Silentel

NATO approved solution for voice and data communication

February 2022

Why to use secure communication?

- Secure communication – neglected area in cybersecurity
- 80% of all communication is made with mobile phones
- Many cases of hacked phones of politicians, businessmen
- Mass usage of surveillance devices
- Legal requirements (classified communication, GDPR, …)
- 10 out of 10 security advisors call for voice and text encryption
- However – many users don’t use reliable secure communication

What to use for secure communication?

Common encryption app

- Designed for mass market
- Security is advantage
- Users – almost everyone

vs.

Certified secure system

- Designed for security
- Complex security is must
- Users – gov & business

Are common encryption apps secure enough?

- Most systems declare E2EE, but it's not *real magic*
- How are data secured if your device is lost?
- Can you verify users' identity / revoke user's account?
- No certification. No independent third party security evaluation. Open source is not enough.
- The ability to protect sensitive information with proven security can determine the difference between success and failure

WikiLeaks

CIA can effectively bypass WhatsApp, Telegram, Signal, Confide

The Guardian

WhatsApp design feature means some encrypted messages could be read by third party

The Hacker News

One photo could have hacked your WhatsApp and Telegram accounts

the japan times

A total of 4225 registered accounts on app Line have been hacked

What is Silentel?

- Silentel is the serious choice for any user who wants to protect and secure his voice calls, messages, chats, sensitive documents, photos or any files against eavesdropping and interception

- Customers including Public Safety authorities, Military, Intelligence services and other Government organizations in more than 50 countries rely on the security and quality of Silentel applications

Silentel guaranteed security

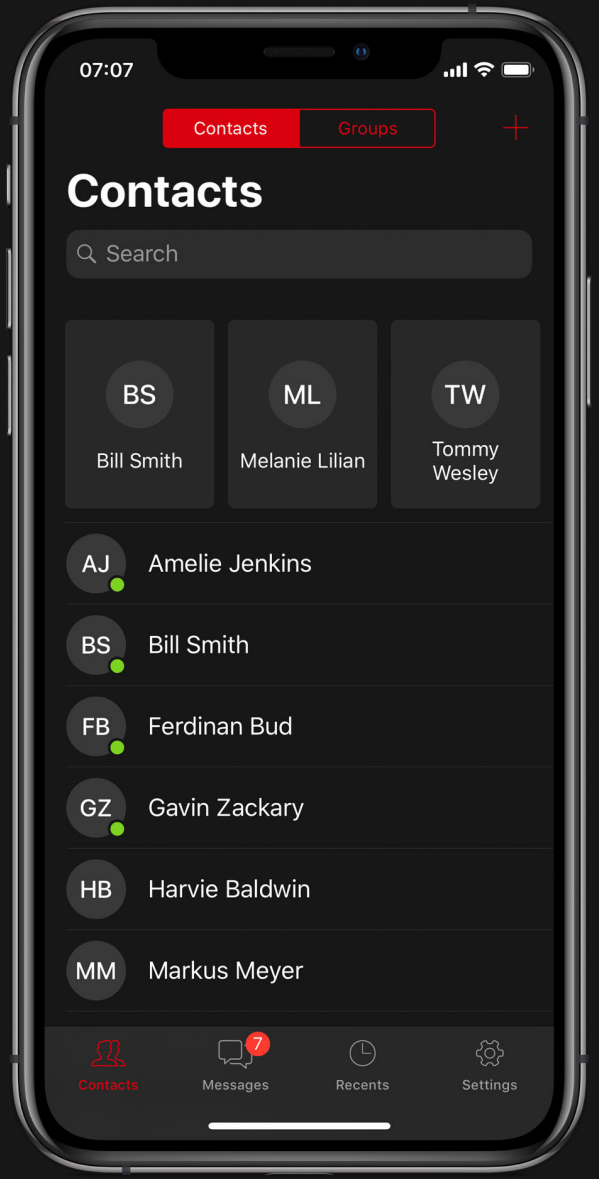
- Silentel is the first solution world-wide for secure mobile communication that was positioned in the NATO Catalogue (NIAPC)
- Since 2006, Silentel is certified by a growing number of National Security Agencies up to levels RESTRICTED and CONFIDENTIAL
- Security by design - using standard commercial devices to protect classified information. Service, maintenance and training costs in case of the Silentel solution are a fraction of the cost of private or dedicated communication systems

