a secure voice call, secure video call, or send a secure message.

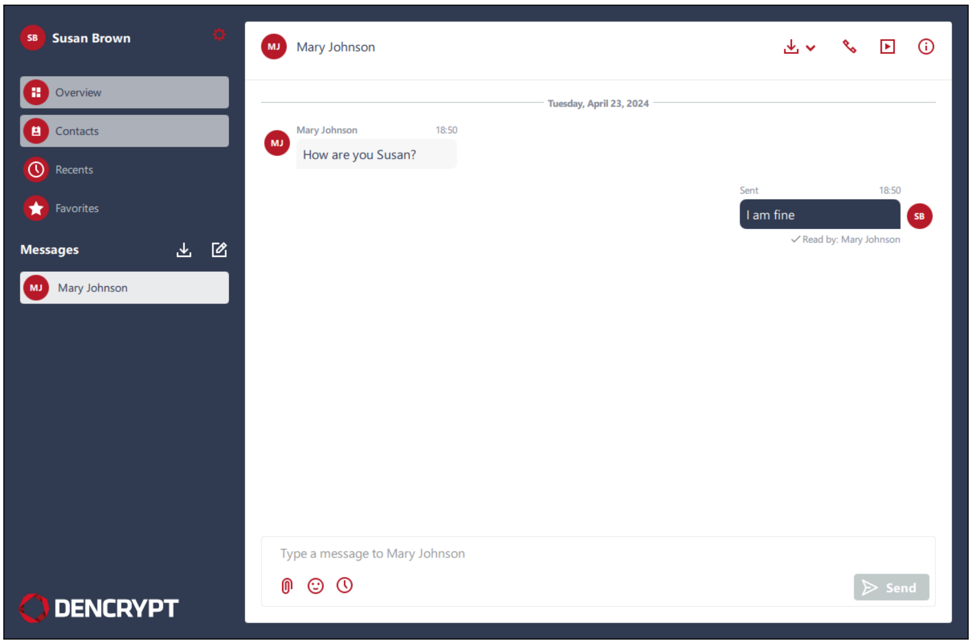


DW David Wilson
Verify A/S - Management - Account Manager

Figure 19: Favorites

4.4 Messages

The Message view lists the active chat rooms. Selecting a chatroom will open the conversation and allow the user to continue the message exchange. Also, team rooms are listed here. (Figure 26)



Tuesday, April 23, 2024

Mary Johnson 18:50
How are you Susan?

Sent 18:50
I am fine
✓ Read by: Mary Johnson

Type a message to Mary Johnson

Figure 20: Message View.

From the conversation window, the are several functionalities are available:

- ⬇: Export conversation (section 4.4.1)
- ☎ : To place a secure audio call (section 5)
- ▶ : To place a secure video call (section 5)
- ℹ: To modify the chat room (section 4.4.2)

4.4.1 Export messages

Messages can be exported in 3 ways. The ⬇-icon in the left pane will export all chat rooms. The ⬇-icon in individual chats has a dropdown to select either the entire chat or individual messages. A message is selected by left clicking with the mouse on a specific message in the chat room. Group and multi-selection is supported by holding shift or control respectively while left clicking with the mouse.

Each chat room is exported to an individual PDF-A along with SHA-512 digist.

The exported PDF will contain the following information:

- Chat room title
- Name of the exporter
- The chat room participants
- Date of the export

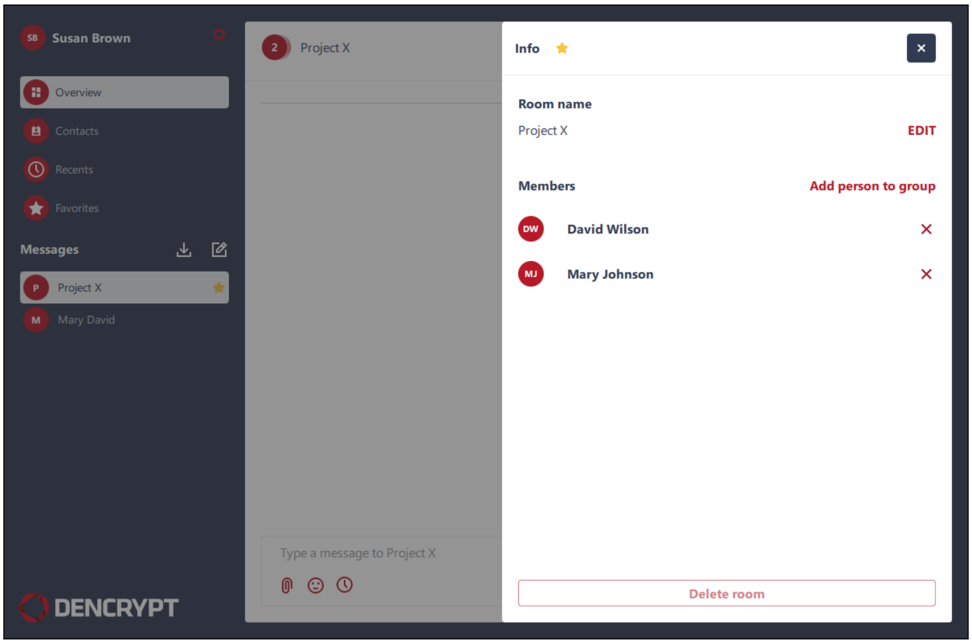
- Number of messages, word count and total number of characters
- For each message:
  - Message was sent or received (right or left aligned respectively)
  - List of contacts who have read and not read the message
  - The name of the sender
  - The message content
  - Time stamp for the message received.

4.4.2 Modify a chat room

Tapping the ⓘ-icon will open the chatroom information view (figure 21). From here, the chatroom can be modified by:

- Tap ★-icon to pin to the top of the list of chat rooms.
- Edit the chatroom title.
- Tap Add person to invite new contacts to the room (figure 23)
- Tap ✕-icon to remove a contact from the chatroom.

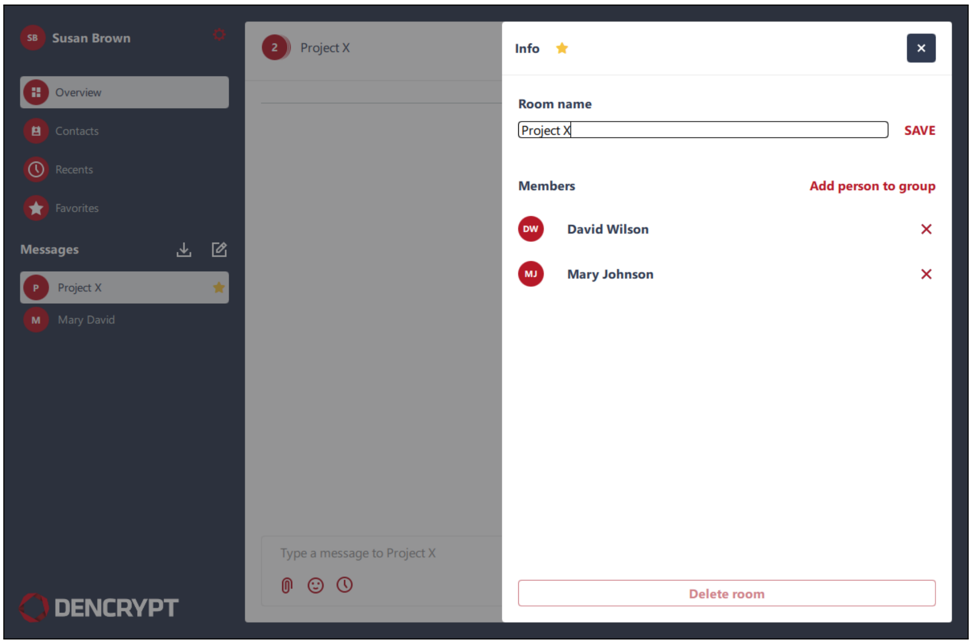
All chatroom members are notified about the changes (figure 24).



