Administrationsguide till Cisco IP-konferenstelefon 8832 för Cisco Unified Communications Manager

Först publicerad: 2017-09-15

Senast ändrad: 2023-06-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

SPECIFIKATIONERNA OCH INFORMATIONEN SOM GÄLLER FÖR PRODUKTERNA I DEN HÄR HANDBOKEN KAN ÄNDRAS UTAN FÖRVARNING. ALLA UTTALANDEN, ALL INFORMATION OCH ALLA REKOMMENDATIONER I DEN HÄR HANDBOKEN ANSES VARA KORREKTA MEN PRESENTERAS UTAN NÅGON GARANTI, VARE SIG UTTRYCKLIG ELLER UNDERFÖRSTÅDD. ANVÄNDARNA MÅSTE TA FULLT ANSVAR FÖR SIN ANVÄNDNING AV ALLA PRODUKTER.

PROGRAMVARULICENSEN OCH DEN BEGRÄNSADE GARANTIN FÖR DEN MEDFÖLJANDE PRODUKTEN INGÅR I DET INFORMATIONSPAKET SOM LEVERERADES TILLSAMMANS MED PRODUKTEN OCH INKLUDERAS MED DENNA REFERENS. KONTAKTA DIN CISCO-REPRESENTANT FÖR EN KOPIA, OM DU INTE HITTAR PROGRAMVARULICENSEN ELLER DEN BEGRÄNSADE GARANTIN.

Följande information avser FCC-efterlevnad av klass A-enheter: Denna utrustning har testats och anses uppfylla gränserna för en digital enhet av klass A, i enlighet med del 15 i FCC-reglerna. Dessa begränsningar är avsedda att tillhandahålla skäligt skydd mot skadliga störningar när utrustningen används i en kommersiell miljö. Denna utrustning genererar, använder och kan utstråla radiofrekvensenergi och om den inte installerats och använts i enlighet med bruksanvisningarna kan den orsaka skadlig interferens i radiokommunikationer. Det är troligt att användning av denna utrustning i ett bostadsområde orsakar skadliga störningar och det krävs då att användare korrigerar störningarna på egen bekostnad.

Följande information avser FCC-efterlevnad av klass B-enheter: Denna utrustning har testats och anses uppfylla gränserna för en digital enhet av klass B, i enlighet med del 15 i FCC-reglerna. De här gränsvärdena är utformade för att tillhandahålla ett rimligt skydd mot skadliga störningar för en installation i ett bostadsområde. Utrustningen genererar, använder och kan utstråla radiofrekvensenergi och kan orsaka störningar i radiokommunikation om den inte installeras och används enligt instruktionerna. Det kan emellertid inte garanteras att störningar inte kommer att inträffa i vissa fall. Om utrustningen orsakar störningar för radio- eller TV-mottagningar, vilket kan fastställas genom att utrustningen stängs av och slås på, så uppmanas användarna att försöka korrigera störningen med en eller flera av följande åtgärder:

- Ändra mottagarantennens riktning eller placering.
- Öka avståndet mellan utrustningen och mottagaren.
- Anslut utrustningen till ett uttag i en annan krets än den som mottagaren är ansluten till.
- Rådgör med säljaren eller en erfaren radio-/TV-tekniker.

Ändringar av denna produkt som inte är tillåtna av Cisco, kan medföra att FCC-godkännandet inte längre gäller och att du inte får använda produkten.

Ciscos användning av TCP-rubrikkomprimering är en tillämpning av ett program som utvecklats av University of California, Berkeley (UCB) som en del av UCB:s publika version av UNIX-operativsystemet. Med ensamrätt. Copyright © 1981, Regents of the University of California.

FÖRUTOM VAD SOM GÄLLER I EVENTUELLA ANDRA GARANTIER GÖRS ALLA DOKUMENTATIONSFILER OCH ALL PROGRAMVARA SOM TILLHÖR DE HÄR LEVERANTÖRERNA TILLGÄNGLIGA I BEFINTLIGT SKICK. CISCO OCH OVANNÄMNDA LEVERANTÖRER FRÅNSÄGER SIG ALLA GARANTIER, UTTRYCKLIGA ELLER UNDERFÖRSTÅDDA, INKLUSIVE MEN UTAN BEGRÄNSNING TILL GARANTIER GÄLLANDE SÄLJBARHET, LÄMPLIGHET FÖR ETT VISST ÄNDAMÅL OCH ICKE-INTRÅNG, ELLER EVENTUELLA GARANTIER SOM UPPSTÅR FRÅN HANTERING, ANVÄNDNING ELLER HANDELSPRAXIS.

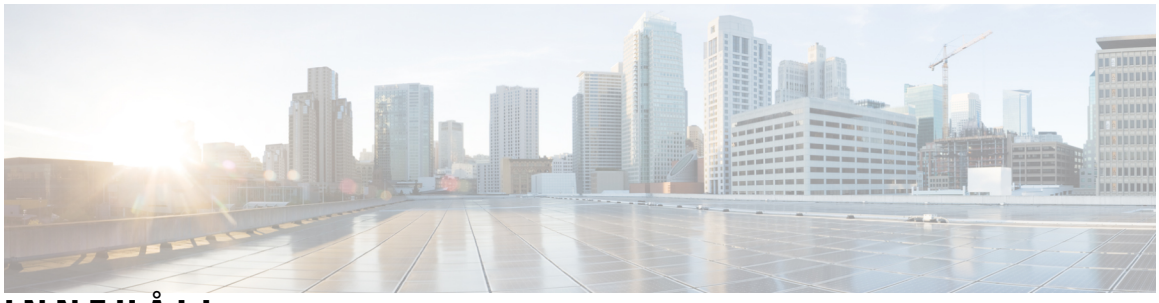
CISCO ELLER DESS LEVERANTÖRER SKALL UNDER INGA OMSTÄNDIGHETER VARA ANSVARIGA FÖR INDIREKTA ELLER SPECIELLA SKADOR, ELLER FÖLJDSKADOR ELLER TILLFÄLLIGA SKADOR, INKLUSIVE, UTAN BEGRÄNSNING, VINSTFÖRLUSTER ELLER FÖRLUST AV ELLER SKADA I DATA SOM UPPSTÅR FRÅN ANVÄNDNINGEN ELLER OFÖRMÅGAN ATT ANVÄNDA DENNA BRUKSANVISNING, ÄVEN OM CISCO ELLER DESS UNDERLEVERANTÖRER HAR BLIVIT UNDERRÄTTADE OM ATT DET FINNS RISK FÖR SÅDANA SKADOR.

De IP-adresser och telefonnummer som används i det här dokumentet är inte avsedda att vara verkliga adresser och telefonnummer. Alla exempel, kommandoutdata, diagram och övriga bilder som ingår i dokumentet är endast avsedda som illustration. All användning av verkliga IP-adresser eller telefonnummer i illustrationssammanhang är oavsiktlig och slumpmässig.

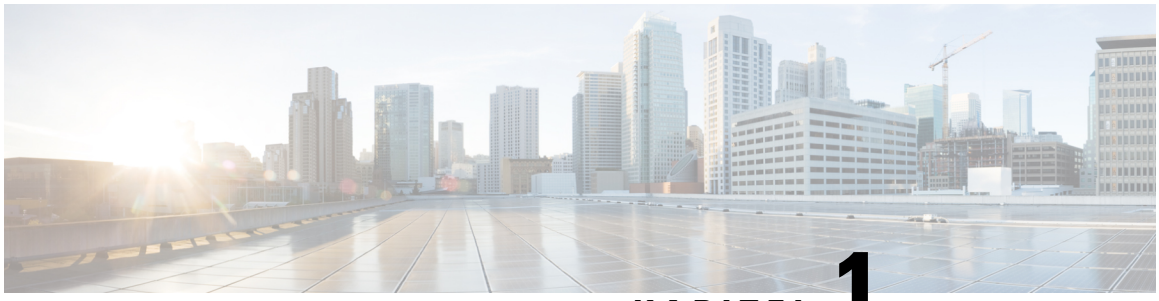
Alla utskrivna versioner och kopior av dokumentet betraktas som okontrollerade. Den senaste aktuella versionen finns alltid online.

Cisco har fler än 200 kontor runtom i världen. Adresser och telefonnummer står på Ciscos webbplats, på adressen www.cisco.com/go/offices.

Cisco och Ciscos logotyp är varumärken eller inregistrerade varumärken som tillhör Cisco Systems, Inc. och/eller dess dotterbolag i USA och andra länder. Visa en lista med Ciscos varumärken på följande URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Tredje parts varumärken som nämns tillhör deras respektive ägare. Användning av ordet partner avser inte att ett partnerskap bildats mellan Cisco och något annat företag. (1721R)



INNEHÅLL



KAPITEL 1

Ny och ändrad information

Ny och ändrad information för den fasta programvaran 14.2(1)

Följande information är ny eller ändrad för version 14.2 (1) av den fasta programvaran.

Funktion	Ny eller ändrad
Support för SIP OAuth på SRST	Säkerhetsförbättringar för telefonens nätverk, på sidan 72

Ny och ändrad information för version 14.1 (1) av den fasta programvaran

Följande information är ny eller ändrad för version 14.1 (1) av den fasta programvaran.

Funktion	Ny eller ändrad
SIP OAuth för Proxy TFTP-stöd	Säkerhetsförbättringar för telefonens nätverk, på sidan 72
Migrering av telefon utan övergångsladdning	Migration av din telefon till en multiplattformstelefon direkt, på sidan 91

Ny och ändrad information för version 14.0(1) av den fasta programvaran

Tabell 1. Ny och ändrad information

Funktion	Ny eller ändrad
Bättre övervakning av samtalsparkering	Produktspecifik konfiguration, på sidan 95
Förbättringar av SIP OAuth	Säkerhetsförbättringar för telefonens nätverk, på sidan 72
Förbättringar av OAuth för MRA	Mobil åtkomst och fjärråtkomst genom Expressway, på sidan 116
Förbättrat användargränssnitt	Survivable Remote Site Telephony, på sidan 64

Från och med version 14.0 av den fasta programvaran har telefonerna stöd för DTLS 1.2. För DTLS 1.2 krävs Cisco ASA (Adaptive Security Appliance) version 9.10 eller senare. Du konfigurerar lägsta DTLS-version för en VPN-anslutning i ASA. Mer information finns i *ASDM Bok 3: Konfigurationsguide för Cisco ASA-serien VPN ASDM* på https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

Ny och ändrad information för version 12.8 (1) av den fasta programvaran

Följande information är ny eller ändrad för version 12,8 (1) av den fasta programvaran.

Funktion	Nytt eller ändrat innehåll
Telefondatamigrering	Ändra en användares telefonmodell, på sidan 52
Lägga till ytterligare information om fältet för webbåtkomst	Produktspecifik konfiguration, på sidan 95

Ny och ändrad information för version 12.7 (1) av den fasta programvaran

Det behövdes inga uppdateringar av administrationshandboken för version 12.7(1) av den fasta programvaran.

Ny och ändrad information för version 12.6 (1) av den fasta programvaran

Det behövdes inga uppdateringar av administrationshandboken för version 12.6 (1) av den fasta programvaran.

Ny och ändrad information för version 12.5 (1) SR3 av den fasta programvaran

Alla referenser till dokumentationen om Cisco Unified Communications Manager har uppdaterats för att stödja alla utgåvor av Cisco Unified Communications Manager.

Tabell 2. Administrationshandbok för Cisco IP-telefon 8832 – revideringar i version 12.5 (1) SR3 av fast programvara

Uppdatering	Uppdaterat avsnitt
Stöd för aktiveringskodregistrering och mobilåtkomst och Remote Access	Aktiveringskodregistrering och mobilåtkomst och Remote Access, på sidan 29
Stöd för användning av problemrapportverktyget från Cisco Unified Communications Manager.	Skapa en telefonproblemrapport från Cisco Unified Communications Manager, på sidan 162

Ny och ändrad information för version 12.5 (1) SR2 av den fasta programvaran

Det behövdes inga uppdateringar av administrationshandboken för version 12.5 (1) SR2 av den fasta programvaran.

Version 12.5 (1) SR2 av den fasta programvaran ersätter version 12.5 (1) och 12.5 (1) SR1 av den fasta programvaran. Version 12.5 (1) och version 12.5 (1) SR1 av den fasta programvaran ersätts av version 12.5 (1) SR2 av den fasta programvaran.

Ny och ändrad information för version 12.5 (1) SR1 av den fasta programvaran

Följande tabell innehåller ändringarna i *Cisco IP-konferenstelefon 8832 – administrationshandbok för Cisco Unified Communications Manager* för version 12.5 (1) SR1 av den fasta programvaran.

Tabell 3. Revideringar av Cisco IP-konferenstelefon 8832 – Administrationshandbok för version 12.5 (1) SR1

Uppdatering	Nytt eller uppdaterat avsnitt
Stöd för Elliptic Curve	Säkerhetsfunktioner som stöds, på sidan 73

Ny och ändrad information inför version 12.5 (1) av den fasta programvaran

Följande tabell innehåller ändringarna i *Cisco IP-konferenstelefon 8832 – administrationshandbok för Cisco Unified Communications Manager* för version 12.5(1) av den fasta programvaran.

Tabell 4. Revideringar av Cisco IP-konferenstelefon 8832 – Administrationshandbok för version 12.5 (1)

Uppdatering	Nytt eller uppdaterat avsnitt
Stöd för viskningssökning i Cisco Unified Communications Manager Express	Interaktion med Cisco Unified Communications Manager Express, på sidan 22
Stöd för inaktivering av TLS-chiffer	Produktspecifik konfiguration, på sidan 95
Stöd för Enbloc-uppringning för Inter-Digit Timer T.302 Enhancement.	Produktspecifik konfiguration, på sidan 95

Ny och ändrad information för version 12.1 (1) av den fasta programvaran

Följande tabell beskriver ändringarna i *Cisco IP-konferenstelefon 8832 – administrationshandbok för Cisco Unified Communications Manager* för version 12.1(1) av den fasta programvaran.

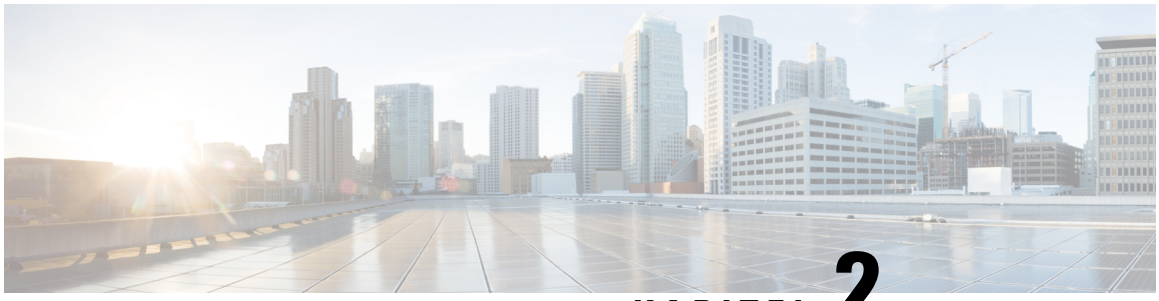
Uppdatering	Nytt eller uppdaterat avsnitt
Stöd för	• Telefonströmförsörjning, på sidan 18 • Olika sätt att strömförsörja konferenstelefonen, på sidan 32 • Installera konferenstelefonen, på sidan 31
Stöd för trådlösa mikrofoner	• Cisco IP-konferenstelefon 8832, på sidan 9 • Trådlös mikrofon (endast 8832), på sidan 13 • Installera trådlösa förlängningsmikrofoner, på sidan 36 • Installera mikrofonens trådlösa laddningsvagga, på sidan 37

Uppdatering	Nytt eller uppdaterat avsnitt
Stöd för sammanlänkning	• Cisco IP-konferenstelefon 8832, på sidan 9 • Sammanlänkningsläge, på sidan 31 • Installera konferenstelefonen i kedjekopplingsläge, på sidan 38 • En telefon i kedjekopplingsläge fungerar inte, på sidan 161
Stöd för	• Installera konferenstelefonen, på sidan 31 • Olika sätt att strömförsörja konferenstelefonen, på sidan 32
Stöd för Wi-Fi	• Installera konferenstelefonen, på sidan 31 • Olika sätt att strömförsörja konferenstelefonen, på sidan 32 • Ställa in domännamnsfältet, på sidan 46 • Aktivera det trådlösa nätverket på telefonen, på sidan 46 • Konfigurera det trådlösa nätverket i Cisco Unified Communications Manager., på sidan 47 • Ställa in trådlöst nätverk från telefonen, på sidan 48 • Ange antalet WLAN-autentiseringsförsök, på sidan 49 • Aktivera uppmaningsläge för WLAN, på sidan 50 • Ställa in en Wi-Fi-profil med hjälp av Cisco Unified Communications Manager, på sidan 50 • Ställa in en Wi-Fi-grupp med hjälp av Cisco Unified Communications Manager, på sidan 52
Stöd för mobilåtkomst och Remote Access genom Expressway	• Mobil åtkomst och fjärråtkomst genom Expressway, på sidan 116 • Driftsättningsscenarier, på sidan 117 • Konfigurera bestående inloggningsuppgifter för inloggning med Expressway, på sidan 118
Stöd för aktivering eller inaktivering av TLS 1.2 för åtkomst till webbservrar	Produktspecifik konfiguration, på sidan 95
Stöd för G722.2 AMR-WB ljudkodek	• Cisco IP-konferenstelefon 8832, på sidan 9 • Samtalsstatistikfält, på sidan 134

Ny och ändrad information för version 12.1 (1) av den fasta programvaran

DEL I

Om Cisco IP-konferenstelefon



KAPITEL 2

Maskinvara för Cisco IP-konferenstelefon

Cisco IP-konferenstelefon 8832

Cisco IP Conference Phone 8832 och 8832NR förbättrar människocentrerad kommunikation. I den kombineras HD-ljud och 360-graderstäckning för mellanstora till stora konferensrum och ledningskontor. Den erbjuder en högklassig ljudupplevelse med dubbelriktad handsfree-högtalare för bredbandsljud (G.722) i full duplex. Den här telefonen är en enkel lösning som uppfyller behoven för många olika typer av rum.

Figur 1. Cisco IP-konferenstelefon 8832

Konferenstelefonen har känsliga rundupptagande (360 graders) mikrofoner. Upptagningen innebär att du kan tala i normal samtalsvolym och höras tydligt från upp till 3 meters avstånd. Telefonen innehåller även teknologi som förhindrar interferens från mobiltelefoner och andra trådlösa enheter, vilket säkerställer tydlig kommunikation utan störningar. Telefonen har en färgskärm och programstyrda knappar som ger åtkomst till

användarfunktionerna. Med enbart basenheten har telefonen täckning för ett rum på 6,1 x 6,1 m och upp till tio personer.

Telefonen kan användas med två kabelanslutna mikrofoner. Om du placerar mikrofonerna en bit bort från basenheten får du bättre täckning i ett större rum och för fler personer. Med basenheten och mikrofoner har konferenstelefonen täckning för ett rum på 6,1 x 10 m och upp till 22 personer.

Telefonen har även stöd för Bluetooth som kan användas för trådlösa förlängningsmikrofoner, som levereras i set om två. Med basenheten och mikrofoner har konferenstelefonen täckning för ett rum på 6,1 x 12,2 m och upp till 26 personer. För att få täckning i ett rum på 6,1 x 12,2 m rekommenderar vi att du placerar varje mikrofonen högst 3 meter från basstationen.

Du kan ansluta två basenheter för att öka täckningen i ett rum. Den här konfigurationen kräver den valfria sammanlänkningsatsen och kan stödja upp till två förlängningsmikrofoner (kabelanslutna eller trådlösa, men inte i en blandad kombination). Om du använder mikrofoner med sladd i sammanlänkningssatsen, ger konfigurationen täckning för ett rum upp till 6,1 x 15,2 m och upp till 38 personer. Om du använder trådlösa mikrofoner i sammanlänkningssatsen, ger konfigurationen täckning för ett rum upp till 6,1 x 17,4 m och upp till 42 personer.

Cisco IP-konferenstelefon 8832NR-versionen (icke-radio) har inte stöd för Wi-Fi, trådlösa förlängningsmikrofoner eller Bluetooth.

En Cisco IP-telefon, liksom andra enheter, måste konfigureras och hanteras. Dessa telefoner kan koda och avkoda följande kodek:

- G.711 a-law
- G.711 mu-law
- G.722
- G722.2 AMR-WB
- G.729a/G.729ab
- G.726
- iLBC
- Opus

⚠

Försiktighet Användning av mobiltelefon, GSM-telefon eller en kombinerad sändare och mottagare i närheten av en Cisco IP-telefon kan orsaka störningar. För mer information, se tillverkarens dokumentation av den störande enheten.

Cisco IP-telefon har även traditionella telefonfunktioner som vidarekoppling och överföring, återuppringning, kortnummer, konferenssamtal och röstmeddelandesystem. Cisco IP-telefon har också en mängd andra funktioner.

I likhet med andra nätverksenheter måste du konfigurera Cisco IP-telefoner för att förbereda dem för åtkomst till Cisco Unified Communications Manager och resten av IP-nätverket. Genom att använda DHCP, har du färre inställningar att konfigurera på en telefon. Nätverket kan kräva och du kan även manuellt konfigurera information som: en IP-adress, TFTP-server och subnätsinformation.

Cisco IP-telefon kan interagera med andra tjänster och enheter i IP-nätverk för att förbättra funktionaliteten. Till exempel kan du integrera Cisco Unified Communications Manager med företagets LDAP3-standardkatalog för att låta användare söka efter kontaktinformation till medarbetare direkt från sina IP-telefoner. Du kan

också använda XML för att låta användarna få tillgång till information som väder, lager, dagens citat och annan webbaserad information.

Slutligen, eftersom en Cisco IP-telefon är en nätverksenhet, kan du få detaljerad statusinformation från den direkt. Denna information kan hjälpa dig med felsökning av problem som användare kan stöta på när de använder sina IP-telefoner. Du kan även få statistik om ett aktivt samtal eller versioner av den fasta programvaran på telefonen.

För att fungera i IP-telefoninätet måste Cisco IP-telefonen ansluta till en nätverksenhet, som en Cisco Catalyst-växel. Du måste också registrera Cisco IP-telefonen i Cisco Unified Communications Manager-systemet innan du skickar och tar emot samtal.

Cisco IP-konferenstelefon 8832 – knappar och maskinvara

På bilden nedan visas Cisco IP-konferenstelefon 8832.

Figur 2. Cisco IP-konferenstelefon 8832 – knappar och funktioner

I följande tabell beskrivs knapparna på Cisco IP-konferenstelefon 8832.

Tabell 5. Cisco IP-konferenstelefon 8832 – Knappar

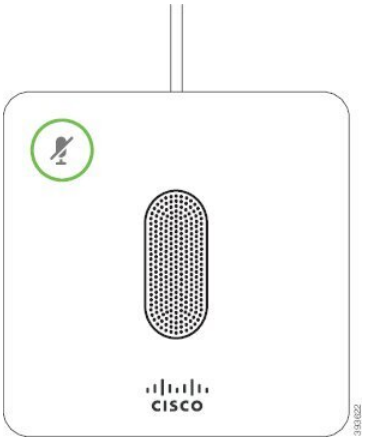
1	Lysdiod	Anger samtalsstatus: • Grönt fast sken – aktivt samtal • Grönt blinkande sken – inkommande samtal • Grönt pulserande sken – parkerat samtal • Rött fast sken – mikrofonen avstängd

2	Port för mikrofon	Den kabelanslutna mikrofonen ansluts via porten.
3	Knapp för **Tyst**	Aktiverar och inaktiverar mikrofonen. När mikrofonljudet är av lyser LED-lampan röd.
4	Programstyrda knappar	Åtkomst till funktioner och tjänster.
5	Navigeringsknapp och **Välj**-knapp	Bläddra genom menyer, markera objekt och välja det markerade objektet.
6	**Volym**-knapp	Justerar volymen på högtalartelefonen (lur av) och ringsignalvolym (lur på). När du justerar volymen lyser lysdioderna vitt för att visa volymändringen.

Kabelansluten mikrofon (endast 8832)

Cisco IP Conference Phone 8832 har stöd för två kabelanslutna mikrofoner, tillgängliga som valfria tillbehör. Använd förlängningsmikrofonerna i större rum eller i ett överfullt rum. För bästa resultat rekommenderar vi att du placerar mikrofonerna mellan 0,91 m och 2,1 m från telefonen.

Figur 3. Kabelansluten mikrofon



När du är i ett samtal lyser förlängningsmikrofonens LED-lampa runt knappen **Ljud av** grönt.

När mikrofonljudet stängs av är LED-lampan röd. När du trycker på **Ljud av**-knappen stängs ljudet av för både telefonen och övriga mikrofoner.

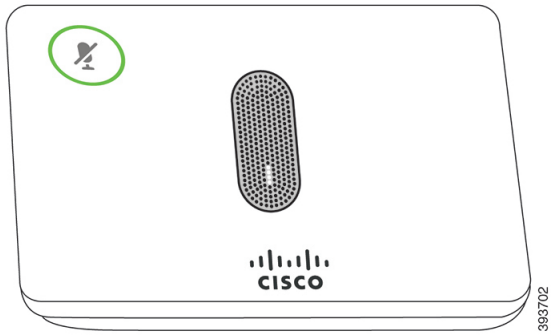
Relaterade ämnen

Installera kabelanslutna förlängningsmikrofoner, på sidan 35

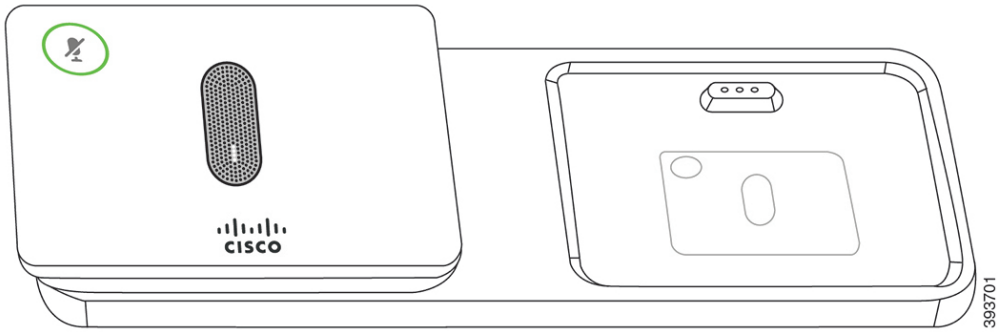
Trådlös mikrofon (endast 8832)

Cisco IP Conference Phone 8832 har stöd för två kabelanslutna förlängningsmikrofoner som erbjuds med en laddningsvagga som tillbehör. När den trådlösa mikrofonen placeras på laddningsvaggan, lyser led-lampan på vaggan i vitt.

Figur 4. Trådlös mikrofon



Figur 5. Trådlös mikrofon placerad på laddningshållaren



När konferenstelefonen används i ett samtal lyser mikrofonens LED-lampa, vid **Ljud av**-knappen, grönt.

När mikrofonljudet är avstängt lyser LED-lampan rött. När du trycker på **Ljud av**-knappen stängs ljudet av för både telefonen och övriga mikrofoner.

Om telefonen är sammanlänkad med en trådlös mikrofon (till exempel trådlös mikrofon 1) och du ansluter den trådlösa mikrofonen till en laddare kan du trycka på **Visa detaljer**-funktionsknappen för att se laddningsnivån för den mikrofonen.

När telefonen är sammanlänkad med en trådlös mikrofon och du ansluter en sladdansluten mikrofon, bryts anslutningen till den trådlösa mikrofonen och telefonen sammanlänkas med den sladdanslutna mikrofonen. Ett meddelande visas på den telefonen skärmen som anger att sladdansluten mikrofon är ansluten.

Relaterade ämnen

Installera trådlösa förlängningsmikrofoner, på sidan 36
Installera mikrofonens trådlösa laddningsvagga, på sidan 37

Relaterad dokumentation

Läs följande avsnitt om du vill ha mer relevant information.

Dokumentation för Cisco IP-konferenstelefon 8832

Hitta dokumentation som är specifik för ditt språk, din telefonmodell och samtalskontrollsystem på sidan med produktsupport för Cisco IP-telefon i 7800-serien.

Dokumentation för Cisco Unified Communications Manager

Se *Cisco Unified Communications Manager Dokumentationshandboken* och andra publikationer som är specifika för din version av Cisco Unified Communications Manager. Navigera från dokumentationens webbadress som följer:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Dokumentation för Cisco Unified Communications Manager Express

Se de publikationer som gäller för ditt språk, din telefonmodell och din utgåva av Cisco Unified Communications Manager Express. Navigera från dokumentationens webbadress som följer:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html

Servicedokumentation för Cisco Hosted Collaboration

Se *Cisco Hosted Collaboration Solution Dokumentationshandboken* och andra publikationer som är specifika för din version av Cisco Hosted Collaboration Solution. Navigera från webbadressen som följer:

https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

Dokumentation för Cisco Business Edition 4000

Se *Cisco Business Edition 4000 Dokumentationshandboken* och andra publikationer som är specifika för din version av Cisco Business Edition 4000. Navigera från webbadressen som följer:

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-4000/tsd-products-support-series-home.html

Dokumentation, support och säkerhetsriktlinjer

Mer information om hur du hämtar dokumentation, får support, ger feedback om dokumentationen, granskar säkerhetsriktlinjer och information om rekommenderade alias och allmänna Cisco-dokument finns i den

månatliga *What's New in Cisco Product Documentation* där det också finns en lista över alla nya och reviderade tekniska Cisco-dokument på:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Prenumerera på *Nyheter i Cisco-dokumentationen* som en RSS-feed och välj innehåll som ska levereras direkt till ditt skrivbord med ett enkelt läsarprogram. RSS-feeden är en kostnadsfri service och Cisco stöder för närvarande RSS version 2.0.

Översikt över Ciscos produktsäkerhet

Den här produkten innehåller kryptografiska funktioner och lyder under USA:s och det lokala landets lagar rörande import, export, överföring och användning. Leverans av kryptografiska produkter från Cisco innebär inte ett godkännande för tredje part att importera, exportera, distribuera eller använda kryptering. Importörer, exportörer, distributörer och användare ansvarar för att USA:s och det lokala landets lagar följs. Genom att använda den här produkten förbinder du dig att följa tillämpliga lagar och regleringar. Om du inte kan följa USA:s och lokala lagar skall du omedelbart returnera produkten.

