

Common Criteria Configuration Guide

SecuSUITE v5.0
SteelBox v5.0

Version 1.1



Contents

1	Acronyms	5
2	References.....	6
3	Document history	7
4	Variants of the TOE.....	8
5	General Common Criteria Configuration	11
6	Security Functionality covered by the Common Criteria Evaluation	12
7	Setting up secure voice communication with SecuSUITE	13
7.1	Supported devices and firmware	13
8	Installing and activating the SecuSUITE app	14
8.1	Installing the SecuSUITE app	14
8.2	Activating the SecuSUITE app.....	14
8.3	Setting a device screen lock	15
8.3.1	Android	15
8.3.2	iOS	16
8.4	SecuSUITE app can ask for an additional layer of security	16
8.5	Additional notifications about battery optimization (optional)	16
8.6	Onboarding and empty home page	18
9	SecuSUITE app	19
9.1	SecuSUITE home page	19
9.1.1	Further actions on the home page	20
9.1.1.1	Android	20
9.1.1.2	iOS	20
9.2	Your contacts in the app	21
9.2.1	VIP contacts	22
9.2.2	Display of contact card	22
9.2.3	Updating, editing, or deleting SecuSUITE contacts	23
9.2.3.1	Exception: Manually updating, editing, or deleting manually added SecuContacts or VIP contacts.....	23
10	Secure calls.....	24
10.1	Making a one-to-one SecuSUITE call	24
10.1.1	Call integration on iPhones for one-to-one calls	26

10.1.2	Icons for call status	27
10.1.3	Information about call participants.....	27
10.1.4	Authentication	28
10.2	Accepting secure calls with SecuSUITE	28
10.2.1	SecuSUITE background operation.....	28
10.2.2	Receiving SecuSUITE calls	29
10.2.3	Receiving concurrent calls	29
10.2.4	Placing SecuSUITE calls in the background	30
10.3	Saving a secure contact	31
10.4	Starting a secure group call.....	33
10.4.1	Start or join a secure group call from an existing group chat.....	33
10.4.2	Beginning a new group call	34
10.4.3	Setting up a new group call.....	35
10.4.4	Invite additional participants during an ongoing group call.....	36
10.4.5	Information about group call participants.....	37
10.4.6	Call integration on iPhones for group calls.....	38
10.5	Bluetooth audio options during a call.....	39
10.6	Types of secure calls.....	40
10.6.1	Indications for different types of calls	40
10.6.2	Complete list of call scenarios.....	41
10.6.3	The risks of call forwarding	41
11	Secure messaging	42
11.1	One-to-one chat	42
11.1.1	Inside a one-to-one chat	43
11.1.2	Message actions	43
11.1.3	Delivery and Read Receipts	44
11.2	Group chat	45
11.2.1	Adding people to an existing group	45
11.2.2	Group settings.....	46
11.2.3	Delivery and Read Receipts in Group chats.....	46
11.3	Receiving secure messages	47
11.4	Replying to messages.....	48
12	Share content	49

12.1	Share content in chats on Android	49
12.2	Share content through share extension on Android	51
12.3	Share content on iOS	52
13	Settings.....	53
13.1	SecuSUITE settings.....	53
13.1.1	Account information	53
13.2	General phone settings.....	53
13.2.1	Notifications.....	53
13.2.2	Disable voice dictation.....	53
13.2.3	Bluetooth settings	54
13.3	Download options for shared content	54
14	SecuSUITE Client Updates	56
	Update of 3 rd party libraries.....	56
14.1	Client Software Version	56
14.2	Client update via App Stores	56
15	SecuSUITE FAQ	58
15.1	What if I can't hear call audio?	58
15.2	What's my phone number?	58
15.3	What prefixes do I need to dial?.....	58
15.4	How can I reach someone who is not registered in my tenant?	58
15.5	Why can't I see the contact of an important person in my tenant?	58
15.6	What does each sound notification mean?	59
15.7	Why can't I share a selected file?	59

1 Acronyms

Term	Definition
CCTL	Common Criteria Testing Laboratory
CLI	Command Line Interface (Local console and SSH access)
CRL	Certificate revocation list
CSR	Certificate signing request
ECC	Elliptic curve cryptography
NDCPP	Network devices collaborative protection profile
RSA	Rivest-Shamir-Adleman cryptosystem
RTP	Real-time transport protocol
SCA	Secure client authentication
SGLVN	SecuGATE LVN
SSH	Secure shell
TOE	Target of evaluation
TSF	Target of evaluation security function

2 References

Ref.	Document
[A]	SecuGATE Common Criteria User Guide version 0.7
[B]	Protection Profile for Application Software Version 1.4
[C]	Extended Package for Voice and Video over IP (VVoIP) Version 1.0
[D]	SecuSUITE Client v5.0 and SteelBox v5.0 Security Target Version 0.6

3 Document history

Version	Date	Status	Author	Comments
0.9	18-Sep-2022	Draft	BlackBerry	For Gossamer review
1.0	29-Sep-2022	Final	BlackBerry	Updated after Review
1.1	05-Dec-2022	Final	BlackBerry	Review comments addressed

4 Variants of the TOE

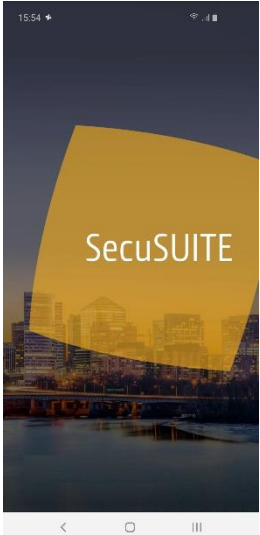

The TOE is represented either by an instance of the BlackBerry SecuSUITE 5.0 application or the rebranded CACI SteelBox 5.0 client. Both representations are identical from functional perspective and only differ in the look and feel and from App Store publishing perspective (separate product and publisher).

Compared to the SecuSUITE client, the SteelBox variant has:

- Updated Product Name shown in headlines and notifications (where applicable)
- Application package names used for App Store publishing
- Own start-up splash screen and EULA text
- Own Status icon (used in status bar and notification center)

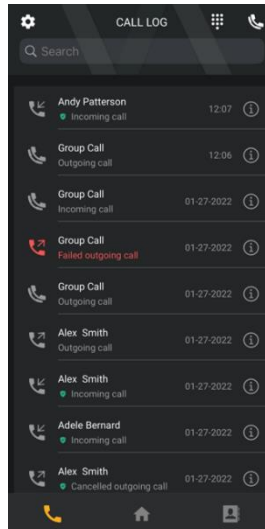
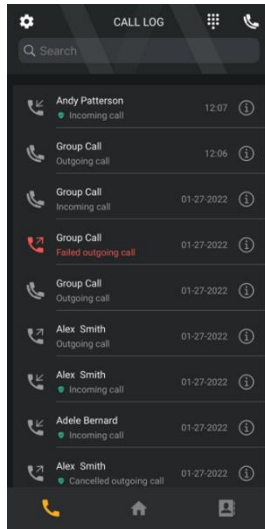
All configuration guidance provide in this CC documentation refers to the SecuSUITE and SteelBox clients even if only “SecuSUITE” is mentioned in one of the following chapters.

Examples of the graphical deltas between the two representations of the TOE:

UI Screen	SecuSUITE Client	SteelBox Client	Comment
<p>Splash Screen</p>	 <p>The image shows the SecuSUITE splash screen. It features a dark background with a cityscape at night. A large, semi-transparent yellow shape is overlaid on the cityscape, and the word "SecuSUITE" is written in white text across it.</p>	 <p>The image shows the SteelBox splash screen. It has a dark background. At the top, it says "CACI" in white with "EVER VIGILANT" below it. In the middle, there is a logo for "SteelB-X" with "Secure Mobile Communications" underneath. At the bottom, it says "Powered by BlackBerry" and "Enabled by Microsoft Azure".</p>	<p>Different splash screens shown during start-up</p>

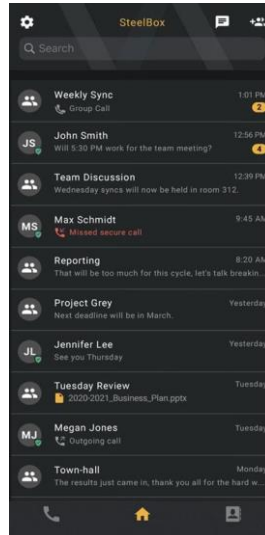
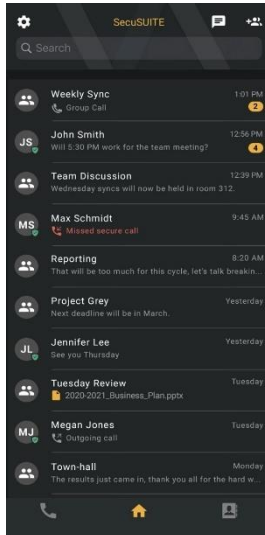
UI Screen	SecuSUITE Client	SteelBox Client	Comment
-----------	------------------	-----------------	---------

Call Log

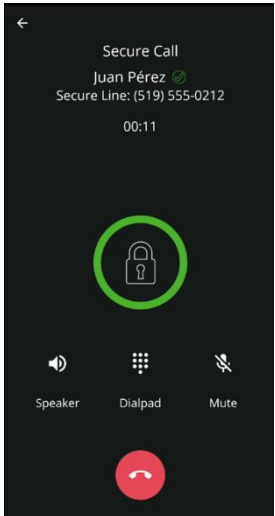
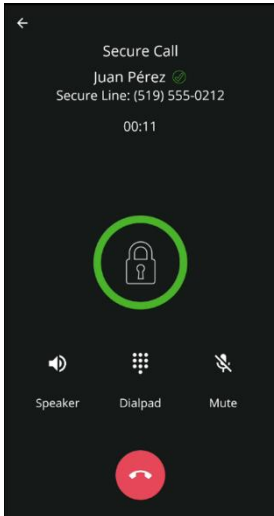
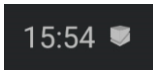
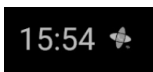


Call Log screen is identical

Home Screen



Different product name in header

UI Screen	SecuSUITE Client	SteelBox Client	Comment
Call Screen	 The screenshot shows a 'Secure Call' interface for Juan Pérez. The status bar at the top is black with a white lock icon in the center, circled in green. Below the call controls, there are three icons: Speaker, Dialpad, and Mute. At the bottom is a red end-call button.	 The screenshot shows a 'Secure Call' interface for Juan Pérez. The status bar at the top is black with a white lock icon in the center, circled in green. Below the call controls, there are three icons: Speaker, Dialpad, and Mute. At the bottom is a red end-call button.	Call Screen is identical for SecuSUITE and SteelBox except for the icons shown in the status bar: SteelBox:  15:54 [lock icon] SecuVOICE:  15:54 [lock icon]

For the remainder of the document the screen shots shown are taken from the SecuSUITE variant of the TOE.

5 General Common Criteria Configuration

The TOE is configured during the client enrollment process performed between the TOE and the BlackBerry SecuGATE 5.0 backend automatically.

Key generation schemes (FCS_CKM.1(1))

Cryptographic keys used for the generation of client TLS certificates are created based on the client configuration submitted by the BlackBerry SecuGATE server (ESC) during initial client enrollment. The configuration is defaulted in SecuGATE Server to the usage of NIST p-384 curve and cannot be changed.

The key generation scheme used during TLS related key establishment is selected by the SecuGATE and defaulted to NIST p-384 and cannot be changed. Please see paragraph 7.7.2 and 7.7.3 of [A].

Key establishment scheme (FCS_CKM.2)

The TOE supports only ECDHE as key establishment scheme.

TLS configuration (FCS_TLSC_EXT.1.1)

By default, the TOE supports only TLS 1.2 and offers two cipher suites (TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) for the trusted connections to the ESC. The cipher suite is selected by the SecuGATE server during TLS handshake and currently defaulted to TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and can be configured in the SecuGATE.

TLS Signature Algorithms Extension (FCS_TLSC_EXT.3)

By default, the TOE supports two signature hash algorithms (SHA384, SHA512) in the signature_algorithms extension of the Client HELLO message.

Hashing

The TOE uses SHA-1 for the SRTP cipher suite, SHA-256 for SIP Digest Authentication via TLS and SHA-384 and SHA512 for the TLS cipher suites. The applied hashing functions cannot be configured by the security administrator.

X.509 Certificates for mutual authentication (FCS_TLSC_EXT.2 and FIA_X509_EXT.2.1)

The TOE is provisioned with X.509 certificates to be used for mutual TLS authentication during the initial client registration process executed between the TOE and the SecuGATE server. The initial registration process is described in chapter [Activating the SecuSUITE app](#).

SRTP Cipher Suite configuration (FCS_SRTP_EXT.1.2)

The Ciphersuite used by the SecuSUITE client cannot be configured by the user or the admin. By default, the client uses AEAD_AES_256_GCM when communicating with other SecuSUITE v5.0 clients. For backwards compatibility with SecuSUITE v4.0 clients also AES_256_CM_HMAC_SHA1_80 is supported and used.

The ports used for exchanging RTP packets are defined by the SecuGATE during call establishment.

The SRTP NULL algorithm is disabled in the TOE and no configuration is necessary to disable the NULL cipher.

Used cryptographic engine

The TOE uses a built-in SafeLogic CryptoComply engine and utilizes NIST approved algorithms. The version and type of the cryptographic engine cannot be changed by the security administrator or SecuSUITE user.

6 Security Functionality covered by the Common Criteria Evaluation

The security functionality that has been covered by the common criteria evaluation relates to the claims outlined in the SecuSUITE Security Target document [D]. These claims cover, for instance, TLS trusted channels, including x.509 authentication, certificate validation and signature checking.

Additionally, to those claims, the SecuSUITE client implements end-to-end protection of the SRTP session key exchanged between the caller parties. This scheme is on top of the standard SDES/SRTP scheme demanded by the VVoIP Extended Profile [C] and, as a result, **not covered** by the common criteria evaluation of the SecuSUITE client.

The related key generation and certificate validation schemes applied for the end-to-end protection utilize the same implementation as the related schemes used for the TLS protected trusted channels. However, the end-to-end protection of the SRTP session key has not been explicitly tested by the CCTL during the evaluation.

Breakout and Secure Landing Calls

Besides the peer to peer calls between SecuSUITE clients registered to the same infrastructure, the TOE together with the SecuGATE server allows forwarding of secure calls to a PBX within a secure network.

For that the SecuGATE administrator can configure call forwarding to endpoints reached through a PBX (another SIP server connected to local/internal landline phones and potentially connected to outside phone lines). If so configured, a SecuSUITE client can then place calls to additional endpoints beyond the SecuGATE through the configured PBX; however, because the call signaling and call data travels beyond the SecuGATE itself, its security ultimately lies beyond the SecuSUITE client and SecuGATE SIP server's control.

The SecuSUITE client differentiates between calls deemed secure (called "Secure Landing") and calls that are considered unprotected as they're routed potentially unencrypted to external numbers over untrusted networks (called "Breakout").

The ability of the SecuGATE SIP server to route calls to additional endpoints through a PBX lies beyond the scope of this ASPP₁₄/PKG TLS₁₁/VVoIPASEP₁₀ evaluation and is not covered by the common criteria evaluation of the SecuSUITE client.

7 Setting up secure voice communication with SecuSUITE

With SecuSUITE®, you can make high-level security calls on your Android™ or iOS® device, no matter what network you are connected to. Your calls are encrypted end-to-end and protected against eavesdropping.

Important: SecuSUITE is based on a voice infrastructure that your organization must provide. All users of the app must be registered in this infrastructure to activate SecuSUITE. This must be set up by your administrator.

If you download SecuSUITE yourself, you can easily perform the activation ([8 Installing and activating the SecuSUITE app](#)). After successful activation, you can use the app for end-to-end encrypted voice communication.

To use SecuSUITE, you will need an Internet connection (Wi-Fi or mobile data).

7.1 Supported devices and firmware

The evaluated configuration covers the following devices and firmware:

Brand	App Version	Device	Firmware
Apple®	5.0	iPhone 12, 12Pro, 12Pro Max, 12 Mini, iPad Air	iOS® 14
Android™	5.0	Samsung®: S20, S20+, S21, S22, XCover Pro, Samsung A51, Note20	Android™ 11

8 Installing and activating the SecuSUITE app

Before you can use the SecuSUITE app, your administrator must create an account for you. When your account is created, your administrator will provide you with the activation code and the URL of the server (Authentication Server), which you will need in order to register the app on your smartphone. Additionally, your administrator can also provide you with a QR code to activate SecuSUITE. Follow the steps in the next chapters to installation and activation.