Room name
Project X

Members
David Wilson ✕
Mary Johnson ✕

Figure 21: Chatroom info window



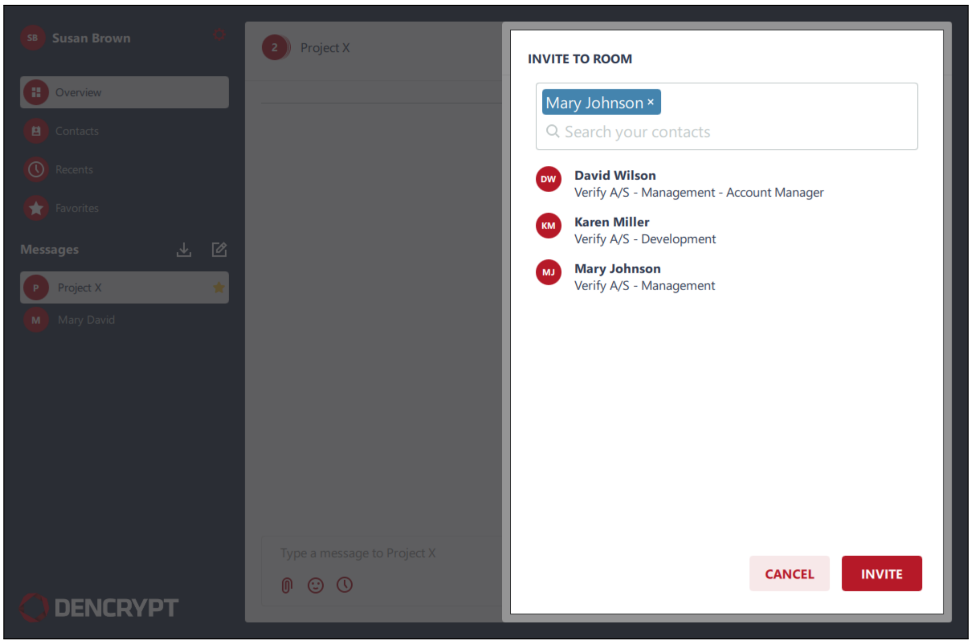
Room name: Project X

Members

David Wilson

Mary Johnson

Figure 22: Add to favorites and change title.



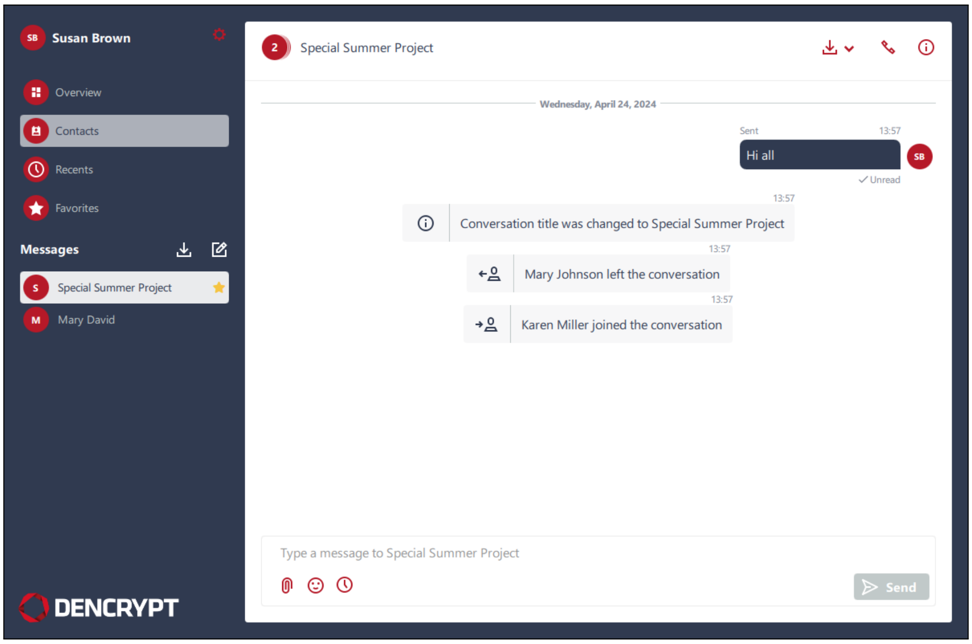
Mary Johnson ×

David Wilson
Verify A/S - Management - Account Manager

Karen Miller
Verify A/S - Development

Mary Johnson
Verify A/S - Management

Figure 23: Add contacts to chatroom



Wednesday, April 24, 2024

Sent 13:57
Hi all
✓ Unread

13:57
Conversation title was changed to Special Summer Project

13:57
Mary Johnson left the conversation

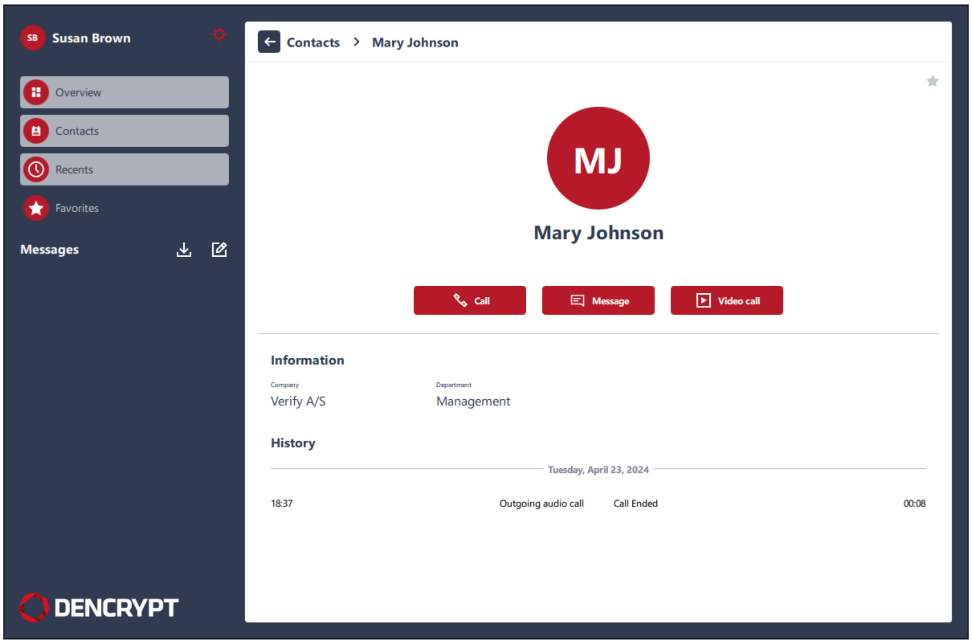
13:57
Karen Miller joined the conversation

Figure 24: Change notifications

5 Making a secure call

Be aware of the security instructions and the surrounding before making a secure call. Refer to [Security instructions 2] for instructions.

A secure call is initiated from Contact details screen or from a chat room by tapping the ☎-icon.



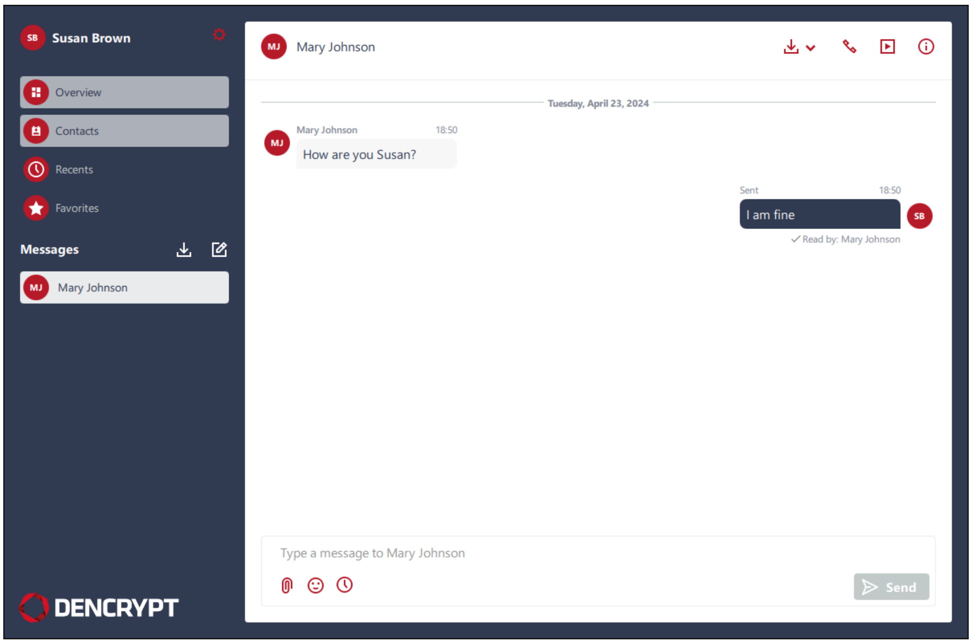
Company: Verify A/S

Department: Management

Tuesday, April 23, 2024

18:37 Outgoing audio call Call Ended 00:08

Figure 25: Place calls from contact details



Tuesday, April 23, 2024

Mary Johnson 18:50
How are you Susan?