Mer information om exportregler för USA finns på https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

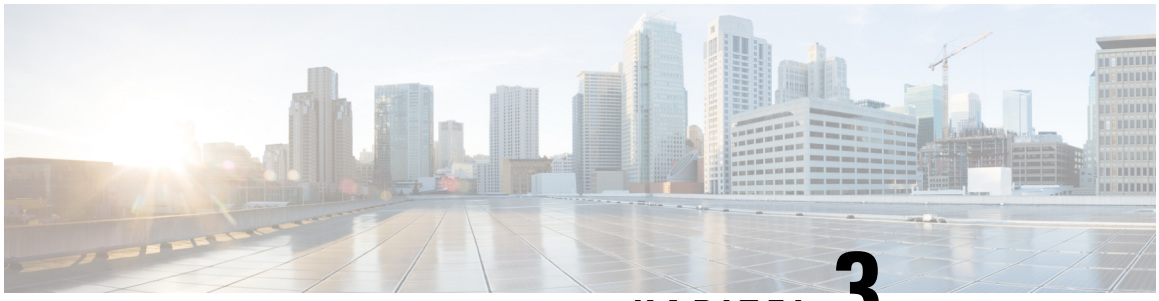
Skillnader i terminologi

I den här dokumentation inbegriper termen *Cisco IP-telefon* Cisco IP-konferenstelefon 8832.

Följande tabell visar några av de terminologiskillnader i *Användarhandbok för Cisco IP-konferenstelefon 8832*, *Administrationshandbok för Cisco IP-konferenstelefon 8832 för Cisco Unified Communications Manager* och dokumentationen för Cisco Unified Communications Manager.

Tabell 6. Skillnader i terminologi

Användarhandbok	Administrationshandbok
Meddelandeindikatorer	Meddelande väntar-indikator (MWI)
Röstsvarssystem	Röstmeddelandesystemet



KAPITEL 3

Tekniska detaljer

Fysiska och driftsmiljörelaterade specifikationer

Följande tabell visar de fysiska och driftsmiljömässiga specifikationerna för konferenstelefonen.

Tabell 7. Fysiska och driftsmässiga specifikationer

Specifikation	Värde eller Intervall
Driftstemperatur	0 ° till 40 °C
Relativ luftfuktighet	10 % till 90 % (icke-kondenserande)
Förvaringstemperatur	-10 ° till 60 °C
Höjd	278 mm
Bredd	278 mm
Djup	61,3 mm
Vikt	1 852 g
Ström	IEEE PoE klass 3 via en PoE-injektor. Telefonen är kompatibel med Protocol och LLDP-PoE (Link Layer Discovery Protocol - Power Andra alternativ är en PoE Ethernet-injektor, om de anslutna LAN- för Cisco IP-konferenstelefon 8832.

Specifikation	Värde eller Intervall
Säkerhetsfunktioner	Säker start
Kablar	USB-C
Distanskrav	Enligt Ethernet-specifikationen antas den maximala kabellängden mel

Mer information finns i *Datablad för Cisco IP-konferenstelefon 8832*: https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html

Telefonströmförsörjning

Cisco IP Conference Phone 8832 kan använda följande strömkällor:

- PoE (Power over Ethernet)-distribution med en
- Icke-PoE Ethernet-distribution med en
- Implementering av WiFi med en strömadapter för Cisco IP-konferenstelefon 8832

Tabell 8. Riktlinjer för strömförsörjning till Cisco IP-konferenstelefon

Strömtyp	Riktlinjer
PoE-ström – Tillhandahålls av eller Cisco IP-konferenstelefon 8832 Ethernet-koppling via USB-C-kabeln som är ansluten till telefonen.	Om du använder eller Cisco IP-konferenstelefon 8832 Ethernet-koppling behöver du se till att omkopplaren har en reservströmkälla för att säkerställa avbrottsfri drift av telefonen. Se till att CatOS- eller IOS-versionen som körs i din omkopplare har stöd för distribution till telefonen. I dokumentationen till din omkopplare står operativsystemets versionsinformation. När du installerar en telefon som drivs med PoE ska du ansluta injektorn till nätverket innan du ansluter USB-C-kabeln till telefonen. När du tar bort en telefon som använder PoE ska du koppla bort USB-C-kabeln från telefonen innan du tar bort strömkällan från adaptern.
Extern strömförsörjning • Icke-PoE Ethernet-distribution med en • Implementering av WiFi med en strömadapter för Cisco IP-konferenstelefon 8832 • Implementering av icke-PoE Ethernet med Cisco IP-konferenstelefon 8832 Ethernet-koppling och en strömadapter för Cisco IP-konferenstelefon 8832	När du installerar en telefon som drivs med extern ström ska du ansluta injektorn till strömkällan och Ethernet innan du ansluter USB-C-kabeln till telefonen. När du tar bort en telefon som använder extern ström ska du koppla bort USB-C-kabeln från telefonen innan du tar bort strömkällan från adaptern.

Strömavbrott

För att komma åt akutsamtalstjänster genom telefonen måste telefonen få ström. Vid ett strömavbrott fungerar inte service- eller akutsamtalstjänster förrän strömmen är återupprättad. Vid avbrott eller störningar i strömförsörjningen kan du behöva återställa eller konfigurera om utrustningen innan du kan använda service- och akutsamtalstjänsterna.

Energispar

Du kan minska mängden energi som Cisco IP-telefon förbrukar genom att använda energisparläget eller energisparplusläget.

Energisparläge

I energisparläget är bakgrundsbelysningen på skärmen släckt när telefonen inte används. Telefonen är kvar i energisparläge under schemalagd period eller tills användaren trycker på någon knapp.

Energisparplus (EnergyWise)

Cisco IP-telefon stöder Cisco Energywise (energisparplusläge). När nätverket innehåller en Energywise-styrenhet (till exempel en Cisco-växel med aktiverad EnergyWise) kan du konfigurera dessa telefoner för viloläge (avstängning) och uppvakning (start) i ett schema för att ytterligare minska strömförbrukningen.

Ställ in varje telefon för att aktivera eller inaktivera EnergyWise-inställningar. Om Energy är aktiverat kan du konfigurera vilo- och uppvakningstid och andra parametrar. Dessa parametrar skickas till telefonen som en del av telefonens XML-konfigurationsfil.

Relaterade ämnen

Schemalägga energisparläge för Cisco IP-telefon, på sidan 107
Schemalägga EnergyWise för Cisco IP-telefon, på sidan 109

Nätverksprotokoll

Cisco IP Conference Phone 8832 har stöd för flera branschstandards- och Cisco-nätverksprotokoll som krävs för röstkommunikation. Följande tabell ger en översikt över de nätverksprotokoll som telefonerna stöder.

Tabell 9. Nätverksprotokoll som stöds på Cisco IP-konferenstelefon

Nätverksprotokoll	Syfte	Att tänka på vid användning
BootP (Bootstrap Protocol)	BootP aktiverar en nätverksenhet, som till exempel telefonen, för att identifiera viss startinformation, som till exempel IP-adressen.	—
CDP (Cisco Discovery Protocol)	CDP är ett enhetsidentifieringsprotokoll som körs på alla Cisco-utrustningar. En enhet kan använda CDP för att annonsera sin existens till andra enheter och få information om andra enheter i nätverket.	Telefonen använder CDP för att kommunicera i QoS-konfigurationsinformation (Quality of Serv

Nätverksprotokoll	Syfte	Att tänka på vid användning
DHCP (Dynamic Host Configuration Protocol)	DHCP allokerar en IP-adress dynamiskt och tilldelar den till nätverksenheter. Med DHCP kan du ansluta en IP-telefon till nätverket och ta telefonen i drift utan att behöva tilldela en IP-adress manuellt eller konfigurera ytterligare nätverksparametrar.	DHCP är aktiverat som standard. Om det är inaktiv TFTP-server på varje telefon lokalt. Vi rekommenderar att du använder DHCP-anpassat som alternativvärdet. Ytterligare stöd för DHCP-ko Communications Manager. **OBS!** Om du inte kan använda alternativ 150
HTTP (Hypertext Transfer Protocol)	HTTP är standardprotokollet för överföring av information och flyttning av dokument över Internet och webben.	Telefonerna använder HTTP för XML-tjänster, rese
HTTPS (Hypertext Transfer Protocol Secure)	HTTPS är en kombination av Hypertext Transfer Protocol med SSL-/TLS-protokollet för att tillhandahålla kryptering och säker identifiering av servrar.	Webbprogram med både HTTP- och HTTPS-stöd h HTTPS-URL:en. En låsikon visas för användaren om anslutningen til
IEEE 802.1X	IEEE 802.1X-standarden definierar klientserverbaserad åtkomstkontroll och autentiseringsprotokoll som begränsar obehöriga klienter från anslutning till ett LAN genom offentligt tillgängliga portar. Innan klienten autentiseras tillåter 802.1X-åtkomstkontrollen endast EAPOL-trafik (Extensible Authentication Protocol over LAN) genom porten som klienten är ansluten till. När autentiseringen lyckats kan normal trafik passera genom porten.	I telefonen implementeras IEEE 802.1X-standarden När 802.1X-autentisering har aktiverats på telefone
IP (Internet Protocol)	IP är en meddelandeprotokoll som adresserar och skickar paket över nätverket.	För att kommunicera med IP måste nätverksenheter Identifiering av IP-adresser, subnät och gatewayar til DHCP måste du manuellt tilldela dessa egenskaper Telefonerna har stöd för IPv6-adress. Mer informati Manager.
LLDP (Link Layer Discovery Protocol)	LLDP är ett standardiserat nätverksidentifieringsprotokoll (liknande CDP) som stöds på vissa Cisco-enheter och tredjepartsenheter.	Telefonen har stöd för LLDP i PC-porten.
LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Devices)	LLDP-MED är en utökning av LLDP-standarden och har utvecklats särskilt för röstprodukter.	Telefonen har stöd för LLDP-MED i SW-porten för • Konfiguration av röst-VLAN • Enhetsidentifiering • Energihantering • Lagerhantering Mer information om stöd för LLDP-MED finns i vi https://www.cisco.com/en/US/tech/tk652/tk701/tech
RTP (Real-Time Transport Protocol)	RTP är ett standardprotokoll för att transportera realtidsdata, som interaktiv röst och video över datanätverk.	Telefoner använder RTP-protokollet för att skicka o

Nätverksprotokoll	Syfte	Att tänka på vid användning
RTCP (Real-Time Control Protocol)	RTCP samverkar med RTP för att tillhandahålla QoS-data (som jitter, latens och rundtursfördröjning) i RTP-strömmar.	RTCP är aktiverat som standard.
SDP (Session Description Protocol)	SDP är del av SIP-protokollet som fastställer vilka parametrar som är tillgängliga vid anslutning mellan två ändpunkter. Konferenssamtal upprättas med hjälp av endast de SDP-funktioner som har stöd i alla ändpunkter i konferensen.	SDP-funktioner, till exempel kodektyper och ide Unified Communications Manager eller Media G görs vid själva slutpunkten.
SIP (Session Initiation Protocol)	SIP är IETF-standarden (Internet Engineering Task Force) för multimediakonferenser över IP. SIP är ett ASCII-baserat applikationslagerprotokoll (definierat i RFC 3261) som kan användas för att upprätta, upprätthålla och avsluta samtal mellan två eller flera slutpunkter.	Liksom andra VoIP-protokoll är SIP utformat fö pakettelefoninätverk. Med signalering kan samtal att styra attribut för ett samtal från slutpunktsenh
SRTP (Secure Real-Time Transfer protocol)	SRTP är en utökning av RTP-ljud/videoprofilen (Real-Time Protocol) och säkerställer integriteten i RTP- och RTCP-paket som tillhandahåller autentisering, integritet och kryptering av mediapaket mellan två slutpunkter.	Telefoner använder SRTP för mediakryptering.
TCP (Transmission Control Protocol)	TCP är ett anslutningsorienterat transportprotokoll.	Telefoner använder TCP för att ansluta till Cisco
TLS (Transport Layer Security)	TLS är ett standardprotokoll för att säkra och autentisera kommunikationer.	När säkerheten implementerats använder telefon Manager. Mer information finns i dokumentatio
TFTP (Trivial File Transfer Protocol)	Med TFTP kan du överföra filer över nätverket. På telefonen används TFTP för att få en specifik konfigurationsfil till typen av telefon.	TFTP kräver en TFTP-server i nätverket som ka använder en annan TFTP-server än den som ang genom att använda menyn Nätverksinställning p Mer information finns i dokumentationen till dir
UDP (User Datagram Protocol)	UDP är ett anslutningslöst meddelandeprotokoll för leverans av datapaket.	UDP används endast för RTP-strömmar. SIP-sig

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Interaktion med Cisco Unified Communications Manager

Cisco Unified Communications Manager är en öppen, industristandard samtalsbearbetningssystem. Cisco Unified Communications Manager ställer upp och river ner samtal mellan telefoner, integrera traditionell växelfunktionalitet med företagets IP-nätverk. Cisco Unified Communications Manager hanterar komponenterna i telefonisystemet, som telefoner, åtkomstgateways, och de resurser som krävs för funktioner som samtalskonferenser och ruttplanering. Cisco Unified Communications Manager ger också:

- Firmware för telefoner
- Lista över betrodda certifikat (CTL) och identitetslista över betrodda (ITL) filer med TFTP-och HTTP-tjänster
- Telefonregistrering

- Ring bevarande, så att en mediasession fortsätter om signaleringen försvinner mellan primära Communications Manager och en telefon

Mer information om hur du konfigurerar Cisco Unified Communications Manager för att användas med de telefoner som beskrivs i det här kapitlet finns i dokumentationen för din version av Cisco Unified Communications Manager.

OBS! Om telefonmodellen som du vill konfigurera inte finns i listrutan med telefontyper i Cisco Unified Communications Manager Administration installerar du det senaste enhetspaketet för din version av Cisco Unified Communications Manager från Cisco.com.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Interaktion med Cisco Unified Communications Manager Express

När din telefon samverkar med Cisco Unified Communications Manager Express (Unified CME) måste telefonerna gå till CME-läge.

När en användare anropar konferensfunktionen kan telefonen använda taggen för att välja en lokal konferensbrygga eller nätverksmaskinvara med konferensbrygga.

Telefonerna har inte stöd för följande åtgärder:

- Överför − stöds endast i scenariet vid överföring av kopplat samtal.
- Konferens − stöds endast i scenariet vid överföring av kopplat samtal.
- Delta − stöds med knappen Konferens eller åtkomst till Hookflash.
- Förfrågan − stöds med knappen Förf.
- Bryt in och koppla ihop − stöds inte.
- Direktöverföring− stöds inte.
- Välj – stöds inte.

Användarna kan inte skapa konferens- och överföringssamtal mellan olika linjer.

Unified CME stöder snabbtelefonsamtal, även kallat viskning. Men sökningen avvisas av telefonen under pågående samtal.

Interaktion i röstmeddelandesystemet

Med Cisco Unified Communications Manager kan du integrera med olika röstmeddelandesystem, till exempel röstmeddelandesystemet i Cisco Unity Connection. Eftersom du kan integrera med en mängd olika system, måste du informera användarna om hur man använder det specifika systemet.

Om du vill aktivera funktionen för en användare att överföra till röstbrevlådan, ställer du in ett *xxxxx-uppringningsmönster och konfigurerar det som Vidarekoppling av alla samtal till röstbrevlådan. Mer information finns i dokumentationen till Cisco Unified Communications Manager.

Tillhandahåll följande information till varje användare:

- Hur man får åtkomst till kontot i röstmeddelandesystemet.

  Se till att du har använt Cisco Unified Communications Manager för att konfigurera knappen Meddelanden på en Cisco IP-telefon.

- Initialt lösenord för åtkomst till röstmeddelandesystemet.

  Konfigurera ett standardlösenord för röstmeddelandesystemet till samtliga användare.

- Hur telefonen indikerar att det finns röstmeddelanden som väntar.

  Använd Cisco Unified Communications Manager för att ställa in en metod för meddelande väntar-indikatorn (MWI).

Telefonens konfigurationsfiler

Konfigurationsfiler för en telefon lagras på TFTP-servern och definierar parametrar för anslutning till Cisco Unified Communications Manager. När du gör en ändring i Cisco Unified Communications Manager som kräver att telefonen ska återställas görs vanligtvis automatiskt motsvarande ändring i konfigurationsfilen.

Konfigurationsfiler innehåller också information om vilken bildinläsning telefonen ska köra. Om den här bildinläsningen skiljer sig från den som för tillfället är inläst på en telefon, kontaktar telefonen TFTP-servern och begär relevanta inläsningsfiler.

Om du konfigurerar säkerhetsrelaterade inställningar i Administration av Cisco Unified Communications Manager kommer telefonens konfigurationsfil att innehålla känslig information. För att säkerställa sekretessen i en konfigurationsfil måste du konfigurera den för kryptering. Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager. En telefon begär en konfigurationsfil när den återställs och registreras på Cisco Unified Communications Manager.

En telefon har tillgång till en standardkonfigurationsfil som heter XmlDefault.cnf.xml från TFTP-servern under följande förutsättningar:

- Du har aktiverat autoregistrering i Cisco Unified Communications Manager
- Telefonen inte har lagts till i Cisco Unified Communications Manager-databasen
- Telefonen är registrerad för första gången

Telefonbeteende under överbelastning av nätverket

Allt som försämrar nätverkets prestanda kan påverka telefonens ljud och i vissa fall avbryta samtalet. Orsaker till försämrat nätverk kan inkludera, men är inte begränsat till, följande aktiviteter:

- Administrativa uppgifter, som skanning av en intern port eller en säkerhetsskanning.
- Om ditt nätverk attackeras, t.ex. med en DoS-attack.

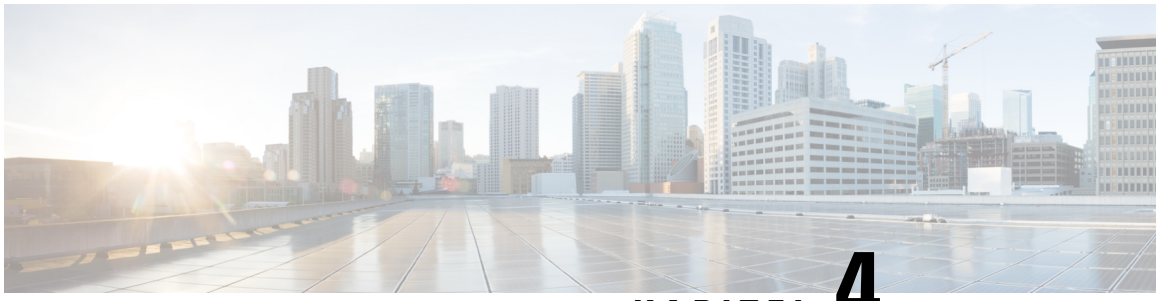
Programmeringsgränssnitt

Cisco har stöd för användning av telefon-API från tredje parts program som har testats och certifierats för Cisco av tredje parts programutvecklare. Alla telefonproblem som är relaterade till icke-certifierade program måste åtgärdas av den tredje parten och kommer inte att åtgärdas av Cisco.

Om du vill ha mer information om hur Cisco stöder certifierade tredje parts program/lösningar finns det på webbplatsen Solution Partner Program.

DEL II

Installation av Cisco IP-konferenstelefon



KAPITEL 4

Installation av telefonen

Kontrollera nätverksinställningen

Vid distribution av ett nytt IP-telefonisystem måste systemadministratörer och nätverksadministratörer slutföra flera inledande konfigurationer för att förbereda nätverket för IP-telefoni. Mer information och en checklista för inställning och konfiguration av ett Cisco IP-telefoninätverk finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

För att telefonen ska fungera felfritt som en ändpunkt i nätverket måste nätverket uppfylla specifika krav. Ett krav är lämplig bandbredd. Telefonerna kräver mer bandbredd än rekommenderade 32 kbps när de registreras i Cisco Unified Communications Manager. Ta hänsyn till detta högre bandbreddskrav när du konfigurerar din QoS-bandbredd. För mer information, se *Cisco Collaboration System 12.x Solution Reference Network design (SRND)* eller senare (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html).

OBS! Telefonen visar datum och tid från Cisco Unified Communications Manager. Den tid som visas på telefonen kan skilja sig från tiden i Cisco Unified Communications Manager med upp till 10 sekunder.

Arbetsordning

Steg 1 Konfigurera ett VoIP-nätverk för att uppfylla följande krav:

- VoIP är konfigurerat på routrar och gatewayar.
- Cisco Unified Communications Manager är installerad i nätverket och konfigurerad för att hantera samtalsbehandling.

Steg 2 Ställ in nätverk för att stödja något av följande:

- DHCP-stöd
- Manuell tilldelning av IP-adress, gateway och nätmask

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Aktiveringskod vid installation för telefoner på företaget

Du kan använda registrering via aktiveringskod för att snabbt ställa in nya telefoner utan autoregistrering. Med denna metod kan du styra den inledande registreringen av telefoner genom att använda något av följande:

- Cisco Unified Communications Bulk Administration Tool (BAT)
- Cisco Unified Communications Manager administrationsgränssnitt
- Administrativa XML-Web Service (AXL)

Aktivera den här funktionen från avsnittet **Enhetsinformation** på sidan Telefonkonfiguration. Välj **Kräv aktiveringskod vid onboarding** om du vill att den här funktionen ska gälla för en specifik telefon på företaget.

Användare måste ange en aktiveringskod innan deras telefoner kan registreras. Registrering via aktiveringskod kan tillämpas på enskilda telefoner, en grupp av telefoner eller i ett nätverk.

Det här är ett enkelt sätt för användare att registrera sina telefoner eftersom de bara behöver ange en aktiveringskod med 16 siffror. Koderna anges manuellt eller med en QR-kod om telefonen har en videokamera. Vi rekommenderar att du använder en säker metod när du tillhandahåller användarna denna information. Om en användare har tilldelats en telefon finns den här koden tillgänglig på självbetjäningsportalen. Granskningsloggen registrerar användarens åtkomst av koden från portalen.

Aktiveringskoder kan endast användas en gång, och de upphör att gälla efter en vecka som standard. Om en kod upphör att gälla måste du tillhandahålla användaren en ny.

Metoden är ett enkelt sätt att skydda nätverket eftersom en telefon inte registreras förrän MIC-certifikatet och aktiveringskoden har verifierats. Den här metoden är också ett enkelt sätt att registrera flera telefoner samtidigt eftersom det innebär att varken TAPS (Tool for Auto-registered Phone Support)-verktyget eller autoregistrering används. Registreringshastigheten är en telefon per sekund eller omkring 3 600 telefoner per timme. Telefoner kan läggas till i Cisco Unified Communications Manager Administrative, med Administrative XML-webbtjänsten (AXL) eller med BAT.

Befintliga telefoner återställs när de har konfigurerats för registrering via aktiveringskod. De registreras inte förrän aktiveringskoden anges och telefonen MIC verifieras. Informera nuvarande användare om att ni tänker införa registrering via aktiveringskod före implementeringen.

Mer information finns i *administrationsguiden för Cisco Unified Communications Manager IM och Presence Service*.

Aktiveringskodregistrering och mobilåtkomst och Remote Access

Du kan använda aktiveringskodregistrering med mobilåtkomst och Remote Access när du distribuerar Cisco IP-telefoner för fjärranvändare. Funktionen är ett säkert sätt att distribuera telefoner utanför företaget när autoregistrering inte krävs. Men du kan konfigurera en telefon för autoregistrering på företaget och aktiveringskoder utanför företaget. Funktionen liknar aktiveringskodregistrering för telefoner på företaget, men den gör aktiveringskoden tillgänglig för telefoner utanför företaget.

Aktiveringskodregistrering för mobilåtkomst och Remote Access kräver Cisco Unified Communications Manager 12.5 (1) SU1 eller senare, och Cisco Expressway X 12.5 eller senare. Smart Licensing bör också aktiveras.

Du kan aktivera den här funktionen från Cisco Unified Communications Manager administration, men observera följande:

- Aktivera den här funktionen från avsnittet **Enhetsinformation** på sidan Telefonkonfiguration.
- Välj **Kräv aktiveringskod för registrering** om du vill att funktionen enbart ska verkställas på en enda telefon på företaget.
- Välj **Tillåt aktiveringskod via MRA** och **Kräv aktiveringskod för registrering** om du vill använda aktiveringskoden för en enskild telefon utanför företaget. Om telefonen är lokal ändras den till mobil- och Remote Access-läge och använder Expressway. Om telefonen inte kan nå Expressway registreras den inte förrän den är utanför företaget.

Mer information finns i följande dokument:

- *Administrationsguide för Cisco Unified Communications Manager IM och Presence Service, version 12.0 (1).*
- *Mobilåtkomst och Remote Access genom Cisco Expressway* för Cisco Expressway X12.5 eller senare

Aktivera autoregistrering för telefoner

Cisco IP-telefon kräver Cisco Unified Communications Manager för hantering av samtal. Läs dokumentationen till din utgåva av Cisco Unified Communications Manager eller den sammanhangsberoende hjälpen i Cisco Unified Communications Manager Administration och kontrollera att Cisco Unified Communications Manager är rätt konfigurerat för hantering av telefonen och dirigering och bearbetning av samtal.

Innan du installerar Cisco IP-telefon måste du välja en metod för att lägga telefoner i Cisco Unified Communications Manager-databasen.

Genom att aktivera autoregistrering innan du installerar telefoner kan du:

- Lägga till telefoner utan att först samla in MAC-adresser från telefonerna.
- Automatiskt lägga till en Cisco IP-telefon i Cisco Unified Communications Manager-databasen när du ansluter telefonen fysiskt till ditt IP-telefonnät. Under autoregistreringen tilldelar Cisco Unified Communications Manager nästa tillgängliga sekventiella katalognummer till telefonen.

- Snabbregistrera telefoner i Cisco Unified Communications Manager-databasen och ändra inställningar som katalognummer från Cisco Unified Communications Manager.
- Flytta autoregistrerade telefoner till nya platser och tilldela dem till olika enhetspooler utan att påverka deras katalognummer.

Autoregistrering är inaktiverat som standard. I vissa fall kanske du inte vill använda autoregistrering, till exempel om du vill tilldela ett visst anknytningsnummer till telefonen, eller om du vill använda en säker anslutning med Cisco Unified Communications Manager. Mer information om aktivering av autoregistrering finns i dokumentationen till din utgåva av Cisco Unified Communications Manager. När du konfigurerar klustret för blandat läge genom Cisco CTL-klienten är autoregistrering automatiskt inaktiverat, men du kan aktivera det. När du konfigurerar klustret för osäkert läge genom Cisco CTL-klienten är autoregistrering inte automatiskt aktiverat.

Du kan lägga till telefoner med autoregistrering och TAPS, verktyget för stöd av autoregistrerade telefoner, utan att först samla in MAC-adresser från telefoner.

TAPS samverkar med BAT-verktyget för massadministration för att uppdatera en grupp telefoner som redan har lagts till i Cisco Unified Communications Manager-databasen med MAC-exempeladresser. Använd TAPS att uppdatera MAC-adresser och hämta fördefinierade konfigurationer för telefoner.

Cisco rekommenderar att du använder autoregistrering och TAPS om du lägger till färre än 100 telefoner i nätverket. Om du lägger till mer än 100 telefoner i nätverket ska du använda BAT-verktyget för massregistrering.

Om du vill använda TAPS kan du eller slutanvändaren slå ett TAPS-katalognummer och följa röstinstruktionerna. När processen är klar, innehåller telefonen katalognummer och andra inställningar, och telefonen uppdateras i Cisco Unified Communications Manager Administration med rätt MAC-adress.

Kontrollera att autoregistrering är aktiverat och rätt konfigurerat i Cisco Unified Communications Manager Administration innan du ansluter en Cisco IP-telefon till nätverket. Mer information om hur du aktiverar och konfigurerar autoregistrering finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Autoregistrering måste vara aktiverat i Cisco Unified Communications Manager Administration för att TAPS ska fungera.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och klicka på **System** > **Cisco Unified CM**.

Steg 2 Klicka på **Sök** och välj server.

Steg 3 Gå till **Autoregistreringsinformation** och konfigurera dessa fält.

- **Universell enhetsmall**
- **Universell radmall**
- **Starta anknytningsnummer**
- **Avsluta katalognummer**

Steg 4 Avmarkera kryssrutan **Automatisk registrering är inaktiverad i den här Cisco Unified Communications Manager**.

Steg 5 Klicka på **Spara**.

Steg 6 Klicka på **Använd konfig**.

Sammanlänkningsläge

Du kan ansluta två konferenstelefoner med en och de USB-C kablar som ingår i sammanlänkningssatsen för att expandera ljudtäckningsområdet i ett rum.

I sammanlänkningsläget båda enheter får ström via Smart-adaptern som är ansluten till en strömadapter. Du kan bara använda en extern mikrofon per enhet. Du kan använda en kombination av mikrofoner med sladd med enheterna eller en kombination av trådlösa mikrofoner med enheterna, men inte en blandad kombination av mikrofonerna. När en sladdansluten mikrofon är ansluten till en av enheterna kopplas eventuella trådlösa mikrofoner som är ansluten till samma enhet isär. Vid ett aktivt samtal, är på LED-lamporna och menyalternativen på telefonens skärm på båda enheterna synkroniserade.

Relaterade ämnen

Installera konferenstelefonen i kedjekopplingsläge, på sidan 38
En telefon i kedjekopplingsläge fungerar inte, på sidan 161

Installera konferenstelefonen

När telefonen ansluter till nätverket påbörjas telefonens startprocess och registreras i Cisco Unified Communications Manager. Om du inaktiverar DHCP-tjänsten måste du konfigurera nätverksinställningarna på telefonen.

Om du har använt autoregistrering, måste du uppdatera den specifika konfigurationsinformation för telefonen som associera telefonen med en användare, ändra knapptabellen, eller katalognummer.

När telefonen är ansluten kontrollerar den om en senare firmware-version behöver installeras.

Se Installera konferenstelefonen i kedjekopplingsläge, på sidan 38 om du använder konferenstelefonen i kedjekopplingsläge.