Note: The app must be secured by a mandatory device screen lock. The activation process will be simpler if you set the screen lock before starting (8.3 [Setting a device screen lock](#)).

8.1 Installing the SecuSUITE app

1. Open the app store on your device and search for **SecuSUITE**.
2. Download the app.
3. Tap **Install**.
4. After installation is completed, select **Open**.
5. You will be prompted to give SecuSUITE several permissions: contacts, microphone, manage phone calls, manage storage, notifications, appear on top, do not disturb, etc. Allow all permissions. The phone's contacts is the only sensitive information repository that SecuSUITE accesses.

Note: In iOS and in the more recent Android versions, you may not see all requests immediately, as they will only ask for permissions when necessary (e.g., for camera only when you use it for the first time).

The TOE uses following full list of hardware resources from the underlying platform:

- Network connectivity – SecuSUITE requires access to a network to communicate with the SecuGATE server.
- Camera – SecuSUITE allows scanning of a QR code using the phone's camera.
- Microphone – SecuSUITE uses the microphone to record voice data.
- Bluetooth – SecuSUITE can use Bluetooth devices, such as Bluetooth headsets.
- Biometrics – The platform OS might use biometrics as the authentication factor. SecuSUITE requests access to use the platform keystore via biometrics if the phone is set up with a biometric authentication factor.
- Notifications – SecuSUITE sends notifications to the user of incoming calls, texts and alerts.
- External Storage – SecuSUITE's text messaging system allows attachments, which are possibly stored in the phone's external storage.

8.2 Activating the SecuSUITE app

After installing the SecuSUITE app, you must activate it. You will need the activation code and the address of the Secure Client Authentication (SCA) server that is part of your organization's infrastructure. Both will be provided to you by your SecuSUITE administrator. To simplify this process, a QR code can be found in the activation email that you will receive from your administrator. Step 3 in the activation email will have a QR code that will look similar to the one below:



1. Open the SecuSUITE app. You will see the activation screen.
2. Accept requests from the app when prompted.
3. On the activation screen, you can activate your user account by using a QR code or by manually typing the activation code and the server URL provided in the activation email.

Note: If you select the QR code option, you must accept a permission prompt for your camera, tap **ALLOW**.

To use the QR code, tap the QR code icon and aim your smartphone camera within the provided area to capture the QR code image (Above is a **sample QR code**, please make sure that you scan the one provided on your activation email only). Without the QR code, simply type in the activation code and SCA server URL provided in the email.

Note: The TOE uses the URL entered by the user or derived from the QR code information as a reference identifier for the TLS certificate validation. For the reference identifier the CN field and SAN fields are supported (SAN fields takes preference).

4. You will see the activation being processed.
5. The **SecuSUITE Client Addendum** will eventually be displayed. Please read it carefully. At the bottom, tap the box next to **I agree to the terms ...** ⇒ **I Agree**.
6. If your device has not been secured with a screen lock prior to this step, you will be prompted to set this up before proceeding ([8.3 Setting a device screen lock](#)).
7. After the completed activation, SecuSUITE will open. If your administrator has configured the need for an additional layer of security, you will be prompted to define a PIN for the app. Additionally, you will be asked to allow the use of any device biometric authentication methods that you have set up, such as fingerprint or Face ID.
8. Your phone contacts are loaded as **Contacts** in the app. They will not be marked with a shield or padlock yet.
9. All active SecuSUITE contacts from the tenant which the SecuSUITE administrator has organized you into are displayed as **SecuContacts**. These contacts are marked with a green shield.

Note: This step depends on a server setting made by your admin called **Secure Contacts Push**.

After successful activation, you can make end-to-end encrypted phone calls and send secure text messages to other SecuSUITE users.

8.3 Setting a device screen lock

8.3.1 Android

1. Open system **Settings** ⇒ **Lock Screen** ⇒ **Screen Lock Type**.

2. Select one or more types of locks: pattern, PIN, password, or Biometrics such as face, iris, and fingerprint.
3. Define the screen lock.

8.3.2 iOS

1. Open system **Settings** ⇒ **Touch ID and Passcode/Face ID and Passcode**.
2. Select one or more types of locks: **Passcode**, **Touch ID** (if supported), or **Face ID** (if supported).
3. Define the screen lock.

8.4 SecuSUITE app can ask for an additional layer of security

If more restriction is desired to protect the SecuSUITE app, a separate PIN request can be activated by your administrator.

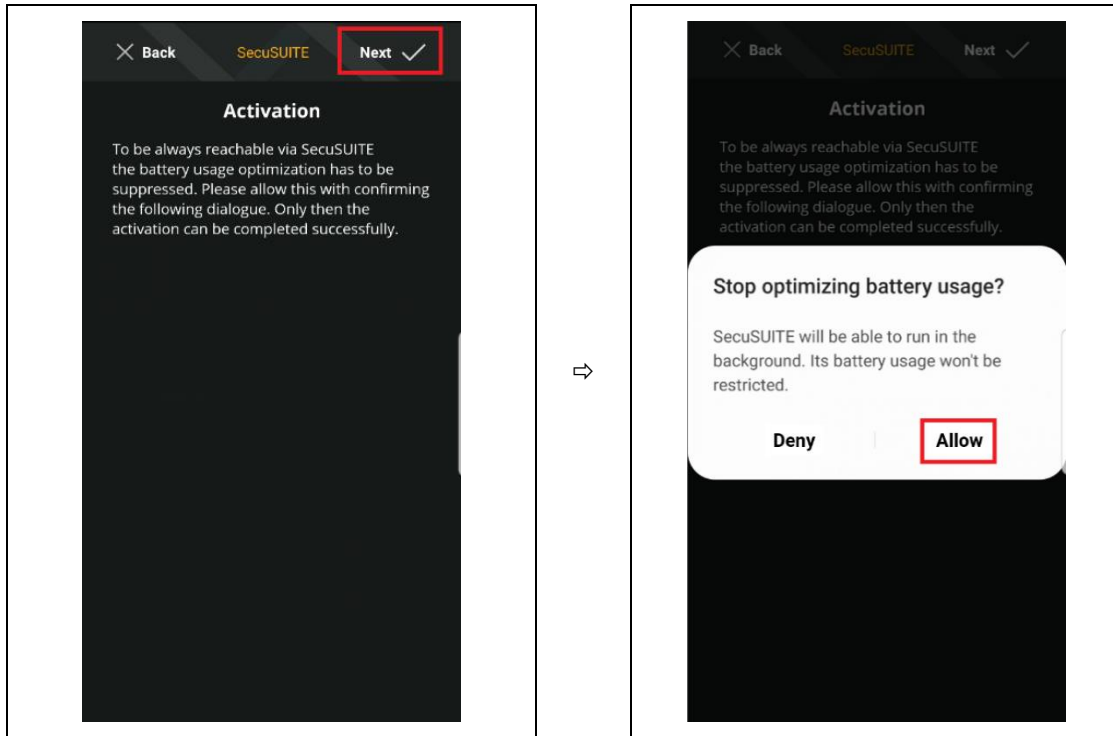
If this has occurred, you will need to define an additional PIN during the activation process, exclusive to the SecuSUITE app. After doing so, you can also link your fingerprint or other biometric authentications to unlock SecuSUITE. This will mostly be used as an alternative to the PIN. When access to the app is requested, use either the PIN or the substitute.

8.5 Additional notifications about battery optimization (optional)

If your organization uses specific settings in the background, you will encounter two additional notifications during the activation process.

The first notification informs you of a conflict between battery usage optimization and SecuSUITE being continuously reachable.
Tap on ⇒ **Next**.

The second notification originates from Android and warns you that SecuSUITE will always be allowed to run on battery.
Tap on ⇒ **Allow**.



Even when you are not using SecuSUITE, the app will never go into deep sleep mode but will always run in the background to receive calls and messages.

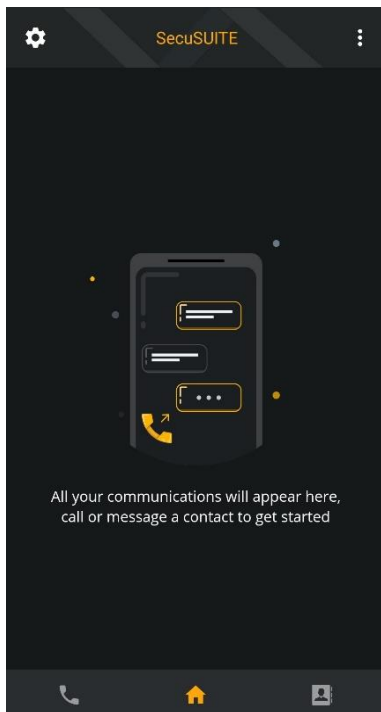
Note: If you do **not** see any of these notifications, SecuSUITE will still be reachable in the background. If these notifications appear, you will need to click 'allow' for these settings.

8.6 Onboarding and empty home page

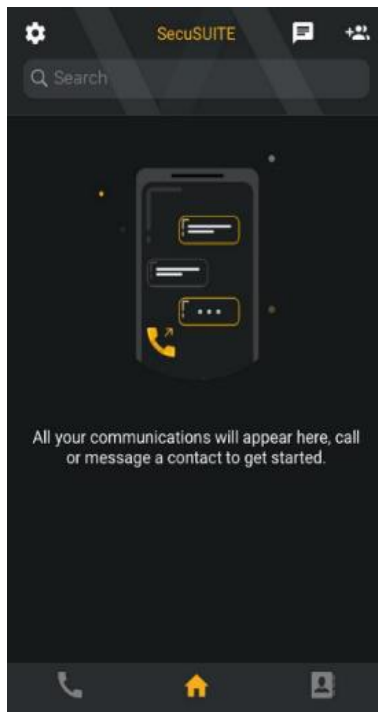
You will be shown a short onboarding tutorial explaining some of the features of SecuSUITE. If this is your first time using SecuSUITE, we highly recommend viewing this tutorial. It can also be skipped.

First sight of the homepage:

on Android



on iOS



9 SecuSUITE app

9.1 SecuSUITE home page

When you first open the SecuSUITE app, you will see the **home page**. It is empty until you have made a call or have sent a message for the first time. The screenshot below shows some of the sample content (this example is on iOS).

The screenshot shows the SecuSUITE app interface on an iOS device. At the top, there is a settings gear icon, the app name 'SecuSUITE', a search bar, a messages icon, and a group chat icon. Below this is a list of communication items, each with a contact icon, name, and latest message. The home page icon at the bottom is highlighted in orange. Callouts provide detailed instructions for each element.

- Settings:** Tap settings to access Bluetooth controls, media-download options and account details.
- Search:** Tap to compose a new one-to-one chat.
- Group Chat Icon:** Click to create a new group chat.
- Unread Number:** The unread number will display the number of new items in a conversation.
- Note:** On the home-page, only the latest interaction with a contact is shown, whether it is a call or a message.
- Group Chat:** Tap on a group chat to access the conversation.
- Call Icon:** Tap the call icon to see your entire call history.
- Home Page:** The current page you are on is highlighted in orange. In this case it is the home page showing all your communications.
- Contacts:** Tap here to view all your contacts.

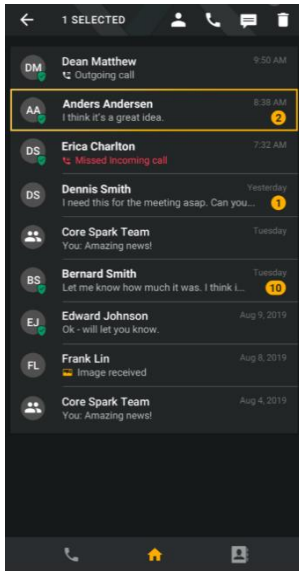
Note: The picture above shows the home page in iOS. Some details may look different on Android systems, which are explained in this manual.

9.1.1 Further actions on the home page

In addition to the actions above, more actions are available on the SecuSUITE home page, such as deleting single entries or in bulk. To Perform these additional actions on IOS or Android, proceed below:

9.1.1.1 Android

To gain access to further actions on the home screen, press and hold one or more chats until it is marked with an orange frame.



In the top right corner, you will find additional actions. This list will display only what is possible from your selection.

One to one interaction:



- View contact details
- Call contact
- Compose message
- Delete chat

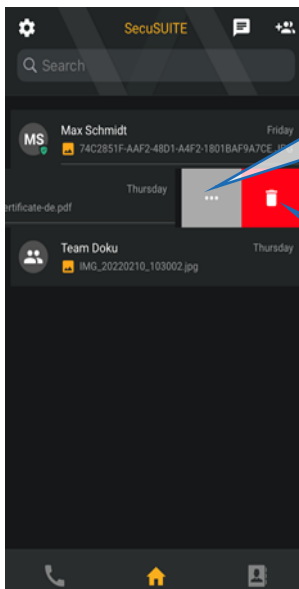
Group Chat:



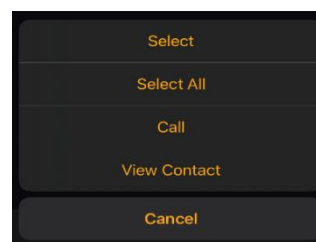
- View group details
- Compose message
- Leave group
- Delete and leave chat

9.1.1.2 iOS

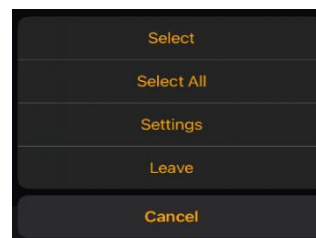
To gain access to further actions on the home screen, you can either press and hold on one entry or swipe it to the left to see the options.



One-to-one interaction:



Group chat:



9.2 Your contacts in the app

Go to the **Contacts** screen to view the contacts in your app. The contacts listed here are split into two tabs (shown on iOS):

- **SecuContacts:** This will display all active SecuSUITE users of your tenant (except [VIP contacts](#)) and those you confirmed as secure after the first secure call. With these contacts, you can establish end-to-end encrypted calls and chats.
Note: The display of the SecuSUITE contacts from your tenant depends on the activation of Secure Contacts Push (SCP) in your organization.
- **Contacts:** This will display your original phone contacts from your phone. Some of them may also be SecuSUITE users. After a successful SecuSUITE call or chat, you will be asked to confirm if the contact is secure, and upon confirmation will be added to your **SecuContacts**.

The screenshot shows the BlackBerry Contacts app interface. At the top, there is a search bar and two tabs: 'SecuContacts' and 'Contacts'. Below the tabs, a list of contacts is displayed, each with a name, company/department, and icons for chat and call. A vertical alphabetical index is on the right side. Callouts provide the following information:

- Search:** Enter the name of a contact into the search field to find a contact in **SecuContacts** and **Contacts**.
- SecuContacts Tab:** The **SecuContacts** tab displays SecuSUITE contacts and those you confirmed as secure after a successful call.
- Secure Contacts:** All secure contacts are marked with a **green shield**.
- Contact Details:** **Company and department** (if they were entered by the admin) are visible **details** of a contact. To see more details, tap on a contact.
- Group Chat:** Use these icons to... create a **group chat**.
- Group Call:** Start a **Group Call** or **rearrange** the sorting of contacts by first or last name. with this icon.
- Native Contacts:** The **Contacts** tab shows your native phone contacts.
- Refresh:** Refresh the contact list by dragging down the screen.
- One-to-One Chat:** Use these icons to... start a **one-to-one chat**.
- Call:** to start a **call** with the contact.

Important! A red shield shows that something is amiss, or a manipulation or violation has occurred with a user's phone. Do not share restricted content with this person until you have found out what has caused the red shield icon to appear.

The contacts are refreshed automatically upon the first launch of the day. However, you can refresh it manually by dragging down the screen ([9.2.3 Updating, editing, or deleting SecuSUITE contacts](#)).

9.2.1 VIP contacts

Some SecuSUITE users have **VIP status**. Their number-name combination is not distributed or shared with **SecuContacts** and SecuSUITE users. However, VIPs can see all other active SecuSUITE users from their tenant as well as other VIP users.

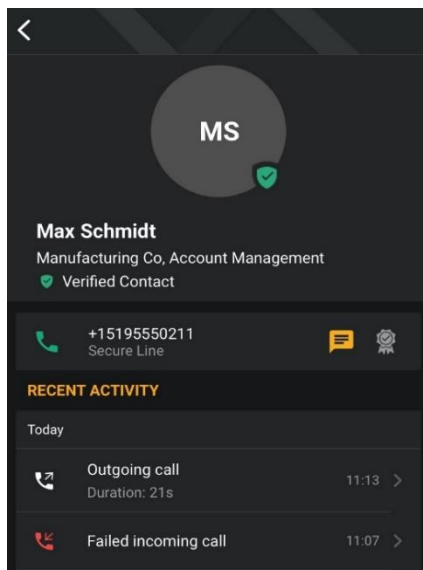
After a VIP user calls another SecuSUITE user securely, the other user will be prompted to save them as a secure contact. Only then will the VIP user appear in the **SecuContacts** list.

