

# Tele2 Växel

## Användning av SIP-terminaler och annan utrustning

### Om detta dokument

I växelplattformen finns möjlighet att öppna ett konto för att ansluta en terminal som har stöd för SIP och uppfyller vissa andra förutsättningar. I det här dokumentet har vi samlat allmän information om anslutning och konfiguration, samt information om Tele2s åtagande gällande terminaler och anslutningar.

### Innehåll

1.	Allmän information.....	2
2.	Information och tips för anslutning .....	3
2.1	Nätinformation och brandväggsinställningar .....	3
2.2	Certifikat.....	3
2.3	TLS.....	3
2.4	Anslutningsdetaljer.....	3

## 1. Allmän information

Tele2 stödjer ett urval SIP-terminaler av olika slag. Dessa hålls testade och verifierade för kompatibilitet med tjänster från Tele2. Tele2 kan inte garantera en viss funktionalitet över tid, men vi har som ambition att kunna meddela om förändringar i kompatibilitet om så sker. Det kan till exempel vara

- att en telefon eller annan hårdvara slutar fungera med en tjänst för att dess tillverkare inte längre uppdaterar den för att stödja moderna säkerhetskrav eller de kommunikationsmetoder och ljudcodec som det finns stöd för i tjänsten.
- att en telefon eller annan hårdvara behöver uppgraderas till en ny firmware för att fortsätta fungera eller för att upprätthålla rimlig säkerhetsnivå.
- att en telefon eller annan hårdvara tappar viss funktionalitet t.ex. vid förändring i tjänsten, eller när hårdvaran uppgraderas till en firmware som krävs för att fortsätta fungera i tjänsten.

För information om vilka terminaler som vid var tid rekommenderas till växelplattformen, kontakta Tele2 kundservice.

Tele2 ansvarar inte för kompatibilitet mellan terminaler och kringutrustning hos kunden, som t.ex. porttelefoner, faxmaskiner, högtalarsystem, headsets och liknande. Tele2 kan arbeta med felsökning och anpassning av konfiguration enligt vid var tid gällande prislista.

Om du som kund har terminaler, av Tele2 rekommenderade eller andra modeller och vill ansluta dem till växelplattformen är det ofta möjligt att genomföra. Vi vill dock tydliggöra följande:

- Tele2 hanterar inte returer, garantiåtaganden eller reparationer för utrustning som inte är köpt från Tele2.
- För terminaler som inte säljs av Tele2 eller för frågor som härleds till kundens datanätverk eller internetanslutning ges rådgivning och utförs felsökning endast enligt best effort.
- Du som kund ansvarar för att använda terminaler och firmware i dessa som ger en adekvat säkerhetsnivå utöver de minimikrav som vid var tid finns för anslutning till växelplattformen.
- Om enheten är ansluten till internet via NAT är det i allmänhet inte nödvändigt att öppna för inkommande trafik då detta hanteras automatiskt av routern. Om nätverket kräver öppning för inkommande trafik till enheten ansvarar du som kund för att se till att enheten aldrig är direkt åtkomlig från Internet för något webb- eller kontrollprotokoll. Om detta inte implementeras exponeras enheten för intrångsförsök.

I många fall levereras telefoner och annan hårdvara förkonfigurerad från Tele2s distributörer och kan kopplas in och användas direkt. I andra fall hjälper Tele2s leveransavdelning eller kundservice till med kontouppgifter, men kund får själv ansvara för att terminalerna ställs in rätt och kan anslutas till växelplattformen.

## 2. Information och tips för anslutning

### 2.1 Nätinformation och brandväggsinställningar

För grundläggande information om förutsättningar för anslutning av SIP-enheter till växelplattformen, se vår brandväggsdokumentation på supportsidorna för Tele2 Växel: <https://www.tele2.se/foretag> eller under Produktinformation i Tele2 Service Online.

### 2.2 Certifikat

Växelplattformen använder ett publikt certifikat för kryptering av trafik.

Om enheten validerar rotcertifikat behöver stöd finnas för följande chain of trust:

AddTrust External CA Root

USERTrust RSA Certification Authority (Intermediate)

Sectigo RSA DV/OV/EV Secure Server CA

End Entity [Leaf Certificate]

### 2.3 TLS

All kommunikation med Tele2 Växel-plattformen måste ske över transportprotokollet TLS 1.2 eller TLS 1.3 och enheten måste ha stöd för Forward Secrecy.

Vad är TLS?

Transport Layer Security eller TLS är ett av världens mest använda krypterade kommunikationsprotokoll.

Namnet antyder att TLS används i det sk. transportlagret i en uppkoppling. I en anslutning med TLS kan många typer av säker krypterad kommunikation genomföras, t.ex. HTTP(S) för webbsidor och SIP(S) för mediasessioner (bl.a. telefon- och videosamtal)

- då ofta i kommunikation med SRTP för krypterade mediaströmmar under sessionen (samtalet).

I växelplattformen är även SRTP ett absolut krav.

TLS har funnits i flera versioner, där majoriteten av den utrustning som säljs idag stöder version 1.2. TLS version 1.3 är senaste versionen. De tidigare versionerna 1.0 och 1.1 betraktas idag som osäkra.

### 2.4 Anslutningsdetaljer

Växelplattformens externa adress är [tele2vaxel.se](https://tele2vaxel.se), denna brukar anges i fält för Utgående Proxy eller Proxy beroende på enhet. Se även brandväggsdokumentationen för bl.a. information om portar.

För routing till Kundens organisation inom växelplattformen används organisationens domännamn i plattformen. Detta brukar anges i fält som: Proxy, SIP Registrar, SIP Server och liknande beroende på enhet.

I växelplattformen anges användarnamn för anslutning av tredjepartsenheter enligt `device.anvandarnamn@kundensdoman.se` – i de flesta SIP-enheter anges endast `device.anvandarnamn` i fälten för användarnamn.

Lösenordet som anges i enheten är det som Tele2 tillhandahåller för tredjepartskontot och inte det lösenord som användaren eventuellt loggar in med i webbgränssnittet på [tele2vaxel.se](https://tele2vaxel.se)

Många enheter behöver ställas in att acceptera SRTP i signaleringen under uppsättningen av samtalet. Det uppnås ofta genom att sätta inställningen för SRTP till "Optional". Inställningen finns ofta i en meny som heter Voice, RTP, Media, Audio eller liknande.