

3Koppla System requirements

Compliance with the system requirements in this document is required to get full functionality, stability and high quality in the 3Koppla service. Please also note that older operating systems and hardware are continuously phased out.

3Koppla Mobile app in iOS and Android

The 3Koppla mobile app is available for iOS and Android in smartphones and may be downloaded from Google Play and App Store. The mobile app is supported in:

- iOS 16.6 or higher
- Android 8 or higher (Android 10 will soon be the lowest supported version)

We recommend the latest versions of iOS and Android when new devices are purchased. The lifetime for older versions can be short.

3Koppla in computer web browser

3Koppla Admin (admin.3koppla.tre.se) for 3Koppla organisation administrators is compatible with the latest or recent versions of the following web browsers:

- Google Chrome
- Safari

3Koppla Softphone (3koppla.tre.se) which includes call handling and video conferencing is compatible with the latest or recent versions of:

- Google Chrome
-

3Koppla Softphone Desktop client in computer (installable client)

System requirements for 3Koppla Softphone Desktop client in Windows PC

- Windows 11 or higher

System requirements for 3Koppla Softphone Desktop client in MAC

- MAC OS 13 Ventura or higher



3Koppla Softphone Headset support

3Koppla Softphone supports newer versions of headsets from four brands:

Poly (Plantronics), **Jabra** (only latest software versions), **EPOS** (Sennheiser) and **Yealink** (only Windows).

Corporate network configuration

Firewall and network

For outgoing traffic from 3Koppla:

Create a rule for all UDP and TCP ports for 3Koppla networks [80.83.208.0/20](#).

For this rule, there should be a UDP & TCP Timeout of at least 3720 seconds, as our phones contact us every 3600 seconds. If you can not increase your timeout, contact our support and we can reduce the registration interval on the extension to 240 seconds.

Info

Depending of the vendor of your firewall, the name of this parameter can be different. Here you can find some examples:

FortiGate: Session TTL

Cisco ASA: timeout udp/tcp

Palo Alto Networks: Application Timeout

SonicWall: UDP/TCP Connection Timeout

MikroTik: Connection Tracking Timeout

Juniper SRX: Session-Timeout UDP/TCP

WatchGuard: UDP/TCP Timeout

pfSense: State Timeout Values

For incoming traffic to 3Koppla:

No rules are needed here because the session is initiated from within the network. If the traffic to 3Koppla is in the firewall, disable all ALG / SIP functions, Application Control, and IPS/IDS/IDP. These usually do more harm than good.

Complete information about our network:

Address: 80.83.208.0

Netmask: 255.255.240.0 = 20T

Wildcard: 0.0.15.255

Network: [80.83.208.0/20](#)

Broadcast: 80.83.223.255

HostMin: 80.83.208.1

HostMax: 80.83.223.254

Hosts / Net: 4094



Protocols

Below are the protocols used by equipment supplied for 3Koppla, as well as a description of their function. Different terminal types use different protocols, e.g. HTTPS is preferred for downloading software over e.g. TFTP and HTTP, but in cases where the terminal does not support HTTPS, one of the others is used.

Tre does not recommend blocking traffic to and from terminals based on ports and/or protocols but rather to trust all traffic to and from 3Koppla networks. 3Koppla also does not undertake to use only the protocols below for the future, so a restriction of permitted traffic through firewalls based on the following risks affecting delivered services if the specification below changes. Note that the ports listed in all cases are receiver ports, as a rule rather than exceptions, the equipment uses randomly selected sender ports.

FTP

File Transfer Protocol, RFC959, TCP ports 21 and 20. Used to download terminal configuration and software.

DNS

Domain Name Server, RFC1035, TCP / UDP port 53. DNS functionality is part of a working IP network, and the terminals provided for 3Koppla will not work unless they have access to a working DNS. If the DNS is located outside the firewall, the firewall must allow the terminals to look it up.

Our provisioned phones are configured with Google's DNS 8.8.8.8 and 8.8.4.4.

HTTP

Hyper Text Transfer Protocol, RFC2616, TCP port 80. Used to download terminal configuration and software. No specific configuration is normally required for HTTP to work satisfactorily as this is one of the most commonly used protocols on the Internet.

HTTPS

Hyper Text Transfer Protocol over Secure Socket Layer, RFC2818, TCP port 443. Used to download terminal configuration and software.

TFTP

Trivial File Transfer Protocol, RFC1350, UDP port 69 and dynamically allocated ports for data transfer. Used to download terminal configuration and software.

SNTP / NTP

Simple Network Time Protocol, RFC1305 / RFC1361, UDP port 123. Used to set the time/clock in the terminal.

SIP

Session Initiation Protocol, RFC3261, UDP port 5060. Used to hook up and down calls. SIP traffic runs between our SIP server and the phone. This is by far the most important protocol for your telephony to work.



RTP

Real-Time Transfer Protocol, RFC1889, UDP port 1024-65535. The audio stream between the terminal and the phone during a call flow as RTP. The port used is randomized when a call is initiated. All terminals supplied for 3Koppla use symmetrical RTP, which means that the receiver and sender port for the RTP stream are the same for both incoming and outgoing audio streams. This means that the audio stream that goes from the terminal to us opens the session in the firewall to allow an incoming voice stream over the same session.

SRTP

Secure Real-Time Transfer Protocol. The call is still transported over UDP, but both parties exchanged keys during the connection in the SIP dialogue to enable encryption.

RTCP

Real-Time Control Protocol, RFC3550, UDP port 1024-65535. Some terminals generate RTCP packets that are used in communication between RTP endpoints to convey local statistics and call data, such as information about jitter and any packet losses. This is selected as the RTP port + 1, i.e., if the RTP stream passes port 12480, RTCP will use UDP port 12481.

WSS web socket

WSS is used by our softphone "3Koppla Desktop" and uses port 8443 against "push servers" and port 443 for SIP.

IP-Terminals and provisioning

The following IP/ranges and ports need to be open for the zero-touch provisioning to work.

Gigaset redirect server

148.251.91.32 - 148.251.91.63 ([148.251.91.32/27](#)) **Port:** 80, 443

148.251.246.96 - 148.251.246.127 ([148.251.246.96/27](#)) **Port:** 80, 443

148.251.243.128 - 148.251.243.159 ([148.251.243.128/27](#)) **Port:** 80, 443

Yealink redirect server

IP: 52.29.124.181 **Port:** 443

IP: 3.124.165.251 **Port:** 443

[More info](#)

Snom redirect server

IP: 52.28.89.237 **Port:** 80, 443

Grandstream redirect server

IP: 52.221.130.73 **Port:** 443

Akuvox redirect server

IP: 161.117.206.232 **Port:** 80, 443, 8080



Fanvil redirect server

IP: 119.28.67.228 **Port:** 80, 443

Poly redirect server

Hostname: ztp.polycom.com **Port:** 443

[More info](#)

3Koppla provisioning server:

Gigaset: [80.83.208.0/20](#) **Port:** 80

Gigaset IP PRO: [80.83.208.0/20](#) **Port:** 1449

Yealink: [80.83.208.0/20](#) **Port:** 442

Snom: [80.83.208.0/20](#) **Port:** 447

Grandstream: [80.83.208.0/20](#) **Port:** 1446

Akuvox: [80.83.208.0/20](#) **Port:** 1445

Fanvil: [80.83.208.0/20](#) **Port:** 1448

Poly: [80.83.208.0/20](#) **Port:** 450