Innan du börjar

Se till att du har den senaste firmware-versionen installerad på Cisco Unified Communications Manager. Kontrollera om det finns uppdaterade enhetspaket:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html

Arbetsordning

Steg 1 Välj kraftkällan för telefonen:

- PoE (Power over Ethernet)-distribution med en
- Icke-PoE Ethernet-distribution med en
- Implementering av WiFi med en strömadapter för Cisco IP-konferenstelefon 8832

Mer information finns i Olika sätt att strömförsörja konferenstelefonen, på sidan 32.

Steg 2 Anslut telefonen till växeln.

- Om du använder PoE:
  1. Anslut Ethernet-kabeln till LAN-porten.
  2. Anslut den andra änden av Ethernet-kabeln till antingen eller Cisco IP-konferenstelefon 8832 Ethernet-koppling.
  3. Anslut injektorn till konferenstelefonen med USB-C-kabeln.
- Om du inte använder PoE:
  1. Om du använder Cisco IP-konferenstelefon 8832 Ethernet-koppling kan du koppla in strömadaptern i eluttaget.
  2. Anslut strömadaptern till Ethernet-injektorn med en USB-C-kabel.

     OR

     Om du använder kan du koppla in den i eluttaget.
  3. Anslut Ethernet-kabeln till icke-PoE Ethernet-injektorn eller Ethernet-injektorn.
  4. Anslut Ethernet-kabeln till LAN-porten.
  5. Anslut icke-PoE Ethernet-injektorn eller Ether-injektorn till konferenstelefonen med en USB-C-kabel.
- Om du använder Wi-Fi:
  1. Anslut nätadaptern för Cisco IP-konferenstelefon 8832 till ett eluttag.
  2. Anslut strömadaptern till konferenstelefonen med en USB-C-kabel.

     OBS! Du kan använda icke-PoE Ethernet-injektorn som strömförsörjning till telefonen i stället för strömadaptern. Då måste du ta bort nätverkskabeln. Telefonen kan bara anslutas till Wi-Fi då Ethernet-anslutningen inte är tillgänglig.

Steg 3 Övervaka telefonens startprocess. Detta steg verifierar att telefonen är korrekt konfigurerad.

Steg 4 Om du inte använder autoregistrering måste du konfigurera säkerhetsinställningarna på telefonen manuellt.

Steg 5 Tillåt att telefonen uppgraderas till den aktuella firmwarebilden som finns i Cisco Unified Communications Manager.

Steg 6 Ring samtal med telefonen för att kontrollera att telefonen och funktionerna fungerar korrekt.

Steg 7 Tillhandahåll information till användarna om hur de använder sina telefoner och hur de konfigurerar sina telefonalternativ. Detta steg säkerställer att användarna har tillräcklig information för att kunna använda sina Cisco-telefoner.

Olika sätt att strömförsörja konferenstelefonen

Din konferenstelefon måste strömförsörjas från någon av dessa källor:

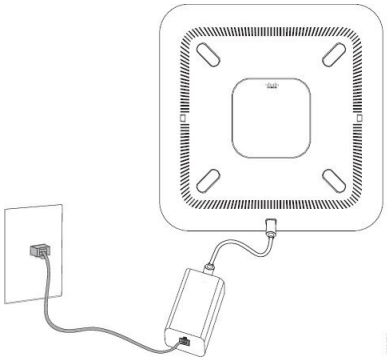
- Power over Ethernet (PoE)

    - Nordamerika
        -
        - Cisco IP-konferenstelefon 8832 Ethernet-koppling
    - Utanför Nordamerika –

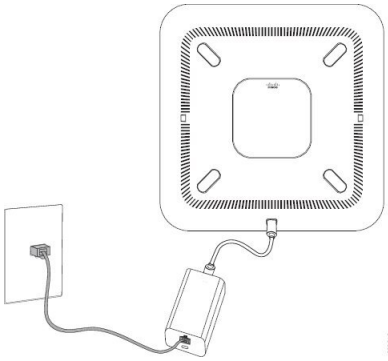
- Icke-PoE Ethernet
    - Nordamerika
        -
        - Cisco IP-konferenstelefon 8832 Ethernet-koppling med en strömadapter för Cisco IP-konferenstelefon 8832 är ansluten till ett eluttag.
    - Utanför Nordamerika –
- WiFi – Använd strömadaptern för Cisco IP-konferenstelefon 8832 är ansluten till ett eluttag.

Figur 6. Konferenstelefon – PoE-strömalternativ

På bilden nedan visas de två PoE-strömalternativen.



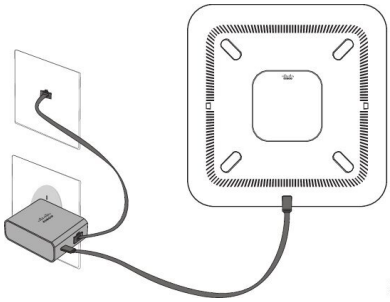
med PoE-strömalternativet



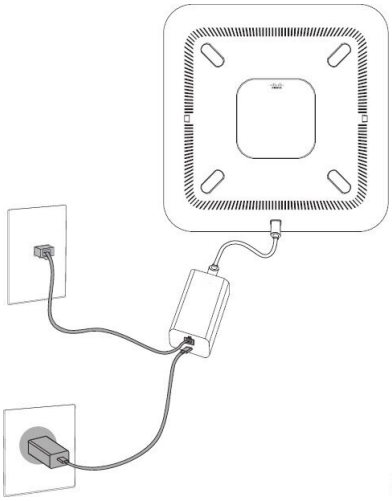
Cisco IP-konferenstelefon 8832 Ethernet-koppling med PoE-strömalternativet

Figur 7. Konferenstelefon – Ethernet-strömalternativ

På bilden nedan visas de två Ethernet-strömalternativen.

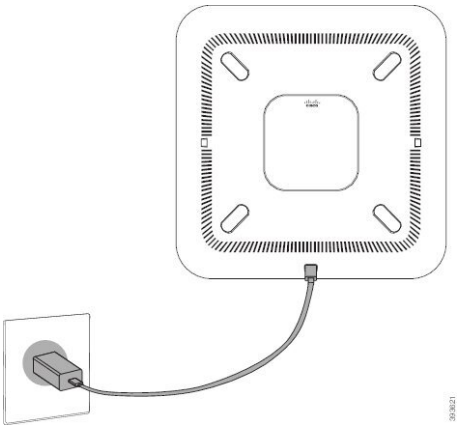


med Ethernet-strömalternativet



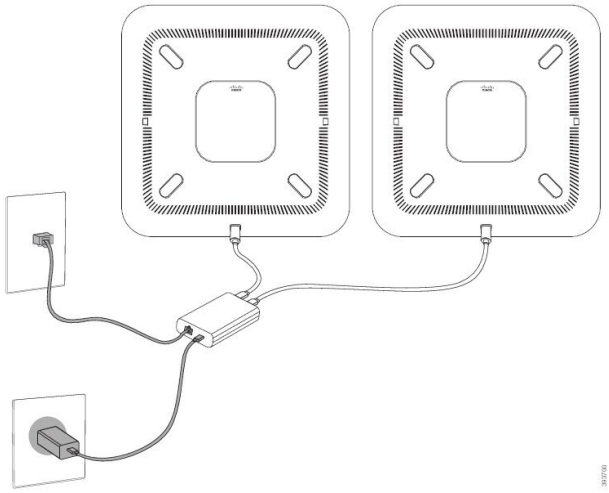
Cisco IP-konferenstelefon 8832 Ethernet-koppling med Ethernet-strömalternativet

Figur 8. Konferenstelefon - strömalternativ, när du är ansluten till ett Wi-Fi-nätverk



Figur 9. Konferenstelefon – strömalternativ, i sammanlänkningsläge

Följande bild visar strömalternativet när telefonen är ansluten i sammanlänkningsläge.



Installera kabelanslutna förlängningsmikrofoner

Telefonen har stöd för valfria kit med två kabelanslutna mikrofoner. Du kan placera mikrofonerna upp till 2,13 m från telefonen. För bästa resultat placerar du mikrofonerna mellan 0,91 m och 2,1 m från telefonen.

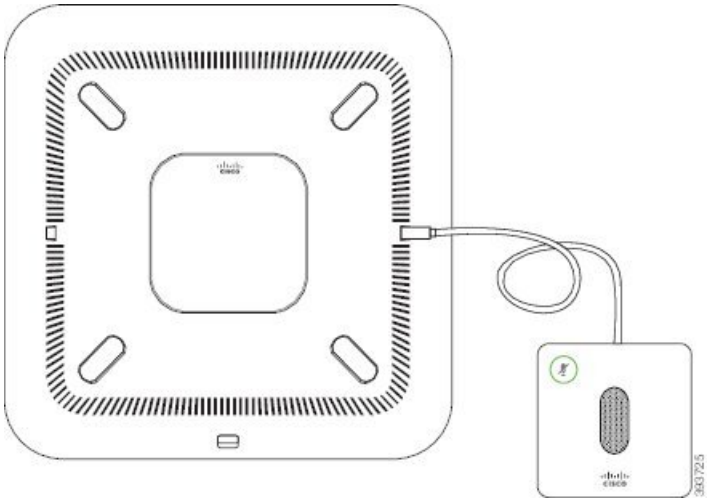
Arbetsordning

Steg 1 Sätt i mikrofonkabeln i porten på telefonens sida.

Steg 2 Förläng mikrofonkabeln till önskat läge.

I följande figur visas installation av en kabelansluten förlängningsmikrofon.

Figur 10. Installera kabelanslutna förlängningsmikrofoner



Installera trådlösa förlängningsmikrofoner

Konferenstelefonen erbjuder alternativet att ansluta två trådlösa förlängningsmikrofoner.

OBS! Du måste använda antingen två mikrofoner med sladd eller två trådlösa mikrofoner med telefonen, men inte en blandad kombination.

När telefonen används i ett samtal lyser förlängningssmikrofonens LED-lampa grönt. Om du vill stänga av ljudet på mikrofonen trycker du på **Ljud av**-knappen. När mikrofonljudet är avstängt lyser LED-lampan rött. När batteriet i mikrofonen börjar ta slut blinkar LED-lampan snabbt.

Innan du börjar

Koppla bort de kabelanslutna mikrofonerna innan du installerar trådlösa mikrofoner. Du kan inte använda både kabelanslutna och trådlösa mikrofoner på samma gång.

Arbetsordning

Steg 1 Placera bordsmonteringsplattan på bordsytan där vill placera mikrofonen.

Steg 2 Ta bort det skyddet från klistret på den dubbelhäftande tejpen under bordsmonteringsplattan. Placera bordsmonteringsplattan så att den fäster på bordsytan.

Steg 3 Koppla in mikrofonen i bordsmonteringsplattan. Det finns inbäddade magneter i mikrofonen så att den kan sättas på plats.

Du kan flytta mikrofonen och den inkopplade bordsmonteringsplattan till en annan plats på bordsytan om det behövs. Var försiktig när du flyttar enheten.

Relaterade ämnen

Trådlös mikrofon (endast 8832), på sidan 13
Installera mikrofonens trådlösa laddningsvagga, på sidan 37

Installera mikrofonens trådlösa laddningsvagga

Du kan använda laddningsvaggan för att ladda den trådlösa mikrofonens batteri.

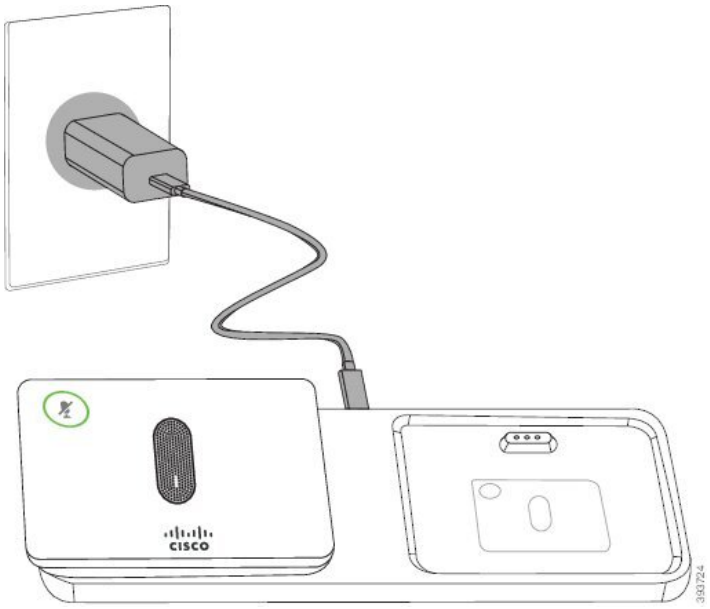
Arbetsordning

Steg 1 Anslut laddningsvaggans nätadapter till ett eluttag.

Steg 2 Anslut ena änden av USB-C kabeln till laddningsvaggan och den andra änden till strömadaptern.

I följande figur visas installation av en trådlös mikrofons laddningsvagga.

Figur 11. Installation av en trådlös mikrofons laddningsvagga



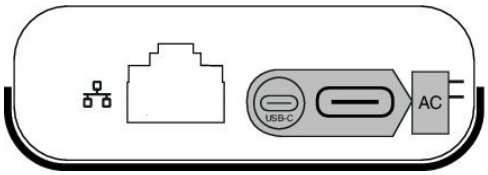
Relaterade ämnen

Trådlös mikrofon (endast 8832), på sidan 13
Installera trådlösa förlängningsmikrofoner, på sidan 36

Installera konferenstelefonen i kedjekopplingsläge

Ett kit för kedjekoppling innehåller en , en kort LAN-kabel, två långa, kraftiga USB-C-kablar och en kortare, tunnare USB-C-kabel. I kedjekopplingsläget kräver konferenstelefonerna extern ström från ett eluttag. Du måste använda för att koppla samman telefonerna. De långa USB-C-kablarna används till telefonen och den korta används till strömadaptern. Se bilden nedan när du ansluter strömadaptern och LAN-porten till .

Figur 12. Strömport och LAN-port för smartadapter



Du kan bara använda en mikrofon per enhet.

OBS! Du måste använda antingen två mikrofoner med sladd eller två trådlösa mikrofoner med telefonen, men inte en blandad kombination.

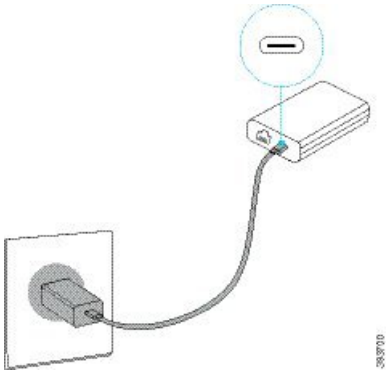
C-USB-kabeln till strömadaptern är tunnare än USB-C-kablarna som ansluter till telefonen.

Arbetsordning

Steg 1 Koppla in strömadaptern i eluttaget.

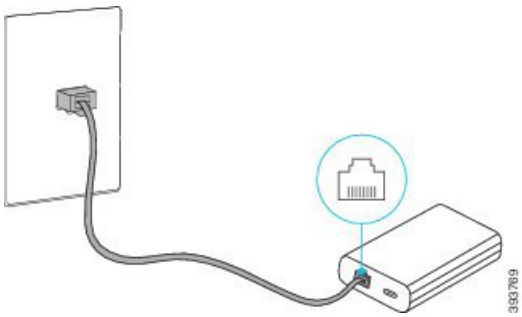
Steg 2 Anslut den korta, tunnare USB-C-kabeln från strömadaptern till .

Figur 13. Smartadapterns USB-port ansluten till eluttaget



Steg 3 Krävs: Anslut ethernetkabeln till och LAN-porten.

Figur 14. Smartadapterns LAN-port ansluten till LAN-porten i vägguttaget

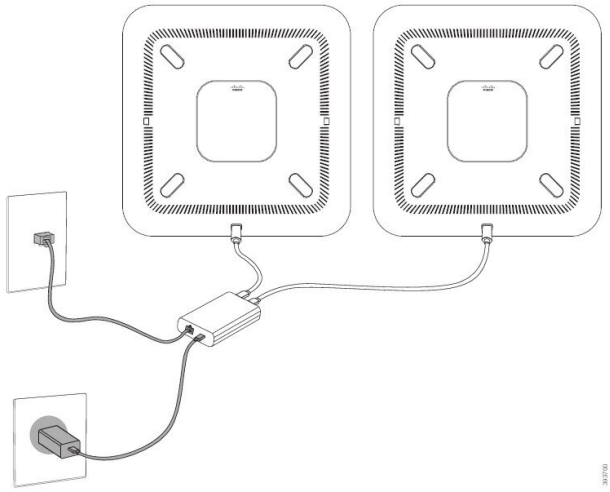


Steg 4 Koppla den första telefonen till med den längre, kraftigare USB-C-kabeln.

Steg 5 Koppla den andra telefonen till med en andra USB-C-kabel.

I följande figur visas installationen av konferenstelefonen i kedjekopplingsläge.

Figur 15. Konferenstelefon i kedjekopplingsläge



Relaterade ämnen

Sammanlänkningsläge, på sidan 31
En telefon i kedjekopplingsläge fungerar inte, på sidan 161

Starta om konferenstelefonen från säkerhetskopian

Cisco IP-konferenstelefon 8832 har en säkerhetskopieringsbild som används för att återställa telefonen om standardbilden blir förstörd.

Om du vill starta om telefonen från säkerhetskopian gör du följande:

Arbetsordning

Steg 1 Håll *-knappen intryckt medan du slår på strömmen till konferenstelefonen.

Steg 2 När LED-lampan lyser grönt (PÅ) och sedan släcks (AV) släpper du *-knappen.

Steg 3 Telefonen startas om från säkerhetskopian.

Ställa in telefonen via inställningsmenyerna

Telefonen innehåller många konfigurerbara nätverksinställningar som du kan behöva modifiera innan telefonen är funktionell för användarna. Du kan komma åt dessa inställningar, och ändra några av dem, genom menyer på telefonen.

Telefonen innehåller följande inställningsmenyerna:

- Nätverksinställning: Här finns det alternativ för visning och konfiguration av en mängd olika nätverksinställningar.
  - IPv4-inställning: Denna undermeny ger ytterligare nätverksalternativ.
  - IPv6-inställning: Denna undermeny ger ytterligare nätverksalternativ.
- Säkerhetsinställning: Här finns det alternativ för visning och konfiguration av en mängd olika säkerhetsinställningar.

OBS! Du kan styra om en telefon har åtkomst till inställningsmenyn eller alternativ på denna meny. Använd fältet **Inställningsåtkomst** i fönstret Administration av Cisco Unified Communications Manager Telefonkonfiguration för att styra åtkomsten. I fältet **Inställningsåtkomst** godtas följande värden:

- Aktiverat: Ger tillgång till inställningsmenyn.
- Inaktiverat: Förhindrar åtkomst till de flesta poster i menyn Inställningar. Användaren har fortfarande åtkomst till **Inställningar** > **Status**.
- Begränsat: Ger tillgång till menyalternativen för Användarinställningar och Status samt ger möjlighet att spara volymändringar. Förhindrar åtkomst till andra alternativ på menyn Inställningar.

Om du inte kan få tillgång till ett alternativ på menyn Admininställningar kontrollerar du fältet **Inställningsåtkomst**.

Du kan konfigurera inställningar som är skrivskyddade på telefonen i Administration av Cisco Unified Communications Manager.

Arbetsordning

Steg 1 Tryck på **Inställningar**.

Steg 2 Välj **Admininställningar**.

Steg 3 Ange lösenord om det behövs och klicka sedan på **Inloggning**.

Steg 4 Välj **Nätverksinställning** eller **Säkerhetsinställning**.

Steg 5 Utför en av dessa åtgärder för att visa önskad meny:

- Använd pilknapparna för att välja önskad meny och tryck sedan på **Välj**.
- Använd knappsatsen på telefonen för att ange numret som motsvarar menyn.

Steg 6 För att visa en undermeny, upprepa steg 5.

Steg 7 Om du vill gå ur en meny trycker du på **Tillbaka**.

Relaterade ämnen

Starta om eller återställa konferenstelefonen, på sidan 169
Konfigurera nätverksinställningarna, på sidan 42
Konfigurera säkerhetsinställningarna

Använda ett telefonlösenord

Arbetsordning

Steg 1 Gå till Cisco Unified Communications Manager Administration och navigera till fönstret med den allmänna telefonprofilkonfigurationen (**Enhet** > **Enhetsinställningar** > **Allmän telefonprofil**).

Steg 2 Ange ett lösenord för alternativet Lås upp lösenord för lokal telefon.

Steg 3 Använd lösenordet för den allmänna telefonprofilen som telefonen använder.

Text och menyalternativ från telefonen

När du redigerar värdet av en inställning följer du dessa riktlinjer:

- Använd pilarna på styrplattan för att markera det fält som du vill redigera. Tryck på **Välj** på styrplattan för att aktivera fältet. När fältet är aktiverat kan du ange värden.
- Använd knapparna på knappsatsen för att mata in siffror och bokstäver.
- Tryck på knappen en eller flera gånger för att visa en viss bokstav. Tryck på knappen en eller flera gånger för att visa en viss bokstav. Tryck till exempel på knappen **2** en gång för ”a,” snabbt två gånger för ”b” och snabbt tre gånger för ”c.” När du pausar flyttas markören automatiskt framåt och du kan ange nästa bokstav.
- Tryck på funktionsknappen om du gör fel. Denna funktionsknapp raderar tecknet till vänster om markören.
- Tryck på **Återgå** innan du trycker på **Använd** att ignorera eventuella ändringar som du har gjort.
- Om du vill ange en punkt (till exempel i en IP-adress) trycker du på ***** på knappsatsen.
- Om du vill ange kolon i en IPv6-adress punkt trycker du på ***** på knappsatsen.

OBS! Cisco IP-telefon har flera metoder för att återställa eller återskapa inställningar om det behövs.

Konfigurera nätverksinställningarna

Arbetsordning

Steg 1 Tryck på **Inställningar**.

Steg 2 Välj **Admin.inställningar** > **Nätverksinställning** > **Ethernet-inställning**.

Steg 3 Ange fälten enligt beskrivningen i Fält för nätverksinställningar, på sidan 42.
När du har fyllt i fälten kan du behöva starta om telefonen.

Fält för nätverksinställningar

Menyn Nätverksinställning innehåller fält och undermenyer för IPv4 och IPv6.

Om du vill ändra vissa fält måste du inaktivera DHCP.

Tabell 10. Menyn Nätverksinställning

Post	Typ	Standard	Beskrivning
Ställa in IPv4	Meny		Se tabellen ”Undermeny för IPv4-inställning”. Det här alternativet visas endast i aktiverat läge eller i dualstackläge.
Ställa in IPv6	Meny		Se tabellen ”Undermeny för IPv6-inställning”.
Värdnamn	Sträng		Telefonens värdnamn. Om du använder DHCP tilldelas det här namnet automatiskt.
Domännamn	Sträng		Namn på DNS-domän där telefonen befinner sig. Om du vill ändra det här fältet måste du inaktivera DHCP.
Operativt VLAN-ID			Operativt VLAN som är konfigurerat i en Cisco Catalyst-växel där telefonen är medlem.
Administrativt VLAN-ID			Extra-VLAN där telefonen är medlem.

Post	Typ	Standard	Beskrivning
SWport-inställning	Autoförhandla 10 Halv 10 Full 100 Halv 100 Full	Autoförhandla	Hastighet och duplex i växelporten, där: • 10 halv = 10-BaseT/halv duplex • 10 full = 10-BaseT/full duplex • 100 halv = 100-BaseT/halv duplex • 100 full = 100-BaseT/full duplex
LLDP-MED: SW-port	Inaktiverad Aktiverad	Aktiverad	Anger om LLDP-MED har aktiverats i väljarporten.

Tabell 11. Undermeny för IPv4-inställning

Post	Typ	Standard	Beskrivning
DHCP	Inaktiverad Aktiverad	Aktiverad	Aktiverar eller inaktiverar användningen av DHCP.
IP-adress			IPv4-adress till telefonen. Om du vill ändra det här fältet måste du inaktivera DHCP.
Nätmask			Nätmask som telefonen använder. Om du vill ändra det här fältet måste du inaktivera DHCP.
Standardrouter 1			Standardrouter som telefonen använder. Om du vill ändra det här fältet måste du inaktivera DHCP.
DNS-server 1			Primär DNS-server (DNS-server 1) som telefonen använder. Om du vill ändra det här fältet måste du inaktivera DHCP.
DNS-server 2			Primär DNS-server (DNS-server 2) som telefonen använder.
DNS-server 3			Primär DNS-server (DNS-server 3) som telefonen använder.
Alt. TFTP	Nej Ja	Nej	Anger om telefonen använder en alternativ TFTP-server.

Post	Typ	Standard	Beskrivning
TFTP-server 1			Primär TFTP-server som telefonen använder. Om du anger På för Alternativ TFTP måste du ange ett annat värde än noll för TFTP-server 1. Om varken den primära TFTP-servern eller reserv-TFTP-servern finns i CTL- eller ITL-filen på telefonen, måste du låsa upp filen innan du kan spara ändringar i alternativet för TFTP-server 1. I så fall kan telefonen ta bort filen när du sparar ändringar i alternativet för TFTP-server 1. En ny CTL- eller ITL-fil hämtas från den nya adressen för TFTP-server 1. Se anmärkningar om TFTP efter den sista tabellen.
TFTP-server 2			Sekundär TFTP-server som telefonen använder. Om varken den primära TFTP-servern eller reserv-TFTP-servern finns i CTL- eller ITL-filen på telefonen, måste du låsa upp filen innan du kan spara ändringar i alternativet för TFTP-server 2. I så fall kan telefonen ta bort filen när du sparar ändringar i alternativet för TFTP-server 2. En ny CTL- eller ITL-fil hämtas från den nya adressen för TFTP-server 2. Se anmärkningar om TFTP efter den sista tabellen.
DHCP-adressen släppt	Nej Ja	Nej	

Tabell 12. Undermeny för IPv6-inställning

Post	Typ	Standard	Beskrivning
DHCPv6 aktiverad	Inaktiverad Aktiverad	Aktiverad	Aktiverar eller inaktiverar användningen av IPv6 DHCP.
IPv6-adress			Telefonens IPv6-adress. Om du vill ändra det här fältet måste du inaktivera DHCP.

Post	Typ	Standard	Beskrivning
IPv6-prefixlängd			Längd på IPv6-adressen. Om du vill ändra det här fältet måste du inaktivera DHCP.
IPv6-standardrouter 1			IPv6-standardrouter. Om du vill ändra det här fältet måste du inaktivera DHCP.
IPv6 DNS-server 1			Primär IPv6 DNS-server Om du vill ändra det här fältet måste du inaktivera DHCP.
Alternativ IPv6 TFTP	Nej Ja	Nej	Anger om telefonen använder en alternativ IPv6 TFTP-server.
IPv6 TFTP-server 1			Primär IPv6 TFTP-server som telefonen använder. Se anmärkningar om TFTP efter den här tabellen.
IPv6 TFTP-server 2			Sekundär IPv6 TFTP-server som telefonen använder. Se anmärkningar om TFTP efter den här tabellen.
IPv6-adressen släppt	Nej Ja	Nej	

Innan IPv6-alternativen kan konfigureras på enheten måste IPv6 vara aktiverat och konfigurerat i Cisco Unified Communications Administration. Följande enhetskonfigurationsfält gäller för IPv6-konfiguration:

- IP-adresseringsläge
- Inställning av IP-adresseringsläge för signalering

Om IPv6 är aktiverad i Unified-klustret är standardinställningen för IP-adresseringsläget IPv4 och IPv6. I det här adresseringsläget hämtar och använder telefonen en IPv4-adress och en IPv6-adress. Den kan använda den IPv4- och IPv6-adress som behövs för media. Telefonen använder antingen IPv4- eller IPv6-adressen för samtalskontrollsignalering.

Mer information om IPv6 finns i

- ”Allmän enhetskonfiguration” i *Handbok om funktioner och tjänster för Cisco Unified Communications Manager* under kapitlet ”IPv6-stöd i Cisco Unified Communications-enheter”.
- *IPv6-driftsättningsguide för Cisco Collaboration Systems version 12.0* finns här: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

Anmärkningar om TFTP

När telefonen söker efter TFTP-servern, prioriterar telefonen manuellt tilldelade TFTP-servrar, oavsett protokoll. Om din konfiguration består av både IPv6 och IPv4 TFTP-servrar, prioriterar telefonen den ordning som används för TFTP-servern genom att prioritera manuellt tilldelade IPv6 TFTP-servrar och IPv4 TFTP-servrar. Telefonen söker efter TFTP-servern i följande ordning:

1. Alla manuellt tilldelade IPv4 TFTP-servrar
2. Alla manuellt tilldelade IPv6-servrar
3. DHCP-tilldelade TFTP-servrar
4. DHCPv6-tilldelade TFTP-servrar

Information om CTL- och ITL-filer finns i *Säkerhetshandboken till Cisco Unified Communications Manager*.

Ställa in domännamnsfältet

Arbetsordning

Steg 1 Ställ in alternativet DHCP-aktiverat på **Nej**.

Steg 2 Bläddra till alternativet Domännamn, tryck på **Välj** och ange ett nytt domännamn.

Steg 3 Tryck på **Använd**.

Aktivera det trådlösa nätverket på telefonen

Kontrollera att Wi-Fi-täckningen på den plats där det trådlösa nätverket distribueras är lämpligt för sändning av röstpaket.

En fast och säker roamingmetod rekommenderas för Wi-Fi-användare. Vi rekommenderar att du använder 802.11r (FT).

Fullständig konfigurationsinformation finns i *Driftsättningsguide för Cisco IP-telefon 8832 trådlöst nätverk* på den här platsen:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

Driftsättningsguiden för Cisco IP-telefon 8832 trådlöst nätverk innehåller följande konfigurationsinformation:

- Konfiguration av trådlöst nätverk
- Konfiguration av trådlöst nätverk i Cisco Unified Communications Manager Administration
- Konfiguration av trådlöst nätverk på Cisco IP-telefon

Innan du börjar

Se till att Wi-Fi har aktiverats på telefonen och att Ethernet-kabeln är bortkopplad.

Arbetsordning

Steg 1 Om du vill aktivera programmet trycker du på **Inställningar**.

Steg 2 Välj **Admininställningar** > **Nätverksinställning** > **Wi-Fi-klientinställning** > **Trådlöst**.

Steg 3 Tryck på **På**.

Konfigurera det trådlösa nätverket i Cisco Unified Communications Manager.

