Australian Government
Department of Home Affairs

Signal app use in Home Affairs

Start and Manage Groups

Private Signal group chat

All group chats through Signal iOS are private.

NOTE: Chat backup is not to be enabled within the Signal application. In line with the department's Records Management Policy official decisions made on this platform must be documented and saved to TRIM.

Characteristics

- This group only includes Signal users.
- Everyone in the group can communicate with each other.
- All messages are private.
- All communication transmits over the internet.
- All communication is free of charge.
- There is no size limit for groups.
- You can name the group and set a group avatar.
- Members can choose to leave the group at anytime.

Steps to create

1. In Signal, tap compose > new group in the top right.
2. Tap the contact names that you would like to add to the group. **Member** will appear next to any contacts that have been selected.
3. Optional: Tap **Name this group chat** to change the name of the group.
4. Optional: Tap the group avatar to set an image that all group members will see.
5. Tap **Create** to ***immediately*** create a group with all the members. Any member can start messaging in the group.
6. Send a message in the group.

More information

Contact IT Support on s. 22(1)(a)(ii) or email s. 22(1)(a)(ii) @homeaffairs.gov.au

Visit the Signal homepage

Australian Government
Department of Home Affairs

Signal app use in Home Affairs

Voice or Video Calling

NOTE: In line with the department's Records Management Policy official decisions made on this platform must be documented and saved to TRIM.

Like all Signal messages, voice and video calls are private too. You will be prompted to grant the Camera and Microphone permissions the first time you make or receive a Signal call.

Here's how to start a voice or video call on your iOS device:

1. In Signal, tap compose to view your Signal contact list.
2. Select a contact or enter a number to open that conversation.
3. Tap the phone.
4. For a video call, tap the camera to show video from **your** side of the call.
5. Your call screen will show
   a. Connecting - while waiting for the call to connect with your contact.
   b. Ringing - when your contact's phone is online and ringing.
   c. Call timer - after your call has been answered.

More information

Contact IT Support on s. 22(1)(a)(ii) or email the Telecoms Asset team at s. 22(1)(a)(ii) @homeaffairs.gov.au

Visit the Signal homepage

Australian Government
Department of Home Affairs

OFFICIAL: Sensitive

Signal app use in Home Affairs

What's happening?

The Department has enabled access to the Signal application from 7 April 2020 as an approved encrypted messaging platform on corporate iOS devices, replacing the use of the WhatsApp messaging platform.

What is Signal?

Signal is a cross-platform messaging service that uses standard mobile service numbers as identifiers and uses robust end-to-end encryption. Signal can be used for up to PROTECTED voice, messaging and video conferencing when used on a Department device and with no external parties in attendance.

NOTE: In line with the department's Records Management Policy official decisions made on this platform must be documented and saved to TRIM.

Benefits of using Signal

- Signal uses standard mobile service numbers as identifiers and uses end-to-end encryption for all communications.
- Signal supports secure one-to-one and group messages, which can include files, voice notes, images and videos.
- Signal also support one-to-one secure video and voice calls.
- Signal is designed to never collect or store any sensitive information. Signal messages and calls cannot be accessed by anyone other than the intended recipients and all sensitive information is only stored on the sender and recipient devices.
- Signal messages can be sent with an expiry time after which messages are deleted from the sender recipient devices.
- Encryption keys are only stored on the sender and recipient devices.
- Each Signal conversation has a unique safety number that allows you to verify the security of your messages and calls with specific contacts.

Installing Signal on your iOS device

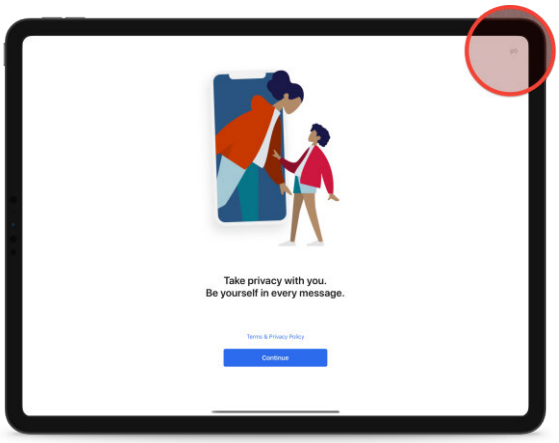
Signal can be downloaded and installed from the Apple App Store by following these steps:

iPhone

1. Check that your iOS device is running the most recent iOS version and update iOS if required.
2. Install and open Signal.
3. Follow the on-screen instructions to complete the registration process.

iPad

4. Check that your iOS device is running the most recent iOS version and update iOS if required.
5. Install and open Signal.
6. Follow the on-screen instructions to
   a. link the iPad to your phone or
   b. Select the unlink icon in the top right to register this iPad as a separate device and number.



Already using an iPad? Update to the latest version or follow these troubleshooting steps for linking.

Initial configuration advice

Notification Privacy

Even when your iOS device is locked with a password, anyone who picks it up can still read the message and the sender's name from your lock screen. To avoid this follow these steps in the Signal app:

- Click Settings > Notifications > Show. To receive notifications with no information about the sender or the content of your messages, turn on "No Name or Content."