Note: Since a VIP user's contact is manually entered on your phone, it will not be updated automatically.

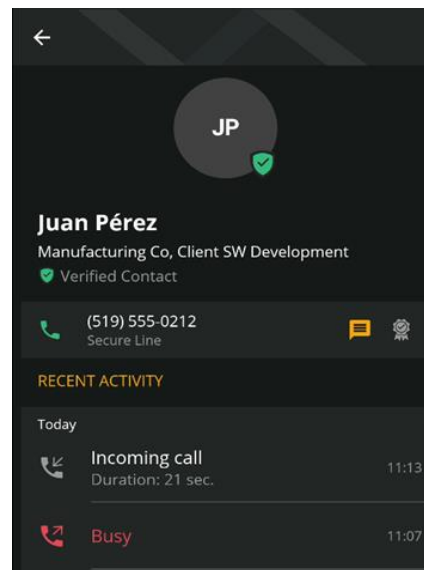
9.2.2 Display of contact card

Within your SecuSUITE contacts in the SecuSUITE app, you can see additional information about your contacts. Aside from the name, the contact details also show company and department information if the tenant admin has entered them. Finally, you can also see your recent activities with this contact.

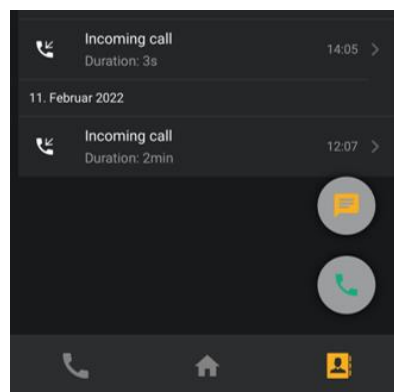
iOS



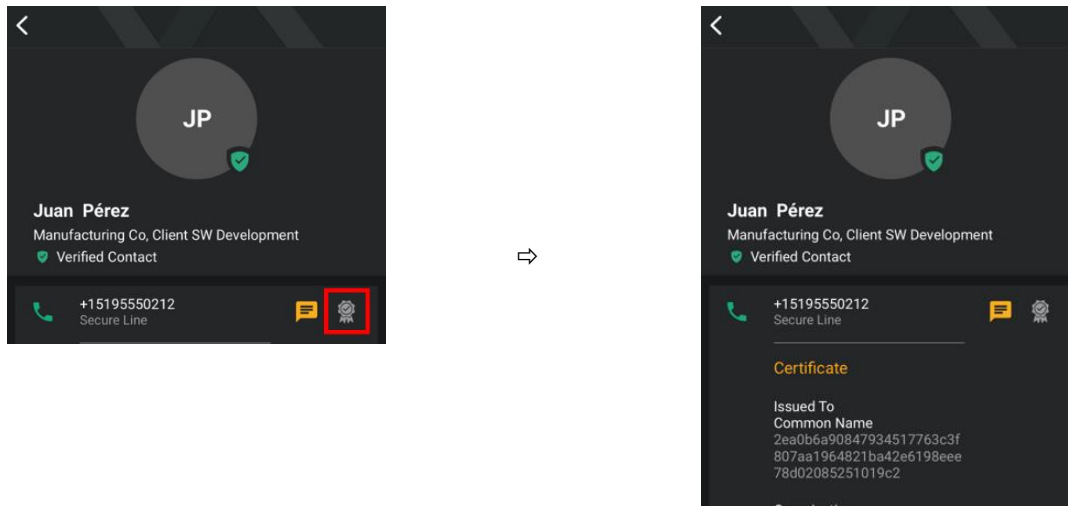
Android



Additionally, on iOS when moving down in a contact's card, e.g., to look through the call history, a message icon and a call icon will appear at the bottom right corner. Use these shortcuts to open the chat with this contact or to call the contact.



Each SecuContact is saved with a unique certificate that you can view after your first call with that contact. To view a contact's certificate details, tap on the grey certificate symbol.



9.2.3 Updating, editing, or deleting SecuSUITE contacts

Generally, it is not possible to change the data of contacts in the app.

- SecuSUITE contacts are managed in the backend, so changes will be updated in your app automatically.
- Phone contacts must be edited or deleted in the native phone app, and these changes will be reflected in the SecuSUITE app.

Contacts are refreshed automatically upon the first launch of the day. You can also manually update the contacts by dragging the screen down.

After a few seconds, you will see the updated contact list.



9.2.3.1 Exception: Manually updating, editing, or deleting manually added SecuContacts or VIP contacts

Other SecuSUITE users who are assigned to a different tenant or that are created as VIP contacts in your own tenant will not automatically appear in your SecuContacts list. However, they can be called securely via SecuSUITE from the Contacts tab if you have them saved in your phone's native contacts app. Alternatively, you can simply enter their number in the call log.

After a call with one of these SecuSUITE users you will be asked to confirm their identity and manually add them to your SecuContacts list. Since these entries are manually added, you can edit or delete the details associated with the phone number by going to the contact details for that person and tapping **Edit** at the top right corner.

10 Secure calls

SecuSUITE does not interact with the native phone app of your device. You can continue to make regular phone calls.

Your phone number for SecuSUITE is set by your administrator. This is not necessarily the number from the SIM card, but in most cases, it makes sense to also use this for SecuSUITE so other SecuSUITE participants can reach you with your known number.

Note: To check the phone number assigned to your SecuSUITE account, look in  (Settings) ⇒ **Account** ⇒ **Account Number**.

If your organization has activated Secure Landing, your administrator will define a second number for your SecuSUITE account. This is needed if a landline device inside your organization's protected phone infrastructure wants to call you securely. Your administrator will provide this number and any additional steps to you.

Secure calls require a stable data connection. Either Wi-Fi or mobile data will work. If SecuSUITE is not connected, Android phones show a red bar with **"There is a problem with your connection. Check your network."** A disconnect icon can be seen in the notification tray. When SecuSUITE is connected, the logo will display clearly in the notification tray. You can try to reconnect by switching between Wi-Fi and mobile data.

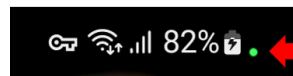
With Android 12, you are signaled directly on the display during a call that the device's microphone is active. When the microphone is activated, a green microphone icon appears briefly in the upper right corner. The icon then turns into a small green dot.

If the microphone is active, the small green dot at the top will remain visible.

Microphone is activated



If the microphone is active



10.1 Making a one-to-one SecuSUITE call

Secure calls can be made to other SecuSUITE users within your organization. There are additional types of secure calls, e.g., group calls ([10.4 Starting a secure group call](#)) or calling landline numbers inside the protected network of your organization.

As soon as the recipient accepts your call, a secure connection is established. You can verify the status of the encryption by watching the circle around the lock icon on the screen ([10.1.2 Icons for call status](#)).

You can start a secure call from every main screen of the app.

- **Contacts Screen:**

In the SecuContacts tab you will see the contacts that you can call securely.

The **Contacts** tab shows the contacts from your native phone. They may also be SecuSUITE users, so you can try to call them. If a secure call is not possible, your attempt will be terminated.



To make a secure call, tap on the **green phone icon** next to the contact.


- **Home Screen:**


Tap on a **single contact** entry


Tap on the **phone icon** to start the call

Note: On Android, these icons are reversed.

- **Call Log:** If you have had a previous call with a contact or a group, you can find it in the call log. Tap on the entry to start a call. If you want to dial a number, tap on the symbol for the dial pad  in the top right corner. To start a secure group call, tap on the group call icon:  in the top right corner

 icon opens the dial pad.

Tap on  icon to start a secure group call.

Tap on  icon to open the call details between you and that contact.

Tap on one of the call log entries to start a secure call.

Note: SecuSUITE uses a **data connection** for secure calls instead of your mobile network's audio connection, which is what your phone typically uses for voice communication.

10.1.1 Call integration on iPhones for one-to-one calls

For iOS devices only, SecuSUITE uses CallKit Support. SecuSUITE calls will appear on the screen like an ordinary iOS call and can be handled as native phone calls are.

Incoming call from SecuSUITE			Ongoing call with SecuSUITE:
An incoming SecuSUITE call will be displayed like a usual incoming call and can be accepted in the following ways below:			An active SecuSUITE call when started or accepted with the iOS call app is displayed like a usual call screen.
On locked screen:	On unlocked screen:	On open app:	

Note: The SecuSUITE symbol and "SecuSUITE Audio" are always displayed to identify the secure call.

10.1.2 Icons for call status

	Incoming/Outgoing call ringing	Key-agreement	Secure call	Breakout into unsecure network
	Call is ringing.	Call accepted. A secure connection is about to be established.	A secure connection (mobile to mobile or secure work line) is now established. You can start talking.	The call is decrypted and forwarded into an unsecure network. Your call is not secure.
Android & iOS				

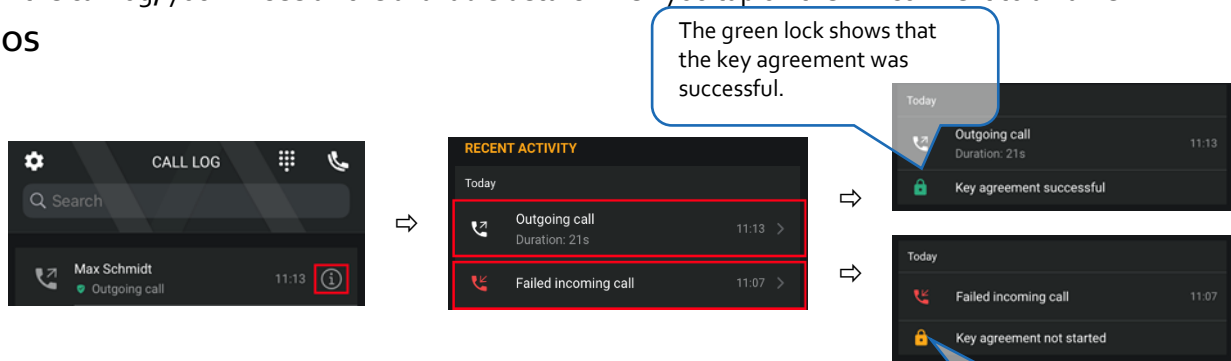
Note: You will see the same symbols whether you are making or receiving a call. You can start speaking as soon as the lock icon is closed.

10.1.3 Information about call participants

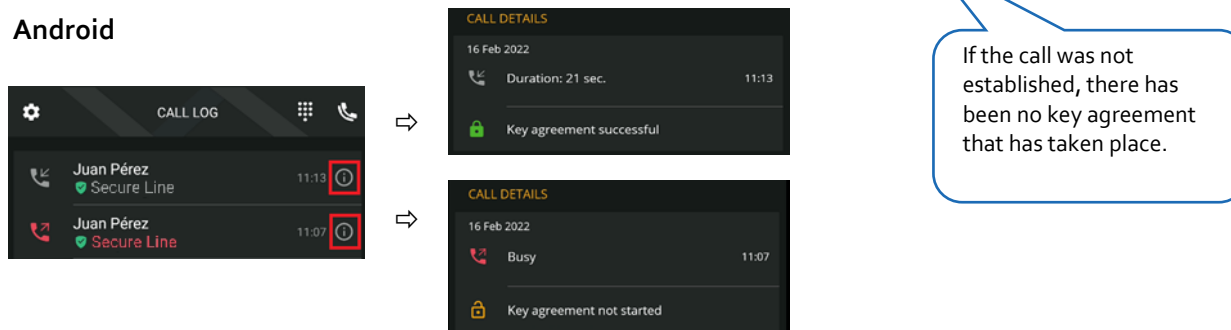
Important information about the other participant is transmitted even in a call attempt. It is displayed on the call screen and later in the general call log, as well as in the call log of each contact.

In the call log, you will see all the available details when you tap on the icon next to a name.

iOS



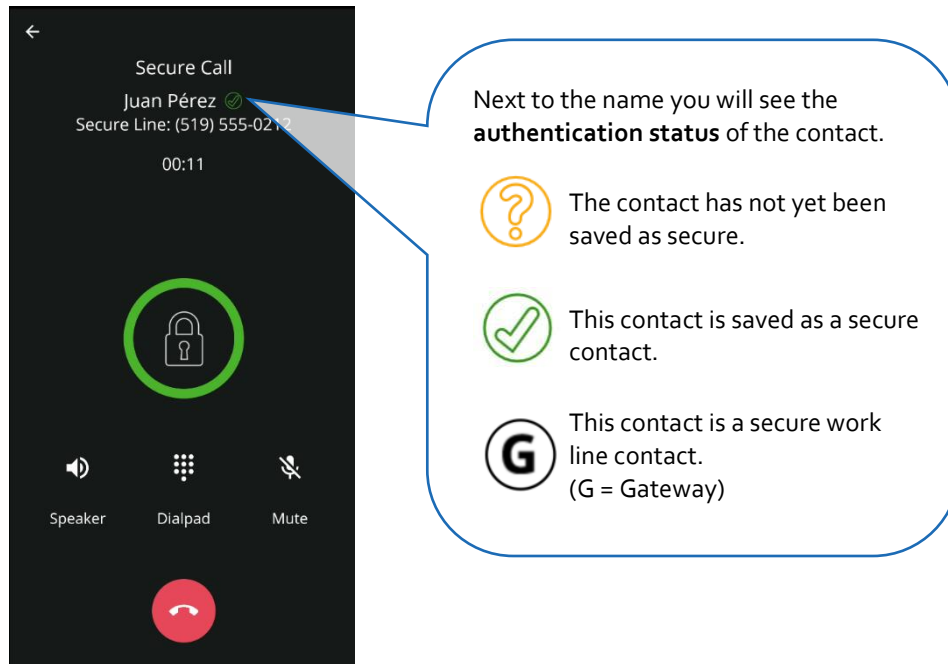
Android



10.1.4 Authentication

During a call, you can see if your contact is a confirmed secure contact by looking at the icon next to the name. After a call is completed, you may be asked to add the contact as a secure contact if they are another SecuSUITE user (10.3 Saving a secure contact).

SecuSUITE shows the status of authentication through different icons.

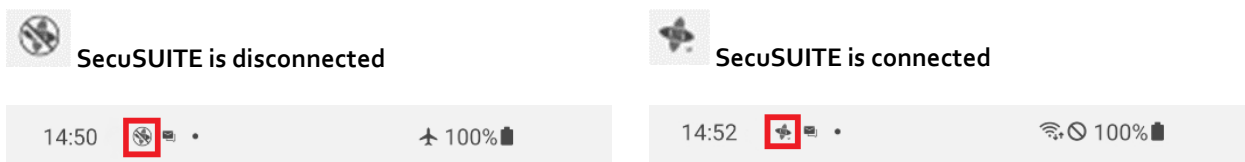


10.2 Accepting secure calls with SecuSUITE

10.2.1 SecuSUITE background operation

To ensure your device receives secure calls via SecuSUITE, the app runs in the background even when locked. To do this, SecuSUITE needs an active Internet connection.