I Cisco Unified Communications Manager Administration måste du aktivera en parameter som kallas ”Wi-Fi” för konferenstelefonen.

OBS! I fönstret Telefonkonfiguration i Cisco Unified Communications Manager Administration (**Enhet** > **Telefon**) använder du den trådbundna MAC-adressen när du konfigurerar MAC-adressen. Registrering av Cisco Unified Communications Manager använder inte den trådlösa MAC-adressen.

Gör följande i Cisco Unified Communications Manager Administration:

Arbetsordning

Steg 1 Om du vill aktivera det trådlösa nätverket på en specifik telefon gör du följande:

a) Välj **Enhet** > **Telefon**.
b) Leta reda på telefonen.
c) Välj inställningen **Aktiverad** för Wi-Fi-parametern i avsnittet Produktspecifik konfigurationslayout.
d) Markera kryssrutan **Åsidosätt allmänna inställningar**.

Steg 2 Så här aktiverar du trådlöst nätverk för en grupp av telefoner:

a) Välj **Enhet** > **Enhetsinställningar** > **Allmän telefonprofil**.
b) Välj inställningen **Aktiverad** för Wi-Fi-parametern.

OBS! Kontrollera att konfigurationen i det här steget fungerar genom att avmarkera kryssrutan **Åsidosätt allmänna inställningar** som nämns i steg 1d.

c) Markera kryssrutan **Åsidosätt allmänna inställningar**.
d) Associera telefonerna med den allmänna telefonprofilen i **Enhet** > **Telefon**.

Steg 3 Så här aktiverar du trådlöst nätverk för alla WLAN-kompatibla telefoner i nätverket:

a) Välj **System** > **Företagstelefonkonfiguration**.
b) Välj inställningen **Aktiverad** för Wi-Fi-parametern.

OBS! Kontrollera att konfigurationen i det här steget fungerar genom att avmarkera kryssrutan **Åsidosätt allmänna inställningar** som nämns i steg 1d och steg 2c.

c) Markera kryssrutan **Åsidosätt allmänna inställningar**.

Ställa in trådlöst nätverk från telefonen

Innan en Cisco IP-telefon kan ansluta till ett WLAN måste du konfigurera nätverksprofilen för telefonen med lämpliga WLAN-inställningar. Du kan använda menyn **Nätverksinställning** på telefonen för att nå undermenyn **Wi-Fi-klientinställning** och ställa in WLAN-konfigurationen.

OBS! Alternativet **Wi-Fi-klientinställning** visas inte på menyn **Nätverksinställning** när Wi-Fi är inaktiverat i Cisco Unified Communications Manager.

Ytterligare information finns i *Cisco IP-konferenstelefon 8832 driftsättningsguide för WLAN*, som finns här: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html.

Innan du börjar

Konfigurera det trådlösa nätverket från Cisco Unified Communications Manager.

Arbetsordning

Steg 1 Tryck på **Inställningar**.

Steg 2 Välj **Admininställningar** > **Nätverksinställning** > **Wi-Fi-klientinställning**.

Steg 3 Ställ in den trådlösa konfigurationen enligt beskrivningen i tabellen nedan.

Tabell 13. Menyalternativ för Wi-Fi-klientinställning

Alternativ	Beskrivning	Om du vill ändra
Trådlös	Slår på eller av trådlösa radio för en Cisco IP-telefon.	Bläddra till alternativet **Trådlöst** och växlingskontrollen för att ändra inställ mellan På och Av.
Nätverksnamn	Det gör att du kan ansluta till ett trådlöst nätverk med hjälp av fönstret **Välj ett nätverk**. I detta fönster finns det två programstyrda knappar; **Bakåt** och **Övrigt**.	I fönstret **Välj ett nätverk** väljer du d som du vill ansluta till.
Inloggningsåtkomst för Wi-Fi	Fönstret för Wi-Fi-inloggning visas.	Bläddra till alternativet **Inloggningsåt Wi-Fi** och använd växlingskontrollen fö inställningen mellan På/Av.
Ställa in IPv4	På undermenyn för konfiguration av IPv4-installation kan du göra följande: • Aktivera eller inaktivera att telefonen använder den IP-adress som DHCP-servern tilldelar. • Ange IP-adress, nätmask, standardroutrar, DNS-server och alternativa TFTP-servrar manuellt. Mer information om fälten för IPv4-adress finns i tabellen Undermeny för inställning av IPv4.	Bläddra till **IPv4-inställning** och tryc

Alternativ	Beskrivning	Om du vill ändra
Ställa in IPv6	På undermenyn för konfiguration av IPv6-installation kan du göra följande: • Aktivera eller inaktivera telefonen att använda den IPv6-adress som antingen är tilldelad av DHCPv6-servern eller fått SLAAC via en IPv6-aktiverad router. • Ange IPv6-adress, prefixlängd, standardroutrar, DNS-server och alternativa TFTP-servrar manuellt. Mer information om fälten för IPv6-adress finns i tabellen Undermeny för inställning av IPv6.	Bläddra till **IPv6-inställning** och t
MAC-adress	Unik MAC-adress (Media Access Control) för telefonen.	Endast visning. Kan inte konfigure
Domännamn	Namn på DNS-domän där telefonen befinner sig.	Se Ställa in domännamnsfältet, på

Steg 4 Tryck på **Spara** för att göra ändringarna eller tryck på **Återställ** för att ignorera anslutningen.

Ange antalet WLAN-autentiseringsförsök

En begäran om autentisering är en bekräftelse av användarens inloggningsuppgifter. Det inträffar när en telefon som redan har anslutit till ett Wi-Fi-nätverk försöker återansluta till Wi-Fi-servern. Exempel är vid en Wi-Fi-sessionstimeout eller när en Wi-Fi-anslutning avbryts och sedan återupptas.

Du kan konfigurera hur många gånger en trådlös telefon skickar en autentiseringsbegäran till Wi-Fi-servern. Standardantalet försök är 2, men du kan ställa in den här parametern från 1 till 3. Om en telefon misslyckas med autentiseringen uppmanas användaren att logga in igen.

Du kan använda WLAN-autentiseringsförsök för enskilda telefoner, en grupp telefoner eller alla Wi-Fi-telefoner i nätverket.

Arbetsordning

Steg 1 Gå till Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon** och leta reda på telefonen.

Steg 2 Navigera till det produktspecifika konfigurationsområdet och ställ in fältet **WLAN-autentiseringsförsök**.

Steg 3 Välj **Spara**.

Steg 4 Välj **Använd konfig**.

Steg 5 Starta om telefonen.

Aktivera uppmaningsläge för WLAN

Aktivera uppmaningsläge för WLAN-profil 1 om du vill att en användare skall logga in på trådlöst nätverk när deras telefon startas eller återställs.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon**.

Steg 2 Leta reda på telefonen som du ska ställa in.

Steg 3 Navigera till det produktspecifika konfigurationsområdet och ställ in fältet **Uppmaningsläge för WLAN-profil 1** till **Aktivera**.

Steg 4 Välj **Spara**.

Steg 5 Välj **Använd konfig**.

Steg 6 Starta om telefonen.

Ställa in en Wi-Fi-profil med hjälp av Cisco Unified Communications Manager

Du kan konfigurera en Wi-Fi-profil och sedan tilldela profilen på de telefoner som har stöd för Wi-Fi. Profilen innehåller de parametrar som krävs för telefoner för att ansluta till Cisco Unified Communications Manager med Wi-Fi. När du skapar och använder en Wi-Fi-profil behöver du eller dina användare inte konfigurera det trådlösa nätverket för enskilda telefoner.

Wi-Fi-profiler stöds i Cisco Unified Communications Manager version 10.5 (2) eller senare. EAP-FAST, PEAP-GTC och PEAP-MSCHAPv2 stöds i Cisco Unified Communications Manager version 10.0 och senare. EAP-TLS stöds i Cisco Unified Communications Manager 11.0 och senare.

Med en Wi-Fi-profil kan du förhindra eller begränsa ändringar i Wi-Fi-konfigurationen på användarens telefon.

Vi rekommenderar att du använder en säker profil med TFTP-kryptering för att skydda nycklar och lösenord när du använder en Wi-Fi-profil.

När du ställer in telefonerna för autentisering med EAP-FAST, PEAP MSCHAPv2 eller PEAP GTC måste användarna ha enskilda användar-ID:n och lösenord när de loggar in på sina telefoner.

Telefonerna har stöd för endast ett servercertifikat som kan installeras med SCEP eller manuellt, men inte båda metoderna. Telefonerna har inte stöd för TFTP-metoden för installation av certifikat.

Arbetsordning

Steg 1 Öppna Cisco Unified Communications Manager Administration och välj **Enhet** > **Enhetsinställningar** > **Trådlös LAN-profil**.

Steg 2 Klicka på **Lägg till nytt**.

Steg 3 Ställ in följande parametrar i avsnittet **Information för trådlös LAN-profil**:

- **Namn**– ange ett unikt namn för Wi-Fi-profilen. Det här namnet visas på telefonen.
- **Beskrivning**– ange en beskrivning av Wi-Fi-profilen så att du kan urskilja den här profilen från andra Wi-Fi-profiler.

- **Kan ändras av användaren**– välj ett alternativ:
  - **Tillåten**– anger att användaren kan göra ändringar i Wi-Fi-inställningarna på sin telefon. Detta alternativ är valt som standard.
  - **Otillåten**– anger att användaren inte kan göra ändringar i Wi-Fi-inställningarna på sin telefon.
  - **Begränsad**– anger att användaren kan ändra Wi-Fi-användarnamnet och lösenordet på sin telefon. Men användare tillåts inte att göra ändringar i övriga Wi-Fi-inställningar på telefonen.

Steg 4 Ange följande parametrar i avsnittet **Trådlösa inställningar**:

- **SSID (nätverksnamn)**– ange nätverksnamnet som finns tillgängligt användarmiljön som telefonen kan anslutas till. Det här namnet visas i listan över tillgängliga nätverk på telefonen och telefonen kan ansluta till det här trådlösa nätverket.
- **Frekvensband**– alternativen är Auto, 2,4 GHz och 5 GHz. Det här fältet fastställer vilken frekvensbandbredd som den trådlösa anslutningen använder. Om du väljer Auto försöker telefonen använda 5 GHz-band först och använder endast 2,4 GHz-band om 5 GHz inte är tillgängligt.

Steg 5 I avsnittet **Autentiseringsinställningar** anger du **Autentiseringsmetod** till en av följande: EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP och Ingen.

När du har ställt in det här fältet kan du se ytterligare fält som du måste ställas in.

- **Användarcertifikat**– krävs för EAP-TLS-autentisering. Välj **Fabriksinstallerat** eller **Användarinstallerat**. Telefonen kräver ett certifikat som kan installeras antingen automatiskt från SCEP eller manuellt från administrationssidan på telefonen.
- **PSK lösenkod**– krävs för PSK-autentisering. Ange lösenfras på 8–63 ASCII-tecken eller 64 hexadecimala tecken.
- **WEP-nyckel**– krävs för WEP-autentisering. Ange WEP-nyckeln på 40/102 eller 64/128 ASCII- eller hexadecimala tecken.
  - 40/104 ASCII är 5 tecken.
  - 64/128 ASCII är 13 tecken.
  - 40/104 HEX är 10 tecken.
  - 64/128 HEX är 26 tecken.
- **Ange delade inloggningsuppgifter**: krävs för autentisering med EAP-FAST, PEAP-MSCHAPv2 och PEAP-GTC.
  - Om användaren hanterar användarnamn och lösenord kan du lämna fälten **Användarnamn** och **Lösenord** tomma.
  - Om alla användare delar samma användarnamn och lösenord kan du ange informationen i fälten **Användarnamn** och **Lösenord**.
  - Ange en beskrivning i fältet **Lösenordsbeskrivning**.

OBS! Om du måste tilldela unika användarnamn och lösenord för varje användare behöver du skapa en profil till varje användare.

Steg 6 Klicka på **Spara**.

Och sedan då?

Tillämpa WLAN-profilgruppen till en enhetspool (**System** > **Enhetspool**) eller direkt till telefonen (**Enhet** > **Telefon**).

Ställa in en Wi-Fi-grupp med hjälp av Cisco Unified Communications Manager

Du kan skapa en trådlös LAN-profilgrupp och lägga till valfri trådlös LAN-profil i gruppen. Profilgruppen kan sedan tilldelas till telefonen när du ställer in telefonen.

Arbetsordning

Steg 1 Öppna Cisco Unified Communications Manager Administration och välj **Enhet** > **Enhetsinställningar** > **Trådlös LAN-profilgrupp**.

Du kan även definiera en trådlös LAN-profilgrupp från **System** > **Enhetsgrupp**.

Steg 2 Klicka på **Lägg till nytt**.

Steg 3 I avsnittet **Information om trådlös LAN-profilgrupp** anger du ett gruppnamn och beskrivning.

Steg 4 I avsnittet **Profiler för den här trådlösa LAN-profilgruppen** väljer du tillgänglig profil i listan **Tillgängliga profiler** och flyttar den valda profilen till listan **Valda profiler**.

När fler än en trådlös LAN-profil är markerad använder telefonen endast den första trådlösa LAN-profilen.

Steg 5 Klicka på **Spara**.

Kontrollera att telefonen startar

När telefonen har ström startar den automatiskt en startdiagnostikprocess.

Arbetsordning

Slå på telefonen.

När huvudskärmen visas har den startat korrekt.

Ändra en användares telefonmodell

Du eller din användare kan ändra en användares telefonmodell. Ändringen kan krävas av flera orsaker, till exempel:

- Du har uppdaterat Cisco Unified Communications Manager (Unified CM) till en programvaruversion som inte stöder telefonmodellen.
- Användaren vill ha en annan telefonmodell än den aktuella modellen.
- Telefonen måste repareras eller bytas ut.

Unified CM identifierar den gamla telefonen och använder den gamla telefonens MAC-adress för att identifiera den gamla telefonkonfigurationen. Unified CM kopierar den gamla telefonkonfigurationen till posten för den nya telefonen. Den nya telefonen har därmed samma konfiguration som den gamla telefonen.

Begränsning: Om den gamla telefonen har fler linjer eller linjeknappar än den nya telefonen kommer dessa linjer inte att konfigureras på den nya telefonen.

Telefonen startas om när konfigurationen är klar.

Innan du börjar

Ställ in Cisco Unified Communications Manager enligt instruktionerna i *Funktionskonfigurationshandboken för Cisco Unified Communications Manager*.

Du behöver en ny, oanvänd telefon som levereras med förinstallerad version 12.8 (1) av fasta programvaran eller senare.

Arbetsordning

Steg 1 Stäng av den gamla telefonen.

Steg 2 Slå på den nya telefonen.

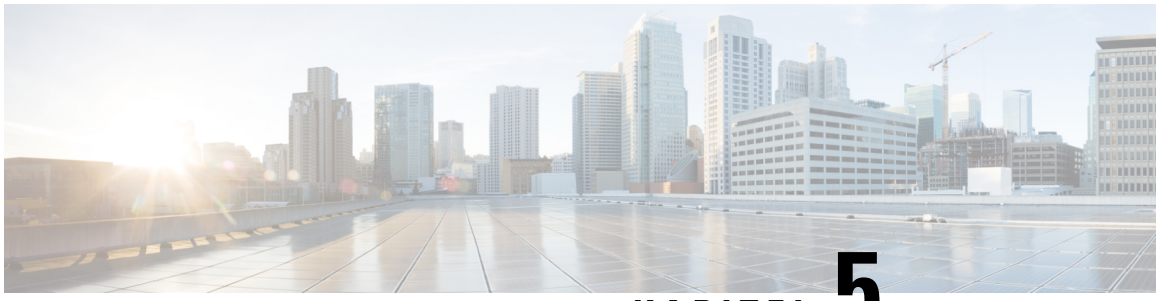
Steg 3 Välj **Ersätt en befintlig telefon** på den nya telefonen.

Steg 4 Ange den gamla telefonens primära anknytning.

Steg 5 Om den gamla telefonen har en PIN-kod anger du samma PIN-kod.

Steg 6 Tryck på **Skicka**.

Steg 7 Om det finns mer än en enhet för användaren markerar du enheten som du ska ersätta och trycker på **Fortsätt**.



KAPITEL 5

Telefoninstallation i Cisco Unified Communications Manager

Konfigurera en Cisco IP-konferenstelefon

Om autoregistrering är inte aktiverat och telefonen finns i Cisco Unified Communications Manager-databasen, måste du konfigurera Cisco IP-telefon i Cisco Unified Communications Manager Administration manuellt. Vissa uppgifter i detta förfarande är valfria, beroende på ditt system och användarnas behov.

Mer information om stegen finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Utför konfigurationsstegen i följande procedur med Cisco Unified Communications Manager Administration.

Arbetsordning

Steg 1 Samla in följande information om telefonen:

- Telefonmodell
- MAC-adress: se Fastställ telefonens MAC-adress, på sidan 59
- Fysiska platsen för telefonen
- Namn eller användar-ID för telefonanvändaren
- Enhetsgrupp
- Partition, samtalssökområde och platsinformation
- Katalognummer som tilldelas telefonen

- Cisco Unified Communications Manager-användaren som ska associeras med telefonen
- Telefonanvändningsinformation som påverkar mallen för programstyrda knappar, telefonens funktioner, IP-telefontjänster eller telefonprogram

Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager och på sidor via relaterade länkar.

Steg 2 Kontrollera att du har tillräckligt med enhetslicenser för din telefon.

För mer information, se licensdokumentet till din utgåva av Cisco Unified Communications Manager.

Steg 3 Definiera Enhetsgrupper. Välj **System** > **Enhetsgrupp**.

Enhetsgrupper definierar gemensamma egenskaper för enheter, till exempel region, datum-/tidgrupp och mall för programstyrda knappar.

Steg 4 Definiera den allmänna telefonprofilen. Välj **Enhet** > **Enhetsinställningar** > **Allmän telefonprofil**

Allmänna telefonprofiler innehåller data som Cisco TFTP-servern kräver, samt gemensamma telefoninställningar som Stör ej och funktionskontrollalternativ.

Steg 5 Definiera ett sökområde för samtal. Gå till Cisco Unified Communications Manager Administration och klicka på **Samtalsdirigering** > **Kontrollklass** > **Sökområde för samtal**.

Ett sökområde för samtal är en samling av partitioner som söks igenom för att avgöra hur ett ringt nummer dirigeras. Enhetens sökområde för samtal och katalognumrets sökområde för samtal används tillsammans. Katalognumrets CSS har företräde framför enhetens CSS.

Steg 6 Konfigurera en säkerhetsprofil för enhetstyp och protokoll. Välj **System** > **Säkerhet** > **Telefonsäkerhetsprofil**.

Steg 7 Ställ in telefonen. Välj **Enhet** > **Telefon**.

a) Leta reda på telefonen du vill ändra eller lägg till en ny telefon.
b) Konfigurera telefonen genom att fylla i de obligatoriska fälten i rutan Enhetsinformation i fönstret Telefonkonfiguration.

- MAC-adress (obligatoriskt): Se till att värdet består av 12 hexadecimala tecken.
- Beskrivning: Ange en användbar beskrivning för att hjälpa dig om du behöver söka efter information om användaren.
- Enhetsgrupp (obligatoriskt)
- Allmän telefonprofil
- Sökområde för samtal
- Plats
- Ägare (användare eller anonym) och om användaren är markerad, ägarens användar-ID

Enheten med standardinställningarna läggs till i Cisco Unified Communications Manager-databasen.

Mer information om produktspecifika konfigurationsfält finns i ”?” Knapphjälp i fönstret Telefonkonfiguration och den relaterade länken.

OBS! Om du vill lägga till både telefonen och användaren i Cisco Unified Communications Manager-databasen samtidigt finns det mer information i dokumentationen till din utgåva av Cisco Unified Communications Manager.

c) Gå till området med protokollspecifik information i detta fönster genom att välja en enhetssäkerhetsprofil och ange säkerhetsläge.

OBS! Välj en säkerhetsprofil baserat på den övergripande säkerhetsstrategin för företaget. Om telefonen inte har stöd för säkerhet, väljer du en osäkrad profil.

d) Gå till området med anknytningsinformation och markera kryssrutan Aktivera Extension Mobility om den här telefonen har stöd för Cisco Extension Mobility.

e) Klicka på **Spara**.

Steg 8 Välj **Enhet** > **Enhetsinställningar** > **SIP-profil** för att konfigurera SIP-parametrar.

Steg 9 Välj **Enhet** > **Telefon** för att konfigurera katalognummer (linjer) på telefonen genom att fylla i de obligatoriska fälten i katalognummerkonfigurationsfönstret.

a) Sök efter telefonen.

b) Gå till telefonkonfigurationsfönstret och klicka på Linje 1 till vänster i fönstret.

Konferenstelefoner har bara en linje.

c) I katalognummer anger du ett giltigt nummer som kan ringas.

OBS! Detta fält bör innehålla samma antal som visas i fältet Telefonnummer i fönstret Slutanvändarkonfiguration.

d) Gå till listrutan Flödespartition och välj partitionen som katalognumret tillhör. Om du inte vill begränsa åtkomsten till katalognumret väljer du <None> för partitionen.

e) Gå till listrutan Sökområde för samtal och välj ett sökområde för samtalet. Det värde som du väljer gäller alla enheter som använder detta katalognummer.

f) Gå till området för inställning av vidarekoppling och samtalshämtning och välj alternativ (till exempel Vidarebefordra alla, Vidarekoppla upptaget internt) och motsvarande destinationer som samtal ska kopplas till.

Exempel:

Om du vill att inkommande interna och externa samtal som får en upptagetton ska vidarekopplas till röstbrevlådan för denna linje, markerar du kryssrutan Röstbrevlåda bredvid Vidarekoppla upptaget internt och Vidarekoppla upptaget externt i den vänstra kolumnen i området för inställning av vidarekoppling och samtalshämtning.

g) Gå till Linje 1 i rutan Enhet och konfigurera följande fält:

- Visning (fält med internt uppringar-ID): Du kan ange förnamn och efternamn på användaren av denna enhet, så att detta namn visas för alla interna samtal. Lämna det här fältet tomt om du vill visa telefonanknytningen i systemet.
- Mask för externt telefonnummer: Ange telefonnummer (eller mask) som används för att skicka nummerpresentationsinformation när ett samtal rings från denna linje. Du kan ange högst 24 siffror och ”X” tecken. X representerar katalognumret och måste finnas i slutet av mönstret.

Exempel:

Om du anger en mask som 408902XXXX och får ett externt samtal från anknytning 6640 visas en nummerpresentation som 4089026640.

Denna inställning gäller endast för den aktuella enheten om du inte markerar kryssrutan till höger (Uppdatera delade enhetsinställningar) och klickar på **Propagera markerade**. Kryssrutan till höger visas bara om andra enheter delar detta katalognummer.

h) Välj **Spara**.

Mer information om katalognummer finns i dokumentationen till din utgåva av Cisco Unified Communications Manager och på sidorna via relaterade länkar.

Steg 10 (Valfritt) Associera användaren med en telefon. Klicka på **Associerade slutanvändare** längst ned i telefonkonfigurationsfönstret för att associera en användare till den linje som konfigureras.

a) Använd **Sök** och sökfälten för att hitta användaren.
b) Markera rutan bredvid användarens namn och klicka på **Lägg till markerade**.

Användarnamnet och användar-ID visas i rutan Användare som associeras med linje i fönstret Katalognummerkonfiguration.

c) Välj **Spara**.

Användaren är nu associerad med Linje 1 på telefonen.

Steg 11 (Valfritt) Associera användaren med enheten:

a) Välj **Användarhantering** > **Slutanvändare**.
b) Använd sökrutorna och **Sök** för att lokalisera användaren du har lagt till.
c) Klicka på användar-ID:et.
d) Gå till området Katalognummerassociationer på skärmen och ställ in Primär anknytning i listrutan.
e) (Valfritt) Gå till området Mobilitetsinformation och markera rutan Aktivera mobilitet.
f) I området med behörighetsinformation kan du använda knapparna **Lägg till i åtkomstkontrollgrupp** om du vill lägga till den här användaren i användargrupper.

Du kanske till exempel vill lägga till användaren i en grupp som definieras som en CCM-standardslutanvändargrupp.

g) Om du vill visa information om en grupp markerar du gruppen och klickar på **Visa detaljer**.
h) Gå till området Extension Mobility och markera rutan Aktivera Extension Mobility Cross Cluster om användaren kan använda tjänsten Extension Mobility Cross Cluster.
i) Gå till området Enhetsinformation och klicka på **Enhetsassociationer**.
j) Använd sökfälten och **Sök** för att hitta den enhet som du vill koppla till användaren.
k) Välj enheten och klicka på **Spara valda/ändringar**.
l) Klicka på **Kör** bredvid den relaterade länken ”Tillbaka till användare” i det övre högra hörnet på skärmen.
m) Välj **Spara**.

Steg 12 Anpassa mallar för funktionsknappar. Välj **Enhet** > **Enhetsinställningar** > **Funktionsknappmall**.

Använd sidan för att lägga till, ta bort eller ändra ordning på funktionsknappar som visas på användarens telefon för att uppfylla användningsbehoven.

Konferenstelefonen har särskilda krav för programstyrda knappar. Se relaterade länkar för mer information.

Steg 13 Konfigurera tjänster för Cisco IP-telefoner och tilldela tjänster. Välj **Enhet** > **Enhetsinställningar** > **Telefontjänster**.

Tillhandahåller IP-telefontjänster i telefonen.

OBS! Användare kan lägga till eller ändra tjänster på sina telefoner med Cisco Unified Communications självbetjäningsportal.

Steg 14 (Valfritt) Lägg till användarinformation i den globala katalogen för Cisco Unified Communications Manager. Välj **Användarhantering** > **Slutanvändare** och klicka sedan på **Lägg till ny** och konfigurera de obligatoriska fälten. Obligatoriska fält är markerade med en asterisk (*).

OBS! Om ditt företag använder en LDAP-katalog (Lightweight Directory Access Protocol) för att lagra information om användare kan du installera och konfigurera Cisco Unified Communications som används med befintliga LDAP-katalog, se Inställning av företagskatalog, på sidan 121. När fältet Aktivera synkronisering från LDAP-server har aktiverats kan du inte lägga till ytterligare användare från Cisco Unified Communications Manager Administration.

a) Ställ in användar-ID och efternamn i motsvarande fält.
b) Ange ett lösenord (för självbetjäningsportalen).
c) Tilldela en PIN-kod (för Cisco Extension Mobility och den personliga katalogen).
d) Associera användaren med en telefon.

Ger användare kontroll över sin telefon med vidarekoppling av samtal eller tillägg av kortnummer eller tjänster.

OBS! Vissa telefoner, till exempel i konferensrum, har inte någon associerad användare.

Steg 15 (Valfritt) Associera en användare med en användargrupp. Välj **Användarhantering** > **Användarinställningar** > **Åtkomstkontrollgrupp**.

Tilldelar användare en gemensam förteckning över roller och behörigheter som gäller för alla användare i en användargrupp. Administratörer kan hantera användargrupper, roller och behörigheter för att kontrollera åtkomstnivån (och därmed säkerhetsnivån) för systemanvändare.

För att slutanvändarna ska få åtkomst till Cisco Unified Communications självbetjäningsportal måste du lägga till användare i standardslutanvändargruppen i Cisco Communications Manager.

Relaterade ämnen

Produktspecifik konfiguration, på sidan 95
Cisco IP-konferenstelefon – funktioner och inställningar, på sidan 91
Dokumentation för Cisco Unified Communications Manager, på sidan 14
Konfigurera en ny mall för programstyrda knappar, på sidan 92

Fastställ telefonens MAC-adress

När du ska lägga till telefoner i Cisco Unified Communications Manager måste du fastställa MAC-adress till telefonen.

Arbetsordning

Gör på något av följande sätt:

- Välj **Inställningar** > **Telefoninformation** på telefonen och titta i MAC-adressfältet.
- Titta på MAC-etiketten på baksidan av telefonen.

- Visa webbsidan för telefonen och klicka på **Enhetsinformation**.

Telefontilläggsmetoder

När du har installerat Cisco IP-telefon kan du välja ett av följande alternativ för att lägga till telefoner i Cisco Unified Communications Manager-databasen.

- Lägga till telefoner individuellt med hjälp av Cisco Unified Communications Manager Administration
- Lägga till flera telefoner med massadministrationsverktyget (BAT)
- Autoregistrering
- BAT och verktyg för stöd av automatisk registrerade telefoner (TAPS)

Innan du lägger till telefoner individuellt eller med BAT behöver du ta reda på telefonens MAC-adress. Mer information finns i Fastställ telefonens MAC-adress, på sidan 59.

Mer information om massadministrationsverktyget finns i dokumentationen till din utgåva av Cisco Unified Communications Manager release.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Lägga till telefoner individuellt

Samla in information om MAC-adressen och telefoninformation för telefonen som du vill lägga till i Cisco Unified Communications Manager.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon**.

Steg 2 Klicka på **Lägg till nytt**.

Steg 3 Välj telefontyp.

Steg 4 Välj **Nästa**.

Steg 5 Fyll i information om telefonen, inklusive MAC-adressen.

För fullständiga instruktioner och begreppsmässig information om Cisco Unified Communications Manager, se dokumentationen till din utgåva av Cisco Unified Communications Manager.

Steg 6 Välj **Spara**.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Lägga till telefoner med BAT-telefonmall

Med Cisco Unified Communications BAT kan du utföra massåtgärder som registrering av flera telefoner.

Om du vill lägga till telefoner endast med BAT (och inte i kombination med TAPS) måste du ha relevanta MAC-adresser till varje telefon.

Mer information om hur du använder BAT finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Arbetsordning

Steg 1 Gå till Cisco Unified Communications Administration och välj **Massadministration** > **Telefoner** > **Telefonmall**.

Steg 2 Klicka på **Lägg till nytt**.

Steg 3 Välj en telefontyp och klicka på **Nästa**.

Steg 4 Ange information om telefonspecifika parametrar som Enhetsgrupp, Telefonknappsmall och Enhetssäkerhetsprofil.

Steg 5 Klicka på **Spara**.