Silentel features

for secure communication

Secure Contacts

- Silentel app uses own contacts which are separated from other phone contacts
- After logging out, contacts are completely deleted and do not remain in the phone
- The contact list for each user is created by the group admin via the Silentel Studio interface

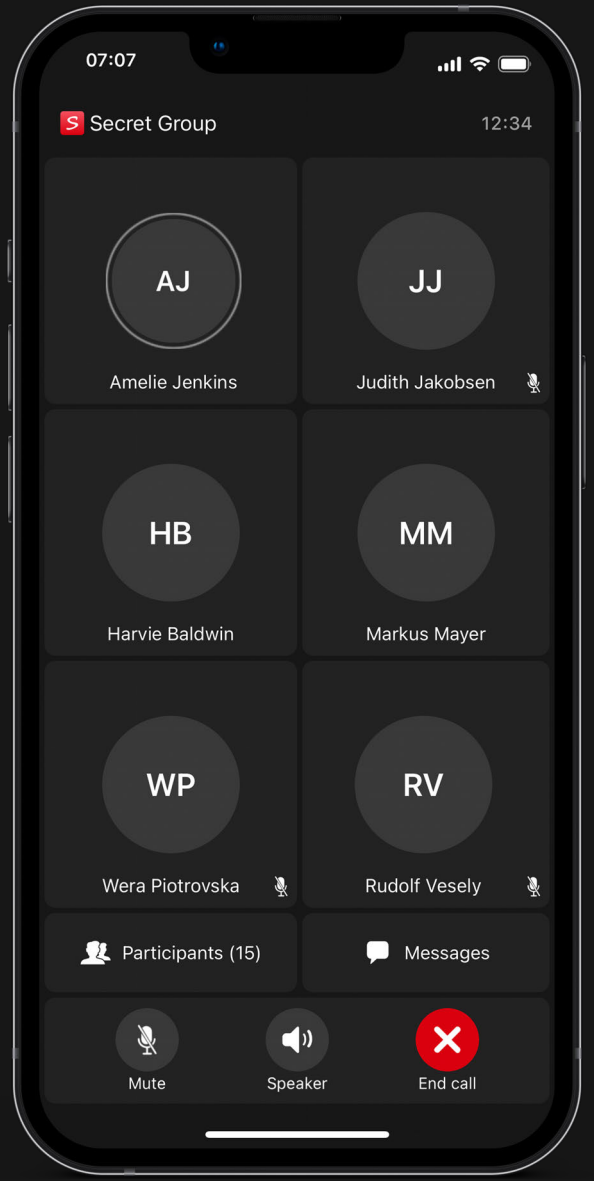


Secure Voice calls

- Standard voice calls between two participants but encrypted by the sender and decrypted only by the receiver
- During the call it is possible to:
  - Add more participants - create a conference
  - Mute (unmute) the microphone
  - Switch to speaker (speakerphone)
  - Switch to Bluetooth (handsfree)

Secure Conference

- Conference call with comprehensive features which you can know from specialized conferencing systems
- Group admin with rights to manage participants and their privileges
- Enhanced user interface including tile's view, speaking status, mute participants, and more