Sent 18:50
I am fine
✓ Read by: Mary Johnson

Figure 26: Place calls from message View.

A secure call can only be made when Dencrypt Connex has a working internet connection. Secure calls are not possible during flight mode and with a poor data connection.

A secure audio call is initiated by tapping the Call button, which opens the Call screen. A secure video call is started by tapping the Video call button.

During the call setup, a status message will show the progress of the call setup. The call setup process is active until the call is answered, the call is timed out, or the receiving party rejects the call.

Once the call is answered, Dencrypt Connex authorizes the calling parties, exchanges encryption keys, and establishes a secure connection. When a secure connection is established, an audible notification is played, and the screen will display Authenticated, as shown in figure Figure 27. Audio is only transmitted when the connection is secured.

The usual call functionalities are available during a secure call, such as microphone muting and enabling speaker mode. During a secure video call, also disabling the camera is possible.

Tap the ⚙-icon to open the audio settings to configure input/output devices.

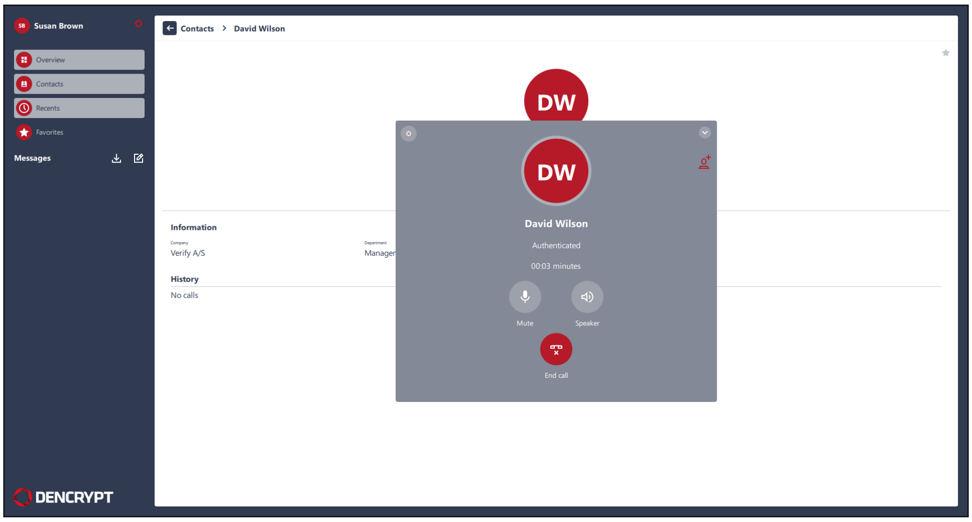


Figure 27: Secured voice call.

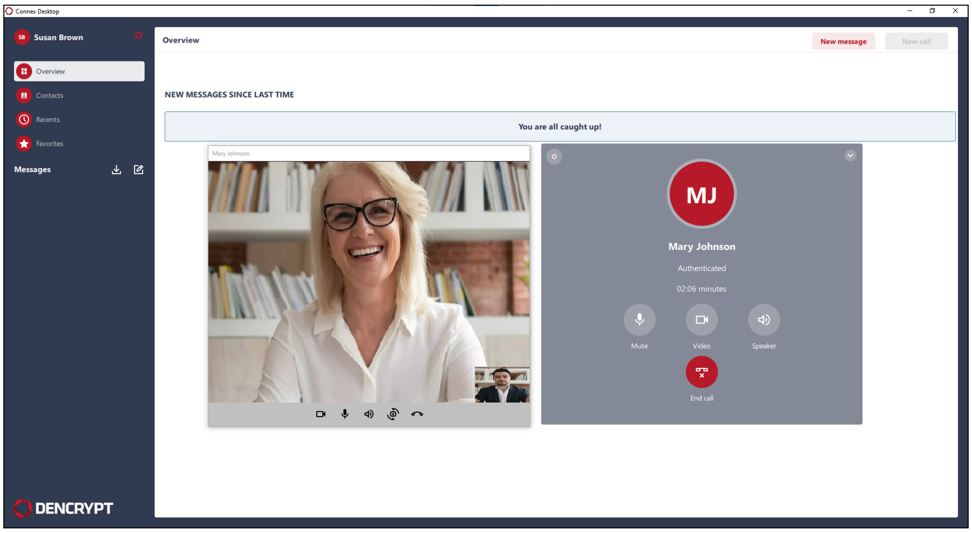


Figure 28: Secured video call.

5.1 Group calls

Group calls can be established by adding contacts to an ongoing conversation. Video group calls are not supported.

Add participants to an ongoing secure call.

Step 1: Establish a secure call [Making a secure call 5].

Step 2: Tap the 👤+-icon to open the phonebook.

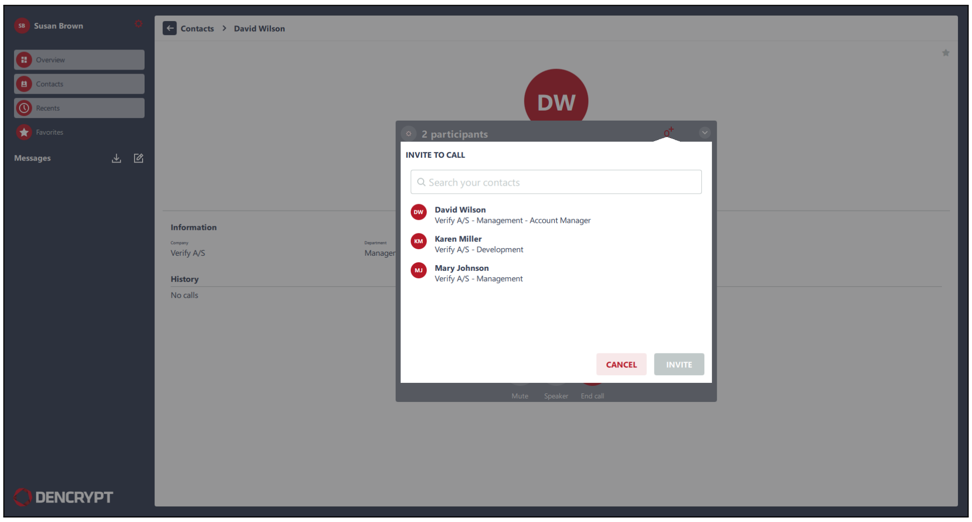
Step 3: Locate a contact in the phonebook and tap Invite. This will pause the ongoing call and establish a new secure call.

Step 4: Combine the two conversations by tapping Merge. The first call is resumed and merged with the second call.

Step 5: The In-call screen displays a list of participants.

Step 6: Repeat step 2 - 4 to add more participants.

Step 7: Tap End call button for a participant to remove the contact from the conversation.