On **Android**, a notification indicates that SecuSUITE is connected:



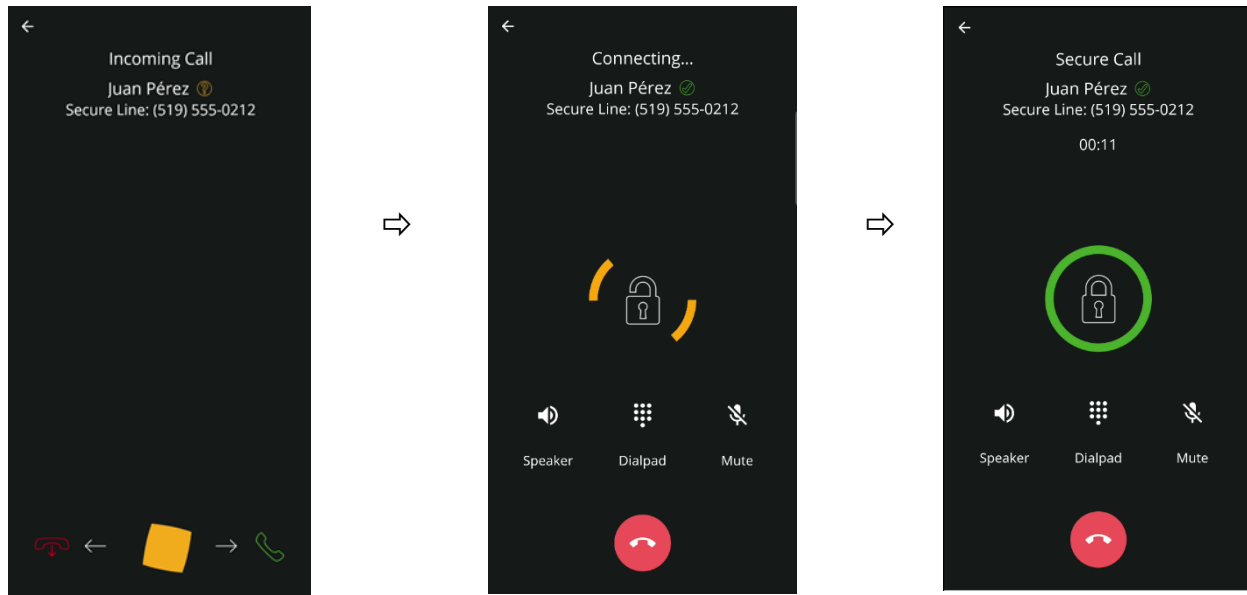
Note: After rebooting your device, SecuSUITE will prompt you to enter your device password to verify your identity, and any additional authentication that has been enabled.

10.2.2 Receiving SecuSUITE calls

Swipe the middle icon to the right to accept the call or to the left to decline the call.

If accepted, wait while the key agreement is performed.

The call is active. You can now start talking (and listening, of course).



After the first secure call with a SecuSUITE number, you will be asked to save this contact as a secure contact or to confirm their identity ([10.3 Saving a secure contact](#)).

Note: On iPhone, a secure call that you receive looks like an ordinary iPhone call except for the banner **SecuSUITE Audio**.

10.2.3 Receiving concurrent calls

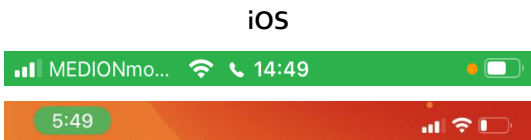
SecuSUITE and the phone app of your device are not connected. Concurrent call attempts lead to the following scenarios:

- **While you are in a call using the native phone app, and someone calls you with SecuSUITE:**
Android: The SecuSUITE caller hears the sound for an occupied line, and their call attempt is aborted. In the status bar of your device, you will see the icon for a missed call from SecuSUITE.
Note: If you do not want to see missed calls from SecuSUITE in the status bar, turn it off in the SecuSUITE Settings ([13.2.1 Notifications](#)).
iOS: When the SecuSuite call rings, the iOS device has a callkit screen with the option to decline, end and accept, or hold and accept. If you hold and accept, your native call will resume when your SecuSUITE call has ended.
- **You are in a secure call with SecuSUITE while someone calls you with SecuSUITE:** The caller hears the sound for an occupied line, and their call attempt is aborted. In the status bar of your device, you will see the icon for a missed call from SecuSUITE.
- **You are in a secure call with SecuSUITE while somebody calls you with the native phone app:** The native call will show on the display of your device. Accepting it will end the SecuSUITE call. Decline the native call if you want to continue your SecuSUITE call.

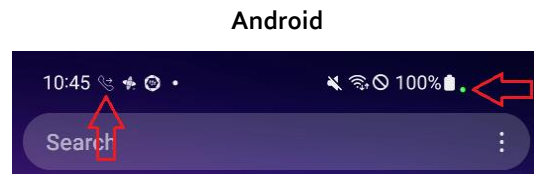
10.2.4 Placing SecuSUITE calls in the background

You can put an active SecuSUITE call in the background if you tap on home or recent apps. In this way, you can continue to use your smartphone while the call is active.

To bring the call back to the foreground, tap on the app again, or...

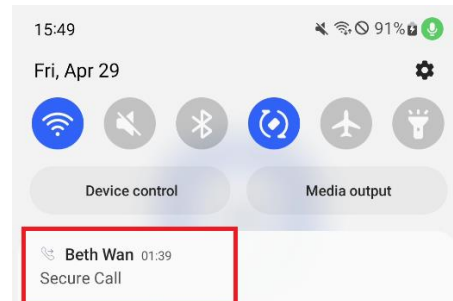


... on **iOS** devices that support Touch ID, tap on the green bar above (first bar). On devices that support Face ID, there is a green bubble instead on which you can tap to re-access the call.



... on **Android**, a green dot on the right side shows that the call is active by indicating you are using the microphone, while on the phone icon you can see if the call is incoming or outgoing.

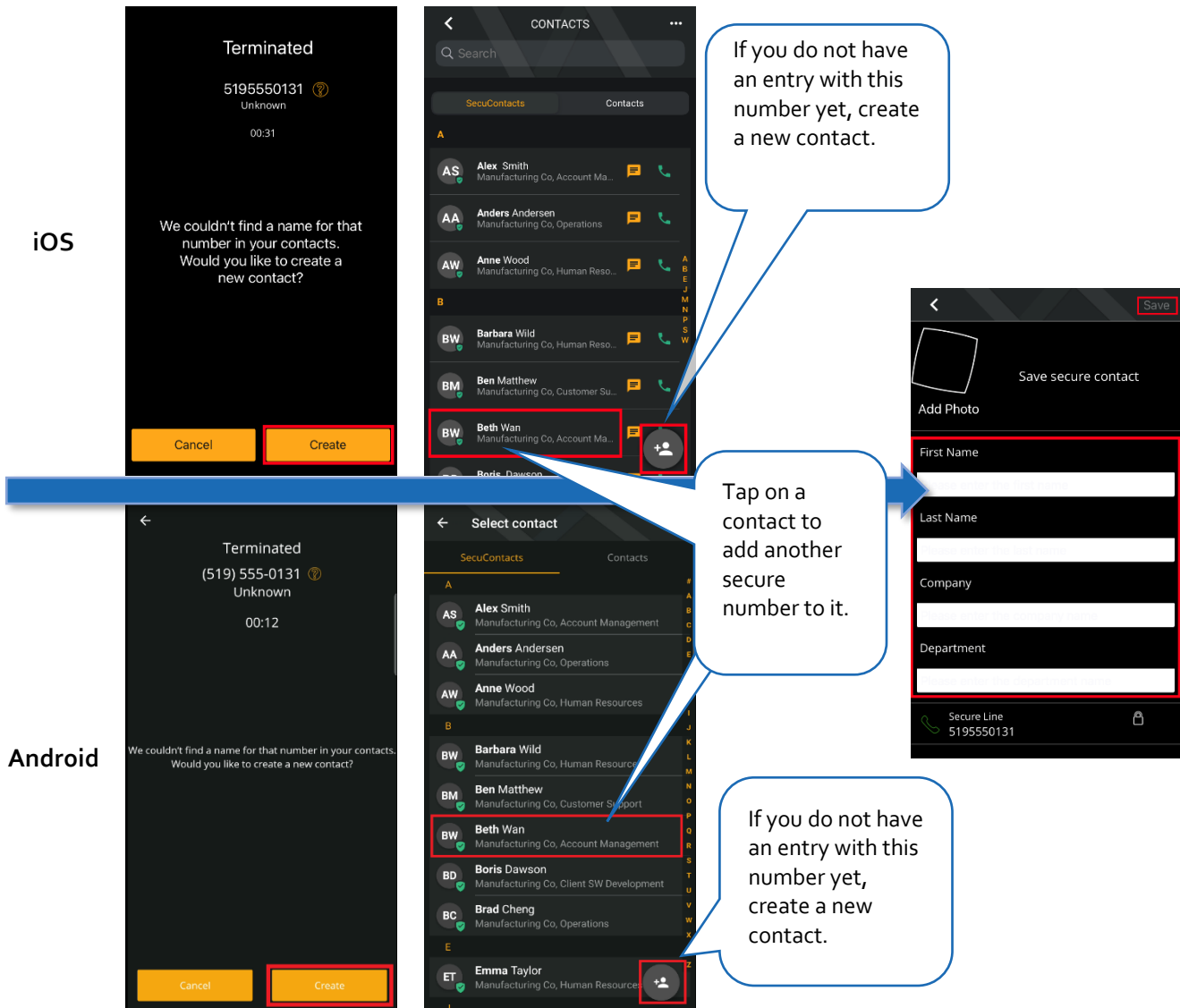
Use the notification to get back to the call screen:



During an ongoing call, you can also use other functionalities of the SecuSUITE app, e.g., messaging.

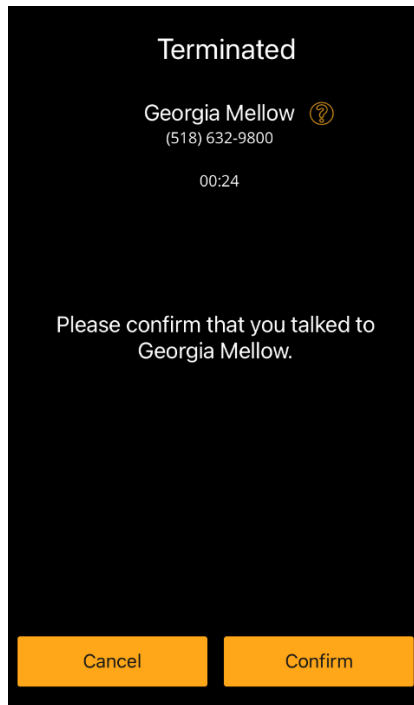
10.3 Saving a secure contact

After you have made a successful SecuSUITE call with a member in the **SecuContacts** tab, no further action is required from you. However, secure calls are also possible with other contacts. After a successful call with a number not on your SecuContacts list, you can save them as a **secure contact**. You can either **create a new contact** or **add a number** to an existing contact. You can also choose not to save a secure contact. After another secure call with this number, you will see the same prompt.



Note: You can save several numbers in one contact entry. Select a contact name to assign the new number. The old number will remain associated with this contact.

If you already had this contact saved (e.g., in your personal contacts) but this was your first secure call, you will be asked to verify their identity (shown on iOS):



Note: Once you have done that, you can change contact information of manually confirmed SecuContacts within SecuSUITE ([9.2.3.1 Exception: Manually updating, editing, or deleting manually added SecuContacts or VIP contacts](#)).

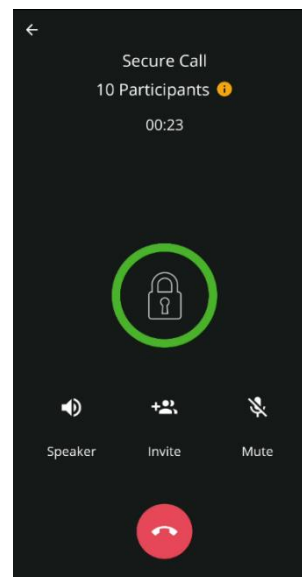
10.4 Starting a secure group call

Secure calls can be made to multiple users of SecuSUITE in your organization. As soon as the recipient(s) accepts your call, a secure connection is established. You can verify the status of encryption by watching the circle around the lock icon on the screen (10.1.2 Icons for call status).

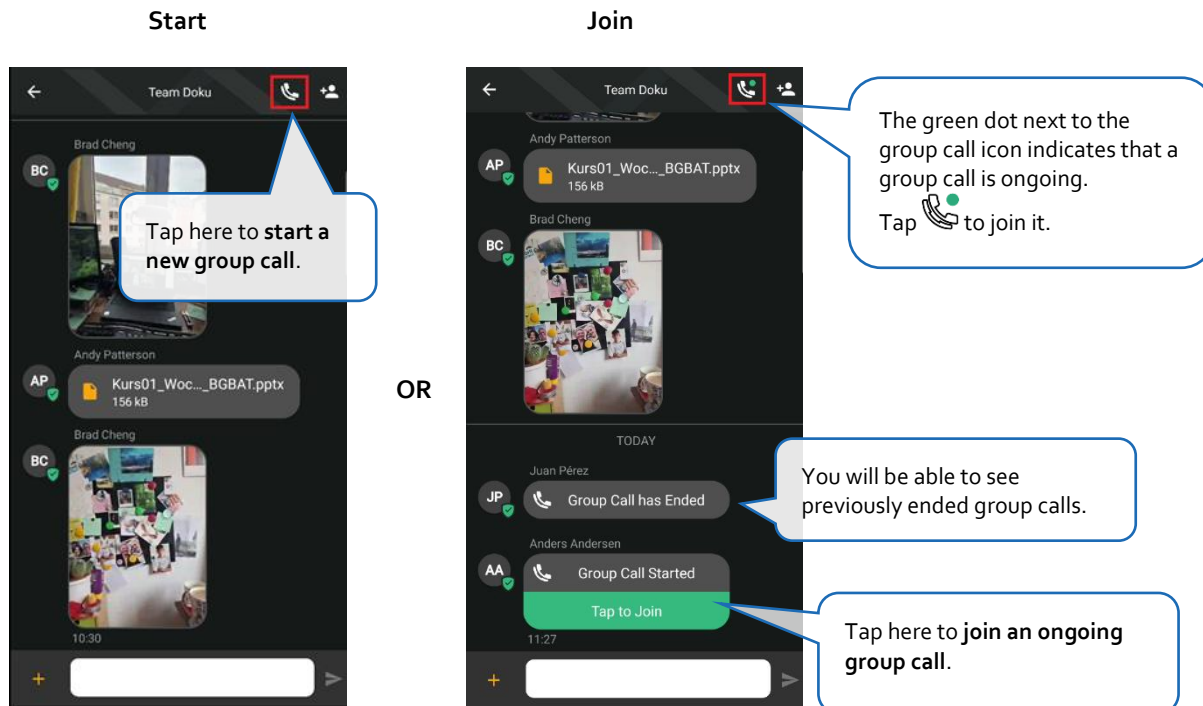
SecuSUITE allows you to have group calls with other SecuSUITE users via your phone data connection. You can begin a secure group call **from the SecuSUITE contacts screen, call log, or from an existing group chat.**

Group calls are a quick way to get up to 12 people in a call.

Note: Some graphics may show unique illustrations of iOS or Android.



10.4.1 Start or join a secure group call from an existing group chat



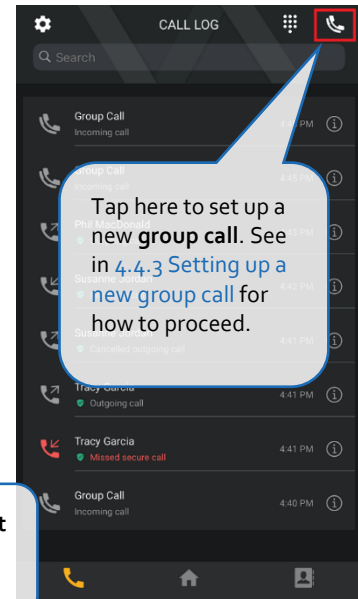
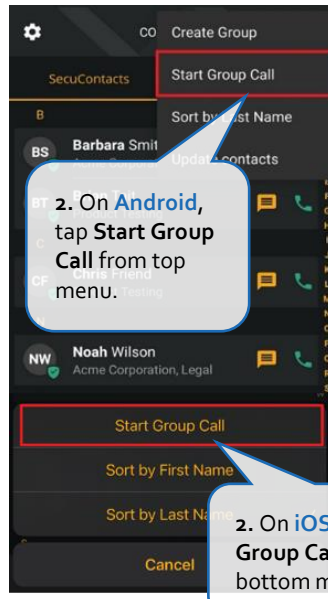
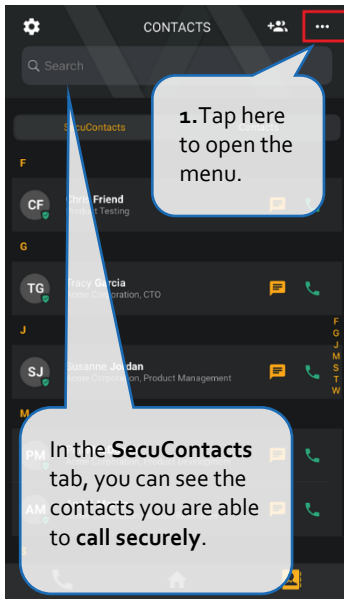
Note: If multiple group members try to start a new group call at the same time, this may cause an error and the call will not be established.

10.4.2 Beginning a new group call

If you wish to begin a new group call (instead of connecting through an existing group chat), you must choose one of two ways to start the call. The process will be identical following the initial start from either the contacts screen or the call log.