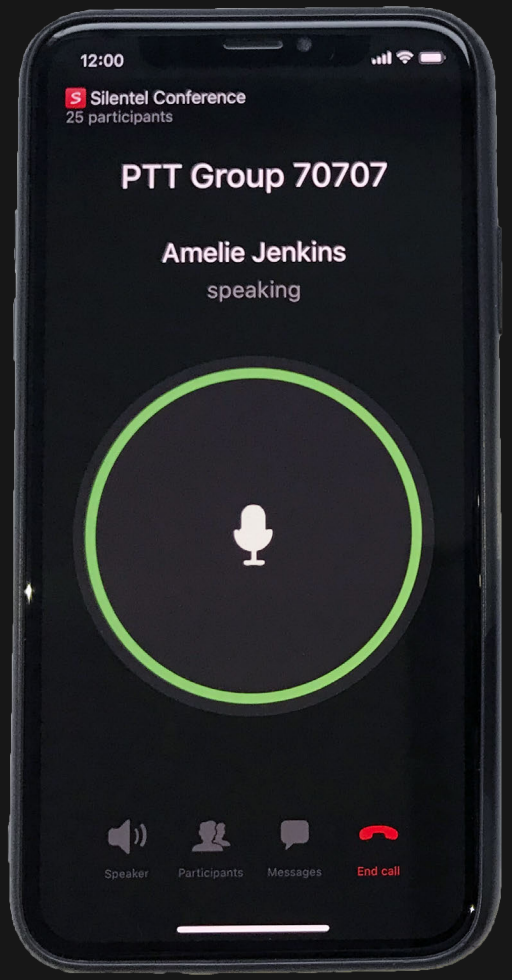
Secure Conference

Why Silentel is leading alternative when secure conference is needed

	Zoom	Microsoft Teams	Cisco Webex	Silentel
Conference mode	✓	✓	✓	✓
Push-To-Talk mode				✓
Headsets & speakerphones support	✓	✓	✓	✓
Chat Messaging & sending files	✓	✓	✓	✓
Message expiration Custom expiration for all sent messages				✓
Managing group participants Add / remove user, delete group, etc.	✓	✓	✓	✓
Group admin role Admin for user group management			✓	✓
User privileges Make calls, send messages, mute participants, etc.				✓
On-premises installation			✓	✓
Certified security				✓

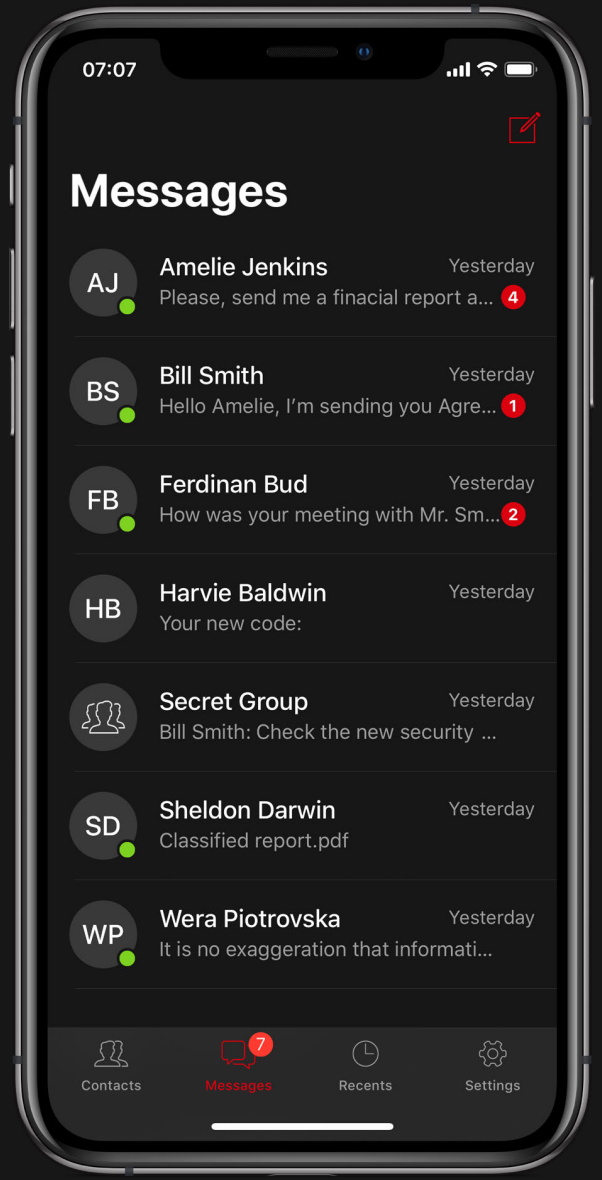
Secure PTT Conference

- PTT functionality exactly in the same way as police and other public safety responders know it and are used to it
- Possibility to connect headset and/or external PTT button