INVITE TO CALL

Search your contacts

David Wilson
Verify A/S - Management - Account Manager

Karen Miller
Verify A/S - Development

Mary Johnson
Verify A/S - Management

Information

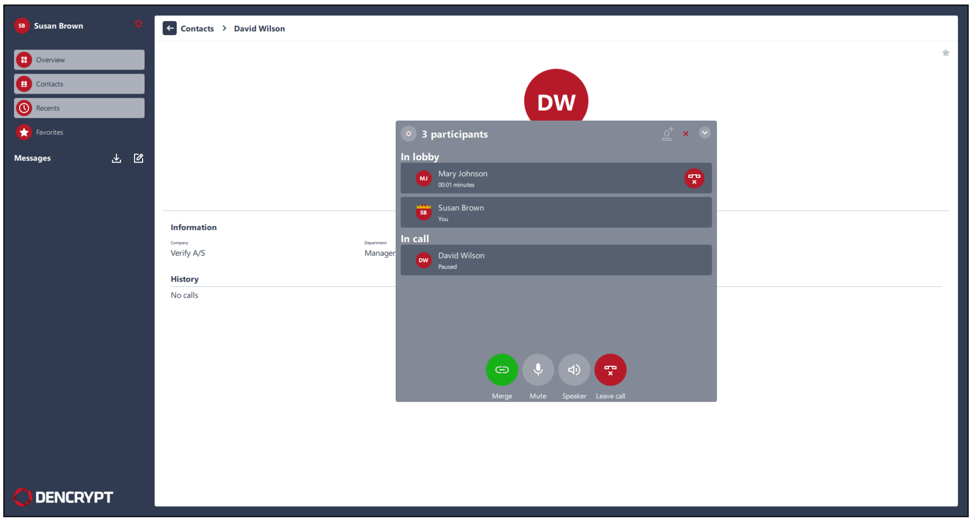
Company: Verify A/S

Department: Manager

History

No calls

Figure 29: Invite participant to call



Information

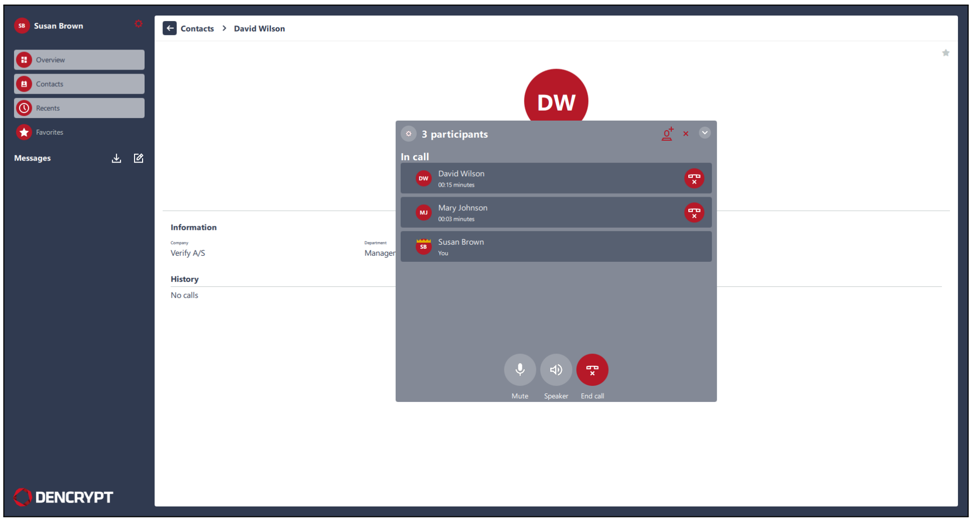
Company
Verify A/S

Department
Manager

History

No calls

Figure 30: Merge calls



Information

Company
Verify A/S

Department
Manager

History

No calls

Figure 31: Merge calls

5.2 Incoming secure calls

Incoming secure voice calls are alerted by notifications and on the incoming call screen

When answering the call, the Dencrypt Connex authorizes the calling parties, exchanges encryption keys, and establishes a secure connection. A waiting tone is played during the setup process, indicating that the secure channel is being established. Voice data is only transmitted when the secure channel is established.

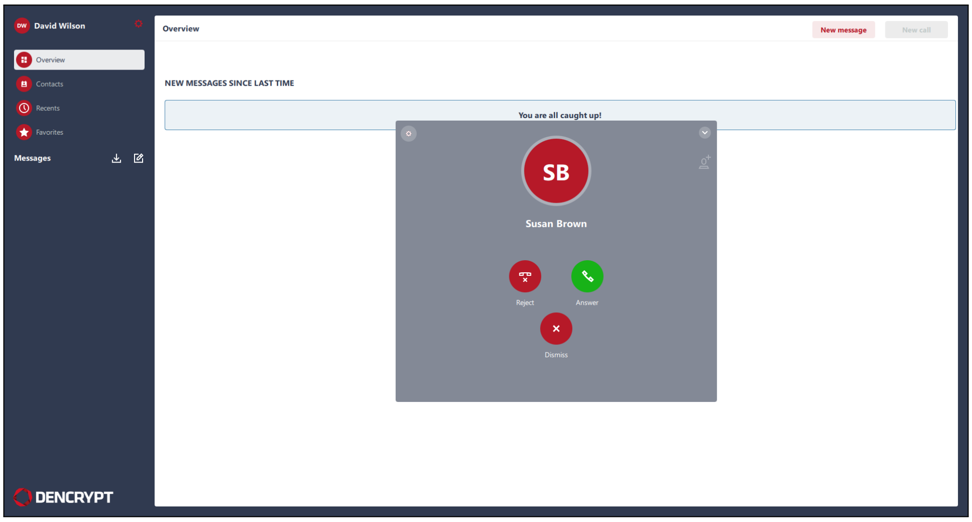


Figure 32: Incoming call

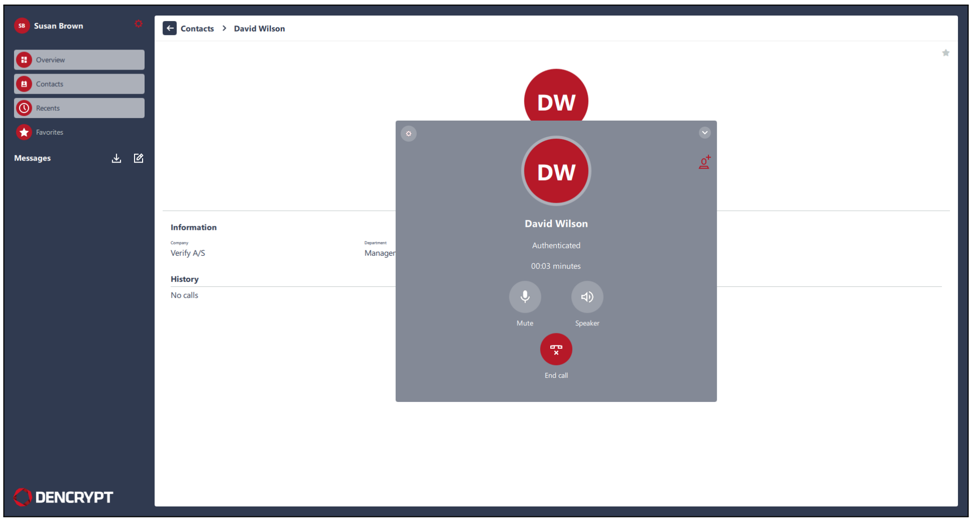


Figure 33: Secured voice call.

6 Sending a secure message

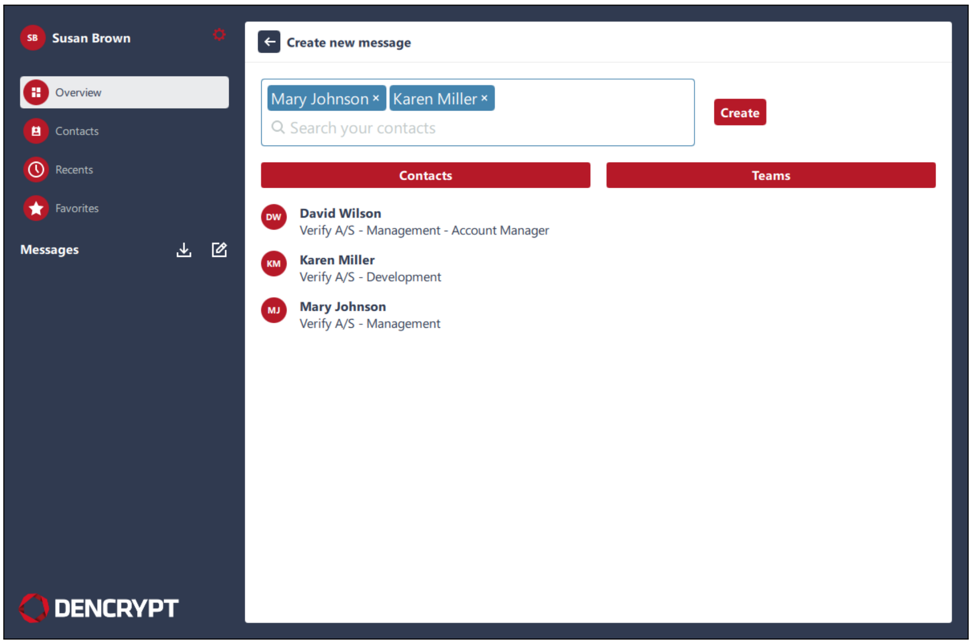
The Messages sections list all the ongoing conversations (chat rooms). Initially, the message conversation list is empty.

Creating a conversation

Step 1: Tap the ✎-icon to create a new message, or from the contact detail screen: Tap Message (figure 12).