Steg 6 Välj **Enhet** > **Telefon** > **Lägg till ny** för att lägga till en telefon med hjälp av BAT-telefonmallen.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Lägga till användare i Cisco Unified Communications Manager

Du kan visa och underhålla information om användare som är registrerade i Cisco Unified Communications Manager. I Cisco Unified Communications Manager kan även alla användare utföra dessa uppgifter:

- Gå till företagskatalogen och andra anpassade kataloger från en Cisco IP-telefon.
- Skapa en personlig katalog.
- Konfigurera kortnummer och vidarekopplingsnummer.
- Prenumerera på tjänster som är tillgängliga från en Cisco IP-telefon.

Arbetsordning

Steg 1 Om du vill lägga till användare individuellt går du till Lägga till användare direkt i Cisco Unified Communications Manager, på sidan 62.

Steg 2 Om du vill lägga till användare i grupp använder du Verktyg för massadministration. Med den här metoden kan du också ställa in ett identiskt standardlösenord för alla användare.

Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Lägga till en användare från en extern LDAP-katalog

Om du har lagt till en användare till en LDAP-katalog (en icke-Cisco Unified Communications Server katalog), kan du omedelbart synkronisera LDAP-katalogen till Cisco Unified Communications Manager som du lägger till användaren och användaren telefon.

OBS! Om du inte synkronisera LDAP-katalog till Cisco Unified Communications Manager omedelbart, LDAP Directory Synchronization Schedule i LDAP-katalog fönstret avgör när nästa autosynchronization är planerad. Synkronisering måste ske innan du kan associera en ny användare till en enhet.

Arbetsordning

Steg 1 Logga in på Cisco Unified Communications Manager Administration.

Steg 2 Välj **System** > **LDAP** > **LDAP-katalog**.

Steg 3 Använd **Sök** för att hitta LDAP-katalogen.

Steg 4 Klicka på LDAP katalognamn.

Steg 5 Klicka på **Utför full synkronisering nu**.

Lägga till användare direkt i Cisco Unified Communications Manager

Om du inte använder en LDAP-katalog kan du lägga till en användare direkt med Cisco Unified Communications Manager Administration genom att följa dessa steg.

OBS! Om LDAP är synkroniserat kan du inte lägga till en användare med Cisco Unified Communications Manager Administration.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Användarhantering** > **Slutanvändare**.

Steg 2 Klicka på **Lägg till nytt**.

Steg 3 I fönstret Användarinformation anger du följande:

- Användar-ID: Ange slutanvändarens identifieringsnamn. Cisco Unified Communications Manager tillåter inte ändring av användar-ID efter att det har skapats. Du kan använda följande specialtecken: =, +, <, >, #,;, \,, "", och blanksteg. **Exempel**: johndoe

- Lösenord och Bekräfta lösenord: Ange fem eller fler alfanumeriska tecken eller specialtecken för slutanvändarlösenord. Du kan använda följande specialtecken: =, +, <, >, #,;, \,, ””, och blanksteg.
- Efternamn: Ange slutanvändarens efternamn. Du kan använda följande specialtecken: =, +, <, >, #, ;, \, , ””, och blanksteg. **Exempel**: doe
- Telefonnummer: Ange det primära numret till slutanvändaren. Slutanvändare kan ha flera linjer på sina telefoner. **Exempel:**: 26640 (John Does interna företagstelefonnummer)

Steg 4 Klicka på **Spara**.

Lägga till en användare i en slutanvändargrupp

Om du vill lägga till en användare i Cisco Unified Communications Manager Standard-slutanvändargruppen gör du så här:

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Användarhantering** > **Användarinställningar** > **Åtkomstkontrollgrupp**.

Sökfönstret och fönstret Lista användare visas.

Steg 2 Ange lämpliga sökkriterier och klicka på **Sök**.

Steg 3 Välj länken för **CCM-standardslutanvändare**. Fönstret med användargruppskonfigurationen för CCM-standardslutanvändare visas.

Steg 4 Välj **Lägg till användare i slutanvändargrupp**. Fönstret Sök och Lista användare öppnas.

Steg 5 Använd listrutorna med Sök användare för att hitta de användare som du vill lägga till och klicka på **Sök**.

En lista över användare som matchar dina sökkriterier visas.

Steg 6 I listan med poster som visas klickar du i kryssrutan bredvid de användare som du vill lägga till i denna användargrupp. Om listan är lång kan du använda länkarna längst ner för att se fler resultat.

OBS! Listan över sökresultat visar inte användare som redan tillhör användargruppen.

Steg 7 Välj **Lägg till markerade**.

Associera telefoner med användare

Du kan associera telefoner med användare i fönstret Slutanvändare i Cisco Unified Communications Manager.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Användarhantering** > **Slutanvändare**.

Fönstret Sök och Lista användare öppnas.

Steg 2 Ange lämpliga sökkriterier och klicka på **Sök**.

Steg 3 I listan med poster som visas väljer du länken för användaren.

Steg 4 Välj **Enhetsassociation**.

Fönstret Användarenhetsassociation öppnas.

Steg 5 Ange lämpliga sökkriterier och klicka på **Sök**.

Steg 6 Välj den enhet som du vill koppla till användaren genom att markera rutan till vänster på enheten.

Steg 7 Välj **Spara valda/ändringar** för att associera enheten med användaren.

Steg 8 Gå till listrutan Relaterade länkar i övre högra hörnet av fönstret och välj **Tillbaka till användare** och klicka på **Kör**.

Slutanvändarkonfiguration öppnas och tillhörande enheter som du har valt visas i rutan Kontrollerade enheter.

Steg 9 Välj **Spara valda/ändringar**.

Survivable Remote Site Telephony

SRST säkerställer att de grundläggande telefonfunktionerna är tillgängliga om kommunikationen med Cisco Unified Communications Manager bryts. I det här fallet kan telefonen fortsätta med ett pågående samtal och användaren kan få tillgång till en del av de tillgängliga funktionerna. Om en växling inträffar vid fel får användaren ett varningsmeddelande på telefonen.

Det finns mer information om SRST i https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html

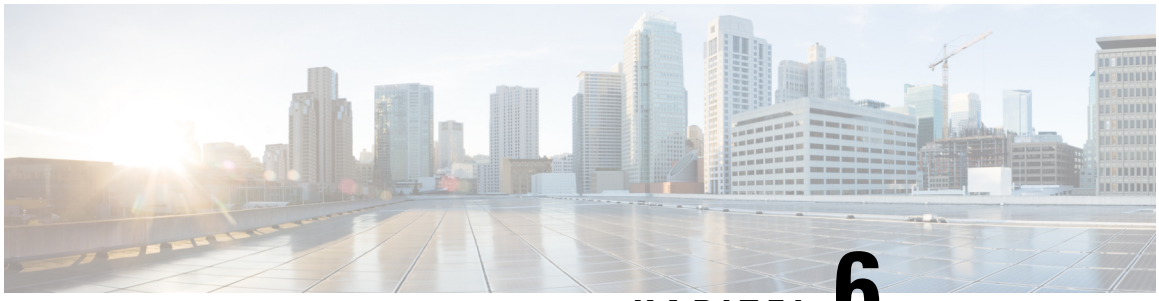
Följande tabell beskriver tillgängliga funktioner under felväxlingen.

Tabell 14. Stöd för SRST-funktioner

Funktion	Stöds	Anteckningar
Nytt samtal	Ja	
Avsluta samtal	Ja	
Ring igen	Ja	
Svara	Ja	
Parkera	Ja	
Återuppta	Ja	

Funktion	Stöds	Anteckningar
Konferenssamtal	Ja	Endast 3-vägs och endast lokal mix.
Konferenslista	Nej	
Överföring	Ja	Endast konsultativa samtal.
Överföring till aktiva samtal (direktöverföring)	Nej	
Autosvar	Ja	
Samtal väntar	Ja	
Samtals-ID	Ja	
Presentation av Unified-session	Ja	Konferens är den enda funktion som stöds på grund av andra funktionsbegränsningar.
Röstmeddelanden	Ja	Röstmeddelanden kommer inte att synkroniseras med andra användare i Cisco Unified Communications Manager-klustret.
Vidarebefordra alla samtal	Ja	Vidarekoppling är endast tillgänglig på telefonen som ställer in vidarekopplingen eftersom det inte finns några synliga delade linjer i SRST-läge. Inställningar för Vidarekoppling av alla funktioner behålls inte vid felväxling till SRST från Cisco Unified Communications Manager eller felåterställning från SRST tillbaka till Communications Manager. Ursprungliga vidarekopplingar av alla samtal som fortfarande är aktiva i Communications Manager anges när enheten återansluts till Communications Manager efter felväxlingen.
Snabbval	Ja	
Till röstbrevlåda (iDivert)	Nej	Den programstyrda knappen iDivert visas inte.
Linjefilter	Delvis	Linjer stöds men kan inte delas.
Parkeringsövervakning	Nej	Den programstyrda knappen Parkera visas inte.
Förbättrad indikation för meddelande väntar	Ja	Indikator för antalet meddelanden visas på telefonskärmen.
Dirigerad parkering av samtal	Nej	Den programstyrda knappen visas inte.
Återställning från förfrågan	Ja	

Funktion	Stöds	Anteckningar
Fjärrparkering	Nej	Samtal visas som lokalt parkerade samtal.
Meet me	Nej	Den programstyrda knappen för Meet Me visas inte.
Hämta	Ja	
Hämta grupp	Nej	Den programstyrda knappen visas inte.
Hämta annan	Nej	Den programstyrda knappen visas inte.
Spårning	Ja	
QRT	Ja	
Svarsgrupp	Nej	Den programstyrda knappen visas inte.
Mobilitet	Nej	Den programstyrda knappen visas inte.
Funktionen Privat	Nej	Den programstyrda knappen visas inte.
Ring igen	Nej	Den programstyrda knappen för att ringa tillbaka visas inte.
Tjänst-URL	Ja	Den programmerbara linjeknappen med en tilldelad tjänst-URL visas inte.



KAPITEL 6

Hantering av självbetjäningsportalen

Översikt över självbetjäningsportalen

I Cisco Unified Communications självbetjäningsportal kan användarna anpassa och styra telefonens funktioner och inställningar.

Som administratör styr du åtkomsten till självbetjäningsportalen. Du måste också ge information till användarna så att de kan få åtkomst till självbetjäningsportalen.

Innan en använare får åtkomst till Cisco Unified Communications självbetjäningsportal, måste du använda Cisco Unified Communications Manager Administration för att lägga till användaren i en standardgrupp för Cisco Unified Communications Manager slutanvändare.

Du måste ge slutanvändare följande information om självbetjäningsportalen:

- URL för att få åtkomst till programmet. Denna URL är:

  `https://<server_name:portnumber>/ucmuser/`, där server_name är värden där webbservern finns installerad och portnumber är portnumret på den värden.

- Ett användar-ID och standardlösenord för att få tillgång till programmet.
- En översikt över de uppgifter som användarna kan utföra med portalen.

Dessa inställningar motsvarar de värden som du angav när du lade till användaren i Cisco Unified Communications Manager.

Mer information finns i dokumentationen till din version av Cisco Unified Communications Manager.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Konfigurera användaråtkomst till självbetjäningsportalen

Innan en användare kan få tillgång till självbetjäningsportalen måste du tillåta åtkomst.

Arbetsordning

Steg 1 I Cisco Unified Communications Manager Administration, välj **användarhantering** > **slutanvändare**.
Steg 2 Sök efter användaren.
Steg 3 Klicka på länken med användar-ID.
Steg 4 Säkerställ att användaren har ett lösenord och PIN-kod har konfigurerats.
Steg 5 Gå till avsnittet med behörighetsinformation och kontrollera att grupplistan innehåller **CCM-standardslutanvändare**.
Steg 6 Välj **Spara**.

Anpassa visningen av självbetjäningsportalen

De flesta alternativ visas i självbetjäningsportalen. Du måste dock ställa in följande alternativ med hjälp av företagsparameterkonfigurationsinställningar i Cisco Unified Communications Manager Administration:

- Visa ringinställningar
- Visa etikettinställningar för linje

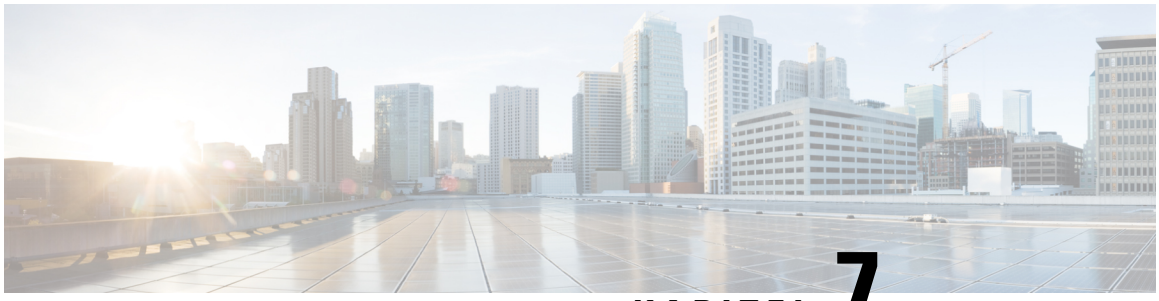
OBS! Inställningarna gäller för alla självbetjäningsportalsidor på din webbplats.

Arbetsordning

Steg 1 Gå till Cisco Unified Communications Manager Administration och välj **System** > **Företagsparametrar**.
Steg 2 Gå till området med självbetjäningsportalen och ställ in fältet **Standardserver för självbetjäningsportal**.
Steg 3 Aktivera eller inaktivera de parametrar som användarna kan nå via portalen.
Steg 4 Välj **Spara**.

DEL III

Administrera Cisco IP-konferenstelefon



KAPITEL 7

Säkerhet för Cisco IP-konferenstelefon

Säkerhetsöversikt för Cisco IP-telefon

Säkerhetsfunktionerna skyddar mot flera hot, bland annat hot mot identiteten på telefonen och data. Dessa funktioner etablerar och upprätthåller autentiserade kommunikationsströmmar mellan telefonen och Cisco Unified Communications Manager-servern och ser till att telefonen använder endast digitalt signerade filer.

Cisco Unified Communications Manager 8.5 (1) och senare inkluderar säkerhet som standard, vilket ger följande säkerhetsfunktioner i Cisco IP-telefon utan att CTL-klienten körs:

- Signering av telefonens konfigurationsfiler
- Kryptering av telefonens konfigurationsfiler
- HTTPS med Tomcat och andra webbtjänster

OBS! Säker signalering och mediafunktioner kräver fortfarande att du kör CTL-klienten och använda maskinvarans eTokens.

Mer information om säkerhetsfunktioner finns i dokumentationen till din Cisco Unified Communications Manager.

Ett LSC-certifikat installeras på telefonerna när du utför de nödvändiga åtgärder som är kopplade till CAPF. Du kan använda Cisco Unified Communications Manager Administration för att konfigurera LSC. Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

En LSC kan inte användas som användarcertifikat för EAP-TLS med WLAN-autentisering.

Alternativt kan du starta installationen av LSC från säkerhetsmenyn på telefonen. På denna meny kan du även uppdatera eller ta bort ett LSC-certifikat.

Cisco IP-konferenstelefon 8832 uppfyller FIPS (Federal Information Processing Standard). För att fungera korrekt kräver FIPS-läget en RSA-nyckelstorlek på 2048 bitar eller mer. Om servercertifikatet RSA inte är 2048 bitar eller mer, kommer telefonen inte att registreras i Cisco Unified Communications Manager och

`telefonen misslyckas med registreringen. Cert-nyckelstorleken är inte FIPS-kompatibel` visas i telefonens statusmeddelanden.

Du kan inte använda privata nycklar (LSC eller MIC) i FIPS-läge.

Om telefonen har en befintlig LSC som är mindre än 2048 bitar, måste du uppdatera LSC-nyckelstorleken till 2 048 bitar eller mer innan du aktiverar FIPS.

Relaterade ämnen

Konfigurera ett LSC-certifikat, på sidan 75
Dokumentation för Cisco Unified Communications Manager, på sidan 14

Säkerhetsförbättringar för telefonens nätverk

Du kan aktivera Cisco Unified Communications Manager 11.5 (1) och 12.0 (1) för att fungera i en förbättrad säkerhetsmiljö. Med dessa förbättringar fungerar telefonen nätverk under ett antal strikta säkerhetskontroller och riskhanteringar för att skydda dig och dina användare.

Cisco Unified Communications Manager 12.5 (1) stöder inte en förbättrad säkerhetsmiljö. Inaktivera FIPS innan du uppgraderar till Cisco Unified Communications Manager 12.5 (1) för att TFTP och andra tjänster ska fungera korrekt.

Förbättrad säkerhetsmiljö innehåller följande funktioner:

- Autentisering av kontaktsökning.
- TCP som standardprotokoll för fjärrgranskningsloggning.
- FIPS-läge.
- En förbättrad policy för inloggningsuppgifter.
- Stöd för SHA-2-serien med grindtecken för digitala signaturer.
- Stöd för RSA-nyckelstorlek på 512 och 4096 bitar.

I Cisco Unified Communications Manager version 14.0 och Cisco IP-telefonens inbyggda programvara version 14.0 finns det stöd för SIP OAuth-autentisering.

OAuth stöds för TFTP (Proxy Trivial File Transfer Protocol) med Cisco Unified Communications Manager version 14.0 (1) SU1 eller senare och fast programvara för Cisco IP-telefon version 14.1 (1). Proxy TFTP och OAuth för proxy TFTP stöds inte på Mobile Remote Access (MRA).

Ytterligare information om säkerhet finns här:

- *Systemkonfigurationshandbok för Cisco Unified Communications Manager*, version 14.0 (1) eller senare (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).
- *Säkerhetshandbok för Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)
- SIP OAuth: *Funktionskonfigurationshandbok för Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)

OBS! Din Cisco IP-telefon kan bara lagra ett begränsat antal ITL-filer. ITL-filerna kan inte överskrida gränsvärdet på 64 K för telefoner och därför måste antalet filer som Cisco Unified Communications Manager skickar till telefonen begränsas.

Säkerhetsfunktioner som stöds

Säkerhetsfunktionerna skyddar mot flera hot, bland annat hot mot identiteten på telefonen och data. Dessa funktioner etablerar och upprätthåller autentiserade kommunikationsströmmar mellan telefonen och Cisco Unified Communications Manager-servern och ser till att telefonen använder endast digitalt signerade filer.

Cisco Unified Communications Manager 8.5 (1) och senare inkluderar säkerhet som standard, vilket ger följande säkerhetsfunktioner i Cisco IP-telefon utan att CTL-klienten körs:

- Signering av telefonens konfigurationsfiler
- Kryptering av telefonens konfigurationsfiler
- HTTPS med Tomcat och andra webbtjänster

OBS! Säker signalering och mediafunktioner kräver fortfarande att du kör CTL-klienten och använda maskinvarans eTokens.

Implementerad säkerhet i Cisco Unified Communications Manager-systemet förhindrar identitetsstöld i telefoner och Cisco Unified Communications Manager-servern, datamanipulering, samtalssignalering och mediströmmanipulering.

Cisco IP-telefoninätverk motverkar hoten genom att etablera och upprätthålla säkra (krypterade) kommunikationsströmmar mellan telefon och server, signera filer digitalt innan de överförs till en telefon och kryptera medieströmmar och samtalssignalering mellan Cisco IP-telefoner.

Ett LSC-certifikat installeras på telefonerna när du utför de nödvändiga åtgärder som är kopplade till CAPF. Du kan använda Cisco Unified Communications Manager Administration för att konfigurera LSC, enligt beskrivningen i säkerhetshandboken för Cisco Unified Communications Manager. Alternativt kan du starta installationen av LSC från säkerhetsmenyn på telefonen. På denna meny kan du även uppdatera eller ta bort ett LSC-certifikat.

En LSC kan inte användas som användarcertifikat för EAP-TLS med WLAN-autentisering.

Telefonerna används med telefonsäkerhetsprofilen, som anger om enheten är osäker eller säker. Mer information om användning av säkerhetsprofilen i telefonen finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Om du konfigurerar säkerhetsrelaterade inställningar i Cisco Unified Communications Manager Administration, innehåller telefonkonfigurationsfilen känslig information. För att säkerställa sekretessen i en konfigurationsfil måste du konfigurera den för kryptering. Mer detaljerad information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Implementerad säkerhet i Cisco Unified Communications Manager-systemet förhindrar identitetsstöld i telefoner och Cisco Unified Communications Manager-servern, datamanipulering, samtalssignalering och mediströmmanipulering.

Följande tabell ger en översikt över de säkerhetsfunktioner som Cisco IP-konferenstelefon 8832 stöder. Mer information om dessa funktioner, Cisco Unified Communications Manager och Cisco IP-telefonsäkerhet finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Tabell 15. Översikt över säkerhetsfunktioner

Funktion	Beskrivning
Bildautentisering	Signerade binära filer (med tillägget .sbn) förhindrar manipula bilden orsakar att en telefon inte godkänns i autentiseringsproc
Installation av kundens arbetsplatscertifikat	Varje telefon kräver ett unikt certifikat för enhetsverifiering. Te du gå till Cisco Unified Communications Manager Administra Proxy Function). Eller så kan du installera ett LSC-certifikat (I
Enhetsautentisering	Sker mellan Cisco Unified Communications Manager-servern o om en säker anslutning mellan telefonen och en Cisco Unified det behövs mellan dessa enheter med hjälp av TLS-protokollet inte kan autentiseras av Cisco Unified Communications Manag
Filautentisering	Validerar digitalt signerade filer som telefonen hämtar. Telefon filen skapades. Filer som inte godkänns vid autentisering skriv bearbetning.
Signaleringsautentisering	Använder TLS-protokollet för att validera att ingen manipuler
Fabriksinstallerade certifikat	Varje telefon innehåller ett unikt fabriksinstallerat certifikatet (identitetsbevis för telefonen och gör det möjligt för Cisco Unif
Säker SRST-referens	När du har konfigurerat en SRST-referens för säkerhet och sed Administration lägger TFTP-servern till SRST-certifikatet i te sedan en TLS-anslutning för att interagera med den SRST-akti
Mediakryptering	Använder SRTP för att säkerställa att mediaströmmarna mella läser data. Här skapas även ett par primärt medianyckelpar för
CAPF (Certificate Authority Proxy funktion)	Implementerar delar av certifikatgenereringsförfarandet som ä nyckelgenereringen och certifikatinstallationen. CAPF kan kon telefonen eller konfigureras för att generera certifikat lokalt.
Säkerhetsprofiler	Anger om telefonen är osäker, autentiserad eller krypterad.
Krypterade konfigurationsfiler	Låter du säkerställa integriteten i telefonens konfigurationsfile
Valfri inaktivering av webbserverfunktioner för en telefon	Du kan förhindra åtkomst till en telefonwebbsida som visar oli
Telefonhärdning	Ytterligare säkerhetsalternativ, som du styr från Cisco Unified • Inaktivera åtkomst till webbsidor för en telefon **OBS!** Du kan visa aktuella inställningar för GARP aktiv

Funktion	Beskrivning
802.1X-autentisering	Telefonen kan använda 802.1X-autentisering för att begära
AES 256-kryptering	Om du är ansluten till Cisco Unified Communications Mar TLS och SIP för signalering och mediakryptering. Då kan te som uppfyller SHA-2-standarder (Secure Hash Algorithm) • För TLS-anslutningar: • TLS_ECDHE_RSA_WITH_AES_256_GCM_S • TLS_ECDHE_RSA_WITH_AES_128_GCM_S • För SRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM Mer information finns i dokumentationen till Cisco Unifie
ECDSA (Elliptic Curve Digital Signature Algorithm)-certifikat	Lade till ECDSA-certifikat i version 11.0 för Cisco Unifie påverkar alla Voice Operating System (VOS)-produkter frå

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Konfigurera ett LSC-certifikat

Den här uppgiften gäller för att ställa in en LSC med autentiseringsmetoden via sträng.

Innan du börjar

Se till att rätt säkerhetskonfiguration används för Cisco Unified Communications Manager och CAPF:

- CTL- eller ITL-filen har ett CAPF-certifikat.
- Kontrollera att CAPF certifikatet har installerats i Cisco Unified Communications Operating System Administration.
- CAPF körs och är konfigurerat.

Mer information om dessa inställningar finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Arbetsordning

Steg 1 Skaffa CAPF-autentiseringskoden som ställdes in när CAPF konfigurerades.

Steg 2 På telefonen väljer du **Inställningar**.

Steg 3 Välj **Admininställningar** > **Säkerhetsinställning**.

OBS! Du kan styra åtkomst till inställningsmenyn med fältet Inställningsåtkomst i fönstret Telefonkonfiguration i Cisco Unified Communications Manager Administration.

Steg 4 Välj **LSC** och tryck på **Välj** eller **Uppdatera**.

Telefonen frågar efter en autentiseringssträng.

Steg 5 Ange autentiseringskoden och tryck på **Skicka**.

Telefonen börjar installera, uppdatera eller ta bort LSC, beroende på hur CAPF är konfigurerat. Under förfarandet visas en serie av meddelanden i LSC-alternativfältet på säkerhetskonfigurationsmenyn så att du kan följa utvecklingen. När proceduren är klar får du ett meddelande om alternativet installerats eller inte installerats på telefonen.

En installation, uppdatering eller borttagning av LSC kan ta lång tid att slutföra.

När telefoninstallationen är klar visas meddelandet `Installerat`. Om telefonen visar `Inte installerat` kanske auktoriseringssträngen är fel eller telefonen kanske inte är aktiverad för uppgradering. Om CAPF-åtgärden raderar LSC visar telefonen `Inte installerad` för att indikera att åtgärden lyckades. CAPF-servern loggar felmeddelanden. Se CAPF-serverdokumentationen för att lokalisera loggarna och förstå innebörden av felmeddelanden.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Aktivera FIPS-läge

Arbetsordning

Steg 1 Gå till Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon** och leta reda på telefonen.

Steg 2 Navigera till det produktspecifika konfigurationsområdet.

Steg 3 Ställ in fältet **FIPS-läge** som Aktiverat.

Steg 4 Välj **Använd konfig**.

Steg 5 Välj **Spara**.

Steg 6 Starta om telefonen.

Säkerhet i telefonsamtal

När säkerhet har implementerats för en telefon kan du identifiera säkra telefonsamtal med hjälp av ikoner på telefonens skärm. Du kan också fastställa om den anslutna telefonen är säker och skyddad beroende på om en säkerhetston spelas upp i början av samtalet.

I ett säkert samtal är all samtalssignalering och alla mediaströmmar krypterade. Ett säkert samtal ger en hög nivå av säkerhet för att ge integritet och sekretess i samtalet. När ett pågående samtal är krypterat ändras samtalsförloppsikonen till höger om samtalslängdstimern på telefonens skärm till följande ikon:  .

OBS! Om samtalet dirigeras genom andra samtalsgrenar än IP, till exempel PSTN, kan samtalet vara osäkert även om det är krypterat inom IP-nätverket och visas med en låsikon.

I ett säkert samtal spelas en säkerhetston upp i början av samtalet för att indikera att den andra anslutna telefonen också tar emot och sänder säkert ljud. Om ditt samtal kopplas till en osäker telefon spelas inte säkerhetstonen upp.

OBS! Säkert samtal stöds mellan två telefoner. Säker konferens, Cisco Extension Mobility och delade linjer kan konfigureras genom en säker konferensbrygga.

När en telefon är konfigurerad som säker (krypterad och pålitlig) i Cisco Unified Communications Manager kan den få status som ”skyddad”. Efter det kan den skyddade telefonen konfigureras för att spela upp en indikeringston i början av ett samtal:

- Skyddad enhet: Om du vill ändra status på en säker telefon till skyddad markerar du kryssrutan Skyddad enhet i telefonkonfigurationsfönstret i Cisco Unified Communications Manager Administration (**Enhet** > **Telefon**).
- Spela upp säkerhetsindikeringston: Om du vill att den skyddade telefonen ska spela upp en indikeringston för säkert eller osäkert läge anger du inställningen Spela upp säkerhetsindikeringston som Sant. Som standard är uppspelning av indikeringston inställt på Falskt. Du ställa in detta alternativ i Cisco Unified Communications Manager Administration (**System** > **Tjänsteparametrar**). Välj servern och sedan Unified Communications Manager-tjänsten. I fönstret Serviceparameterkonfiguration väljer du alternativet i området Funktion – Säkerhetston. Standardvärdet är Falskt.

Identifiering för säkert konferenssamtal

Du kan initiera en säker telefonkonferens och övervaka säkerhetsnivån hos deltagare. En säker telefonkonferens upprättas med hjälp av denna process:

1. En användare initierar konferensen från en säker telefon.
2. Cisco Unified Communications Manager tilldelar en säker konferensbrygga till samtalet.
3. När deltagare läggs till verifierar Cisco Unified Communications Manager säkerhetsläget för varje telefon och upprätthåller en säker nivå för konferensen.
4. Telefonen visar säkerhetsnivån på telefonkonferensen. En säker konferens visas med säkerhetsikonen till höger om **Konferens** på telefonens skärm.

OBS! Säkert samtal stöds mellan två telefoner. För skyddade telefoner är vissa funktioner som konferenssamtal, delade linjer och Extension Mobility (anknytningsmobilitet) inte tillgängliga när säkra samtal har konfigurerats.

Följande tabell ger information om ändringar av konferenssäkerhetsnivåer beroende på säkerhetsnivån i konferensorganisatörens telefon och säkerhetsnivåer hos deltagarna, och tillgången till säkra konferensbryggor.

Tabell 16. Säkerhetsbegränsningar vid konferenssamtal

Säkerhetsnivå i organisatörens telefon	Använd funktion	Säkerhetsnivå hos deltagarna	Resultat av åtgärder
Osäker	Konferens	Säkert	Osäker konferensbrygga Osäker konferens
Säkert	Konferens	Minst en medlem är otillförlitlig.	Säker konferensbrygga Osäker konferens
Säkert	Konferens	Säkert	Säker konferensbrygga Säker krypterad konferensnivå
Osäker	Meet me	Minimal säkerhetsnivå är krypterad.	Organisatören får meddelandet `Uppfyller säkerhetsnivå, samtal avvisas.`
Säkert	Meet me	Minimal säkerhetsnivå är osäker.	Säker konferensbrygga Konferensen tar emot alla samtal.

Identifiering för säkert telefonsamtal

Ett säkert samtal upprättas när din telefon och telefonen i den andra änden har konfigurerats för säkert samtal. Den andra telefonen kan finnas i samma Cisco IP-nätverk eller i ett nätverk utanför IP-nätverket. Säkra samtal kan endast göras mellan två telefoner. Konferenssamtal bör ha stöd för säkert samtal efter inställning av en säker konferensbrygga.