Starting a group call from the Contacts screen:

Starting a group call from the Call Log:



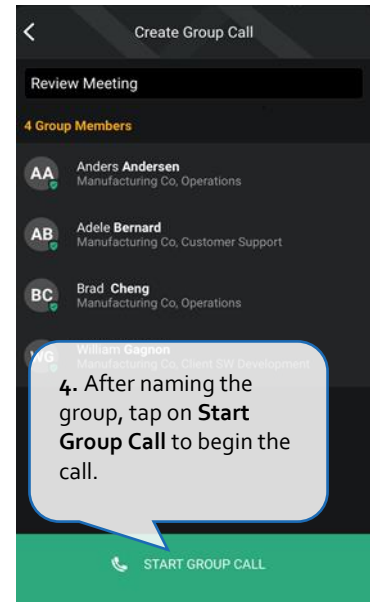
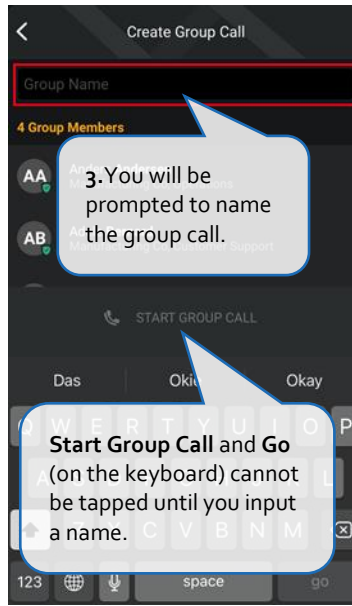
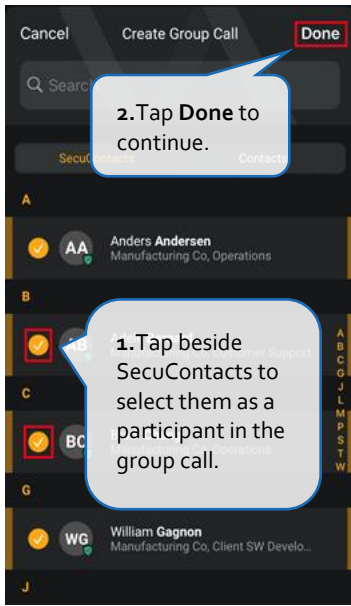
Note: If you try to select a previously concluded group call through the call log, you will receive a pop-up notification that says the group call has ended.

Tip: When creating or participating in a group call, designate one person to start the call and inform the other participants.

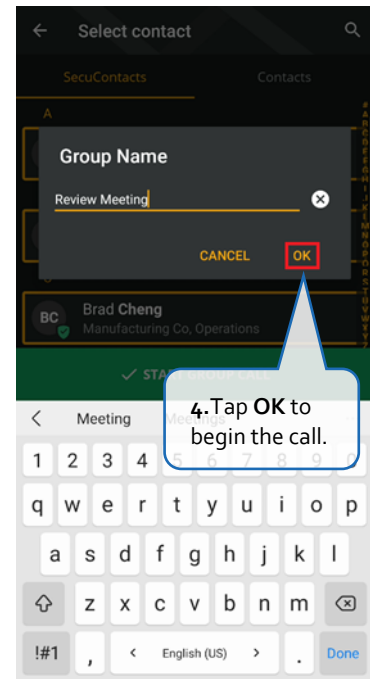
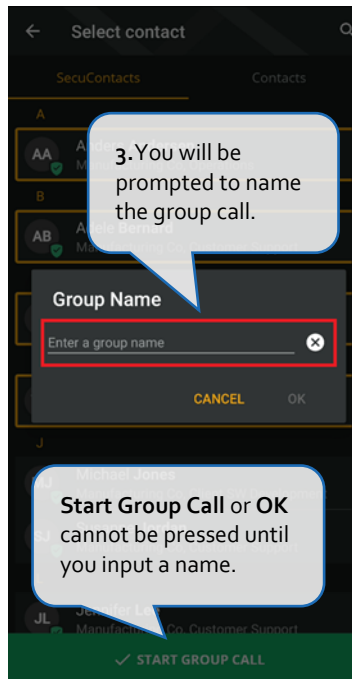
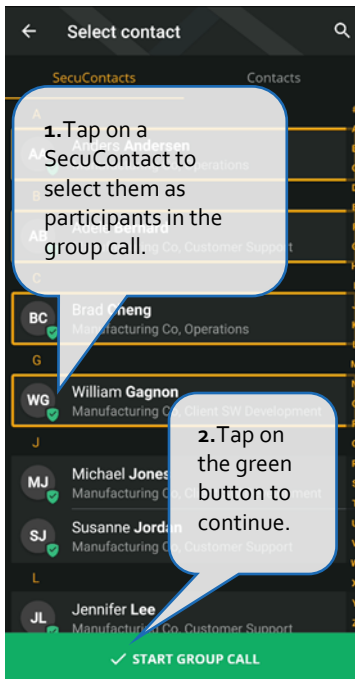
10.4.3 Setting up a new group call

After setting up a group call from either the contacts screen or call log, you will be prompted to select any SecuContacts you wish to participate in the group call. You will also be asked to name the group before the call can start.

iOS



Android



10.4.4 Invite additional participants during an ongoing group call

You may also invite additional participants to a call once it has started.

iOS

1. Tap on **Invite** to request additional participants to join call.

2. Tap beside the names of desired SecuContacts to select and invite them to the call.

3. Tap on **Done** to invite to secure group call.

Android

1. Tap on **Invite** to request additional participants to join call.

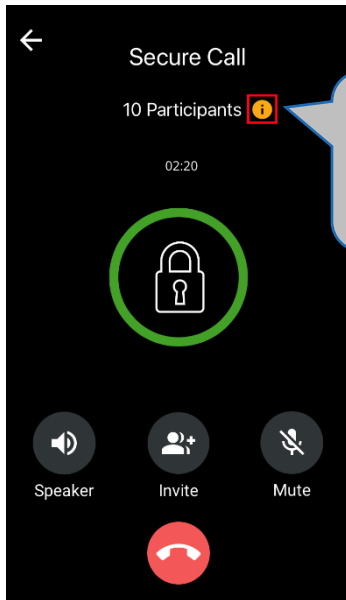
2. Tap on the names of desired SecuContacts to select invite them to the call.

3. Tap on **Invite to Call** to invite to secure group call.

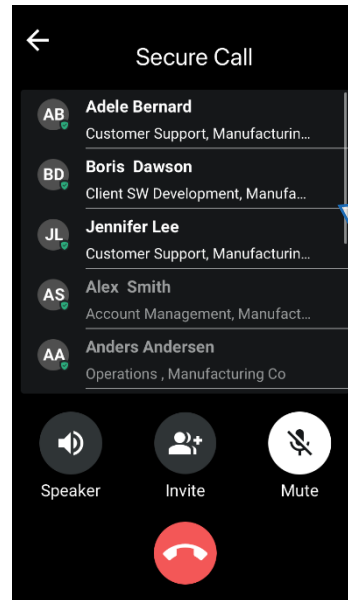
10.4.5 Information about group call participants

During the call, important information about other participants is displayed on the call screen, and later in the general call log after the call ends.

During a group call

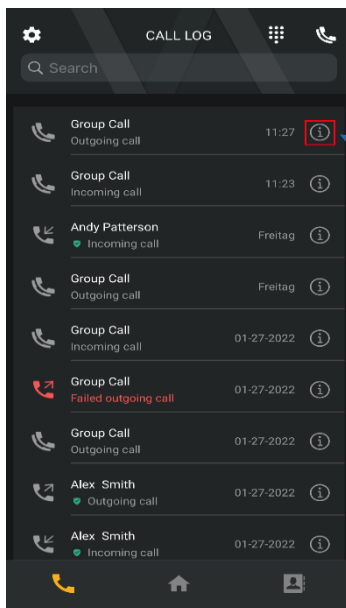


Tap on the information icon to reveal the list of call participants.

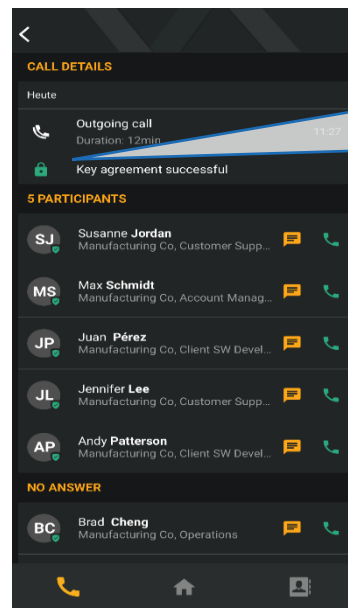


Active call participants appear in solid white text, while inactive group members are greyed out.

Following a group call



Tap on the information icon to reveal the participants that joined each call.



Green lock indicates key agreement was successful.

See list of participants that joined or did not answer (only on iOS).

10.4.6 Call integration on iPhones for group calls

For iOS devices only, SecuSUITE uses CallKit Support. SecuSUITE group calls will appear on the screen like an ordinary iOS call and can be handled as such.

Incoming group call from SecuSUITE			Ongoing group call with SecuSUITE:
An incoming SecuSUITE group call will be displayed like a normal incoming call and can be accepted as followed.			An active SecuSUITE group call, when started or accepted with the iOS call app, is displayed like the usual call screen.
on locked screen:	on unlocked screen:	on open app	

Note: The SecuSUITE symbol and SecuSUITE Audio are always displayed to identify a secure call.

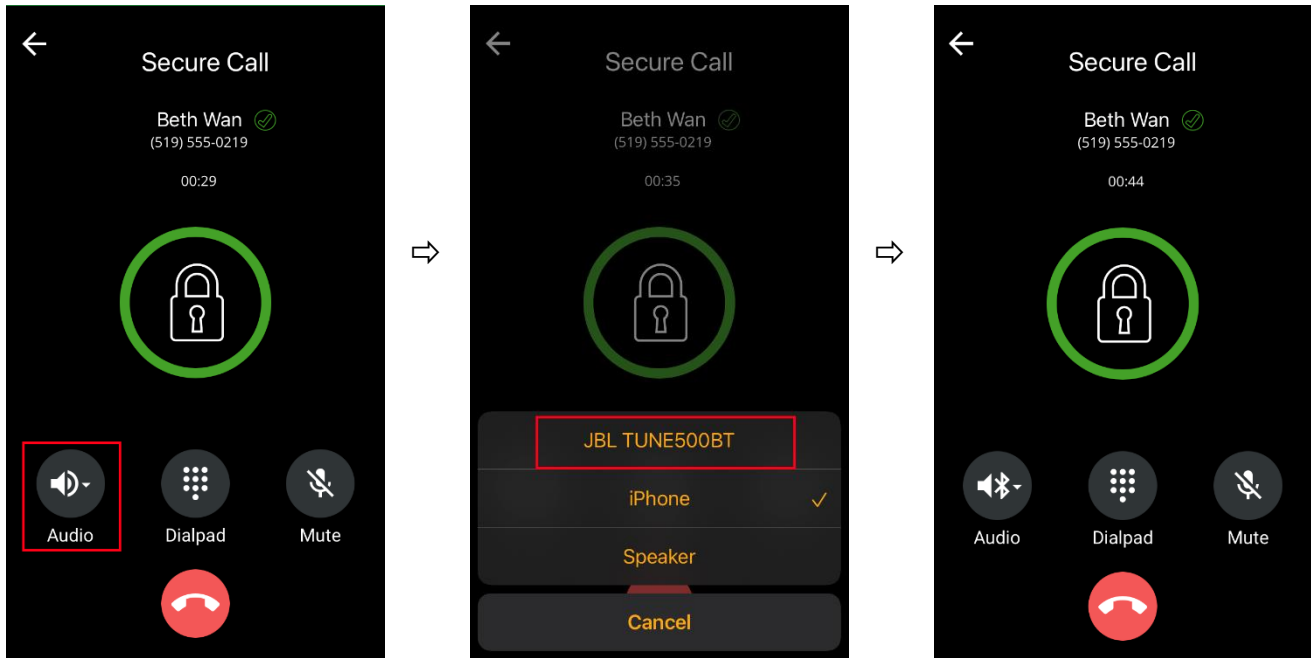
10.5 Bluetooth audio options during a call

During a secure one-to-one or a group call via SecuSUITE, if your phone is connected to an external Bluetooth device for audio such as headphones, you will be able to use the source for audio (**shown on iOS**):

Tap on the audio icon to display your options.

Select the Bluetooth device as the source for audio.

You are now talking/listening through the selected audio source e.g., headphones, as you can see on the audio icon.



Important: Once allowing the use of Bluetooth, the data transfer is **not protected** via SecuSUITE. Since the connection is not suitable for RESTRICTED content you must inform your contact at the beginning of the call!

10.6 Types of secure calls

Secure calls with SecuSUITE are generally made with end-to-end encryption of voice communication and participant authentication. As a result, you can be sure that:

- Nobody can intercept your call.
- Your contact is the person they claim to be.

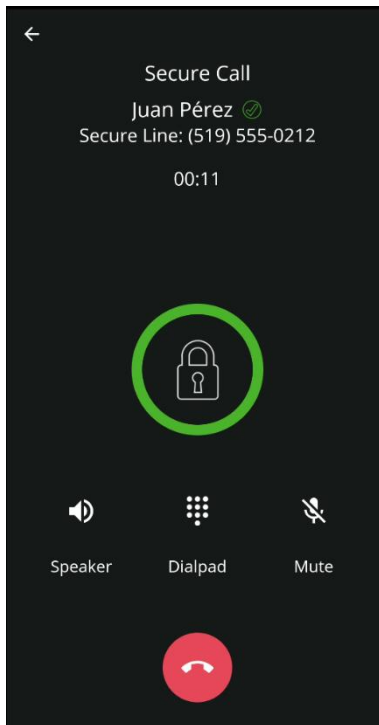
In addition to the direct connection between two SecuSUITE devices, other combinations of devices are also able to make secure calls. These are listed and explained in the following chapter.




These combinations depend on the **Secure Landing** feature: Via SecuSUITE, you can also reach participants inside the secure telephone network of your organization (PBX). If this is implemented in your organization, the PBX is connected to SecuSUITE infrastructure. End-to-end encryption is terminated in the SecuSUITE system, which then transfers unencrypted calls to landline devices in your secure PBX, hence the name, **Secure Landing**.

In every call with SecuSUITE, you can clearly see the type of call you are in to decide if it is secure enough to share confidential content.

10.6.1 Indications for different types of calls

The type of call is indicated directly under the name or number of the caller.



Name	Call Type	Safe for confidential content	Icon in call screen
Secure Line	End-to-end encrypted voice communication	✓	
Secure Work Line	Secure Landing to safe landline inside your organization's PBX	✓	
Breakout into unsecure network	Decryption by Crypto Gateway and forwarding of the unencrypted call into unsecure public phone network	✗	

10.6.2 Complete list of call scenarios

Safe for sharing confidential info?	Call type, devices	Display call screen	Description
Yes	end-to-end-encrypted: SecuSUITE device to SecuSUITE device	Secure Call <Contact Name> Secure Line (Android) <Phone Number>	Two mobile devices with SecuSUITE have established a call. The connection is encrypted end-to-end from one device to the other.
Yes	SecuSUITE device via SecuSUITE system to landline device in protected PBX	Secure Call <Contact Name> Secure Work Line <Phone Number> Gateway@<Domain>	SecuSUITE system terminates the encrypted call from a mobile device with SecuSUITE and forwards it unencrypted into a protected PBX. In this scenario, the unencrypted call is forwarded via the protected PBX to the landline device, so it is still considered secure.
No	SecuSUITE device via SecuSUITE system in unsecure Network (e.g., public telephone network or insufficiently protected PBX)	Secure Call <Contact Name> <type of number> <Phone Number> Breakout into unsecure network	SecuSUITE system terminates the encrypted call and forwards it unencrypted into an unsecure network (e.g., PSTN). The call is not considered secure even though the range between the SecuSUITE device and SecuSUITE system is end-to-end encrypted. This type of protection is suitable for calls abroad or calls made from a hostile environment.