Step 2: Add recipients by typing their names (suggestions are shown while typing) or select from the phonebook.

Step 3: Tap Create to start composing the first message.



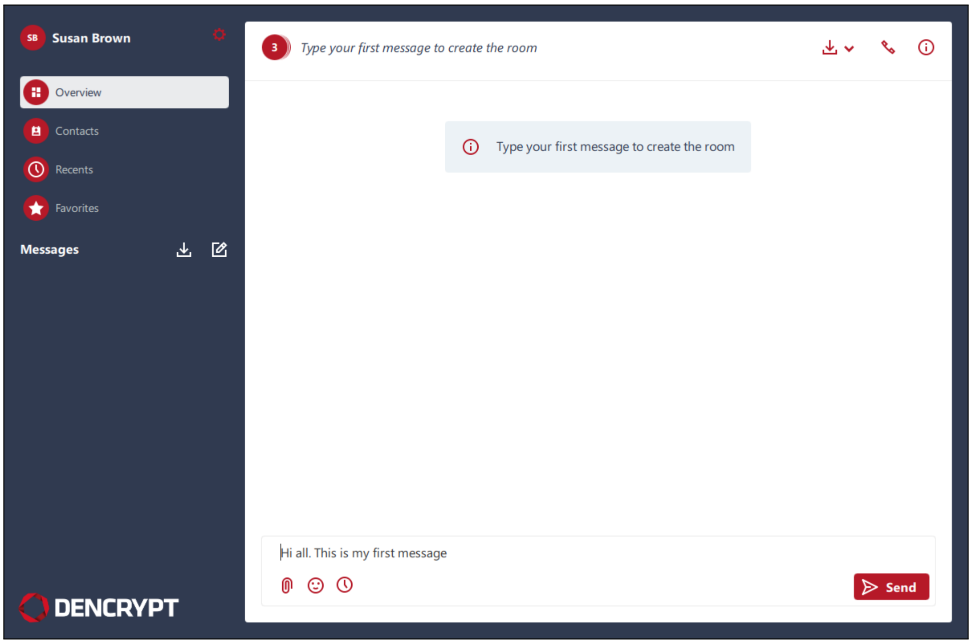
Mary Johnson × Karen Miller ×
Search your contacts

David Wilson
Verify A/S - Management - Account Manager

Karen Miller
Verify A/S - Development

Mary Johnson
Verify A/S - Management

Figure 34: Create new conversation.



Type your first message to create the room

Hi all. This is my first message

Figure 35: Compose a first message.

Sending a secure message

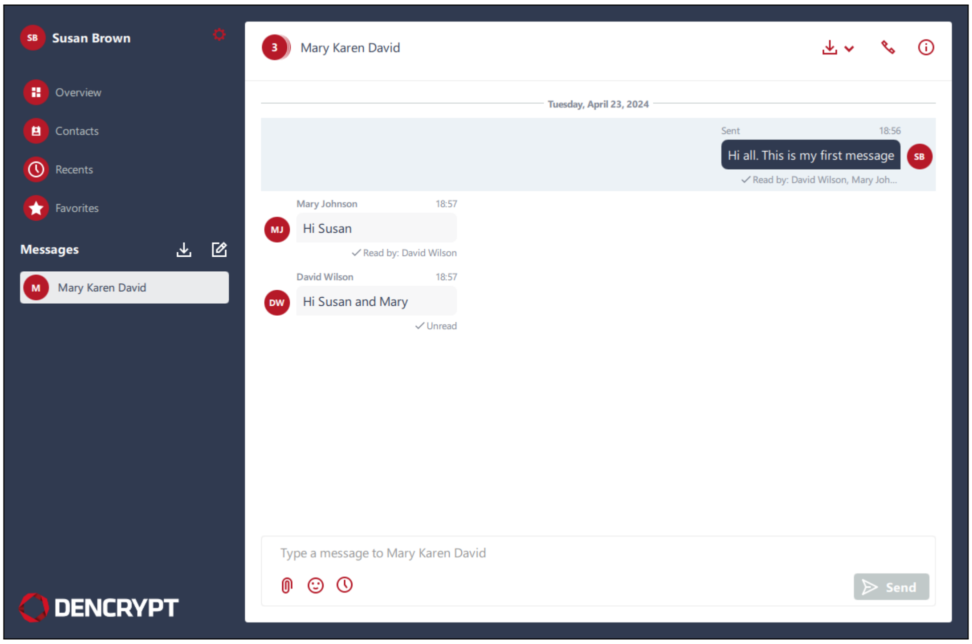
Step 1: Select an existing Conversation or tap 📝-icon icon to create a new.

Step 2: Enter text and tap Send.

The message is encrypted and transmitted immediately when an active data connection exists. A successful transmission is indicated by the status Sent.

A message pending transmission is indicated by status Sending. The message is stored encrypted, and automatic retransmission will be attempted while the app is open.

Incoming messages are alerted by a banner notification (see figure 36). The notification is visible for app. 5 seconds.



Tuesday, April 23, 2024

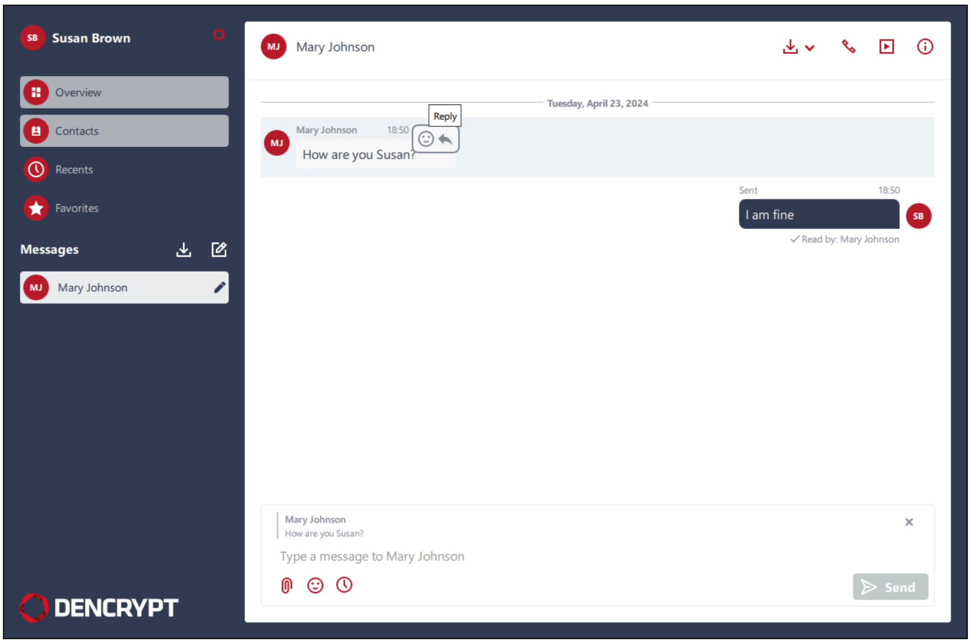
Sent 18:56
Hi all. This is my first message
✓ Read by: David Wilson, Mary Joh...

Mary Johnson 18:57
Hi Susan
✓ Read by: David Wilson

David Wilson 18:57
Hi Susan and Mary
✓ Unread

Figure 36: Message conversation

Individual messages can be replied to by hovering over the message and clicking the reply icon (see figure 37).



Tuesday, April 23, 2024

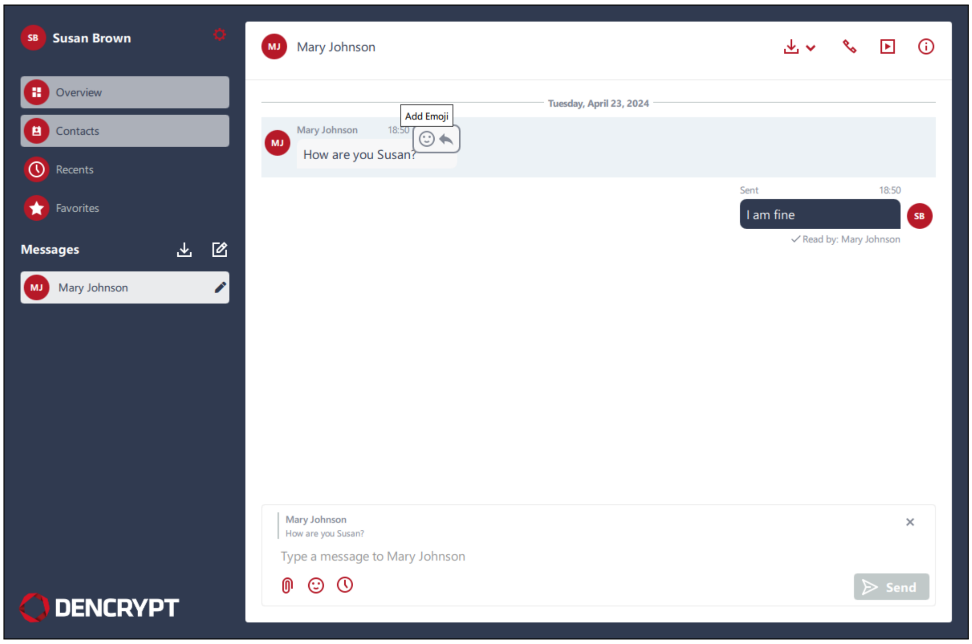
Mary Johnson 18:50
How are you Susan?