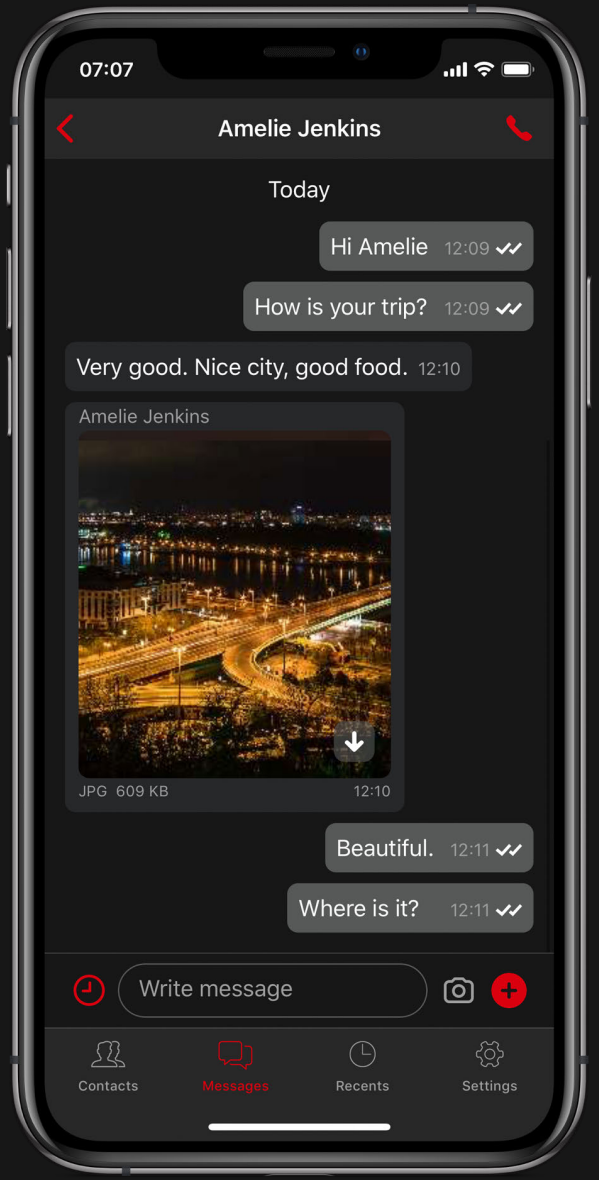
Secure Messages

- The content of the message is encrypted before sending
- Only after the message has been delivered to the receiver, the content is decrypted
- Message expiration - allows the sender to set when messages will be deleted for both (sender and receiver)



Secure File transfer

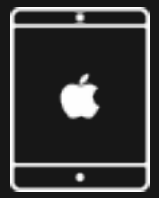
- No information remains being stored on user's device, not even messages or files
- Even when a mobile device is lost or stolen, no Silentel information will ever be available to anybody finding the device.