Ett säkert samtal upprättas med hjälp av denna process:

1. En användare initierar samtal från en säker telefon (skyddat säkerhetsläge).
2. Säkerhetsikonen visas på telefonens skärm. Denna ikon indikerar att telefonen är konfigurerad för säkra samtal, men det betyder inte att den andra anslutna telefonen också är säkrad.
3. Användaren hör en säkerhetston om samtalet kopplas till en annan säker telefon, vilket betyder att båda ändar av konversationen är krypterade och säkra. Om samtalet kopplas till en osäker telefon hör inte användaren någon säkerhetston.

OBS! Säkert samtal stöds mellan två telefoner. För skyddade telefoner är vissa funktioner som konferenssamtal, delade linjer och Extension Mobility (anknytningsmobilitet) inte tillgängliga när säkra samtal har konfigurerats.

Endast skyddade telefoner spelar upp toner vid säkert eller osäkert samtal. I oskyddade telefoner hörs inga toner. Om den övergripande samtalsstatusen ändras under samtalet ändras också indikationstonen och den skyddade telefonen spelar upp en lämplig ton.

I en skyddad telefon kan en ton spelas upp eller inte spelas upp under dessa omständigheter:

- När alternativet Spela upp säkerhetsindikeringston har aktiverats:

- När säker anslutning har etablerats i båda ändar och samtalsstatusen är säker spelar telefonen upp en säkerhetsindikation (tre långa pip med pauser).
- Om en osäker anslutning har etablerats och samtalsstatusen är osäker spelar telefonen upp en osäkerhetsindikation (sex korta pip med korta pauser).

Om alternativet Spela upp säkerhetsindikeringston är inaktiverat spelas ingen ton upp.

Tillhandahålla kryptering för inbrytning

Cisco Unified Communications Manager kontrollerar telefonens säkerhetsstatus när konferenssamtal har etablerats och ändrar säkerhetsindikeringen för konferenssamtalet eller blockerar slutförandet av det för att bibehålla integritet och säkerhet i systemet.

En användare kan inte bryta in i ett krypterat samtal om telefonen som används vid inbrytning inte har konfigurerats för kryptering. När inbrytning i det här fallet misslyckas hörs en felton (spärrton) på telefonen som inbrytningen initierades från.

Om initiatortelefonen har konfigurerats för kryptering kan inbrytningsinitiatorn bryta in i ett osäkert samtal från den krypterade telefonen. När inbrytningen har inträffat klassificeras samtalet som osäkert i Cisco Unified Communications Manager.

Om initiatortelefonen har konfigurerats för kryptering kan inbrytningsinitiatorn bryta in i ett krypterat samtal och telefonen indikerar då att samtalet är krypterat.

WLAN-säkerhet

Eftersom alla WLAN-enheter som finns inom räckvidd kan ta emot all övrig WLAN-trafik är det nödvändigt att säkra röstkommunikation i WLAN. För att säkerställa att inkräktare inte manipulerar eller stoppar rösttrafiken har säkerhetsarkitekturen Cisco SAFE stöd för Cisco IP-telefon och Cisco Aironets AP:er. Mer information om säkerhet i nätverk finns i http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

Ciscos lösning för trådlös IP-telefoni ger säkerhet för trådlösa nätverk som förhindrar obehöriga inloggningar och komprometterad kommunikation med hjälp av följande autentiseringsmetoder som den trådlösa Cisco IP-telefon stöder:

- Öppen autentisering: Alla trådlösa enheter kan begära autentisering i ett öppet system. Åtkomstpunkten som tar emot begäran kan medge autentisering för alla begäranden eller bara för de begäranden som finns med i en lista över användare. Kommunikationen mellan åtkomstpunkt och trådlösa enheter kan vara okrypterad eller så kan enheter användas med WEP (Wired Equivalent Privacy) som säkerhet. Enheter som använder WEP gör endast försök att autentiseras med en åtkomstpunkt som använder WEP.
- Utbyggbar protokollflexibel autentisering via säker tunnelautentisering (EAP-FAST): Den här serverarkitekturen har säkerhet för klienten där EAP-transaktioner krypteras inom en TLS (Transport Level Security)-tunnel mellan åtkomstpunkten och RADIUS-servern, till exempel Cisco ACS (Access Control Server).

  TLS-tunneln använder skyddad PAC (Protected Access Credentials) för autentisering mellan klienten (telefonen) och RADIUS-servern. Servern skickar ett utfärdar-ID till klienten (telefon), som i sin tur väljer lämpligt PAC. Klienten (telefonen) returnerar ett PAC-täckande till RADIUS-servern. Servern dekrypterar PAC med den primära nyckeln. Båda slutpunkterna har nu PAC-nyckeln och en TLS-tunnel skapas. EAP-FAST stöder automatisk PAC-etablering, men du måste aktivera den på RADIUS-servern.

OBS! I Cisco ACS upphör PAC att gälla inom en vecka som standard. Om telefonen har en utgången PAC, tar autentisering med RADIUS-servern längre tid när telefonen får ett nytt PAC. För att undvika fördröjningar i PAC-etableringen kan du sätta PAC-utgångstiden till 90 dagar eller längre på ACS- eller RADIUS-servern.

- Autentisering via EAP-TLS (Extensible Authentication Protocol-Transport Layer Security): EAP-TLS kräver ett klientcertifikat för autentisering och nätverksåtkomst. För kabelanslutna EAP-TLS kan klientcertifikatet vara antingen telefonens MIC eller en LSC. LSC är det rekommenderade certifikatet för klientautentisering vid kabelanslutet EAP-TLS.
- Skyddat PEAP (Extensible Authentication Protocol): Ciscos tillverkarspecifika lösenordsbaserade och växelvisa autentiseringsschema mellan klient (telefon) och RADIUS-server. Cisco IP-telefon kan använda PEAP för autentisering med det trådlösa nätverket. Endast PEAP-MSCHAPV2 stöds. PEAP-GTC stöds inte.

Följande autentiseringsscheman använder RADIUS-servern för att hantera autentiseringsnycklar:

- WPA/WPA2: Använder RADIUS serverinformation för att skapa unika nycklar för autentisering. Eftersom de här nycklarna har genererats på den centrala RADIUS-servern ger WPA/WPA2 högre säkerhet än i förväg delade WPA-nycklar som lagras på åtkomstpunkten och telefonen.
- Säker och snabb roaming: Används med RADIUS-server och information om trådlös domänserver vid hantering och autentisering av nycklar. WDS skapar en cache med säkerhetsreferenser för CCKM-aktiverade klientenheter som ger snabb och säker omautentisering. Cisco IP-telefon 8800-serien stöder 802.11r (FT). Både 11r (FT) och CCKM stöds om du vill tillåta säker och snabb roaming. Cisco rekommenderar starkt att använda luftburen metid via 802.11r (FT).

Med WPA/WPA2 och CCKM anges inte krypteringsnycklarna på telefonen, de härleds automatiskt mellan AP och telefonen. Men EAP-användarnamn och lösenord som används för autentisering måste anges på respektive telefon.

För att säkerställa rösttrafiken har Cisco IP-telefon stöd för WEP, TKIP och AES (Advanced Encryption Standards) för kryptering. När dessa mekanismer används för kryptering, krypteras både signaleringsbaserat SIP-paket och röstbaserat RTP-paket (Real-Time Transport Protocol) mellan åtkomstpunkten och Cisco IP-telefon.

WEP

Med WEP-användning i det trådlösa nätverket sker autentisering vid åtkomstpunkten med hjälp av öppen eller delad nyckelautentisering. WEP-nyckeln som har ställts in på telefonen måste matcha WEP-nyckeln som har konfigurerats på åtkomstpunkten för godkända anslutningar. Cisco IP-telefon har stöd för WEP-nycklar som använder 40-bitarskryptering eller 128-bitarskryptering och är statisk på telefonen och åtkomstpunkten.

EAP- och CCKM-autentisering kan använda WEP-nycklar för kryptering. RADIUS-servern hanterar WEP-nyckeln och skickar en unik nyckel till åtkomstpunkten efter autentisering för kryptering av alla röstpaket. Det innebär att dessa WEP-nycklar kan ändras vid varje autentisering.

TKIP

WPA och CCKM använder TKIP-kryptering som har flera förbättringar jämfört med WEP. TKIP ger paketvisa nyckelchiffer och längre initieringsvektorer (IV) som stärker krypteringen. Dessutom kan ett

MIC (Message Integrity check) säkerställa att krypterade paket inte ändras. TKIP tar bort förutsägbarheten i WEP som hjälper inkräktare att dechiffrera WEP-nyckeln.

AES

En krypteringsmetod som används för WPA2-autentisering. Denna nationella standard för kryptering använder en symmetrisk algoritm som har samma nyckel för kryptering och dekryptering. AES använder CBC (Cipher Blocking Chain)-kryptering i 128 bitar, som stöder nyckelstorlekar som är minst 128, 192 och 256 bitar. Cisco IP-telefon stöder en nyckelstorlek på 256 bitar.

OBS! Cisco IP-telefon har inte stöd för Cisco CKIP (Key Integrity Protocol) med CMIC.

Autentiserings- och krypteringsscheman ställs in i det trådlösa nätverket. VLAN konfigureras i nätverket och på åtkomstpunkterna, och anger olika kombinationer av autentisering och kryptering. Ett SSID kan kopplas till ett VLAN och valt autentiserings- och krypteringsschema. För lyckad autentisering av trådlösa klientenheter måste du konfigurera samma SSID:n med respektive autentiserings- och krypteringsscheman på åtkomstpunkterna och på Cisco IP-telefon.

Vissa autentiseringsscheman kräver en viss typ av kryptering. Med öppen autentisering kan du använda statisk WEP för kryptering som ger ökad säkerhet. Men om du använder delad nyckelautentisering måste du ange statisk WEP för kryptering och du måste konfigurera en WEP-nyckel på telefonen.

OBS!

- När du använder förinställd delad nyckel för WPA eller WPA2 måste den anges statiskt på telefonen. De här nycklarna måste matcha nycklarna som finns på åtkomstpunkten.
- Cisco IP-telefon stöder inte EAP-autobalansering. Om du vill använda EAP-FAST-läge måste du ange det.

Följande tabell visar alla scheman för autentisering och kryptering som finns konfigurerade på Cisco Aironets åtkomstpunkter som har stöd för Cisco IP-telefon. Tabellen visar alternativet för nätverkskonfiguration för den telefon som motsvarar åtkomstpunktens konfiguration.

Tabell 17. Autentiserings- och krypteringsscheman

Konfiguration av Cisco IP-telefon	**Konfiguration av åtkomstpunkten**			
Säkerhetsläge	Säkerhet	Nyckelhantering	Kryptering	Snabb roaming
Ingen	Ingen	Ingen	Ingen	Saknas
WEP	Statisk WEP	Fast	WEP	Saknas
PSK	PSK	WPA	TKIP	Ingen
		WPA2	AES	FT

Konfiguration av Cisco IP-telefon	Konfiguration av åtkomstpunkten			
EAP-FAST	EAP-FAST	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Mer information om hur du konfigurerar autentiserings- och krypteringsscheman på åtkomstpunkter finns i *Konfigurationshandbok för Cisco Aironet* för din modell och version på följande webbadress:

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

Säkerhet för trådlöst LAN

Cisco-telefoner som har stöd för Wi-Fi har flera säkerhetskrav och kräver ytterligare konfiguration. Följande extra steg inbegriper att installera certifikat och konfigurera säkerheten på telefonerna och i Cisco Unified Communications Manager.

Mer information finns i *Säkerhetshandboken till Cisco Unified Communications Manager*.

Administrationssida för Cisco IP-telefon

Ciscos telefoner som har stöd för Wi-Fi har särskilda webbsidor som skiljer sig från andra telefoners sidor. Du kan använda de specialwebbsidorna för att konfigurera telefonens säkerhet när SCEP (Simple Certificate Enrollment Protocol) inte är tillgängligt. Använd de här sidorna manuellt för att manuellt installera säkerhetscertifikat på en telefon, för att hämta ett säkerhetscertifikat eller för att manuellt konfigurera telefonens datum och tid.

Webbsidorna visar även samma information som du ser på andra telefoners sidor, bland annat enhetsinfo, nätverkskonfguration, loggar och statistisk information.

Konfigurera administrationssidan för telefon

Administrationswebbsidan aktiveras när telefonen levereras från fabriken och lösenordet är ”Cisco”. Men om en telefon registreras i Cisco Unified Communications Manager måste administrationswebbsidan vara aktiverad och ha ett nytt lösenord.

Aktivera den här webbsidan och ange inloggningsuppgifterna innan du använder sidan för första gången när telefonen har registrerats.

När administrationswebbsidan är aktiverad är den tillgänglig på HTTPS-porten 8443 (`https://x.x.x.x:8443`, där x.x.x.x är en IP-adress på telefonen).

Innan du börjar

Bestäm ett lösenord innan du aktiverar administrationswebbsidan. Lösenordet kan innehålla en kombination av bokstäver och siffror, och måste vara mellan 8 och 127 tecken långt.

Ditt användarnamn anges permanent till admin.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon**

Steg 2 Leta reda på din telefon.

Steg 3 I **avsnittet Layout för produktspecifik konfiguration** anger du parametern för **Webbadministration** till **Aktivera**.

Steg 4 I fältet **Adminlösenord** anger du ett lösenord.

Steg 5 Välj **Spara** och klicka på **OK**.

Steg 6 Välj **Använd konfig** och klicka på **OK**.

Steg 7 Starta om telefonen.

Öppna webbsidan för telefonadministration

När du vill ha åtkomst till administrationswebbsidorna måste du ange administrationsporten.

Arbetsordning

Steg 1 Hämta telefonens IP-adress:

- Gå till Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon** och leta reda på telefonen. Telefoner som registrerar med Cisco Unified Communications Manager visar IP-adressen i fönstret **Sök och lista telefoner** och högst upp i fönstret **Telefonkonfiguration**.

Steg 2 Öppna en webbläsare och ange följande URL, där *IP_address* är IP-adressen till Cisco IP-telefon:

`https://<IP_address>:8443`

Steg 3 Ange lösenordet i fältet Lösenord.

Steg 4 Klicka på **Skicka**.

Installera ett användarcertifikat från webbsidan för telefonadministration

Du kan installera ett certifikat manuellt på telefonen om SCEP (Simple Certificate Enrollment Protocol) inte är tillgängligt.

Förinstallerat MIC (Manufacturing Installed Certificate) kan användas som användarcertifikat för EAP-TLS.

När användarcertifikatet är installerat måste du lägga till det i listan över betrodda på RADIUS-servern.

Innan du börjar

Innan du kan installera ett användarcertifikat för en telefon måste du ha:

- Ett användarcertifikat sparas på datorn. Certifikatet måste ha ett PKCS #12-format.
- Certifikatets extraheringslösenord.

Arbetsordning

Steg 1 På webbsidan för telefonadministration väljer du **Certifikat**.
Steg 2 Bläddra till certifikatet på datorn.
Steg 3 Ange certifikatets extraheringslösenord i fältet **Extraheringslösenord**.
Steg 4 Klicka på **Överför**.
Steg 5 Starta om telefonen när överföringen är klar.

Installera ett servercertifikat för autentisering från webbsidan för telefonadministration

Du kan manuellt installera ett certifikat från autentiseringsservern på telefonen om SCEP (Simple Certificate Enrollment Protocol) inte är tillgängligt.

Det rot-CA-certifikat som utfärdade RADIUS-servercertifikatet måste installeras för EAP-TLS.

Innan du börjar

Innan du kan installera ett certifikat på en telefon, måste du ha ett certifikat från autentiseringsservern sparat på datorn. Certifikatet måste vara kodat i PEM (Base-64) eller DER.

Arbetsordning

Steg 1 På webbsidan för telefonadministration väljer du **Certifikat**.
Steg 2 Leta upp fältet **Autentiseringsserver CA (adminwebbsida)** och klicka på **Installera**.
Steg 3 Bläddra till certifikatet på datorn.
Steg 4 Klicka på **Överför**.
Steg 5 Starta om telefonen när överföringen är klar.

Om du installerar fler än ett certifikat kan du installera alla certifikat innan du startar om telefonen.

Ta bort ett säkerhetscertifikat manuellt från webbsidan för telefonadministration

Du kan manuellt ta bort ett säkerhetscertifikat från en telefon om SCEP (Simple Certificate Enrollment Protocol) inte är tillgängligt.

Arbetsordning

Steg 1 På webbsidan för telefonadministration väljer du **Certifikat**.

Steg 2 Leta reda på certifikatet på sidan **Certifikat**.

Steg 3 Klicka på **Ta bort**.

Steg 4 Starta om telefonen när borttagningen är klar.

Ange telefonens datum och tid manuellt

Med certifikatbaserad autentisering måste telefonen visa rätt datum och tid. En autentiseringsserver kontrollerar telefonens datum och tid mot certifikatets utgångsdatum. Om telefonens och serverns datum och tider inte stämmer överens slutar telefonen att fungera.

Använd denna procedur för att manuellt ställa in datum och tid på telefonen om telefonen inte får rätt information från nätverket.

Arbetsordning

Steg 1 På webbsidan för telefonadministration bläddrar du till **Datum och tid**.

Steg 2 Gör på något av följande sätt:

- Klicka på **Ställ in telefonen på lokalt datum och tid** för att synkronisera telefonen med en lokal server.
- I fälten **Specificera datum och tid** väljer du månad, dag, år, timmar, minuter och sekunder med hjälp av menyerna. Klicka sedan på **Ställ in telefonen på specifikt datum och tid**.

SCEP-konfiguration

SCEP (Simple Certificate Enrollment Protocol) är standarden för automatisk etablering och förnyelse av certifikat. Den undviker manuell installation av certifikat på telefonen.

Konfigurera de produktspecifika SCEP-parametrarna

Du måste konfigurera följande SCEP-parametrar på din telefonwebbsida

- RA IP-adress
- SHA-1 eller SHA-256 fingeravtryck för rot-CA-certifikatet i SCEP-servern

Cisco IOS-registreringsmyndigheten (RA) fungerar som en proxy för SCEP-servern. Parametrarna som hämtas från Cisco Unified Communications Manager används av SCEP-klienten för telefonen. När du har konfigurerat parametrarna skickar telefonen en `SCEP getcs`-begäran till RA och rot-CA-certifikatet valideras med definierat fingeravtryck.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon**

Steg 2 Lokalisera telefonen.

Steg 3 Bläddra till området **Produktspecifik konfigurationslayout**.

Steg 4 Markera kryssrutan **WLAN SCEP-server** om du vill aktivera SCEP-parametern.

Steg 5 Markera kryssrutan **WLAN rot-CA-fingeravtryck (SHA256 eller SHA1)** om du vill aktivera parametern SCEP QED.

Serversupport för SCEP (Simple Certificate Enrollment Protocol)

Om du använder en SCEP (Simple Certificate Enrollment Protocol)-server kan den automatiskt behålla dina användar- och servercertifikat. Konfigurera RA (Registration Agent) på SCEP-servern:

- Fungera som betrodd punkt för PKI
- Fungera som PKI RA
- Utföra enhetsautentisering med hjälp av en RADIUS-server

Mer information finns i dokumentationen som hör till SCEP-servern.

802.1x-autentisering

Cisco IP-telefon stöder 802.1X-autentisering.

Cisco IP-telefoner och Cisco Catalyst-växlar använder traditionellt Ciscos CDP-protokoll för att identifiera varandra och fastställa parametrar som VLAN-tilldelning och interna strömbehov.

Stödet för 802.1X-autentisering kräver flera komponenter:

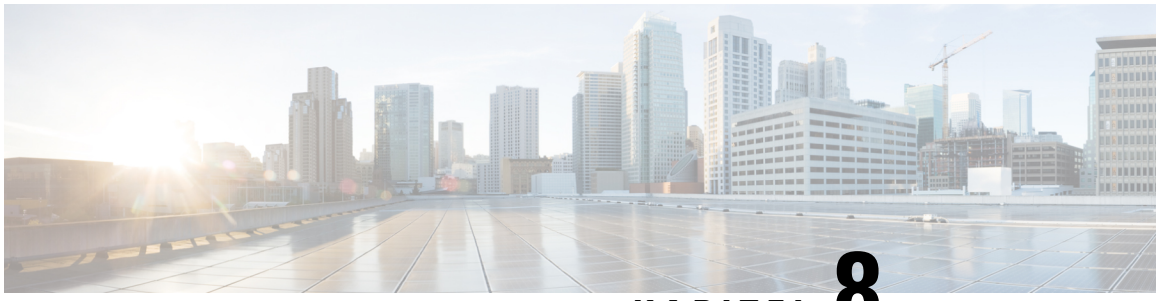
- Cisco IP-telefon: Telefonen initierar begäran om att få tillgång till nätverket. Telefoner innehåller en 802.1X-supplikant. Supplikanten tillåter att nätverksadministratörer kan styra uppkoppling av IP-telefoner till LAN-växelportar. I den aktuella versionen av telefonens 802.1X-supplikant används EAP-FAST och EAP-TLS för nätverksautentisering.
- Cisco Catalyst-växeln (eller en annan tredjepartsväxel): Växeln måste stödja 802.1X, så den kan fungera för auktorisering och överföra meddelanden mellan telefonen och autentiseringsservern. När utväxlingen är klar beviljar eller nekar växeln åtkomst till nätverket för telefonen.

Du måste utföra följande åtgärder för att konfigurera 802.1X.

- Konfigurera de andra komponenterna innan du aktiverar 802.1X-autentisering på telefonen.
- Konfigurera röst-VLAN: Eftersom 802.1X-standarden inte tar hänsyn till VLAN, bör du konfigurera den här inställningen baserat på växelstöd.
  - Aktiverat: Om du använder en växel som stöder multidomänautentisering kan du fortsätta att använda röst-VLAN.
  - Inaktiverat: Om växeln inte stöder multidomänautentisering inaktiverar du röst-VLAN och överväg sedan att tilldela porten till det inbyggda VLAN-nätet.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14



KAPITEL 8

Anpassa Cisco IP-konferenstelefon

Anpassade ringsignaler

Cisco IP-telefonen levereras med två standardringsignaler som implementerats i maskinvaran: Chirp1 och Chirp2. Cisco Unified Communications Manager ger också en standarduppsättning av ytterligare ringsignaler som implementeras i programvaran som pulskodmoduleringsfiler (PCM). PCM-filer, tillsammans med en XML-fil som beskriver ringlistalternativ som finns tillgängliga på webbplatsen, finns i TFTP-katalogen på varje Cisco Unified Communications Manager-server.

Observera Alla filnamn är skiftlägeskänsliga. Om du anger filnamnet med fel skiftläge tillämpas inte ändringarna i telefonen.

Mer information finns i kapitlet Anpassade ringsignaler och bakgrunder i Handbok om konfigurering av funktioner i Cisco Unified Communications Manager.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Konfigurera anpassad telefonringning

Arbetsordning

Steg 1 Skapa en PCM-fil för varje anpassad ringning (en ringning per fil).

Se till att PCM-filerna överensstämmer med de formatriktlinjer som anges i avsnittet om filformat för anpassad ringning.

Steg 2 Ladda upp nya PCM-filer som du har skapat till Cisco TFTP-servern för varje Cisco Unified Communications Manager i klustret.

Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Steg 3 Spara dina ändringar och stäng Ringlist-wb-filen.

Steg 4 Om du vill cachelagra den nya Ringlist-wb-filen:

- Stoppa och starta TFTP-tjänsten med hjälp av Cisco Unified Serviceability
- Inaktivera och återaktivera TFTP-tjänstparametern ”Aktivera cachning av konstant och binfiler vid start” i området Avancerade serviceparametrar.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Filformat för anpassad ringning

I Ringlist-wb.xml-filen definieras ett XML-objekt som innehåller en lista över telefonringningstyper. Den här filen innehåller upp till 50 ringtyper. Varje ringningstyp innehåller en pekare till PCM-filen som används för ringningstypen och den text som visas på ringningstypmenyn på en Cisco IP-telefon för ringningssignalen. Cisco TFTP-servern för varje Cisco Unified Communications Manager innehåller den här filen.

CiscoIPPhoneRinglist XML-objektet använder följande enkla tagguppsättning för att beskriva informationen:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRingList>
```

Följande gäller för definitionsnamnen. Du måste inkludera DisplayName och FileName för varje telefonringningstyp.

- DisplayName anger namnet på den anpassade ringningen för den associerade PCM-filen som visas på Ringningstyp-menyn i Cisco IP-telefon.
- FileName anger namnet på PCM-filen för den anpassade ringningen som ska associeras med DisplayName.

OBS! Fälten DisplayName och FileName får inte överskrida 25 tecken.

Detta exempel visar en Ringlist-wb.xml-fil som definierar två telefonringningstyper:

```
<CiscoIPPhoneRingList>
 <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.rwb</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.rwb</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

PCM-filerna för ringningarna måste uppfylla följande krav för att spelas upp rätt på Cisco IP-telefon:

- Raw PCM (ingen rubrik)
- 8 000 samplingar per sekund

- 8 bitar per sampel
- Mu-law-komprimering
- Max ringningsstorlek = 16 080 samplingar
- Minsta ringningsstorlek = 240 samplingar
- Antal samplingar i ringningen = multipel av 240.
- Ringningen börjar och slutar vid nollgenomgång.

Om du vill skapa PCM-filer för anpassad ringning använder du ett vanligt ljudredigeringspaket som stöder dessa filformat.

Anpassa kopplingstonen

Du kan ställa in dina telefoner så att användarna höra olika kopplingstoner för interna och externa samtal. Beroende på dina behov kan du välja mellan tre kopplingstoner:

- Standard: Olika kopplingstoner för interna och externa samtal.
- Intern: Internkopplingstonen används för alla samtal.
- Extern: Externkopplingstonen används för alla samtal.

Använd alltid kopplingston är ett obligatoriskt fält i Cisco Unified Communications Manager.

Arbetsordning

Steg 1 Gå till Cisco Unified Communications Manager Administration och välj **System** > **Tjänsteparametrar**.

Steg 2 Välj lämplig server.

Steg 3 Välj **Cisco Callmanage** som tjänst.

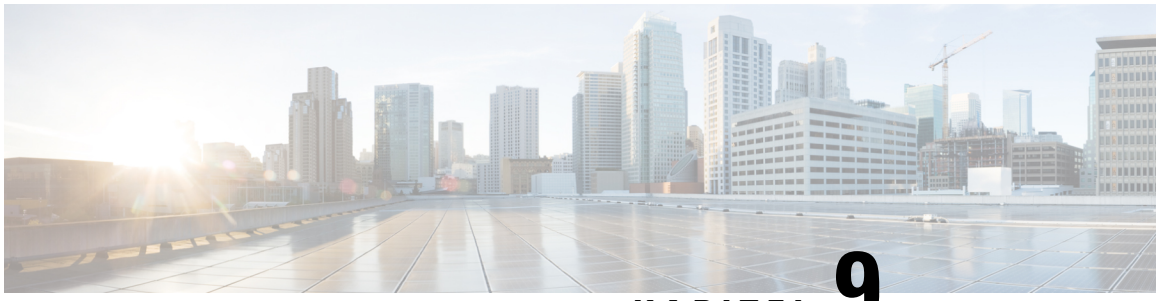
Steg 4 Rulla till rutan Clusterwide parametrar.

Steg 5 Ange **Använd alltid kopplingston** som något av följande:

- Extern
- Intern
- Standard

Steg 6 Välj **Spara**.

Steg 7 Starta om din telefon.



KAPITEL 9

Cisco IP-konferenstelefon – funktioner och inställningar

Stöd för Cisco IP-telefon-användare

Om du är en systemadministratör är du sannolikt den främsta informationskällan för Cisco IP-telefon-användare i nätverket eller på företaget. Det är viktigt att tillhandahålla aktuell och utförlig information till slutanvändare.

Innan det går att använda några av funktionerna på en Cisco IP-telefon (inklusive tjänster och röstmeddelandesystemets alternativ) måste användarna få information från dig eller från nätverksteamet eller måste kunna kontakta dig för att få hjälp. Se till att förse användare med namn på personer att kontakta för att få hjälp och instruktioner för att kontakta dem.

Vi rekommenderar att du skapar en webbsida på din interna supportwebbplats som ger slutanvändare viktig information om deras Cisco IP-telefon.

Överväga att ta med följande typer av information om denna webbplats:

- Användarhandböcker till alla Cisco IP-telefon-modeller som du stöder
- Information om åtkomst till Cisco Unified Communications självbetjäningsportal
- Lista över de funktioner som stöds
- Användarhandbok eller snabbreferens till röstbrevlådan

Migration av din telefon till en multiplattformstelefon direkt

Du kan enkelt migrera din företagstelefonen till en multiplattformstelefon i ett enda steg utan att använda någon fast programvara för överföringen. Allt du behöver göra är att hämta och auktorisera migreringslicensen från servern.

Mer information finns i https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html

Konfigurera en ny mall för programstyrda knappar

Du måste lägga till programstyrda knappar i en knappmall om du vill ge användare åtkomst till alla funktioner. Om du exempelvis vill att användarna ska kunna använda Stör ej-funktionen måste du aktivera den programstyrda knappen. Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Du kanske vill skapa flera mallar. Du kanske vill ha en mall för telefonen i ett konferensrum och en annan mall för en telefon i ett chefskontorsrum.

Den här metoden vägleder dig genom stegen för att skapa en ny mall för programstyrda knappar och tilldela den till en viss telefon. Precis som andra telefonfunktioner kan du även använda mallen för alla konferenstelefoner eller en grupp med telefoner.

Arbetsordning

Steg 1 Logga in på Cisco Unified Communications Manager Administration som administratör.

Steg 2 Välj **Enhet** > **Enhetsinställningar** > **Funktionsknappmall**.

Steg 3 Klicka på **Sök**.

Steg 4 Välj ett av följande alternativ:

- Cisco Unified Communications Manager 11.5 och tidigare versioner –**standardanvändare**
- Cisco Unified Communications Manager 12.0 och senare versioner –**personlig konferensanvändare** eller **offentlig konferensanvändare**.

Steg 5 Klicka på **Kopiera.**

Steg 6 Ändra namnet på mallen.

Till exempel 8832-mall för konferensrum.