Sent 18:50
I am fine
✓ Read by: Mary Johnson

Mary Johnson
How are you Susan?

Figure 37: Message reply

Likewise, a reaction can be attached to a message by hovering over the message and clicking the emoji icon (see figure 38).



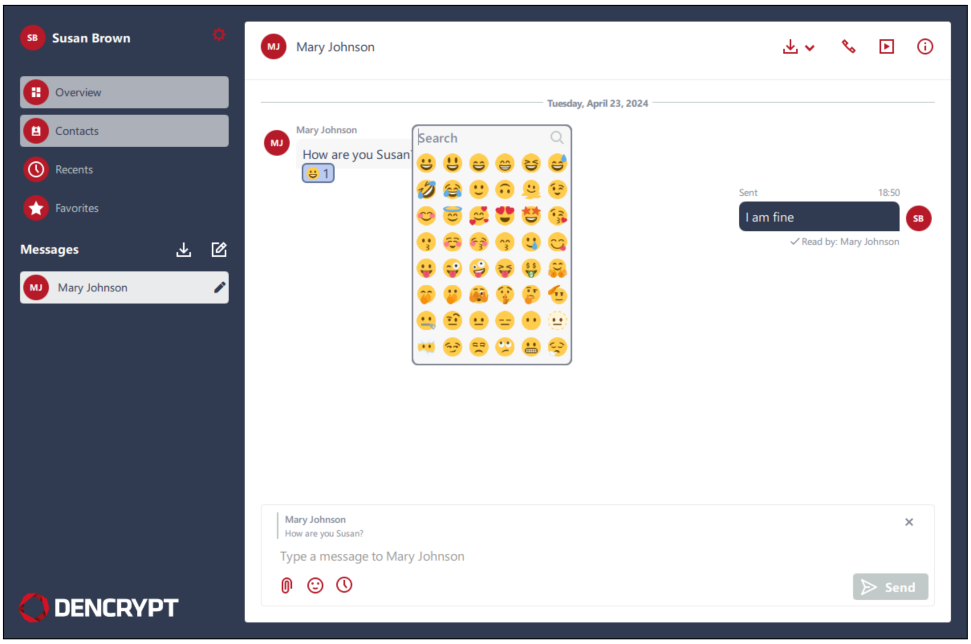
Tuesday, April 23, 2024

Mary Johnson 18:50
How are you Susan?

Sent 18:50
I am fine
✓ Read by: Mary Johnson

Mary Johnson
How are you Susan?
Type a message to Mary Johnson

Figure 38: Message reaction



Tuesday, April 23, 2024

Mary Johnson
How are you Susan
😀 1

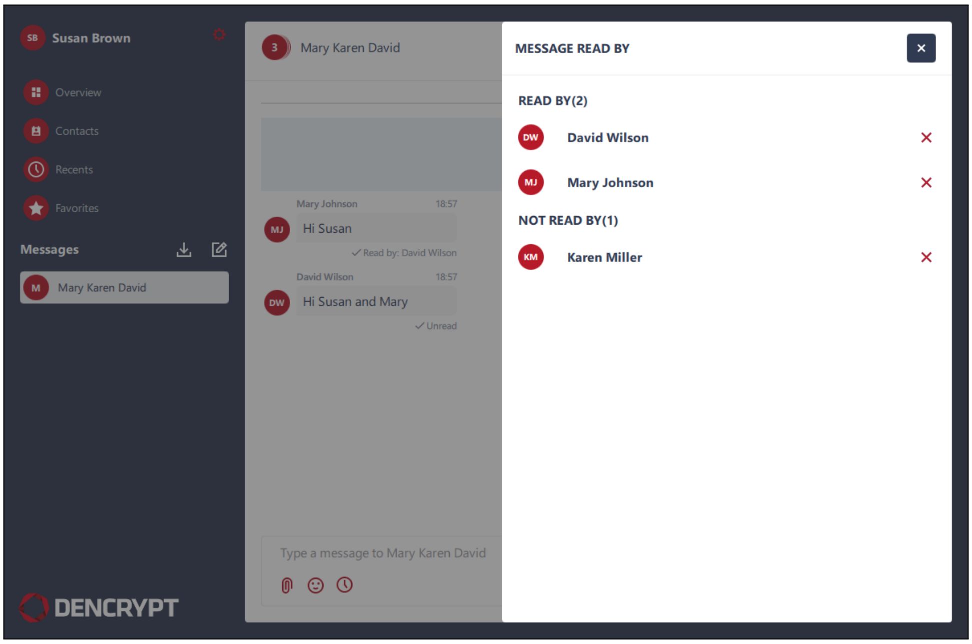
Sent 18:50
I am fine
✓ Read by: Mary Johnson

Mary Johnson
How are you Susan?
Type a message to Mary Johnson

Figure 39: Chat with reaction and reply

6.1 Message delivery status

A delivery status for sent messages is displayed under each message in the conversation screen, indicating who has read the message. Tapping the status field under the message opens a detailed delivery status window.



Mary Johnson 18:57
Hi Susan
✓ Read by: David Wilson

David Wilson 18:57
Hi Susan and Mary
✓ Unread

Figure 40: Delivery status

6.2 Sending attachments

Sending attachments

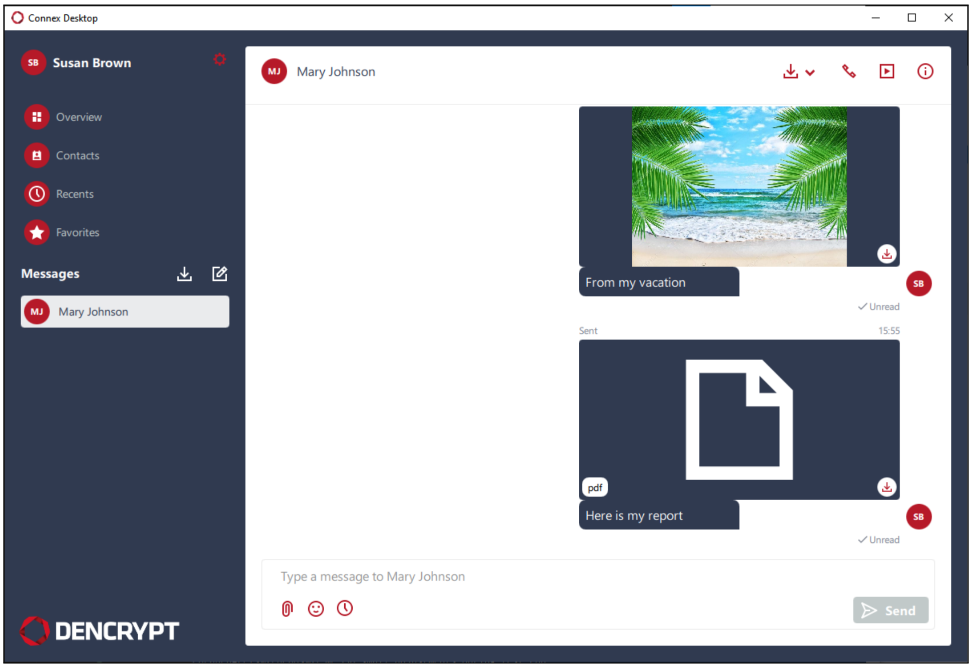
Step 1: Select an existing Conversation or tap ✎-icon icon to create a new.

Step 2: Tap 🖻-icon to open the windows file browser.