10.6.3 The risks of call forwarding

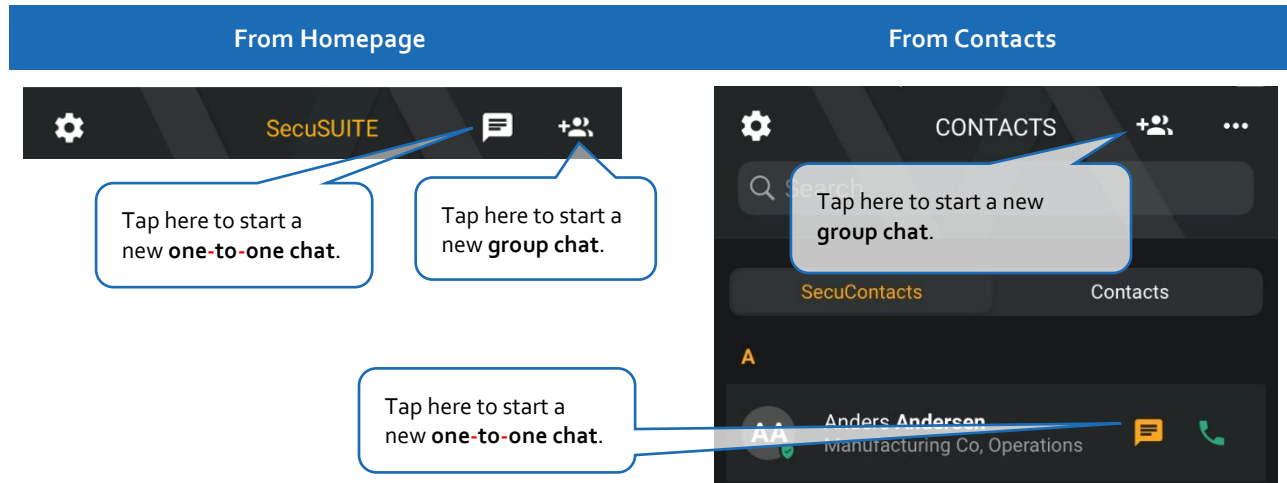
SecuSUITE secures the call between two devices, but if you create an unsecure connection beyond that, the additional range is not protected.

This is the case when **forwarding a call from a secure PBX into an unsecured public telephone network**. The data transfer there is unprotected, e.g., when you are working from home.

Important: Since this connection is not suitable for RESTRICTED content you must inform your contact at the beginning of the call!

11 Secure messaging

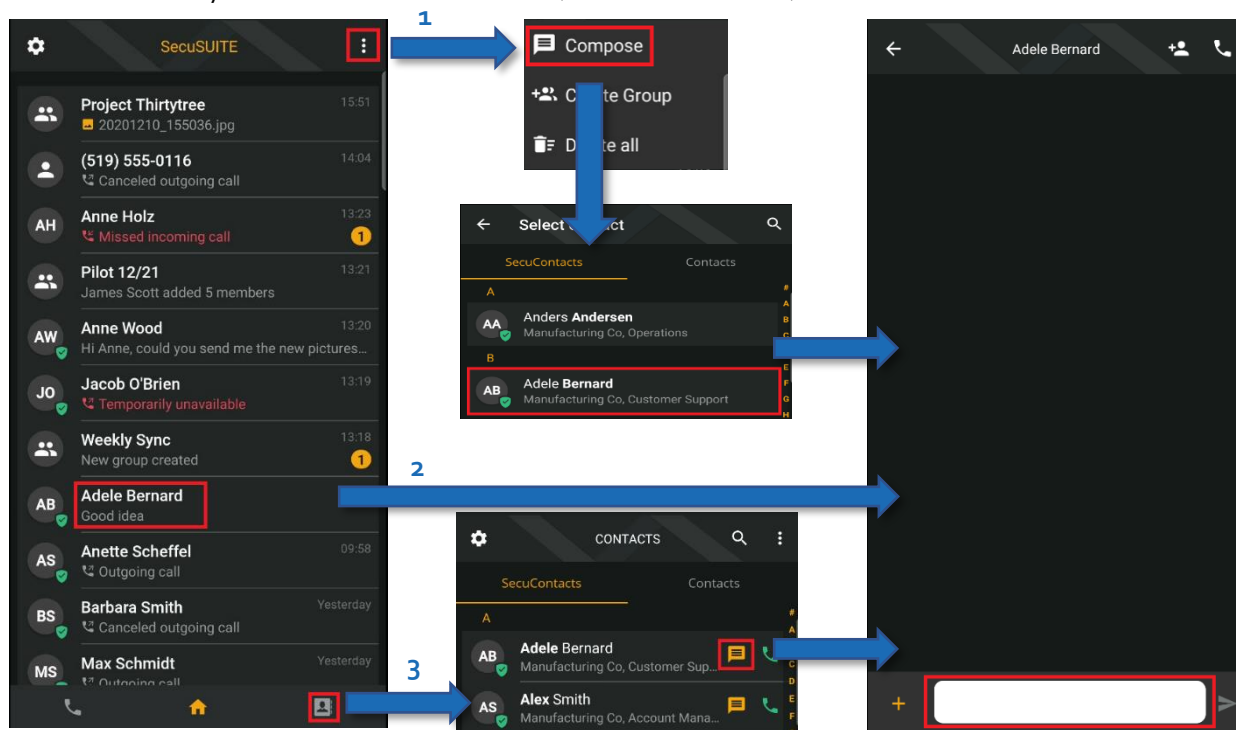
SecuSUITE users can exchange secure text messages in **one-to-one chats** or in **group chats** from the homepage and from the contacts screen (shown on **iOS**):



Important: The keyboard for secure messaging might offer voice dictation through the microphone icon. The voice to text feature uses third party services to receive the audio and send the unencrypted text. **DO NOT** use this feature for restricted content. You can disable this feature in settings as described in chapter [13.2.2 Disable voice dictation](#).

11.1 One-to-one chat

You have three ways to start a one-to-one chat (shown on **Android**):



Only difference on **iOS** (1): Choose the compose icon at the top of the home screen:



11.1.1 Inside a one-to-one chat

11.1.1 Inside a one-to-one chat

Tap here to select content to share.

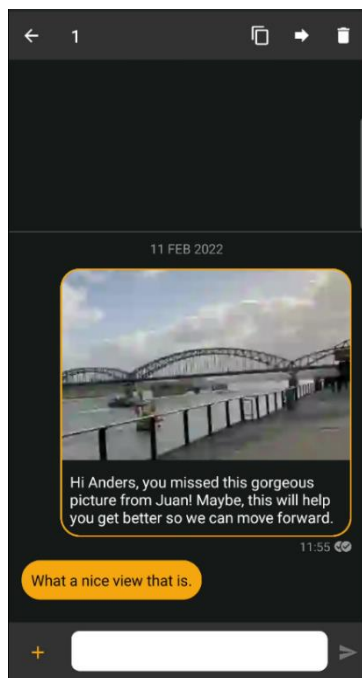
Add another contact (or more) to start a group chat.

1. Tap on this field to bring up the keyboard.

2. Write your message.

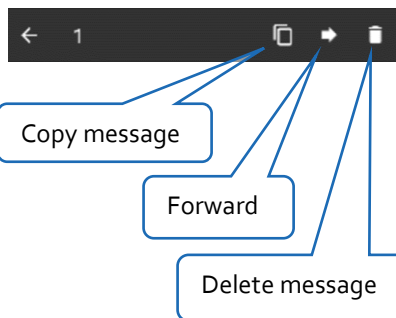
3. Send.

11.1.2 Message actions

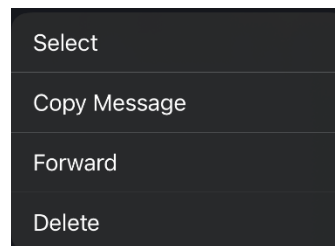


Long tap on a message to view more options.

Android:

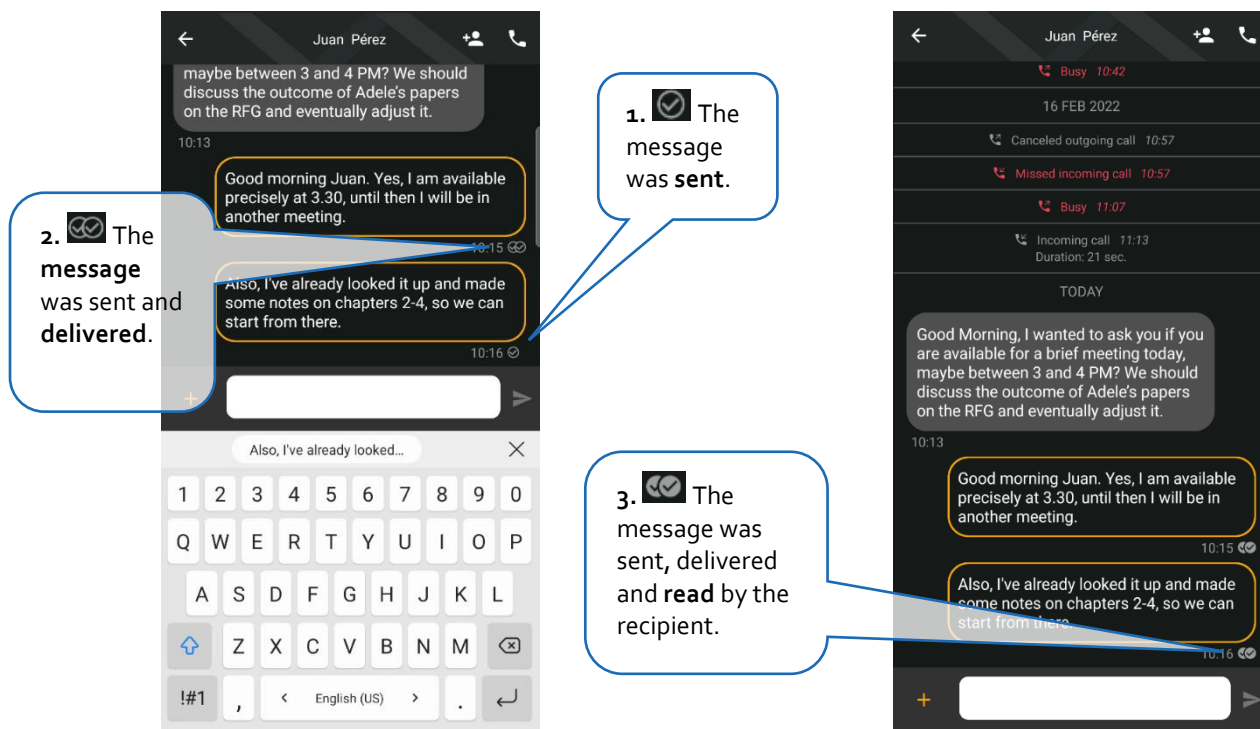


iOS:






11.1.3 Delivery and Read Receipts

Regarding messages sent in a chat, users can now verify their status by checking the receipts below them:

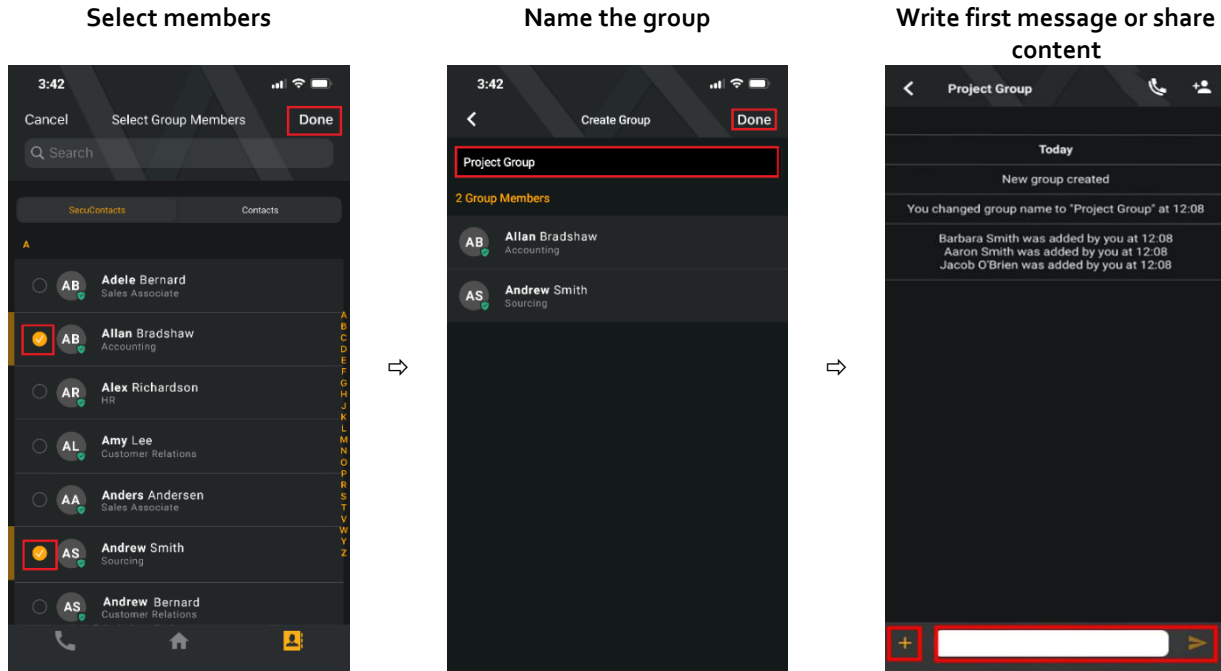


Note: To check the state of any message, you can tap on the message to show or hide the status.

Icon			
Meaning	Sent	Delivered	Read
Explanation	Your message was correctly uploaded onto the server, waiting to deliver to the recipient. If the recipient has no Internet connection or has deactivated SecuSUITE, the message cannot be delivered.	Once you see this icon, the message was delivered to the recipient and can be read.	Your message was read by the recipient. Note: In a group chat, the read receipts show that at least one recipient has read the message (5.2.3 Delivery and Read Receipts in Group chats).

11.2 Group chat

After tapping on the **create group** icon, select all the contacts you want to add to the new group. Give the group a name and after it is successfully created, tap into the empty field to type a first message. Once a group is created all added group members will be notified.



11.2.1 Adding people to an existing group

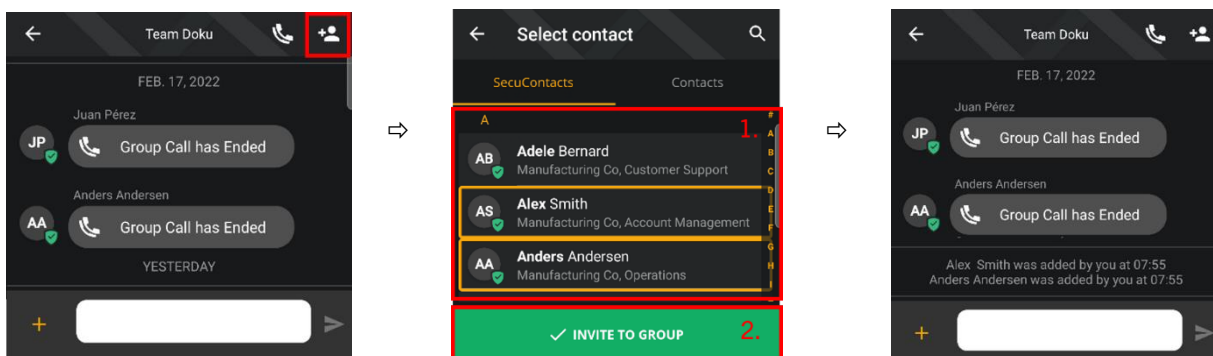
After a group has been created, you can still add more members to the group.

Note: Recently added members will not be able to see the group's chat history.

Tap on the icon in the top right corner.

Select contacts (1.) and tap on **Invite to group** (2.).

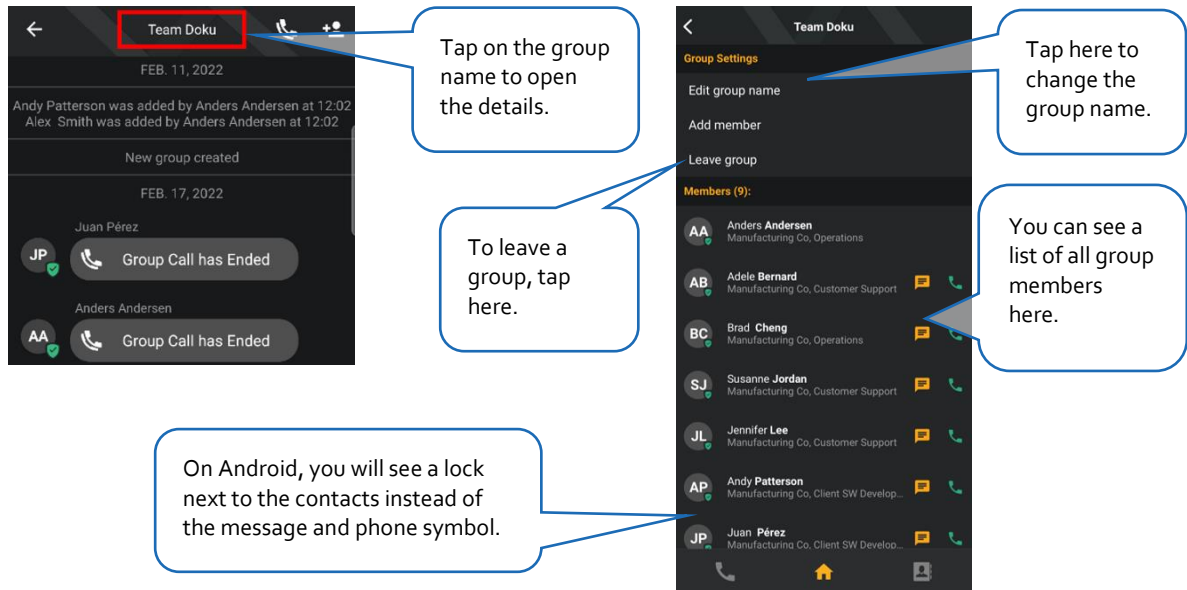
A note will state that the contacts were added.