Multiplatform solution

Silentel is available for most used devices and operating systems

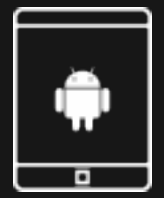
iPhone



iPad

Mac

Android phone

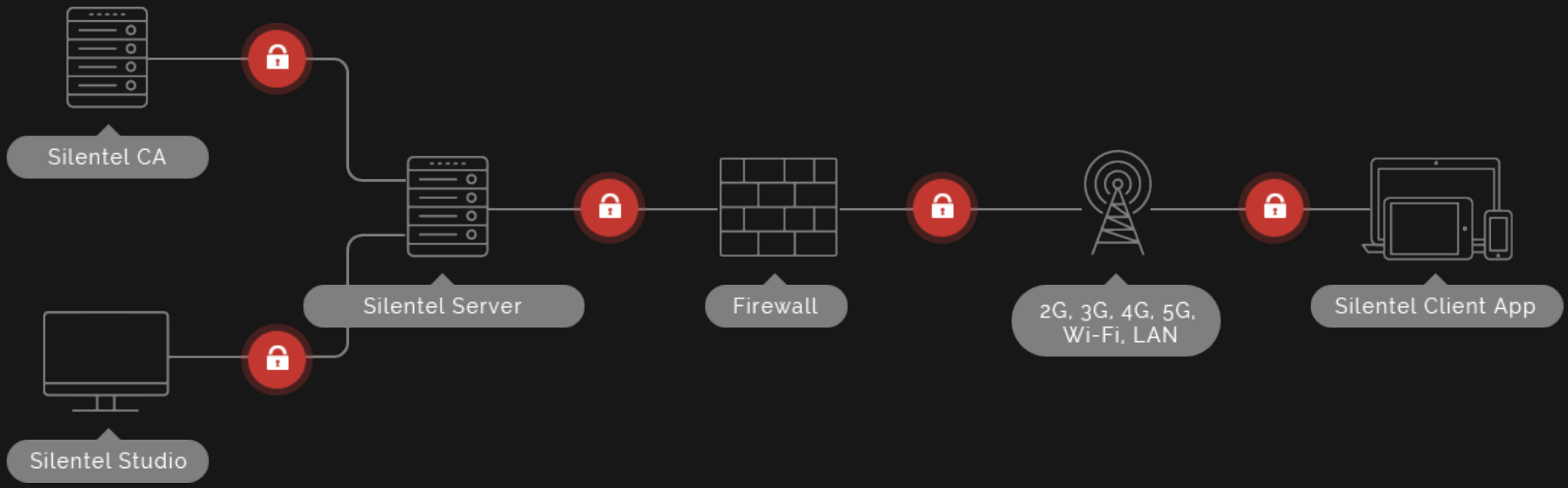


Android tablet

Windows

Silentel architecture & administration

Silentel Server architecture



Silentel Server

Distribution of encrypted communication between clients

Silentel CA

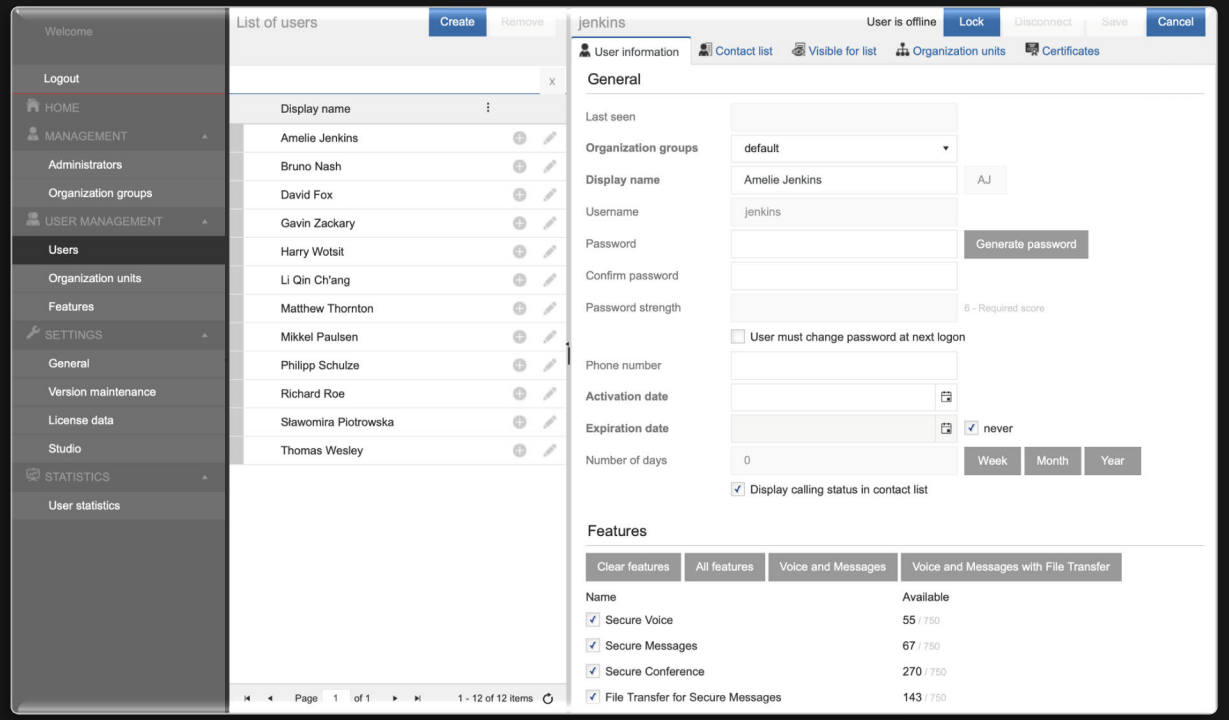
Management and distribution of public keys and certificates (PKI infrastructure)