Step 3: Select the file and tap Open

Step 4: Enter text and tap Send.

Images are previewed. Tap the preview to show the image in full size, or tap ⬇to save an attachment.



From my vacation

Here is my report

Figure 41: Sending attachment

6.3 Message expiry timer

Message expiry is used to set time constraints on a message making it available in defined time periods only.

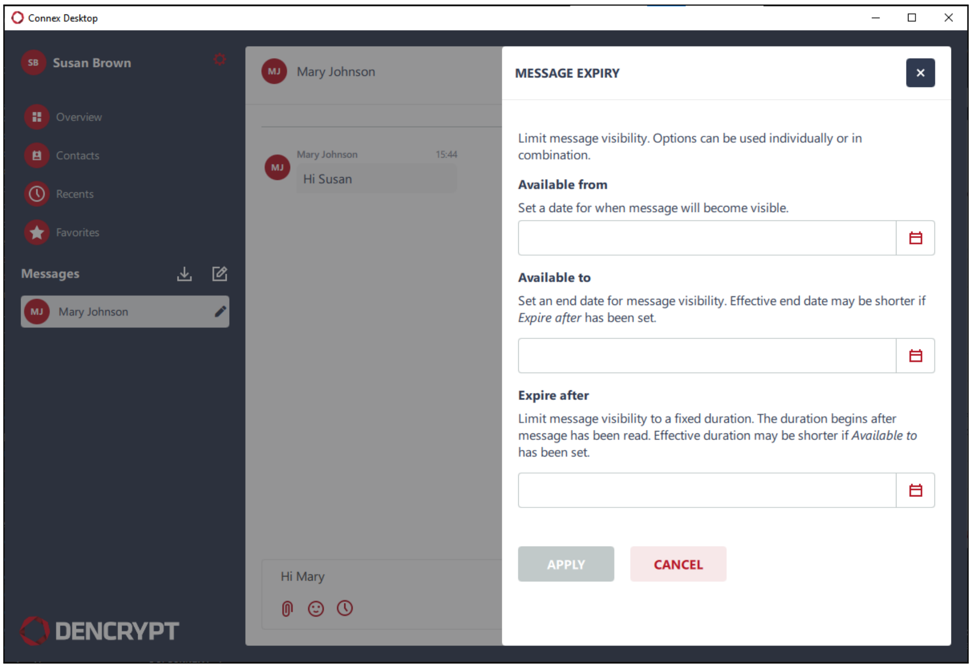
Set time constraints on messages

Step 1: Tap 🕓-i conto open the Message expiry configuration screen.

Step 2: Set one or more condition.

Step 3: Tap Apply

Step 4: Write message and tap Send



Mary Johnson 15:44

Hi Susan

MESSAGE EXPIRY

Limit message visibility. Options can be used individually or in combination.

Available from

Set a date for when message will become visible.

Available to

Set an end date for message visibility. Effective end date may be shorter if *Expire after* has been set.

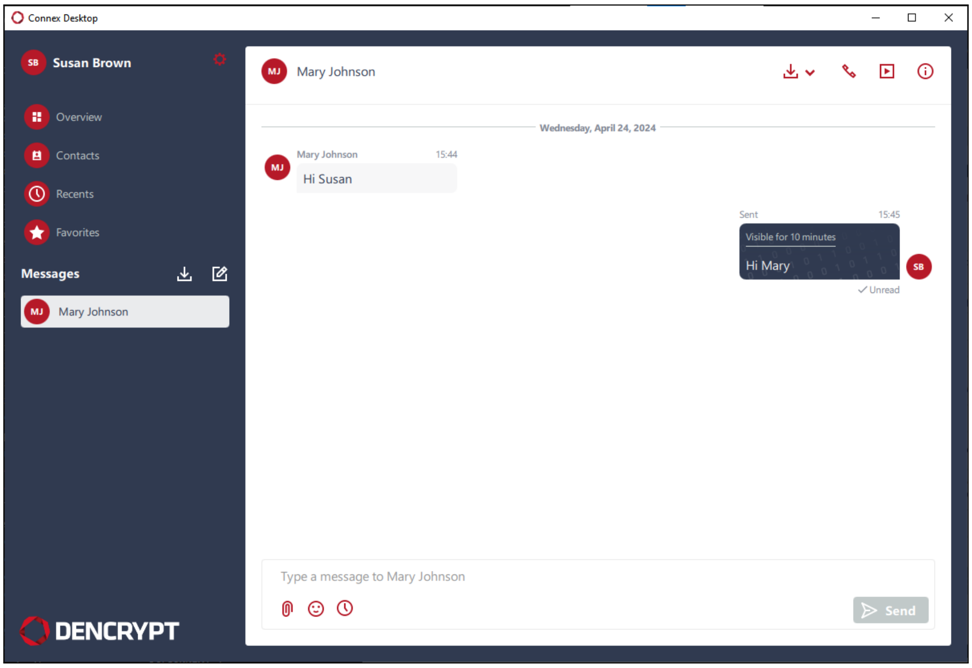
Expire after

Limit message visibility to a fixed duration. The duration begins after message has been read. Effective duration may be shorter if *Available to* has been set.

APPLY CANCEL

Hi Mary

Figure 42: Message expiry configuration



Wednesday, April 24, 2024

Mary Johnson 15:44

Hi Susan

Sent 15:45

Visible for 10 minutes

Hi Mary

✓ Unread

Type a message to Mary Johnson

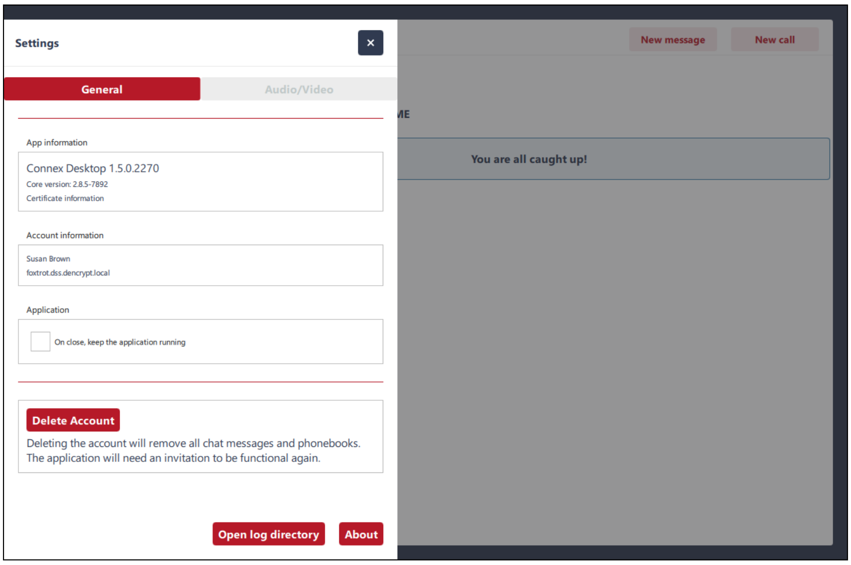
Figure 43: Message send with expiry.

7 Settings

Dencrypt Connex settings are opened by tapping the ⚙-symbol in the top left corner of the main screen.

Most of the configuration of Dencrypt Connex is performed centrally by the system administrator. The Settings menu provides the following information/options:

- **General**
  - App information - Application name and full version number.
  - Account information - Account name and server system domain name.
  - Tap Delete account and accept warning to delete account. Notice: This will permanently delete all data, including call logs, messages, and attachments.
  - Tap Check for updates to show possible new application releases.
- **Audio/Video**
  - Audio Output Device - Selected output device.
  - Audio Input Device - Selected input device.
  - Camera - Selected camera for video calls.
  - Video Resolution - Preferred resolution for the video stream.