Note: If you add contacts to a group while not having an active Internet connection, the note will state **<Contact name> will be added by you**. The contact is added once SecuSUITE is online again.

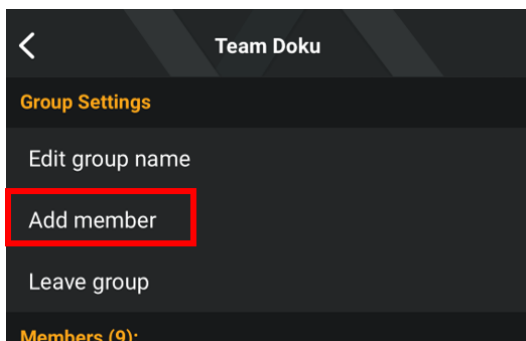
11.2.2 Group settings

You can view group details and adjust some group settings as a creator or as a member. Tap on the name of the group to open the details (shown on iOS).

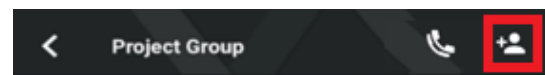


You can also add new group members from the details view:

On iOS, tap on **Add member** in the list of group actions.



On Android, tap on the symbol in the top right corner.



11.2.3 Delivery and Read Receipts in Group chats

Delivery and read receipts are also available in group chats. Once one member has read your message, the icon will change to the following:

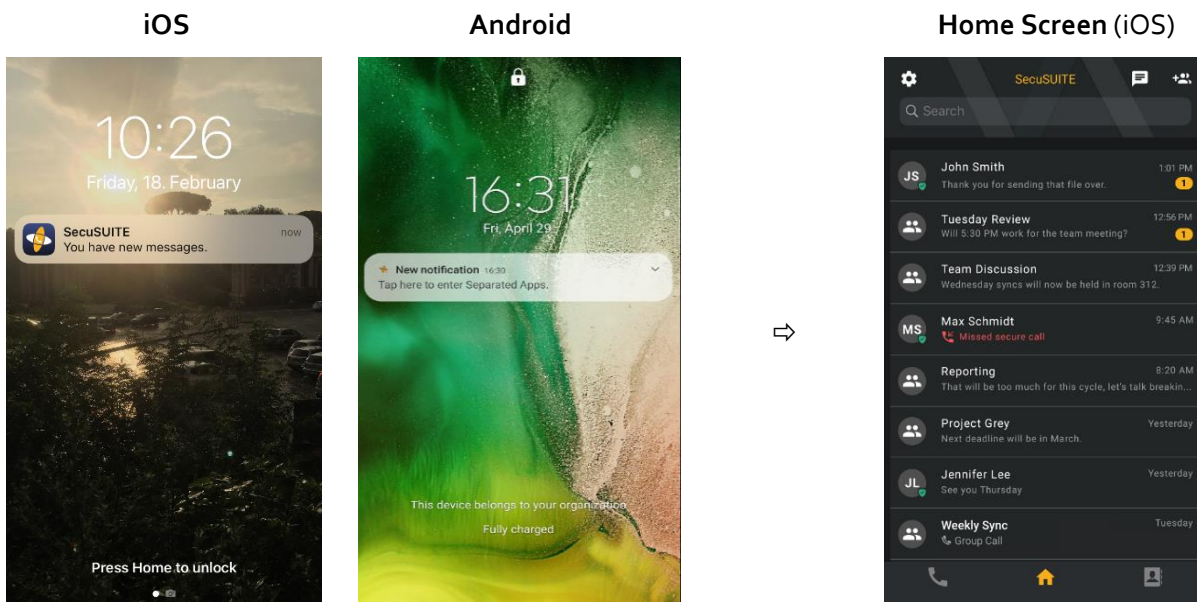
Note: It is not possible to view who has or has not read a message.

11.3 Receiving secure messages

Secure messages will trigger notifications on your phone by default. However, you can deactivate this feature in your phone settings ([13.2.1 Notifications](#)). If notifications remain enabled, SecuSUITE will send alert notifications on the lock screen of your phone if you receive a message or miss a call. The notification will not include the content of the message you have received.

A tap on the notification will either direct you to the conversation screen or the home screen if you have received multiple notifications from different conversations.

The home screen shows the latest activities, including new messages and missed calls.

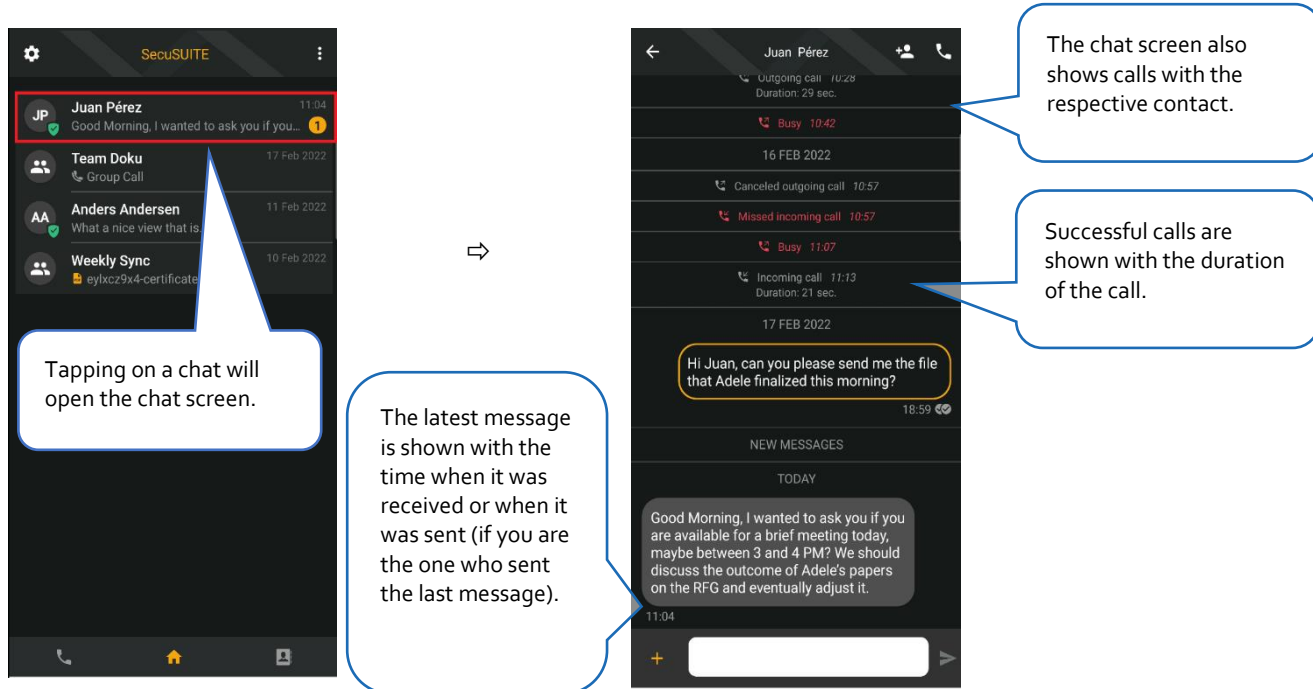


Note: Depending on which Android device you have and the version that it is running on, the notification display on the lock screen might differ slightly from the one illustrated above (Android 12 on Samsung S10).

Note: If another person has added you to a group chat, you will receive this information like an ordinary message.

11.4 Replying to messages

If there is already an existing conversation with a user, you will see the conversation on the home screen. Unread messages in a chat are marked with an orange circle showing the number of unread messages.



12 Share content

You can share content in one-to-one chats and group chats. To share content, simply tap on the + icon left of the text field.

Note: You can only share one attachment at a time.

With Android 12, a new feature allows you to see if you are using the device's microphone (as described in chapter 4 [Secure calls](#)) or the camera. When sharing content on SecuSUITE e.g., you can directly take the picture with your device's camera and share it with your contact. In this case, first a green camera icon will briefly appear on the screen in the upper right side; then this icon turns into a small green dot, which will stay if the camera is in use:

Camera is activated

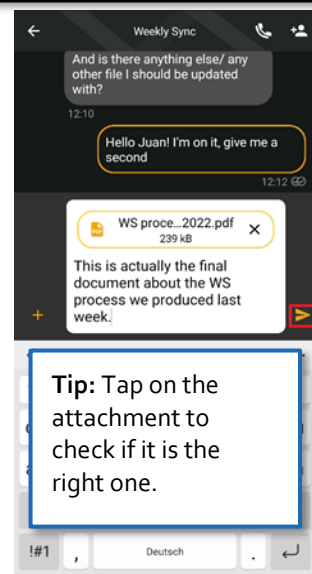
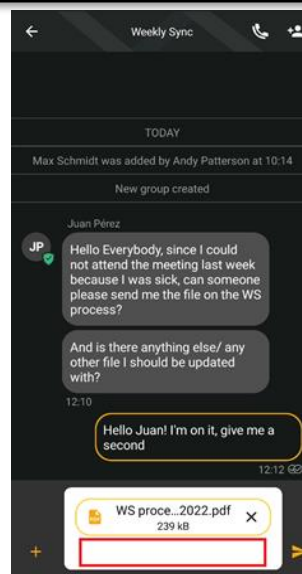
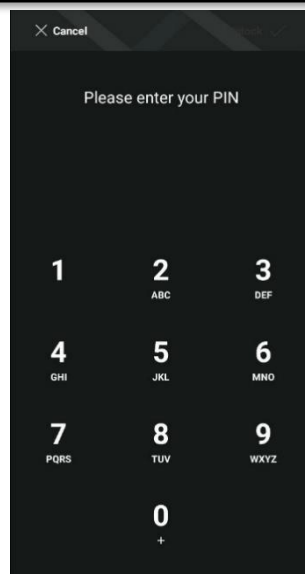
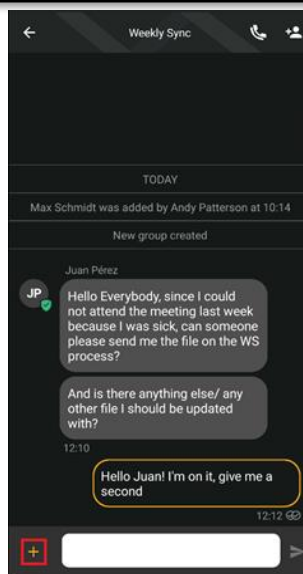


If the camera is active



12.1 Share content in chats on Android

<p>Tap on the + icon and select a source for the content you intend to share.</p>	<p>Once selected, enter the SecuSUITE PIN to access the app again.</p>	<p>To add text, tap into the text field to open the keypad.</p>	<p>Tap on the send icon to share the content.</p>
--	---	--	---

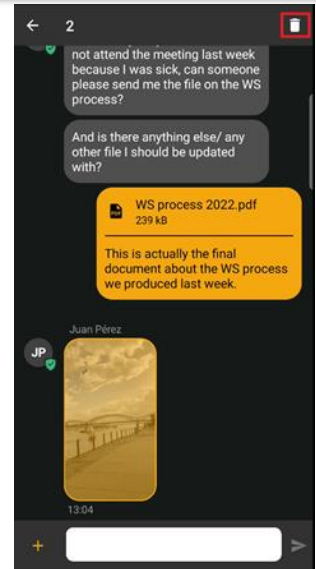
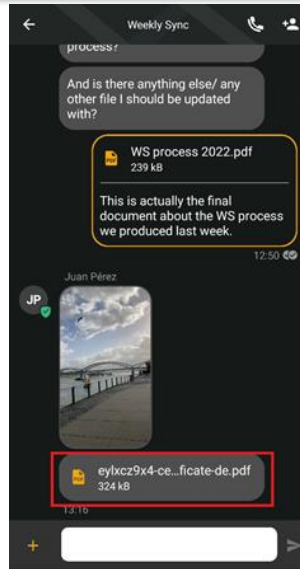
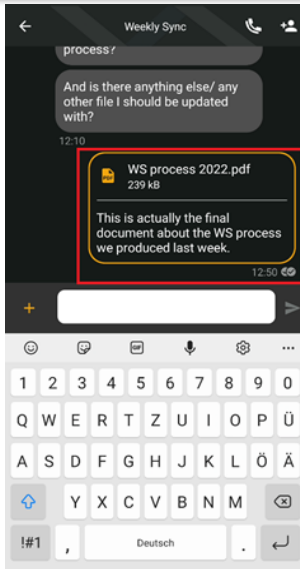


A grey frame and progress bar will show that the content is pending, and the red frame means the content has failed to send. When the frame is orange, it has successfully sent (with timestamp).

Incoming content will need to decrypt and load. You will see a progress bar while the file is being processed.

Pictures and Videos will display a **preview**. Tap on a **file** to open it.

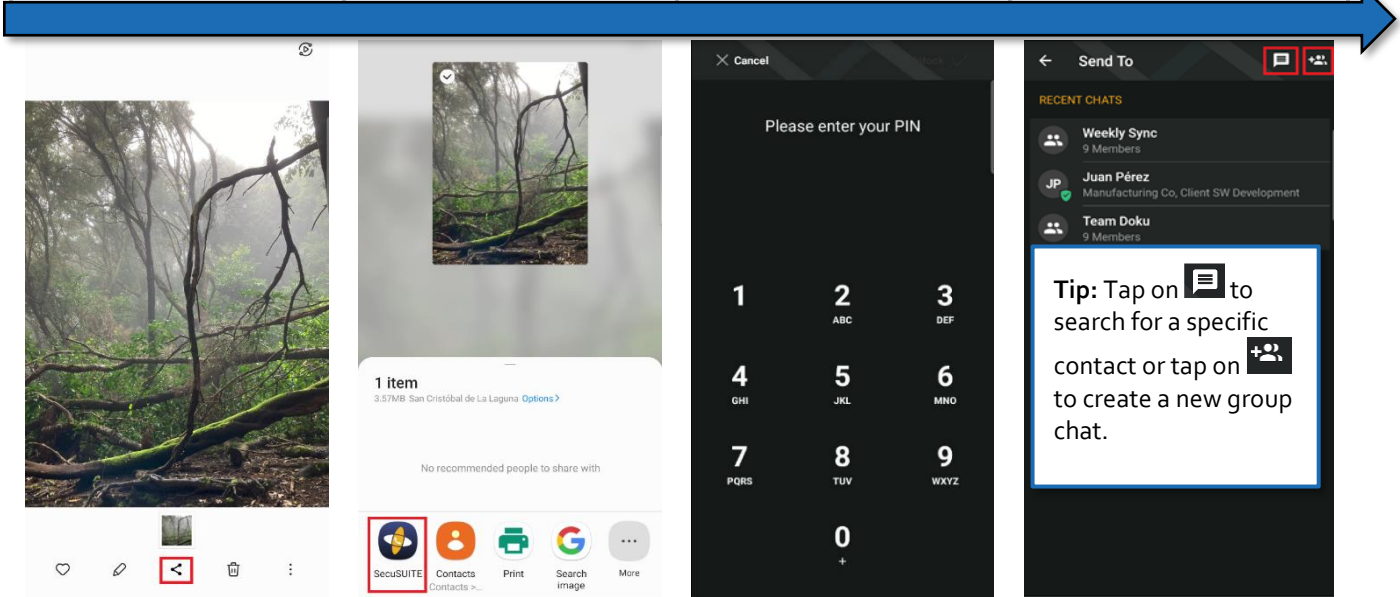
Pressing and holding on shared content (one or several items) will show the option to **delete**.