Silentel Studio

User management and communication groups

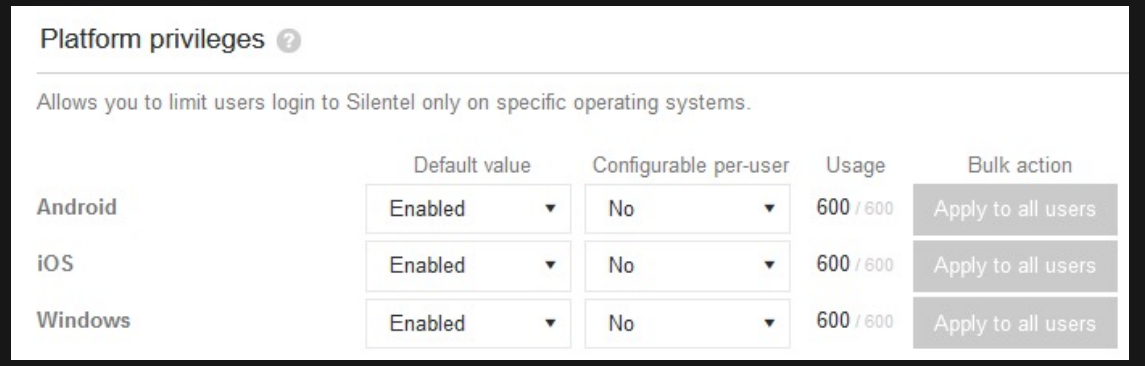
Silentel Studio

- User and group management
- Users’ batch import and export
- Password policy settings
- Platform privileges
- In-App privileges
- Group privileges



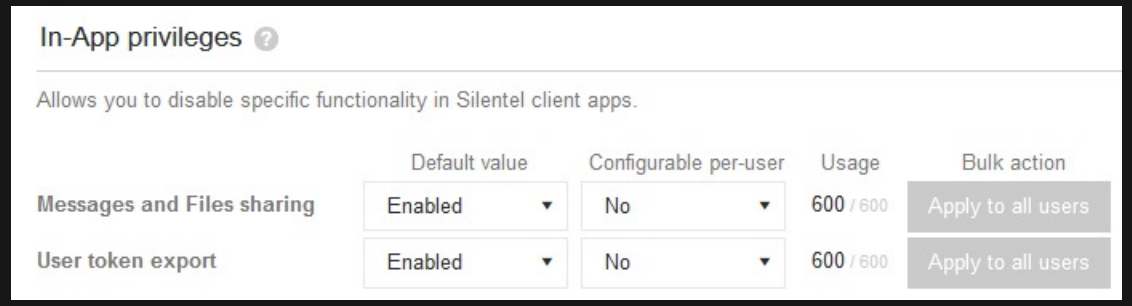
Silentel Studio – Platform privileges

- Enable or disable login to Silentel on specific platforms Android, iOS or Windows
- Each platform can be enabled or disable individually



