Work safely from anywhere.

SINA for smartphones

The software package for your terminal devices — from smartphones to tablets.

SINA Mobile can be seamlessly connected to the SINA infrastructure and it goes without saying that it features the proven, secure encryption found in all SINA products.

The SINA Mobile Software Suite comprises four applications:

- MobileVPN
- MobileCall
- MobileWeb
- MobileScreen

Benefits

- All traffic takes place within the secure SINA network

- No data is permanently stored on the terminal device

- The terminal device requires neither much processing power nor memory

- There is no security risk if the terminal device is lost

- In desktop mode, you can simulate an extended desktop (computing power comes from the backend)

- You always get the latest operating system and app versions without delay.

At the heart of SINA Mobile: MobileVPN

MobileVPN is a protected channel that enables secure communication with all other SINA Mobile applications, the VPN component and a hardware security anchor. This security anchor currently still consists of a microSD token, but in the future SINA Mobile will use a tamper-proof chip (eSim). MobileVPN enables your terminal device to connect to a SINA L3 Box and communicate securely with the data centre.
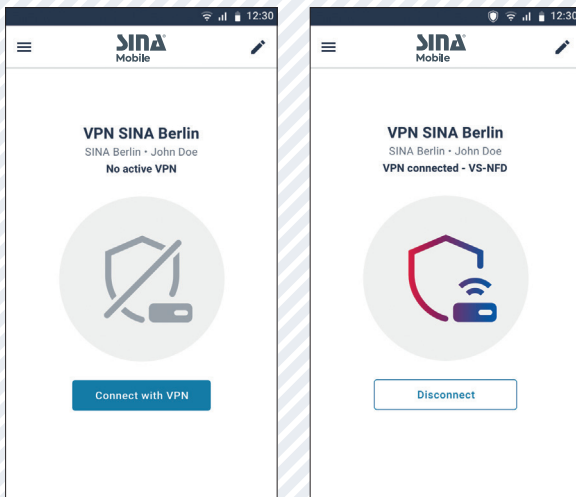
Make secure phone calls: MobileCall

From within SINA Mobile, you can make encrypted phone calls up to classification level German national RESTRICTED (VS-NfD) with other participants in the company network using the VPN tunnel. It is also possible to make cross-network calls – of course while still complying with RESTRICTED requirements.
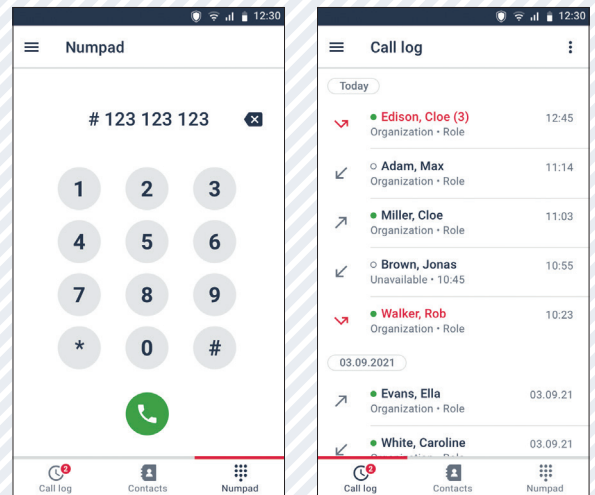
Work securely: MobileWeb

MobileWeb is a browser-based solution that allows you to edit RESTRICTED data via your existing HTML-based web applications, such as Outlook Web access. In order to do this, the browser is transferred to a secure environment. In this way, information can be displayed in the protected browser and processed exclusively there without flowing back to the terminal device. This allows you to work securely on the terminal device up to RESTRICTED classification using any application that has a web interface.

Remote, but highly secure: MobileScreen

This innovative application mirrors the user interface of another Android smartphone that runs virtualised on servers in the backend or cloud. The user works directly with the virtualised mobile phone in the cloud on his/her terminal device.

What can MobileScreen do?

MobileScreen uses a secure VPN connection to pass the sensor information (e.g. GPS sensor, microphone or camera) and actuating devices (e.g. display, loudspeaker) from the terminal device to the virtual instance. The graphical user interface of the virtual operating system is mirrored on the mobile terminal device and so, for the users, it still looks like their native terminal device, even though they are working remotely.

RESTRICTED approval is targeted for this product in 2023.

What is the difference between MobileWeb and MobileScreen?

- MobileScreen can run native Android applications **securely in the data center**, while MobileWeb can only run web based applications in the secure browser.

- MobileScreen requires a **defined hosting environment**, whereas MobileWeb does not require any additional hosting.

The defined hosting environment means no interference: The delays are in the range of 20-50 milliseconds with a fast 5G/LTE connection and are therefore hardly noticeable.

On which devices can SINA Mobile be used?

SINA Mobile is currently only available for SAMSUNG devices. The development on iOS is currently planned, the details of which can be found in the roadmap.

Currently, all devices equipped with a microSD card slot and Android 12 or newer are supported. Within the scope of the future RESTRICTED approval, use will be made of devices selected by the BSI (smartphones and tablets). Further information can be found in the roadmap.

More information:
secunet.com/sina

secunet