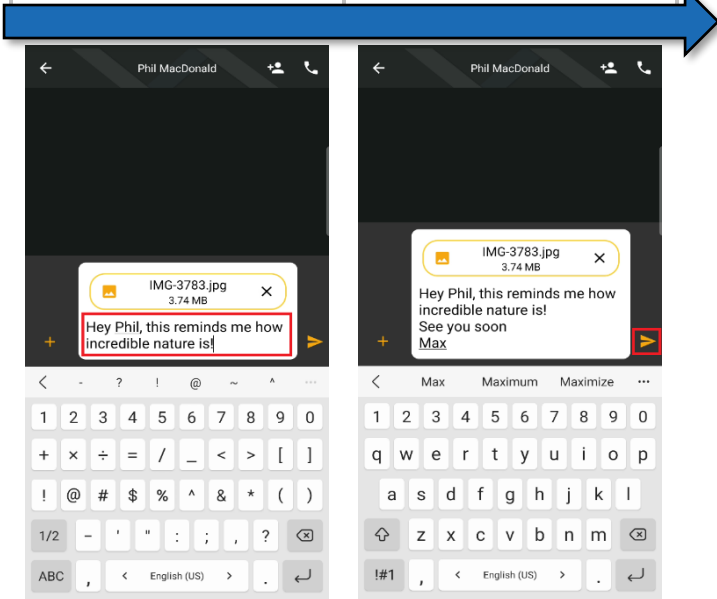
12.2 Share content through share extension on Android

You can now share content from other apps to SecuSUITE. Here's how:

<p>For instance, select a picture from the Photo Gallery and tap on the share icon.</p>	<p>Select SecuSUITE to instantly share the picture with your SecuContacts.</p>	<p>Enter the SecuSUITE PIN to access the app again.</p>	<p>Your recent chats will appear to those you can send this attachment to.</p>
---	--	---	--

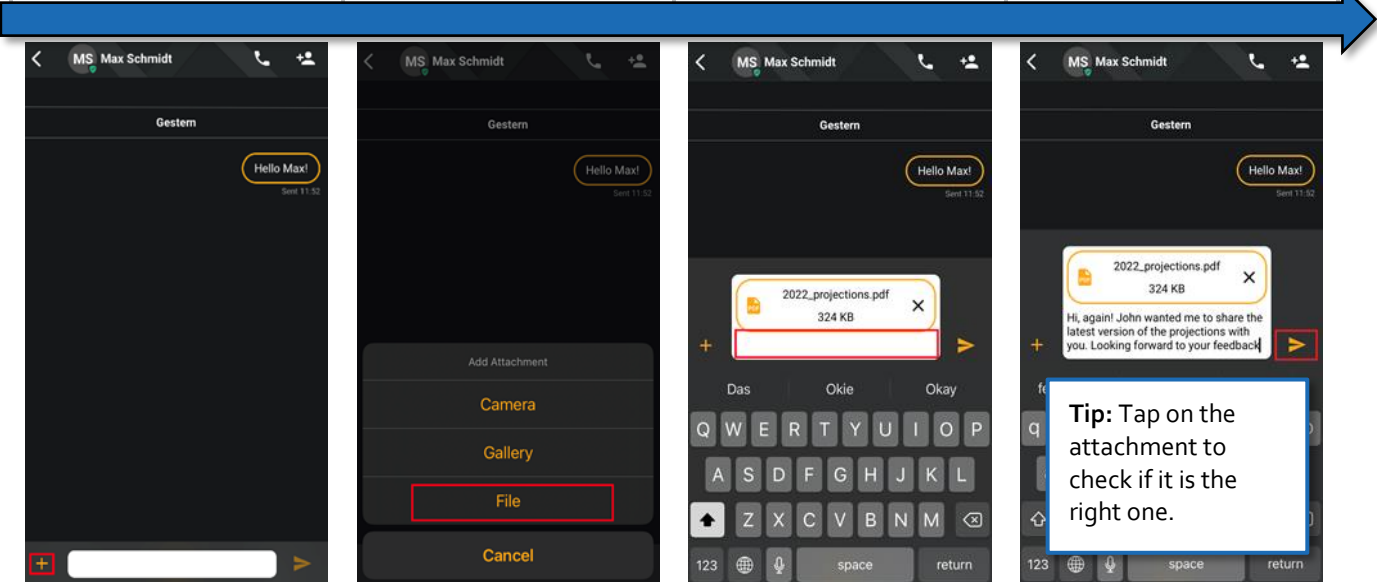


<p>After selecting a contact or group, find the attachment inline. To add text, tap on the text field beneath the file.</p>	<p>Finally, tap on the Send icon to send the attachment.</p>
---	---

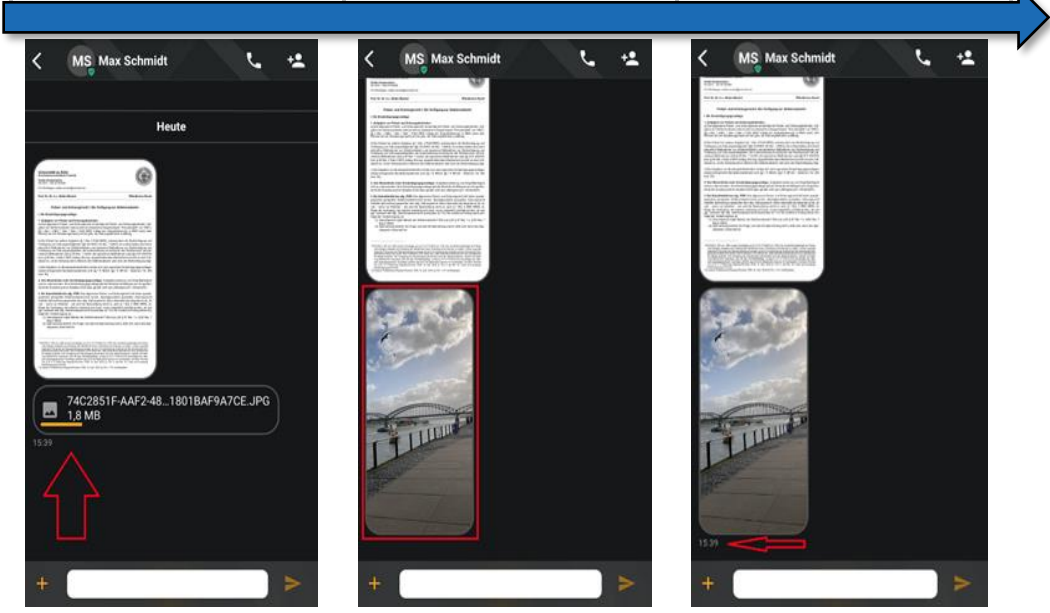


12.3 Share content on iOS

<p>Tap on the + icon next to text input field.</p>	<p>Select a source for the content you intend to share.</p>	<p>To add text, tap into the text field to open the keypad.</p>	<p>Hit the send icon to share the content.</p>
---	--	--	---



<p>Incoming content will need to decrypt and load. You will see a progress bar while the file is being processed.</p>	<p>Tap on the content to enlarge it.</p>	<p>Tap on the frame of the content to show or hide when the attachment was sent.</p>
---	--	--




Note: Pictures, videos, and data to be shared cannot be larger than 100 MB.

13 Settings

13.1 SecuSUITE settings

13.1.1 Account information



In **Account** you will find all the details of your current account in SecuSUITE, including the phone number you are registered with.

Under certain conditions, your administrator will ask you to re-activate your account. First, you will have to delete your account by tapping on **Remove** and confirm with ⇒ iOS: **Remove**/Android: .

Note: When you activate the account anew on the same server, you will only find your contacts. However, your call log, shared content, and membership in groups will be lost. You must be added to these groups again to receive future messages, but you cannot view the group's message history.

13.2 General phone settings

13.2.1 Notifications

Android™	iOS®
<p>You can decide which SecuSUITE notifications you want to get. By default, you will be notified about missed calls and messages.</p> <ol style="list-style-type: none">1. In SecuSUITE, tap  Settings.2. Tap General.3. To see notifications about missed calls switch Missed calls to active.4. To see notifications about secure messages, switch Secure messages to active.	<p>To enable or disable notifications, navigate to your phone's  Settings ⇒ SecuSUITE. From there, you can control whether you want SecuSUITE to notify you with sounds, and whether message alerts will appear on your lock screen.</p> <p>Important: If you disable notification on iOS, the user will not be informed of any incoming calls. This setting will disable all notifications.</p>

13.2.2 Disable voice dictation

Android™	iOS®
<p>Although Android does not come with a native voice dictation feature, there are apps that extend the keyboard by voice dictation.</p> <p>Do not use this feature in SecuSUITE.</p> <p>If your phone is managed by an MDM, such apps could be already disabled by your administrator.</p>	<p>The keyboard for secure messaging offers the usual voice dictation over the microphone icon. The transfer from spoken to written language involves Apple services to receive audio and send the resulting text unencrypted.</p> <p>Do not use this feature in SecuSUITE.</p>

To prevent yourself from using a voice dictation feature in SecuSUITE, you should not operate such apps on the device that you operate SecuSUITE on.




If your phone is managed by an MDM, this feature could already be disabled by your administrator.

To prevent yourself from using it, you can disable it by following these steps:

1. **iPhone Settings**
2. **General**
3. **Keyboard**
4. Disable **Dictation**.

Note: This will disable voice dictation in all apps on your iPhone.

13.2.3 Bluetooth settings

Android™	iOS®
<p>There are two ways for enabling/disabling Bluetooth on your Android based device.</p> <p>You can either go to the Android Quick Settings menu by simply dragging your finger from the top of your screen downward and then tap on the Bluetooth icon ...</p> <p>...or you can also do the same from the General Phone Settings:</p> <ol style="list-style-type: none">1. Go to  Settings2. Tap on Connections3. Enable/disable Bluetooth by moving the bar to the right or to the left.	<p>On iOS, there are two ways for enabling/disabling Bluetooth.</p> <p>On iOS, you can either access the Control Center by dragging your finger from the top of your screen downward (iPhones with Face ID) or from the bottom of your screen upward (iPhones with Touch ID) and then tap on the Bluetooth icon ...</p> <p>...or you can also do the same from the General Phone Settings:</p> <ol style="list-style-type: none">1. iPhone Settings2. Tap on Bluetooth3. Enable/disable Bluetooth by moving the bar to the right or to the left.

Important: Once allowing the use of Bluetooth, for instance, in order to use your Bluetooth device for secure calling, the data transfer is **not protected** via SecuSUITE. Since the connection is not suitable for RESTRICTED content, you must inform your contact at the beginning of the call!

13.3 Download options for shared content

To define the way shared content is downloaded in your app, in SecuSUITE go to **Settings** ⇒ **General** ⇒ **Auto-download media**.

- For automatic download of received content you can either enable:
 - **When connected to Wi-Fi** or
 - **When using mobile data** or

- Both
- Or you can disable everything. Then the content is only downloaded when you tap on it in a chat.

14 SecuSUITE Client Updates

BlackBerry provides timely security updates for the TOE in case vulnerabilities have been discovered. Reported vulnerabilities and defects are investigated and rated based on the potential threat and then scheduled for an upcoming bug fix or roadmap release. The time between disclosure of a vulnerability and the availability of a security update is minimum 10 days (due to the app store publishing process) and BlackBerry aims for a maximum of 50 days. In case of low-risk security issues updates may be provided later as part of a regular release.

BlackBerry is accepting reports about potential vulnerabilities of the SecuSUITE client via the HTTPS protected BlackBerry contact form: <https://www.blackberry.com/us/en/forms/enterprise/contact-us>.

Update of 3rd party libraries

For all included 3rd party libraries, BlackBerry checks regularly for release updates that would address vulnerabilities that have been discovered and published for that component (e.g. via <https://nvd.nist.gov>).

Depending on the classification of the vulnerabilities and impact to the SecuSUITE product, BlackBerry provides updated client releases that include those fixes in a timely manner.

As soon as the fix release is available for the 3rd party component, BlackBerry plans the integration of the updated component release for one of the upcoming SecuSUITE client releases. The time between the public availability of a 3rd party component vulnerability fix and the availability of the SecuSUITE client update is minimum 10 days (due to the app store publishing process) and BlackBerry aims for a maximum of 50 days. In case of low-risk security issues updates may be provided later as part of a regular release.

14.1 Client Software Version

To validate the current version of the SecuSUITE application, please go to **Settings > About SecuSUITE**. Alternatively, the version number can be validated also in the platform application manager

Android™:

Settings > Apps > SecuSUITE (version information at the bottom of the page)

iOS®:

Settings > General > iPhone Storage > SecuSUITE (version information is shown next to the app icon)

14.2 Client update via App Stores

Once available, the client updates are offered via the public application stores. To validate the current version of the SecuSUITE application, please go to **Settings > About SecuSUITE**.

Update of the Android™ client:

1. Open Google Play Store Application
2. At the top right, tap the profile icon
3. Tap **Manage apps & device**. Apps with an update available are labeled "Update available."
4. Tap **Update**.

5. The Play Store application shows the progress of the download and installation
6. Once the installation is complete, the user should validate the release number within the SecuSUITE client in **Settings > About SecuSUITE**

Note: The OS platform automatically validates the application signature that is included in the installation package. In case the signature does not match the certificate of the installed application, the client update process is terminated by the OS, and the user is notified.

Update of the iOS® client

1. Open App Store Application
2. Tap on the user profile icon (on top right of the screen)
3. In case an update is available, the SecuSUITE application is listed under “Available Updates” section
4. Tap on “Update” to initiate the download and installation of the new release.
5. The App Store application shows the progress of the download and installation
6. Once the installation is complete, the user can validate the release number within the SecuSUITE client in **Settings > About SecuSUITE**

Note: The iOS platform automatically validates the application signature before the update is installed. In case the signature does not match the certificate of the installed application, the client update process is terminated by the OS, and the user is notified.


15 SecuSUITE FAQ

15.1 What if I can't hear call audio?

You may not be able to hear call audio if your Wi-Fi network has not opened the required ports. You can end your call and try again, or if it's a group call simply leave and try rejoining. You can also attempt your call over mobile data instead by disconnecting from your Wi-Fi. Please contact your network administrator if the issue persists.

Sometimes it helps to toggle the "mute" switch to off and on again.

15.2 What's my phone number?

The telephone number assigned to your account is not necessarily the same as the phone number of your SIM card, as the administrator is free to define another phone number. Usually, both phone numbers are the same. To find out which phone number is assigned to your SecuSUITE account, tap on  (Settings) in the top bar ⇒ **Account** ⇒ **Account Number**.


For you to receive secure calls from the inside of your organization's protected call environment (PBX), your administrator defines a callback number for you. This is not visible in SecuSUITE Settings, but your administrator will share this number with you when it is set up.

15.3 What prefixes do I need to dial?

An international prefix is only necessary for international numbers. Numbers dialed without a prefix are automatically completed with your national prefix.

To make secure calls into the protected PBX of your organization, you can use specially defined short numbers. Your administrator will provide you with these numbers.

15.4 How can I reach someone who is not registered in my tenant?

If this person has a SecuSUITE account inside your organization, you just need the phone number connected to the app (they can find it in  **Settings** ⇒ **Account** ⇒ **Account Number**). Call this number and after the first secure call you both will be able to save each other as secure contacts and add one another to group chats.

15.5 Why can't I see the contact of an important person in my tenant?

Maybe this person was marked as a **VIP** by the administrator. In this case, their contact data is not shared automatically. If you have their number (or they call you first), you can save it as a SecuContact after your first communication and find it in your contacts from then on.

15.6 What does each sound notification mean?

Action/Situation	Sound Notification
Call establishment	Deep triple tone
Call ringing	Single long, ringing tone
Key agreement	Repeated, short double tone
Connection established	Single high tone
Call end	Descending double tone
Your recipient is already in a phone call	busy tone
Phone or app of the recipient is either not active or outside of network	"The person you have called is temporarily unavailable."
PIN entry needed	"Please unlock"

15.7 Why can't I share a selected file?

SecuSUITE allows you to share pictures, videos, and other files in one-to-one chats and in group chats. However, please note that you can only share one file at a time, and content **cannot be larger than 100MB**.

Legal Notice

© 2022 BlackBerry Limited.

Trademarks, including but not limited to BLACKBERRY, EMBLEM Design, SECUSMART and SECUSUITE are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Android and Google are trademarks of Google Inc. iOS is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. All other trademarks are the property of their respective owners. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any Third party licenses are required to do so. If required, you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor,
The Pearce Building
West Street
Maidenhead, Berkshire
SL6 1RL
United Kingdom