Settings

App information

Connex Desktop 1.5.0.2270
Core version: 2.8.5-7892
Certificate information

Account information

Susan Brown
foxtrot.dss.dencrypt.local

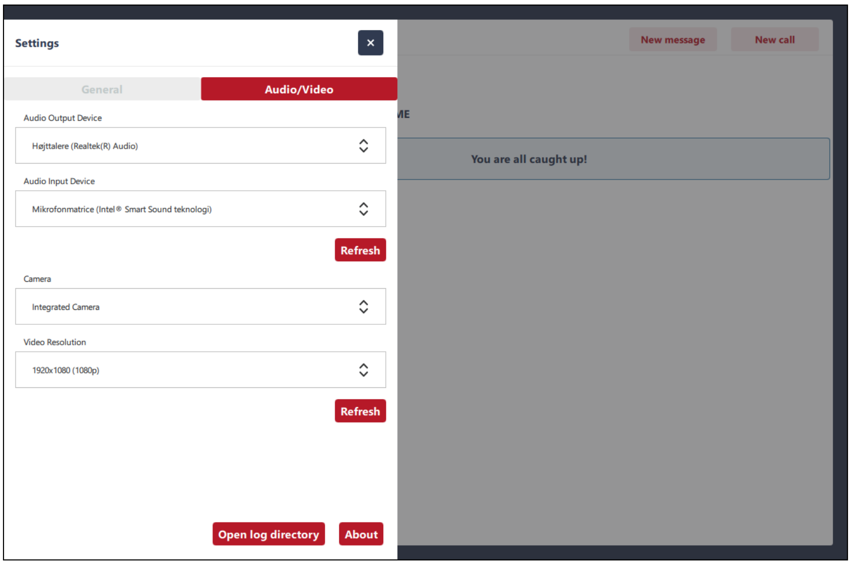
Application

□ On close, keep the application running

Deleting the account will remove all chat messages and phonebooks.
The application will need an invitation to be functional again.

You are all caught up!

Figure 44: Settings menu - General



Audio Output Device: Højttalere (Realtek(R) Audio)

Audio Input Device: Mikrofonmatrice (Intel® Smart Sound teknologi)

Camera: Integrated Camera

Video Resolution: 1920x1080 (1080p)

Figure 45: Settings menu - Audio

Appendices

A Dencrypt Communication Solution

The Dencrypt Communication Solution is an encrypted Voice-over-IP-based communication system that offers encrypted mobile voice/video communication and instant messaging within closed user groups. Once Dencrypt Connex is installed and provisioned, it allows for two or more persons to talk securely or exchange instant messages securely.

The solution consists of Dencrypt Connex , a smartphone application (app) installed on the end-users smartphone, and a Dencrypt Server System as illustrated in Figure 46. The Dencrypt Server System is responsible for setting up the encrypted calls, routing messages, and distributing an individual phonebook to each device, defining to whom calls and messaging can be performed. The server system is also responsible for initiating the provisioning process for the first-time activation.

The server system only facilitates call setup and message routing. It is not capable of decrypting voice calls or messages as these are end-to-end encrypted between devices.

The Dencrypt Connex application is installed from or pushed by a Mobile-Device-Management (MDM) system. The Dencrypt Server System is managed by a system administrator.

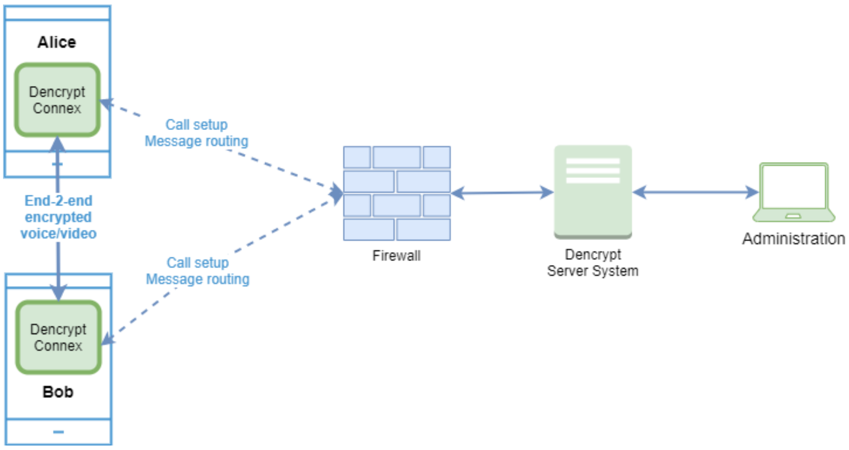


Figure 46: Dencrypt Communication Solution.

A.1 End-2-end encrypted VoIP calls

For secure voice and video calls, an end-to-end encrypted connection between the devices is established using the mobile internet or wifi-networks. Only the data transmission between the devices is protected. The audio/video connection between the user and the device through the microphone, speaker, headset, or screen is not protected as illustrated in Figure 47

Once a connection is established, the exchange of encryption keys happens automatically and directly between the two devices. The key exchange is initiated when a call is answered and a data connection is established. At call termination, encryption keys are permanently removed from the device and cannot be recovered.

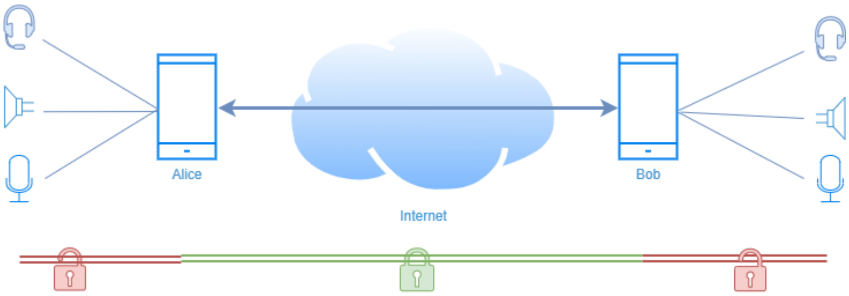


Figure 47: Area of protection for voice/video calls.

A.2 End-2-end encrypted instant messaging

Also, instant messaging is encrypted end-2-end between devices and transmitted, via the Dencrypt Server System, over the mobile internet or wifi-networks. Both the message exchange and the storage on the device (chat history) are protected, whereas the connections to external keyboards or screens are not protected, as shown in Figure 48.

The key exchange happens directly between the communicating devices but is facilitated by the Dencrypt Server System, which also queues the encrypted messages for delivery.

The message history is stored encrypted on the device and requires two keys for decryption: 1) A local key protected by the trusted platform module on the device and 2) a remote key stored on the server system. Hence, the chat history is only accessible when a data connection to the server has been established. The remote key is destroyed when the app is closed.

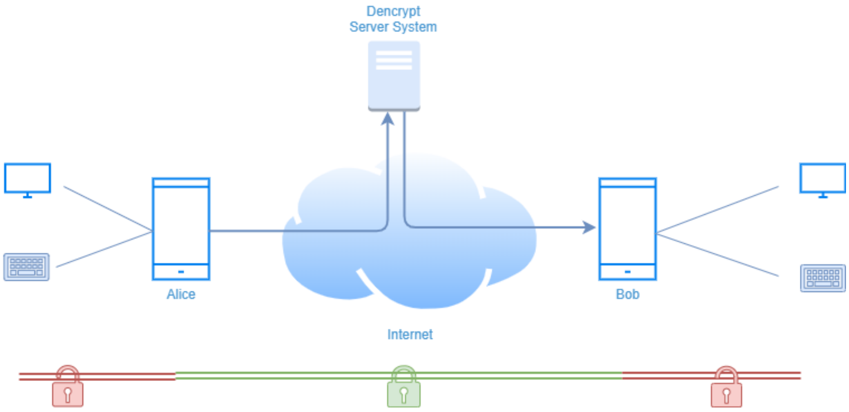


Figure 48: Area of protection for instant messaging

A.3 Authenticated connections

All communication between the Dencrypt Connex and the Dencrypt Server System takes place over mutually authenticated connections. Hence, the server system will only accept connections from authenticated users, and the app will only connect to authorized server systems. The authentication is automatic and does not require user actions besides the initial provisioning.

A.4 Encryption keys

All encryption keys for voice/video calls and for instant messaging are generated automatically when a new conversation is initiated and does not require user actions. Encryption keys are overwritten in memory when a call is terminated or when the app is closed or put in the background.

A.5 Secure phonebook

To ensure that only authorized persons can communicate, the Dencrypt Communication Solution applies a centrally managed and individual phonebook. The phonebook defines with whom a user can communicate. The phonebooks are generated by the system administrator, and updates are pushed to the apps when they connect to the server system. Hence, the phonebook is always up-to-date without any user actions required. The phonebook is stored encrypted on the device using the same key management as for the chat history.

The phonebook concept supports two-way and one-way conversations. Hence, it is possible to receive calls from persons not listed in the phonebook and without being able to call back. Messages received from not listed contacts can be answered.

A.6 Push notifications

Push notification services from are used for alerting on incoming secure calls and messages. The push messages are sent either with empty content or with encrypted content.