Screen Security

The Signal app also gives you options to lock your screen and prevent a preview from being shown unless you are in the app when a message is received:

- Click Settings > Privacy > turn on Screen Lock and set the Timeout to 15 minutes
- Click Settings > Privacy > turn on Enable Screen Security

Additional security advice

Disappearing messages

Disappearing messages should not be enabled in Signal conversations where Departmental business is discussed, and staff must ensure that any official decisions made via an endorsed application are recorded in an approved departmental recordkeeping system.

Safety Numbers

Signal allows you to verify that your session is encrypted and cannot be intercepted by a third party. Each Signal conversation has an automatically generated and unique safety number that allows you to verify the security of your messages and calls with specific contacts.

Verification of safety numbers is a good security practice for sensitive communication. Once a safety number has been marked as verified, any change must be manually approved before sending a new message.

How do you view a safety number?

Open a conversation thread with a contact and look for their safety number. This number verifies a secure and encrypted connection between your device and your contact's device.

- Tap your colleague's name (at the top of the screen) > View Safety Number

Signal advises you whenever a safety number has changed. This allows users to check the privacy of their communication with a contact and helps protect against any attempted communications interception.

The most common scenarios where a safety number advisory is displayed are when a contact switches to a new device or re-installs Signal. However, if a safety number changes frequently or unexpectedly it may be a sign that something is wrong.

Registration Lock

Whether it's your regular device number or a secondary number, you'll need to maintain access to this

number. Why? If you lose access to the number and someone else re-registers it, now they own the Signal number.

You can lock in the registration for your Signal number, using Registration Lock:

- Open the Signal app > Tap in the icon in the top left corner (usually your initials) > Tap Privacy > Scroll down and tap Registration Lock > Enter a PIN number

What else must I do?

- Signal for business use is not to be installed on your departmental PC or laptop or on your personal mobile device.
- Signal software is to remain up to date.
- Screen Lock is to be enabled and Timeout set to 15 minutes.
- Enable Screen Security is to be turned on, this must include blocking screenshots from within Signal.
- Limit the Notifications Content to display Name Only.
- Add Signal PIN to the Registration Lock.
- All communication on Signal iOS is private and end-to-end encrypted.
- Chat backup is not to be enabled
- Signal-to-Signal messages are secure and free to send and receive using any internet connection enabled on your phone, including WiFi and mobile data.
- Having issues installing on an iPhone? Follow these troubleshooting steps.

More information

Contact IT Support on s. 22(1)(a)(ii) or log a Service Request

Security Coordination Centre: s. 22(1)(a)(ii)@homeaffairs.gov.au

Visit the Signal homepage

Videoconferencing

On this page:

Videoconferencing

The Department of Home Affairs has three videoconferencing options providing staff with secure ways to connect, communicate, and collaborate. Videoconferencing or a video conference (VC) is a live, visual connection between two or more people in separate locations for the purpose of communication. It allows staff to hold face-to-face meetings without having to be in a single location.

Videoconference uplift project

We have made some changes to our core videoconferencing system to enable support of Microsoft Teams (Teams) as the departments collaboration solution.

Further information is available:

- Microsoft Teams meeting via One-touch Join (TRIM ADD2025/136445)
- Videoconference Direct Dialling (TRIM ADD2025/136475)

Microsoft Teams

Microsoft Teams has been selected as the department and Australian Border Force's (ABF) preferred collaboration solution.

For quick reference guides, hints and tips, go to the Microsoft Teams for Home Affairs and ABF page.

Signal mobile application

The Signal application is the Department’s approved encrypted text messaging platform, replacing the use of the WhatsApp messaging platform.

Signal is a cross-platform messaging service that uses standard mobile telephone numbers as identifiers and uses robust end-to-end encryption. Signal can be used up to PROTECTED level for voice, messaging, and video conferencing, when used on a Department device and with no external parties in attendance.

Signal resources

- Signal for Home Affairs (TRIM ADD2021/258421)
- Signal Voice and Video Calls (TRIM ADD2021/258487)
- Signal Managing Group Chats (TRIM ADD2021/258552)

Visit the Signal homepage.

For more information and support

The concierge service is available for staff who require assistance scheduling and connecting to any video conferencing room. Concierge staff have baseline AGSVA clearances and an ESC. The concierge has access to the video conferencing system, video conference units and troubleshooting tools. Contact op s. 22(1)(a)(ii) omeaffairs.gov.au for access to these services.

Issue	Contact	Details
Technical issues	IT Support	Phone: s. 22(1)(a)(ii)
Skype videoconferencing concierge services	Optus Video Conferencing	Email: s. 22(1)(a)(ii) @homeaffairs.gov.au
Signal Security concerns	Security Coordination Centre	Email: s. 22(1)(a)(ii) @homeaffairs.gov.au

Last updated: 23 January 2025
Content owner: CORPORATE DIGITAL COLLABORATION SY

Claim ownership Feedback