Steg 7 Klicka på **Spara**.

Steg 8 Gå till sidan **Konfigurera funktionsknapplayout** via menyn högst upp till höger.

Steg 9 Ange funktionerna som ska visas vid respektive samtalsstatus.

Steg 10 Klicka på **Spara**.

Steg 11 Gå tillbaka till **Sök/lista** via menyn högst upp till höger.

Din nya mall visas i listan med mallar.

Steg 12 Välj **Enhet** > **Telefon**.

Steg 13 Sök efter telefonen som ska tilldelas den nya mallen och markera den.

Steg 14 I fältet **Mall för programstyrda knappar** väljer du den nya knappmallen.

Steg 15 Klicka på **Spara** och **Använd konfig**.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Konfigurera telefontjänster för användare

Du kan ge användarna tillgång till Cisco IP-telefon-tjänster på IP-telefonen. Du kan också tilldela en knapp till olika telefontjänster. IP-telefonen hanterar varje tjänst som ett separat program.

Innan en användare kan få tillgång till alla tjänster:

- Använd Administration av Cisco Unified Communications Manager för att konfigurera tjänster som inte finns som standard.
- Kontrollera att dina användare kan få åtkomst till Cisco Unified Communications självbetjäningsportal där de kan välja och prenumerera på tjänster. Det finns ett webbaserat grafiskt användargränssnitt för begränsad konfiguration som kan göras av slutanvändarna. Däremot kan en användare inte prenumerera på någon tjänst som du konfigurerar som ett företagsabonnemang.

Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Innan du konfigurerar tjänster kan du samla in webbadresserna till de webbplatser som du vill konfigurera och kontrollera att användare kan få tillgång till dessa platser från företagets IP-telefonnät. Detta är inte tillämpligt för standardtjänster som Cisco erbjuder.

Arbetsordning

Steg 1 Välj **Enhet** > **Enhetsinställningar** > **Telefontjänster** i Administration av Cisco Unified Communications Manager.

Steg 2 Kontrollera att dina användare kan få åtkomst till Cisco Unified Communications självbetjäningsportal där de kan välja och prenumerera på konfigurerade tjänster.

I Översikt över självbetjäningsportalen, på sidan 67 finns det en sammanfattning av den information som du måste lämna till slutanvändarna.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Telefonfunktionskonfiguration

Du kan ställa in telefoner med en mängd funktioner, baserat på behoven hos användarna. Du kan tillämpa funktionerna på alla telefoner, en grupp av telefoner eller enskilda telefoner.

När du ställer in funktionerna visar fönstret Administration av Cisco Unified Communications Manager information som gäller för alla telefoner och information som är specifik för telefonmodellen. Den information som är specifik för telefonmodellen visas i det produktspecifika konfigurationslayoutområdet i fönstret.

Mer information om fälten som gäller för alla telefonmodeller finns i dokumentationen för Cisco Unified Communications Manager.

När du ställer in ett fält är fönstret som du ställer in fältet i viktigt eftersom det finns en prioritetsordning bland fönstren. Prioritetsordningen:

1. Individuella telefoner (högst prioritet)

2. Grupp av telefoner
3. Alla telefoner (lägsta prioritet)

Till exempel om du inte vill att en viss grupp av användare att få tillgång till telefonens webbsidor, men resten av användarna kan komma åt sidorna, kan du göra så här:

1. Aktivera åtkomst till telefonens webbsidor för alla användare.
2. Inaktivera åtkomst till telefonens webbsidor för varje enskild användare, eller skapa en användargrupp och inaktivera tillgång till telefonens webbsidor för den gruppen av användare.
3. Om en viss användare i användargruppen behöver tillgång till telefonens webbsidor, kan du aktivera det för den specifika användaren.

Relaterade ämnen

Konfigurera bestående inloggningsuppgifter för inloggning med Expressway, på sidan 118

Konfigurera telefonfunktioner som gäller alla telefoner

Arbetsordning

Steg 1 Logga in på Cisco Unified Communications Manager Administration som administratör.
Steg 2 Välj **System** > **Företagstelefonkonfiguration**.
Steg 3 Ange de fält som du vill ändra.
Steg 4 Markera kryssrutan **Åsidosätt enterprise-inställningar** för alla fält som har ändrats.
Steg 5 Klicka på **Spara**.
Steg 6 Klicka på **Använd konfig**.
Steg 7 Starta om telefonerna.

OBS! Det kommer att påverka alla telefoner i organisationen.

Relaterade ämnen

Produktspecifik konfiguration, på sidan 95

Konfigurera telefonfunktioner för en grupp av telefoner

Arbetsordning

Steg 1 Logga in på Cisco Unified Communications Manager Administration som administratör.
Steg 2 Välj **Enhet** > **Enhetsinställningar** > **Allmän telefonprofil**.
Steg 3 Leta reda på profilen.
Steg 4 Navigera till rutan med den produktspecifika konfigurationslayouten och ange fälten.
Steg 5 Markera kryssrutan **Åsidosätt enterprise-inställningar** för alla fält som har ändrats.

Steg 6 Klicka på **Spara**.
Steg 7 Klicka på **Använd konfig**.
Steg 8 Starta om telefonerna.

Relaterade ämnen

Produktspecifik konfiguration, på sidan 95

Konfigurera telefonfunktioner för en enda telefon

Arbetsordning

Steg 1 Logga in på Cisco Unified Communications Manager Administration som administratör.
Steg 2 Välj **Enhet** > **Telefon**
Steg 3 Leta reda på telefonen i samband med användaren.
Steg 4 Navigera till rutan med den produktspecifika konfigurationslayouten och ange fälten.
Steg 5 Markera kryssrutan **Åsidosätt allmänna inställningar** för ändrade fält.
Steg 6 Klicka på **Spara**.
Steg 7 Klicka på **Använd konfig**.
Steg 8 Starta om telefonen.

Relaterade ämnen

Produktspecifik konfiguration, på sidan 95

Produktspecifik konfiguration

I följande tabell beskrivs fälten i rutan med den produktspecifika konfigurationslayouten. Vissa fält i den här tabellen visas endast på sidan **Enhet** > **Telefon**.

Tabell 18. Produktspecifika konfigurationsfält

Fältnamn	Fälttyp eller val	Standard	Beskrivning
Åtkomst till inställningar	Inaktiverad Aktiverad Begränsad	Aktiverad	Aktiverar, inaktiverar eller begränsar åtkomsten till lokala konfigurationsinställningar i appen Inställningar. Menyerna Inställningar och Systeminformation kan öppnas med begränsad åtkomst. Det går också att komma åt en del inställningar på Wi-Fi-menyn. Med inaktiverad åtkomst innehåller inte inställningsmenyn några alternativ.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
Opåkallad ARP	Inaktiverad Aktiverad	Inaktiverad	Aktiverar eller inaktiverar möjligheten att lära in MAC-adresser från Opåkallad ARP i telefonen. Denna funktion krävs för att kunna övervaka eller spela in röstströmmar.
Webbåtkomst	Inaktiverad Aktiverad	Inaktiverad	Aktiverar eller inaktiverar tillgång till telefonens webbsidor via en webbläsare. **Försiktighet** Om du aktiverar det här fältet kan du exponera känslig information om telefonen.
Inaktivera TLS 1.0 och TLS 1.1 för webbåtkomst	Inaktiverad Aktiverad	Aktiverad	Styr användningen av TLS 1.2 för en webserveranslutning. • Inaktiverat – en telefon som konfigurerats för TLS 1.0, TLS 1.1 eller TLS 1.2 kan fungera som en HTTPs-server. • Aktiverat – bara en telefon som konfigurerats för TLS 1.2 kan fungera som en HTTPs-server.
Enbloc-uppringning	Inaktiverad Aktiverad	Inaktiverad	Styr vilken uppringningsmetod. • Inaktiverad – Cisco Unified Communications Manager väntar på att siffertimern går ut när det finns en nummerplan eller routningsmönstret överlappas. • Aktiverat – hela uppringda strängen skickas till Cisco Unified Communications Manager när uppringningen är klar. Om du vill undvika timeout för T.302-timern rekommenderar vi att du aktiverar Enbloc-uppringning när det finns en nummerplan eller routningsmönstret överlappas. Obligatoriska behörighetskoder (FAC) eller ärendekoder (CMC) stöder inte Enbloc-uppringning. Om du använder FAC eller CMC för att hantera samtalsåtkomst och redovisning kan du inte använda den här funktionen.
Dagar bakgr.bel. ej aktiv	Dagar i veckan		Definierar de dagar som bakgrundsbelysningen inte slås på automatiskt vid den tid som anges i fältet Bakgrundsbelysning på tid. Välj dagar från listrutan. Om du vill välja mer än en dag **Ctrl-klickar** du på varje dag som du vill välja. Se Schemalägga energisparläge för Cisco IP-telefon, på sidan 107.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
Tid för bakgrundsbelysning	hh:mm		Definierar tid varje dag som bakgrundsbelysningen slås på automatiskt (utom på de dagar som anges i fältet Bakgrundsbelysning ej aktiv). Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt. Om du till exempel vill stänga av bakgrundsbelysningen automatiskt vid 07:00 (0700), ange 07:00. Om du vill stänga av bakgrundsbelysningen vid 14:00 anger du 14:00 . Om detta fält är tomt, slås bakgrundsbelysningen automatiskt på 00:00. Se Schemalägga energisparläge för Cisco IP-telefon, på sidan 107.
Bakgrundsbelysnings tidsperiod	hh:mm		Definierar den tid som bakgrundsbelysningen är tänd efter att den slagits på vid den tid som anges i fältet Bakgrundsbelysning på tid. Om du till exempel vill ha bakgrundsbelysningen tänd i 4 timmar och 30 minuter efter att den slås på automatiskt, anger du 4:30. Om detta fält är tomt stängs telefonen av vid slutet av dagen (0:00). Om Bakgrundsbelysning på tid är 00:00 och bakgrundsbelysningstiden är tom (eller 24:00) stängs bakgrundsbelysningen inte av. Se Schemalägga energisparläge för Cisco IP-telefon, på sidan 107.
Bakgrundsbel. inaktivitetstimeout	hh:mm		Definierar den tid som telefonen är inaktiv innan bakgrundsbelysningen släcks. Gäller endast när bakgrundsbelysningen varit släckt som planerat i schemat och tänts av en användare (genom att trycka på en knapp på telefonen eller lyfta på luren). Om du till exempel vill släcka bakgrundsbelysningen när telefonen varit inaktiv under 1 timme och 30 minuter efter att en användare tänt bakgrundsbelysningen, anger du 1:30. Se Schemalägga energisparläge för Cisco IP-telefon, på sidan 107.
Bakgrundsbelysning på vid inkommande samtal	Inaktiverad Aktiverad	Aktiverad	Slår på bakgrundsbelysningen när det kommer ett inkommande samtal.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
Aktivera Energisparplus	Dagar i veckan		Definierar schema med dagar då telefonen ska stängas av. Välj dagar från listrutan. Om du vill välja mer än en dag **Ctrl-klickar** du på varje dag som du vill välja. När Aktivera energispar Plus är på visas ett meddelande som varnar om nödfall (E911). **Försiktighet** När energisparplus-läget är aktiverat, inaktiveras alla ändpunkter som konfigurerats för läget för nödsamtal och mottagning av inkommande samtal. Genom att välja det här läget, godkänner du följande: (i) Du tar fullt ansvar för att tillhandahålla alternativa metoder för nödsamtal och ta emot samtal när läget används; (ii) Cisco har inget ansvar i samband med ditt val av läge och allt ansvar i samband med att aktivera läget är ditt ansvar; och (iii) Du informerar användarna fullständigt om effekterna av läget i samtal, uppringning och annat. Om du vill inaktivera Energispar plus måste du avmarkera kryssrutan Tillåt åsidosättning av EnergyWise. Om Tillåt åsidosättning av EnergyWise fortfarande är markerat men inga dagar väljs i fältet Aktivera energisparläge plus, är energisparplus inte inaktiverat. Se Schemalägga EnergyWise för Cisco IP-telefon, på sidan 109.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
Påslagningstid för telefon	hh:mm		Bestämmer när telefonen slås på automatiskt för de dagar som anges i fältet Aktivera energispar plus. Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt. Om du till exempel vill starta telefonen automatiskt vid 07:00 (0700), ange 07:00. Om du vill starta telefonen vid 02:00 anger du 14:00 . Standardvärdet är tomt, vilket betyder 00:00. Påslagningstid för telefon måste vara minst 20 minuter senare än Avstängningstid för telefon. Till exempel om Avstängningstid för telefon är 07:00, kan Påslagningstid för telefon vara tidigast 07:20. Se Schemalägga EnergyWise för Cisco IP-telefon, på sidan 109.
Avstängningstid för telefon	hh:mm		Definierar vilken tid på dagen som telefonen stängs av för de dagar som är markerade i fältet Aktivera energispar plus. Om fälten Avstängningstid för telefon och Påslagningstid för telefon har samma värde stängs telefonen inte av. Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt. Om du till exempel vill stänga av telefonen automatiskt vid 7:00. (0700), ange 7:00. Om du vill stänga av telefonen vid 2:00 anger du 14:00 . Standardvärdet är tomt, vilket betyder 00:00. Påslagningstid för telefon måste vara minst 20 minuter senare än Avstängningstid för telefon. Till exempel om Avstängningstid för telefon är 07:00, kan Påslagningstid för telefon vara tidigast 07:20. Se Schemalägga EnergyWise för Cisco IP-telefon, på sidan 109.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
Tidsgräns för telefon av vid inaktivitet	hh:mm		Anger hur lång tid telefonen måste vara inaktiv innan telefonen stängs av. Tidsgränsen inträffar under följande förhållanden: • När telefonen var i energisparplusläge, som planerat, och gick ur energisparplusläget eftersom telefonanvändaren tryckte på Välj. • När telefonen slås på igen från den anslutna växeln. • När Avstängningstid för telefon infaller men telefonen används. Se Schemalägga EnergyWise för Cisco IP-telefon, på sidan 109.
Aktivera varningsignal	Kryssruta	Omarkerad	När detta är aktiverat instrueras telefonen att spela upp en ljudsignal som startar 10 minuter innan tiden i fältet Avstängningstid för telefon. Den här kryssrutan används endast om listrutan Aktivera energisparläge plus har en eller flera dagar utvalda. Se Schemalägga EnergyWise för Cisco IP-telefon, på sidan 109.
EnergyWise-domän	Högst 127 tecken.		Identifierar EnergyWise-domänen som telefonen är i. Se Schemalägga EnergyWise för Cisco IP-telefon, på sidan 109.
EnergyWise Secret	Högst 127 tecken.		Identifierar det hemliga säkerhetslösenordet som används för att kommunicera med ändpunkterna i EnergyWise-domänen. Se Schemalägga EnergyWise för Cisco IP-telefon, på sidan 109.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
Tillåt åsidosättning av EnergyWise	Kryssruta	Omarkerad	Avgör om du tillåter EnergyWise-domänkontrollantpolicyn att skicka uppdateringar av strömnivån till telefonerna. Följande villkor gäller: • En eller flera dagar måste väljas i fältet Aktivera energisparläge plus. • Inställningarna i Cisco Unified Communications Manager Administration påverkar schemat även om EnergyWise skickar en åsidosättning. Till exempel om telefonen Avstängningstid för telefon anges som 22:00 (10:00 PM) är värdet i fältet Påslagningstid för telefon 06:00 (06:00), och i Aktivera energisparläge plus har en eller flera dagar valts. • Om EnergyWise styr telefonen att stängas av vid 20:00 (8:00), kvarstår direktivet i praktiken (förutsatt att inga telefonanvändaringripanden sker) tills den konfigurerade påslagningstiden för telefonen kl 6:00 • Kl 6:00 slås telefonen på och återupptar mottagning av strömnivåförändringar från inställningarna i Cisco Unified Communications Manager Administration. • Om du vill ändra strömnivån i telefonen igen måste EnergyWise utfärda ett nytt kommando för ändring av strömnivån. Om du vill inaktivera Energispar plus måste du avmarkera kryssrutan Tillåt åsidosättning av EnergyWise. Om Tillåt åsidosättning av EnergyWise fortfarande är markerat men inga dagar väljs i fältet Aktivera energisparläge plus, är energisparplus inte inaktiverat. Se Schemalägga EnergyWise för Cisco IP-telefon, på sidan 109.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
Policy för koppling och direktöverföring	Aktivera samma linje Inaktivera samma linje	Aktivering samma linje, mellan linjer	Styr förmågan hos en användare att koppla och överföra samtal.$$$ • Aktivera samma linje – Användare kan direkt överföra eller koppla ihop ett samtal på nuvarande linje till ett annat samtal på samma linje. • Inaktivera samma linje – Användare kan inte koppla eller överföra samtal på samma linje. Kopplings- och överföringsfunktioner är inaktiverade och användaren kan inte göra någon direkt överföring eller koppla ihop samtal.
Inspelningston	Inaktiverad Aktiverad	Inaktiverad	Styr uppspelning av tonen när en användare talar in ett samtal.
Lokal volym för inspeln.ton	Heltal 0–100	100	Styr volymen på inspelningstonen för den lokala användaren.
Fjärrvolym för inspeln.ton	Heltal 0–100	50	Styr volymen på inspelningstonen för fjärranvändaren.
Inspelningstonens längd	Heltal 1–3 000 millisekunder		Styr varaktigheten på inspelningstonen.
Loggserver	Sträng på upp till 256 tecken		Identifierar IPv4 syslog-servern för resultat från telefonfelsökning. Formatet på adressen är: **adress:<port>@@base=<0-7>;pfs=<0-1>**
Fjärrloggning	Inaktiverad Aktiverad	Inaktiverad	Styr möjligheten att skicka loggar till syslog-servern.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
Loggprofil	Standard Förinställd Telefoni SIP UI Nätverk Media Uppgradera Tillbehör Säkerhet EnergyWise MobilFjärråtkomst	Förinställd	Anger den fördefinierade loggningsprofilen. • Standard – Standardnivå på felsökningsloggning • Förinställd – Skriver inte över lokala den inställningen av felsökningsloggning på telefonen • Telefoni – Loggar information om telefoni- eller samtalsfunktioner • SIP – Loggar information om SIP-signalering • UI – Loggar information om telefonens användargränssnitt • Nätverk – Loggar nätverksinformation • Media – Loggar medieinformation • Uppgradering – Loggar uppgraderingsinformation • Tillbehör – Loggar information om tillbehör • Säkerhet – Loggar säkerhetsinformation • Energywise – Loggar information om energibesparingar • MobilFjärråtkomst – Loggar informationen om mobilåtkomst och Remote Access via Expressway
IPv6-loggserver	Sträng på upp till 256 tecken		Identifierar IPv6 syslog-servern för resultat från telefonfelsökning.
CDP (Cisco Discovery Protocol): Växelport	Inaktiverad Aktiverad	Aktiverad	Styr CDP (Cisco Discovery Protocol) på telefonen.
LLDP-protokoll – Media Endpoint Discover (LLDP-MED): Växelport	Inaktiverad Aktiverad	Aktiverad	Aktiverar LLDP-MED i SW-porten.
LLDP tillgångs-ID	Sträng, upp till 32 tecken		Identifierar resurs-ID som tilldelas till telefonen för lagerhantering.
(EEE) Energy Efficient Ethernet: Växelport	Inaktiverad Aktiverad	Inaktiverad	Styr EEE i växelporten.
LLDP-kraftsprioritet	Okänt Låg hög Kritiskt	Okänt	Tilldelar en telefonströmsprioritet till växeln så att växeln kan ge rätt ström till telefonerna.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
802.1x-autentisering	Användarkontrollerad Inaktiverad Aktiverad	Användarkontrollerad	Anger status på 802.1X-autentiseringsfunktionen. • Användarstyrd – Användaren kan konfigurera 802.1X på telefonen. • Inaktiverat – 802.1X-autentisering används inte. • Aktiverat – 802.1X-autentisering används och du konfigurerar autentisering för telefonerna.
Fjärrkonfiguration för växelport	Inaktiverad Autoförhandla 10 Halv 10 Full 100 Halv 100 Full	Inaktiverad	Här kan du konfigurera hastigheten och duplexfunktionen för telefonens SW-port fjärranslutet. Detta förbättrar prestanda för stora installationer med särskilda portinställningar. Om SW-portarna är konfigurerade för fjärrportkonfiguration i Cisco Unified Communications Manager kan inte data ändras i telefonen.
SSH-åtkomst	Inaktiverad Aktiverad	Inaktiverad	Styr åtkomsten till SSH-daemon genom port 22. Om port 22 lämnas öppen blir telefonen sårbar för överbelastningsattacker.
Ringningsspråk	Standard Japan	Standard	Kontrollerar ringningsmönstret.
Timer för TLS-återupptagande	Heltal 0–3 600 sekunder	3600	Styr funktionen för att återuppta en TLS-session utan att upprepa hela TLS-autentiseringsprocessen. Om fältet anges som 0 är återupptagning av TLS-sessionen inaktiverad.
FIPS-läge	Inaktiverad Aktiverad	Inaktiverad	Aktiverar eller inaktiverar FIPS-läget på telefonen.
Spara samtalslogg från delad linje	Inaktiverad Aktiverad	Inaktiverad	Anger om telefonen ska spela in en samtalslogg från delad linje.
Minsta ringvolym	0 – Tyst 1–15	0 – Tyst	Styr minsta ringvolym för telefonen.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
Peer Firmware Sharing	Inaktiverad Aktiverad	Aktiverad	Gör att telefonen att hitta andra telefoner av samma modell i subnätet och dela uppdaterade firmwarefiler. Om telefonen har en ny firmware kan den delas med andra telefoner. Om en av de andra telefoner har ny firmware kan telefonen hämta firmware från den andra telefonen i stället för från TFTP-servern. Peer-delning av fast programvara: • Begränsar trängsel vid TFTP-överföringar till centraliserade TFTP-fjärrservrar. • Eliminerar behovet av att manuellt kontrollera uppgraderingar av den fasta programvaran. • Minskar telefondriftstopp vid uppgraderingar när ett stort antal telefoner återställs samtidigt. • Hjälper till med uppgraderingar av firmware på kontor eller i fjärranslutna distributionsscenarier som körs över bandbreddsbegränsade WAN-länkar.
Laddningsserver	Sträng på upp till 256 tecken		Identifierar den alternativa IPv4-server som telefonen använder för att få firmware och uppgraderingar.
IPv6-laddningsserver	Sträng på upp till 256 tecken		Identifierar den alternativa IPv6-server som telefonen använder för att få firmware och uppgraderingar.
Identifiera anslutningsfel för Unified CM	Normal Försenat	Normal	Fastställer hur känslig telefonen är för att upptäcka ett anslutningsfel i Cisco Unified Communications Manager (Unified CM), som är det första steget innan enhetsredundans inträffar i en säkerhetskopierad Unified CM/SRST. Giltiga värden anger Normalt (detektering av ett Unified CM-anslutningsfel görs med standardsystemhastigheten) eller Fördröjd (detektering av ett Unified CM-anslutningsfel görs ungefär fyra gånger långsammare än normalt). Välj Normalt om du vill ha snabbare identifiering av ett Unified CM-anslutningsfel. Välj Fördröjd om du föredrar att felöverväxlingen fördröjs något för att se om anslutningen kan återupprättas Den exakta tidsskillnaden mellan Normal och Fördröjd anslutning vid feldetektering beror på många variabler som ständigt förändras.
Särskilt krav-ID	Sträng		Styr anpassade funktioner från ES-laster.

Fältnamn	Fälttyp eller val	Standard	Beskrivning
HTTPS-server	HTTP och HTTPS aktiverat HTTPS endast	HTTP och HTTPS aktiverat	Kontrollerar typen av kommunikation till telefonen. Om du väljer HTTPS endast är telefonkommunikationen säkrare.
Användarens inloggningsuppgifter står kvar under inloggning med Expressway	Inaktiverad Aktiverad	Inaktiverad	Styr om telefonen lagrar användarens inloggningsuppgifter. När detta är inaktiverat får användaren alltid ett meddelande om att logga in på Expressway-servern för mobilåtkomst och Remote Access (MRA). Om du vill göra det enklare för användarna att logga in kan du aktivera det här fältet så att Expressway-inloggningsuppgifterna står kvar. Användaren behöver då bara ange sina inloggningsuppgifter första gången. Varje gång efter detta (när telefonen är påslagen och utanför företaget) är inloggningsinformationen förhandsifylld på inloggningsskärmen. Mer information finns i Konfigurera bestående inloggningsuppgifter för inloggning med Expressway, på sidan 118.
Uppladdnings-URL för kundsupport	Sträng, upp till 256 tecken		Anger webbadressen till problemrapportverktyget (PRT). Om du distribuerar enheter med mobilåtkomst och Remote Access genom Expressway måste du även lägga till PRT-serveradressen i HTTP-serverns Tillåt-lista på Expressway-servern. Mer information finns i Konfigurera bestående inloggningsuppgifter för inloggning med Expressway, på sidan 118.
Inaktivera TLS-chiffer	Se Inaktivera Transport Layer Security-chiffer, på sidan 107.	Ingen	Inaktiverar valt TLS-chiffer. Inaktivera mer än en chifferserie genom att välja och hålla **Ctrl** intryckt på datorns tangentbord.
Dedikera en linje för samtalsparkering	Inaktiverad Aktiverad	Aktiverad	Styr om ett parkerat samtal upptar en linje eller inte. Mer information finns i dokumentationen till Cisco Unified Communications Manager.

Relaterade ämnen

Konfigurera bestående inloggningsuppgifter för inloggning med Expressway, på sidan 118

Inaktivera Transport Layer Security-chiffer

Du kan inaktivera TLS (Transport Layer Security)-chiffer med parametern **Disable TLS Ciphers**. Då kan du anpassa säkerheten för kända problem och justera nätverket med företagets regler för chiffer.

Inget är standardinställningen.

Inaktivera mer än en chifferserie genom att välja och hålla **Ctrl** intryckt på datorns tangentbord. Om du väljer alla telefonchiffer påverkas TLS-tjänsten för telefonen. Du har följande att välja på:

- Ingen
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Mer information om telefonsäkerhet i finns *Cisco IP-telefon 7800 och 8800-serien säkerhet översikt vitboken* (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html).

Schemalägga energisparläge för Cisco IP-telefon

För att spara energi och säkerställa livslängden på telefonens skärm kan du ställa in skärmen så att den stängs av när den inte behövs.

Du kan konfigurera inställningar i Cisco Unified Communications Manager Administration för att stänga av skärmen under en angiven tid vissa några dagar och hela dagen andra dagar. Du kan till exempel välja att stänga av skärmen efter kontorstid på vardagar och hela dagen på lördagar och söndagar.

Du kan vidta någon av följande åtgärder för att slå på skärmen när den är avstängd:

- Tryck på valfri knapp på telefonen.

  Telefonen utför den åtgärd som har definierats för knappen förutom att slå på skärmen.

- Lyft luren.

När du slår på skärmen är den påslagen tills telefonen har varit inaktiv under en angiven tidsperiod, och sedan stängs den av automatiskt.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon**.

Steg 2 Leta reda på telefonen som du ska ställa in.

Steg 3 Navigera till det produktspecifika konfigurationsområdet och ställ in följande fält:

- Visning av dagar ej aktiverat
- Display på-tid
- Display på-varaktighet
- Visa timeout för ledig

Tabell 19. Konfigurationsfält för energisparläge

Fält	Beskrivning
Visning av dagar ej aktiverat	Antal dagar som skärmen inte slås på automatiskt vid den tid som anges i fältet Display på-tid. Välj dagar från listrutan. Om du vill välja mer än en dag Ctrl-klickar du på varje dag som du vill välja.
Display på-tid	Tidpunkt varje dag som skärmen slås på automatiskt (utom på de dagar som anges i fältet Visning av dagar ej aktiverat). Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt. Om du till exempel vill stänga av skärmen automatiskt vid 07:00 anger du **07:00**. Om du vill stänga av skärmen vid 14:00 anger du **14:00** . Om detta fält är tomt slås skärmen automatiskt på 00:00.
Display på-varaktighet	Tidslängd som skärmen är tänd efter att den slagits på vid den tid som anges i fältet Display på-tid. Ange värdet i fältet i formatet *timmar:minuter*. Om du till exempel vill ha skärmen tänd i 4 timmar och 30 minuter efter att den slås på automatiskt, anger du **4:30**. Om detta fält är tomt stängs telefonen av vid slutet av dagen (0:00). **OBS!** Om Display på-tid 0:00 och skärmens varaktighet för påslagen är tom (eller 24:00) förblir skärmen påslagen.
Visa timeout för ledig	Den tidslängd som telefonen är inaktiv innan skärmen släcks. Gäller endast när skärmen varit släckt som planerat i schemat och tänts av en användare (genom att trycka på en knapp på telefonen eller lyfta på luren). Ange värdet i fältet i formatet *timmar:minuter*. Om du till exempel vill släcka skärmen när telefonen varit inaktiv under 1 timme och 30 minuter efter att en användare tänt skärmen, anger du **1:30**. Standardvärdet är 01:00.

Steg 4 Välj **Spara**.

Steg 5 Välj **Använd konfig**.

Steg 6 Starta om telefonen.

Schemalägga EnergyWise för Cisco IP-telefon

För att minska strömförbrukningen kan du konfigurera telefonen för viloläge (avstängning) och uppvakning (start) om det finns en EnergyWise-styrenhet i systemet.

Du kan konfigurera inställningar i Cisco Unified Communications Manager Administration för att aktivera EnergyWise och konfigurera vilo- och uppvakningstider. Dessa parametrar är tätt knutna till konfigurationsparametrarna på telefonens skärm.

När EnergyWise är aktiverat och en vilolägestid är inställd sänder telefonen en begäran till växeln för att aktivera uppvakning vid den konfigurerade tiden. Växeln returnerar antingen ett godkännande eller ett avslag på begäran. Om växeln avvisar begäran, eller om växeln inte svarar, går telefonen inte in i viloläget. Om växeln beviljar begäran går telefonen in i viloläge efter en inaktiv tid, vilket minskar effektförbrukningen till en förutbestämd nivå. En telefon som inte är i viloläge ställs in med vilolägestimern och övergår till viloläge efter den inställda tiden i timern.

Tryck på Välj för att aktivera telefonens uppvakning. Vid den schemalagda uppvakningstiden återställs strömmen till telefonen och aktiverar uppvakning.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon**

Steg 2 Leta reda på telefonen som du ska ställa in.