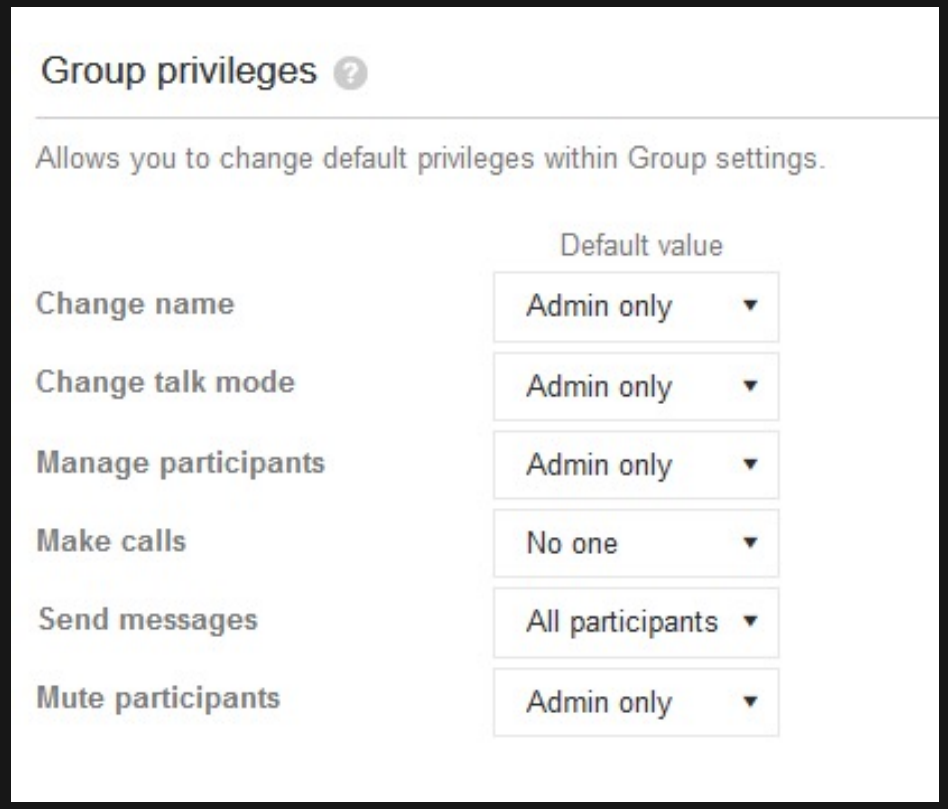
Silentel Studio – In-App privileges

- Restricts sharing of Messages, Files or User token
- When disabled – user cannot share Messages or Files out of Silentel app



Silentel Studio – Group privileges

- Allows to change default privileges for newly created groups
- Once the group is created, privileges can be changed only by group admin(s) via Silentel client app



Highest security designed for users

Make your work go faster	Protect your sensitive communication = ability to minimize the time spent on personal meetings or physical delivery of documents You will save valuable time as well as significantly reduce travelling costs
Save time, money and resources	Easy to use & fast to deploy Users will quickly adapt to a new and simpler way of handling any sensitive or confidential information No special skills neither for use, installation nor maintenance
Solution that fits your needs	Standard turn-key solution can be deployed in a matter of a few hours for the whole organization Tailor-made solutions are available to fit specific needs

Silentel®

Representante para Argentina:
www.gigsrl.com
info@gigsrl.com

ARDACO
DATA & COMMUNICATION SECURITY