Steg 3 Navigera till det produktspecifika konfigurationsområdet och ställ in följande fält.

- Aktivera Energisparplus
- Påslagningstid för telefon
- Avstängningstid för telefon
- Tidsgräns för telefon av vid inaktivitet
- Aktivera varningsignal
- EnergyWise-domän
- EnergyWise Secret
- Tillåt åsidosättning av EnergyWise

Tabell 20. Konfigurationsfält för EnergyWise

Fält	Beskrivning
Aktivera Energisparplus	Väljer schema med dagar då telefonen ska stängas av. Markera flera dagar genom att hålla ned Ctrl-tangenten medan du klickar på dagar i schemat. Inga dagar väljs som standard. När Aktivera energispar Plus är markerat visas ett meddelande som varnar vid nödfall (E911). **Försiktighet** När energisparplus-”läget” är aktiverat, inaktiveras alla ändpunkter som konfigurerats för läget för nödsamtal och mottagning av inkommande samtal. Genom att välja det här läget, godkänner du följande: (i) Du tar fullt ansvar för att tillhandahålla alternativa metoder för nödsamtal och ta emot samtal när läget används; (ii) Cisco har inget ansvar i samband med ditt val av läge och allt ansvar i samband med att aktivera läget är ditt ansvar; och (iii) Du informerar användarna fullständigt om effekterna av läget i samtal, uppringning och annat. **OBS!** Om du vill inaktivera Energispar plus måste du avmarkera kryssrutan Tillåt åsidosättning av EnergyWise. Om Tillåt åsidosättning av EnergyWise fortfarande är markerat men inga dagar väljs i fältet Aktivera energisparläge plus, är energisparplus inte inaktiverat.
Påslagningstid för telefon	Bestämmer när telefonen slås på automatiskt för de dagar som anges i fältet Aktivera energispar plus. Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt. Om du till exempel vill starta telefonen automatiskt vid 07:00 (0700), ange 07:00. Om du vill starta telefonen vid 02:00 anger du 14:00 . Standardvärdet är tomt, vilket betyder 00:00. **OBS!** Påslagningstid för telefon måste vara minst 20 minuter senare än Avstängningstid för telefon. Till exempel om Avstängningstid för telefon är 07:00, kan Påslagningstid för telefon vara tidigast 07:20.
Avstängningstid för telefon	Anger vilken tid på dagen som telefonen stängs av för de dagar som är markerade i fältet Aktivera energispar plus. Om fälten Avstängningstid för telefon och Påslagningstid för telefon har samma värde stängs telefonen inte av. Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt. Om du till exempel vill stänga av telefonen automatiskt vid 7:00. (0700), ange 7:00. Om du vill stänga av telefonen vid 2:00 anger du 14:00 . Standardvärdet är tomt, vilket betyder 00:00. **OBS!** Påslagningstid för telefon måste vara minst 20 minuter senare än Avstängningstid för telefon. Till exempel om Avstängningstid för telefon är 07:00, kan Påslagningstid för telefon vara tidigast 07:20.

Fält	Beskrivning
Tidsgräns för telefon av vid inaktivitet	Hur lång tid telefonen måste vara inaktiv innan telefonen stängs av. Tidsgränsen inträffar under följande förhållanden: • När telefonen var i energisparplusläge, som planerat, och gick ur energisparplusläget eftersom telefonanvändaren tryckte på **Välj**. • När telefonen slås på igen från den anslutna växeln. • När Avstängningstid för telefon infaller men telefonen används. Fältintervallet är 20 till 1 440 minuter. Standardvärdet är 60 minuter.
Aktivera varningsignal	När detta är aktiverat instrueras telefonen att spela upp en ljudsignal som startar 10 minuter innan tiden i fältet Avstängningstid för telefon. Hörbar varning använder telefonens ringsignal, som kort spelas upp vid specifika tidpunkter under tiominutersperioden för varning. Varningsringsignalen spelas upp med den användarinställda ljudnivån. Det hörbara varningsschemat är: • Tio minuter före avstängning spelas ringsignalen upp fyra gånger. • Sju minuter före avstängning spelas ringsignalen upp fyra gånger. • Fyra minuter före avstängning spelas ringsignalen upp fyra gånger. • 30 sekunder före avstängning spelas ringsignalen upp 15 gånger eller tills telefonen stängs av. Den här kryssrutan används endast om listrutan Aktivera energisparläge plus har en eller flera dagar utvalda.
EnergyWise-domän	EnergyWise-domänen som telefonen finns i. Fältets maximala längd är 127 tecken.
EnergyWise Secret	Det hemliga säkerhetslösenordet som används för att kommunicera med ändpunkterna i EnergyWise-domänen. Fältets maximala längd är 127 tecken.

Fält	Beskrivning
Tillåt åsidosättning av EnergyWise	Kryssrutan anger om du tillåter EnergyWise-domänkontrollantpolicyn att skicka uppdateringar av strömnivån till telefonerna. Följande villkor gäller: • En eller flera dagar måste väljas i fältet Aktivera energisparläge plus. • Inställningarna i Cisco Unified Communications Manager Administration påverkar schemat även om EnergyWise skickar en åsidosättning. Till exempel om telefonen Avstängningstid för telefon anges som 22:00 (10:00 PM) är värdet i fältet Påslagningstid för telefon 06:00 (06:00), och i Aktivera energisparläge plus har en eller flera dagar valts. • Om EnergyWise styr telefonen att stängas av vid 20:00 (8:00), kvarstår direktivet i praktiken (förutsatt att inga telefonanvändaringripanden sker) tills den konfigurerade påslagningstiden för telefonen kl 6:00 • Kl 6:00 slås telefonen på och återupptar mottagning av strömnivåförändringar från inställningarna i Unified Communications Manager Administration. • Om du vill ändra strömnivån i telefonen igen måste EnergyWise utfärda ett nytt kommando för ändring av strömnivån. **OBS!** Om du vill inaktivera Energispar plus måste du avmarkera kryssrutan Tillåt åsidosättning av EnergyWise. Om Tillåt åsidosättning av EnergyWise fortfarande är markerat men inga dagar väljs i fältet Aktivera energisparläge plus, är energisparplus inte inaktiverat.

Steg 4 Välj **Spara**.

Steg 5 Välj **Använd konfig**.

Steg 6 Starta om telefonen.

Konfigurera Stör ej

När stör ej (DND) har aktiverats lyser det rött högst upp på konferenstelefonens skärm.

Mer information finns i avsnittet om Stör inte i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon**.

Steg 2 Lokalisera telefonen som ska konfigureras.

Steg 3 Ställ in följande parametrar.

- Stör ej: Med den här kryssrutan kan du aktivera DND på telefonen.
- DND-alternativ: Avstängd ringsignal, avvisa samtal eller använd inställning för allmän telefonprofil.

- DND, meddelande om inkommande samtal: Välj typ av varning om du vill spela upp en varning på en telefon för inkommande samtal när DND är aktiverat.

  OBS! Denna parameter finns i fönstret Allmän telefonprofil och fönstret Telefonkonfiguration. Värdet i telefonkonfigurationsfönstret har företräde.

Steg 4 Välj **Spara**.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Konfigurera meddelande om vidarekoppling av samtal

Du kan styra inställningarna för vidarekoppling av samtal.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon**.

Steg 2 Leta upp telefonen som ska konfigureras.

Steg 3 Konfigurera meddelande om vidarekoppling i motsvarande fält.

Fält	Beskrivning
Samtalspartnerns namn	När den här kryssrutan är markerad visas personens namn i meddelandefönstret. Som standard är kryssrutan markerad.
Uppringarens nummer	När den här kryssrutan är markerad visas uppringarens nummer i meddelandefönstret. Som standard är den här kryssrutan avmarkerad.
Vidarekopplat nummer	När denna kryssruta är markerad visas information om uppringaren som senast vidarekopplade samtalet i meddelandefönstret. Exempel: Om A ringer B, men B har vidarekopplat alla samtal till C och C har vidarekopplat alla samtal till D, innehåller rutan som D ser telefoninformationen från C. Som standard är den här kryssrutan avmarkerad.
Uppringt nummer	När denna kryssruta är markerad visas information om den ursprungliga mottagaren av samtalet i meddelandefönstret. Exempel: Om A ringer B, men B har vidarekopplat alla samtal till C och C har vidarekopplat alla samtal till D, innehåller rutan som D ser telefoninformationen från B. Som standard är kryssrutan markerad.

Steg 4 Välj **Spara**.

Inställning av UCR 2008

De parametrar som stöder UCR 2008 lagras i Cisco Unified Communications Manager Administration. I följande tabell beskrivs dessa parametrar med sökväg för att ändra inställningen.

Tabell 21. Sökväg till parameter UCR 2008

Parameter	Sökväg till administration
FIPS-läge	**Enhet** > **Enhetsinställningar** > **Allmän telefonprofil**
	System > **Företagstelefonkonfiguration**
	Enhet > **Telefoner**
SSH-åtkomst	**Enhet** > **Telefon**
	Enhet > **Enhetsinställningar** > **Allmän telefonprofil**
Webbåtkomst	**Enhet** > **Telefon**
	System > **Företagstelefonkonfiguration**
	Enhet > **Enhetsinställningar** > **Allmän telefonprofil**
System > **Företagstelefonkonfiguration**	
IP-adresseringsläge	**Enhet** > **Enhetsinställningar** > **Allmän enhetskonfiguration**
Inställning av IP-adresseringsläge för signalering	**Enhet** > **Enhetsinställningar** > **Allmän enhetskonfiguration**

Konfigurera UCR 2008 i Allmän enhetskonfiguration

Använd denna procedur för att ställa in följande UCR 2008-parametrar:

- IP-adresseringsläge
- Inställning av IP-adresseringsläge för signalering

Arbetsordning

Steg 1 Använd Cisco Unified Communications Manager Administration och välj **Enhet** > **Enhetsinställningar** > **Allmän enhetskonfiguration**.

Steg 2 Ställ in parametern för IP-adresseringsläget.

Steg 3 Ställ in IP-adresseringsläge för signaleringsparametern.

Steg 4 Välj **Spara**.

Konfigurera UCR 2008 i den allmänna telefonprofilen

Använd denna procedur för att ställa in följande UCR 2008-parametrar:

- FIPS-läge
- SSH-åtkomst
- Webbåtkomst

Arbetsordning

Steg 1 Använd Cisco Unified Communications Manager Administration och välj **Enhet** > **Enhetsinställningar** > **Allmän telefonprofil**.

Steg 2 Ställ in parametern för FIPS-läge som **Aktiverad**.

Steg 3 Ställ in parametern för SSH-åtkomst som **Inaktiverad**.

Steg 4 Ställ in parametern för webbåtkomst som **Inaktiverad**.

Steg 5 Ställ in parametern för 80-bitars SRTCP som **Aktiverad**.

Steg 6 Välj **Spara**.

Konfigurera UCR 2008 i Företagstelefonkonfiguration

Använd denna procedur för att ställa in följande UCR 2008-parametrar:

- FIPS-läge
- Webbåtkomst

Arbetsordning

Steg 1 Gå till Cisco Unified Communications Manager Administration och välj **System** > **Företagstelefonkonfiguration**.

Steg 2 Ställ in parametern för FIPS-läge som **Aktiverad**.

Steg 3 Ställ in parametern för webbåtkomst som **Inaktiverad**.

Steg 4 Välj **Spara**.

Konfigurera UCR 2008 i telefonen

Använd denna procedur för att ställa in följande UCR 2008-parametrar:

- FIPS-läge
- SSH-åtkomst
- Webbåtkomst

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon**.
Steg 2 Ställ in parametern för SSH-åtkomst som **Inaktiverad**.
Steg 3 Ställ in parametern för FIPS-läge som **Aktiverad**.
Steg 4 Ställ in parametern för webbåtkomst som **Inaktiverad**.
Steg 5 Välj **Spara**.

Mobil åtkomst och fjärråtkomst genom Expressway

Mobil åtkomst och fjärråtkomst genom Expressway(MRA) låter fjärrarbetare enkelt och säkert ansluta till företagets nätverk utan att använda en VPN-klienttunnel. Expressway använder TLS för att skydda nätverkstrafiken. För att en telefon ska kunna auktorisera ett Expressway-certifikat och etablera en TLS-session måste en offentlig certifikatutfärdare som är betrodd av telefonens inbyggda programvara signera Expressway-certifikatet. Det är inte möjligt att installera eller lita på andra CA-certifikat som finns i telefoner för att autentisera ett Expressway-certifikat.

Listan över CA-certifikat i telefonens inbyggda programvara finns på http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

Mobil åtkomst och fjärråtkomst genom Expressway (MRA) fungerar med Cisco Expressway. Du måste vara bekant med dokumentationen för Cisco Expressway, inklusive *Cisco Expressway Administrator Guide* och *Cisco Expressway Basic Configuration Deployment Guide*. Cisco Expressway-dokumentation finns tillgänglig på http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html.

Endast IPv4-protokollet stöds för Mobil åtkomst och fjärråtkomst genom Expressway-användare.

Ytterligare information om att arbeta med Mobil åtkomst och fjärråtkomst genom Expressway finns i:

- *Cisco Preferred Architecture for Enterprise Collaboration, designöversikt*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD*
- *Unified Communications mobilåtkomst och Remote Access via Cisco VCS Deployment Guide*
- *Cisco TelePresence Video Communication Server (VCS), konfigurationshandböcker*
- *Driftsättningshandbok för mobilåtkomst och Remote Access genom Cisco Expressway*

Under telefonregistreringsprocessen synkroniserar telefonen datum och tid med NTP-servern. Med MRA används DHCP-alternativet med tagg 42 till att lokalisera IP-adresserna till de NTP-servrar som ska användas för synkronisering av tid och datum. Om DHCP-alternativet med tagg 42 inte finns i konfigurationsinformationen söker telefonen efter taggen 0.tandberg.pool.ntp.org för att identifiera NTP-servrarna.

Efter registrering, använder telefonen information från SIP-meddelandet för att synkronisera datum och tid om inte en NTP-server är konfigurerad i Cisco Unified Communications Manager.

OBS! Om telefonsäkerhetsprofilen för någon av dina telefoner har TFTP-krypterad konfig markerat kan du inte använda telefonen med mobilåtkomst och Remote Access. MRA-lösningen stöder inte enhetsinteraktion med CAPF (Certificate Authority Proxy Function).

SIP OAuth-läge stöds för MRA. I det här läget kan du använda OAuth-åtkomsttoken för autentisering i säkra miljöer.

OBS! För SIP OAuth i MRA-läge ska du bara använda registrering med aktiveringskod samt MRA när du distribuerar telefonen. Aktivering med användarnamn och lösenord stöds inte.

För SIP OAuth-läge behöver du Expressway x14.0 (1) eller senare, eller Cisco Unified Communications Manager 14.0 (1) eller senare.

Mer information om SIP OAuth-läget finns i *Guide till funktionskonfiguration i Cisco Unified Communications Manager* version 14.0 (1) eller senare.

Driftsättningsscenarier

Nedanstående tabell visar olika scenarier med distribution av Mobil åtkomst och fjärråtkomst genom Expressway.

Scenario	Åtgärder
Lokala användare loggar in i företagets nätverk efter distributionen av Mobil åtkomst och fjärråtkomst genom Expressway.	Företagets nätverk identifieras och telefonen registreras med Cisco Unified Communications Manager som normalt.

Scenario	Åtgärder
Externa användare loggar in i företagets nätverk med Mobil åtkomst och fjärråtkomst genom Expressway.	Telefonen känner av att den är utanför företaget, inloggningsfönstret för Mobil åtkomst och fjärråtkomst genom Expressway visas och användaren ansluter till företagets nätverk. Användare måste ha ett giltigt tjänstenamn, användarnamn och lösenord för att ansluta till nätverket. Användare måste också återställa tjänsteläget för att rensa de alternativa TFTP-inställningarna innan de kan få tillgång till företagets nätverk. Detta rensar inställningen för alternativ TFTP-Server så att telefonen identifierar nätverket för distansarbete. Om en telefon ska användas direkt ur lådan kan användare hoppa över återställningen av nätverksinställningarna. Om användarna har DHCP-alternativ 150 eller 66 aktiverat i sin nätverksrouter kanske de inte kan logga in på företagets nätverk. Användare bör inaktivera DHCP-inställningar eller konfigurera sin statiska IP-adress direkt.

Konfigurera bestående inloggningsuppgifter för inloggning med Expressway

När en användare loggar in till nätverket med Mobil åtkomst och fjärråtkomst genom Expressway uppmanas användare att ange tjänstdomän, användarnamn och lösenord. Om du aktiverar parametern Bestående inloggningsuppgifter för inloggning med Expressway lagras användarnas inloggningsuppgifter så att de inte behöver anges på nytt. Den här parametern är inaktiverad som standard.

Du kan konfigurera bestående inloggningsuppgifter för en enskild telefon, en grupp av telefoner eller alla telefoner.

Relaterade ämnen

Telefonfunktionskonfiguration, på sidan 93
Produktspecifik konfiguration, på sidan 95

Problemrapportverktyg

Användare skickar problemrapporter till dig med problemrapportverktyget.

OBS! Loggar från problemrapportverktyget krävs av Cisco TAC vid felsökning av problemen. Loggarna rensas om du startar om telefonen. Samla in loggar innan du startar om telefonerna.

För att skapa problemrapporter kan användare välja problemrapporteringsverktyget och ange datum och tid då problemet uppstod, och en beskrivning av problemet.

Om PRT-överföringen misslyckas kan du få tillgång till PRT-filen för telefonen från webbadressen **`http://<phone-ip-address>/FS/<prt-file-name>`**. Denna URL visas på telefonen i följande fall:

- Om telefonen är i de ursprungliga fabriksinställningarna. URL:en är aktiv i 1 timme. Efter en timme ska användaren försöka skicka telefonloggar igen.
- Om telefonen har hämtat en konfigurationsfil och samtalsstyrningssystemet ger webbåtkomst till telefonen.

Du måste lägga till en serveradress i fältet **Uppladdnings-URL för kundsupport** i Cisco Unified Communications Manager.

Om du distribuerar enheter med mobilåtkomst och Remote Access genom Expressway måste du även lägga till PRT-serveradressen i HTTP-serverns Tillåt-lista på Expressway-servern.

Konfigurera en uppladdnings-URL för kundsupport

Du måste använda en server med ett uppladdningsskript för att kunna ta emot PRT-filer. PRT använder en HTTP POST-mekanism, med följande parametrar som ingår i uppladdningen (genom att använda MIME-multikodning):

- enhetsnamn (exempel: ”SEP001122334455”)
- serialno (exempel: ”FCH12345ABC”)
- användarnamn (användarnamn konfigurerat i Cisco Unified Communications Manager, enhetens ägare)
- prt_fil (exempel: ”probrep-20141021-162840.tar.gz”)

En exempelskript visas nedan. Detta skript tillhandahålls endast som referens. Cisco har inte stöd för uppladdningsskript som installerats på kundens server.

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
```

```
}

?>
```

OBS! Telefoner stöder bara HTTP-URL:er.

Arbetsordning

Steg 1 Konfigurera en server som kan köra PRT-uppladdningsskript.

Steg 2 Skriv ett skript som kan hantera de parametrar som anges ovan, eller redigera den medföljande exempelskript för att passa dina behov.

Steg 3 Ladda upp ditt skript till din server.

Steg 4 Utgå från Cisco Unified Communications Manager och gå till området Produktspecifik konfigurationslayout i det enskilda enhetskonfigurationsfönstret, allmänna telefonprofilfönstret eller företagstelefonkonfigurationsfönstret.

Steg 5 Kontrollera **Uppladdnings-URL för kundsupport** och ange URL-en till din överföringsserver.

Exempel:

http://example.com/prtscript.php

Steg 6 Spara ändringarna.

Ställa in en etikett för en linje

Du kan ställa in en telefon för att visa en textetikett i stället för katalognummer. Använd denna etikett för att identifiera raden med namn eller funktion. Till exempel om ditt användarnamn delar linjer på telefonen, kan du identifiera raden med namnet på den person som delar linjen.

När du lägger till en etikett till en knappexpansionsmodul visas bara de första 25 tecknen för en linje.

Arbetsordning

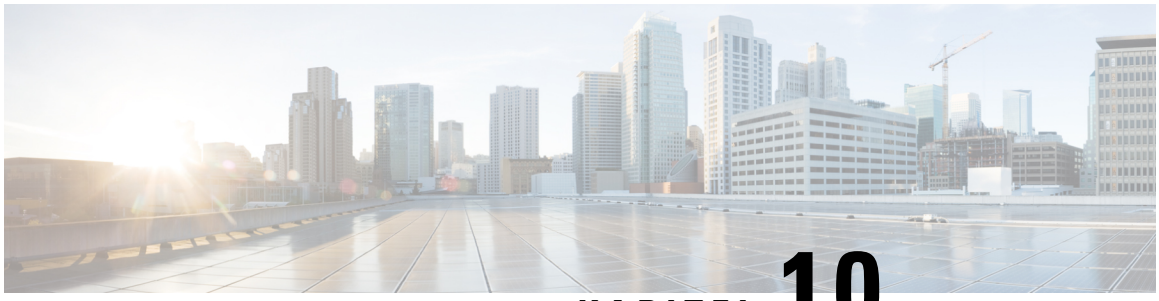
Steg 1 Utgå från Cisco Unified Communications Manager Administration och välj **Enhet** > **Telefon**.

Steg 2 Lokalisera telefonen som ska konfigureras.

Steg 3 Leta rätt på raden instans och ställ in rader text fältet Etikett.

Steg 4 (Valfritt) Om etiketten behöver tillämpas på andra enheter som delar linjen, markerar du kryssrutan Uppdatera delade enhetsinställningar och klickar på **Propagera markerade**.

Steg 5 Välj **Spara**.



KAPITEL 10

Företagskatalog och den personliga katalogen

Inställning av företagskatalog

Företagskatalogen tillåter en användare att slå upp telefonnummer till medarbetare. För att stödja den här funktionen måste du konfigurera företagskataloger.

Cisco Unified Communications Manager använder en Lightweight Directory Access Protocol (LDAP)-katalog för att spara autentiserings- och behörighetsinformation om användare av Cisco Unified Communications Manager program som är gränssnitt för Cisco Unified Communications Manager. Med autentisering upprättas användarrättigheter att få tillgång till systemet. Autentiseringen identifierar telefoniresurser som en användare tillåts att använda, till exempel en särskild telefonanknytning.

Mer information finns i dokumentationen till din version av Cisco Unified Communications Manager.

När du är klar med konfigurationen av LDAP-katalogen kan användare använda företagskatalogtjänsten på sin telefon för att slå upp användare i företagskatalogen.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Inställning av personlig katalog

Den personliga katalogen tillåter en användare att lagra en uppsättning av personliga nummer.

Den personliga katalogen innehåller följande funktioner:

- Personlig adressbok
- Snabbval

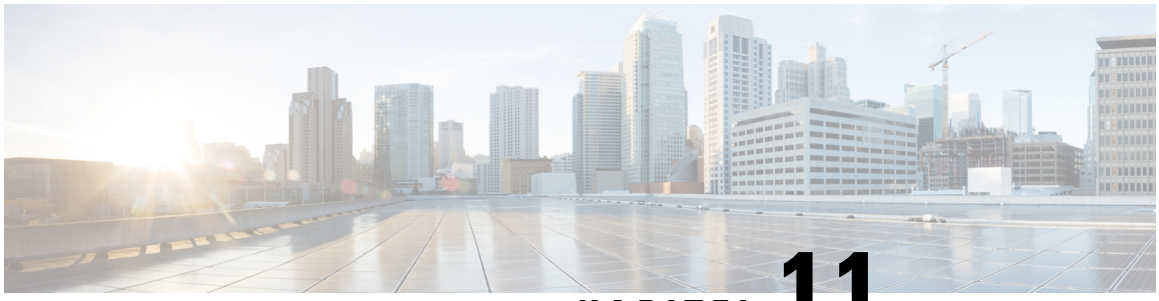
Användare kan använda dessa metoder för att få tillgång till funktioner i den personliga katalogen:

- Från en webbläsare − användare kan öppna adressboken och se kortnummerfunktioner i självbetjäningsportalen i Cisco Unified Communications.
- Från Cisco IP-telefonen – välj **Kontakter** för att söka i företagskatalogen eller användarens personliga katalog.

Om användarna vill konfigurera den personliga katalogen från en webbläsare måste de gå till självbetjäningsportalen. Du måste ge användarna en webbadress och inloggningsuppgifter.

DEL IV

Felsöka Cisco IP-konferenstelefon



KAPITEL 11

Övervakning av telefonsystem

Översikt över telefonsystemövervakning

Du kan visa en mängd information om telefonen med hjälp av telefonens statusmenyn och telefonens webbsidor. Denna information omfattar:

- Enhetsinfo
- Nätverksinstallationsinformationen
- Nätverksstatistik
- Enhetsloggar
- Direktspelningsstatistik

Detta kapitel beskriver den information som du kan få från telefonens webbsida. Du kan använda denna information för att fjärrövervaka driften av en telefon och för att hjälpa till med felsökning.

Relaterade ämnen

Felsökning av telefonen, på sidan 151

Status på Cisco IP-telefonen

Följande avsnitt beskriver hur du visar modellinformation, statusmeddelanden och nätverksstatistik på en Cisco IP-telefon.

- Modellinformation: Visar information om maskinvara och programvara för telefonen.
- Statusmeny: Ger tillgång till skärmar som visar statusmeddelanden, nätverksstatistik och statistik för det aktuella samtalet.

Du kan använda informationen som visas på dessa skärmar för att övervaka driften av en telefon och för att hjälpa till med felsökning.

Du kan också få en stor del av denna information och få annan relaterad information, på distans via telefonens webbsida.

Visa telefoninformationsfönstret

Arbetsordning

Steg 1 Tryck på **Inställningar** > **Systeminformation**.
Steg 2 Om du vill lämna menyn trycker du på **Avsluta**.

Visa statusmenyn

Arbetsordning

Steg 1 Tryck på **Inställningar** > **Status**.
Steg 2 Om du vill lämna menyn trycker du på **Avsluta**.

Visa fönstret Statusmeddelanden

Arbetsordning

Steg 1 Tryck på **Inställningar** > **Status** > **Statusmeddelanden**.
Steg 2 Om du vill lämna menyn trycker du på **Avsluta**.

Statusmeddelandefält

Följande tabell beskriver de statusmeddelanden som visas på statusmeddelandeskärmen på telefonen.

Tabell 22. Statusmeddelanden på en Cisco IP-telefon

Meddelande	Beskrivning	Möjlig förklaring och åtgärd
Det gick inte att hämta någon IP-adress från DHCP	Telefonen har inte tidigare tagit emot en IP-adress från en DHCP-server. Detta kan inträffa när du konfigurerar direkt ur lådan eller för en fabriksåterställning.	Kontrollera att DHCP-servern är tillgän är tillgänglig för telefonen.
TFTP-storleksfel	Konfigurationsfilen är för stor för filsystemet på telefonen.	Slå av telefonen.

Meddelande	Beskrivning	Möjlig förklaring och åtgärd
Fel i ROM CRC	Den hämtade programfilen är skadad.	Skaffa en ny kopia av telefonens in placera den i TFTPPath-katalogen. den här katalogen när TFTP-serverp Annars kan filerna skadas.
Duplicerad IP	En annan enhet använder den IP-adress som är tilldelad till telefonen.	Om telefonen har en statisk IP-adre har tilldelat en dubblett av IP-adres Om du använder DHCP ska du kon DHCP-serverkonfigurationen.
Raderar CTL- och ITL-filer	Raderar CTL- och ITL-filer	Ingen. Detta meddelande är endast
Fel: Uppd av språk	En eller flera lokaliseringsfiler kunde inte hittas i TFTP-sökvägskatalogen eller är inte giltiga. Språket har inte ändrats.	Gå till Cisco Unified Operating Sys kontrollera att följande filer ligger i Management: • De finns i katalogen med samn nätverket: • tones.xml • De finns i katalogen med samn • glyphs.xml • dictionary.xml • kate.xml
Hittar inte filen <Cfg File>	Den namnbaserade filen och standardkonfigurationsfilen fanns inte på TFTP-servern.	Konfigurationsfilen för en telefon sk i Cisco Unified Communications M telefonen inte finns i Cisco Unified Manager-databasen genererar TFTP att **`CFG-filen saknas`** • Telefonen är inte registrerad m Communications Manager. Du måste manuellt lägga till te Communications Manager om registrering av telefoner. • Om du använder DHCP ska du DHCP-servern pekar på rätt T • Om du använder statiska IP-ad konfigurationen av TFTP-serv
Hittar Inte Filen <CTLFile.tlv>	Detta meddelande visas på telefonen när Cisco Unified Communications Manager-klustret inte är i säkert läge.	Ingen påverkan, telefonen kan fortf Unified Communications Manager.

Meddelande	Beskrivning	Möjlig förklaring och åtgärd
IP-adress släppt	Telefonen är konfigurerad för att släppa IP-adressen.	Telefonen fortsätter vara inaktiv tills de återställer DHCP-adressen.
IPv4 DHCP-tidsgräns	IPv4 DHCP-servern svarade inte.	Nätverket är upptaget: Felen bör lösas minskar. Ingen nätverksanslutning mellan IPv4 telefonen: Kontrollera nätverksanslutni IPv4 DHCP-servern är nere: Kontrolle IPv4 DHCP-servern. Fel kvarstår: Överväg att tilldela en sta
IPv6 DHCP-tidsgräns	IPv6 DHCP-servern svarade inte.	Nätverket är upptaget – felen bör lösas minskar. Ingen nätverksanslutning mellan IPv6 telefonen: Kontrollera nätverksanslutni IPv6 DHCP-servern är nere: Kontrolle IPv6 DHCP-servern. Fel kvarstår: Överväg att tilldela en sta
IPv4 DNS-timeout	IPv4 DNS-servern svarade inte.	Nätverket är upptaget: Felen bör lösas minskar. Ingen nätverksanslutning mellan IPv4 telefonen: Kontrollera nätverksanslutni IPv4 DNS-servern är nere: Kontrollera DNS-servern.
IPv6 DNS-timeout	IPv6 DNS-servern svarade inte.	Nätverket är upptaget: Felen bör lösas minskar. Ingen nätverksanslutning mellan IPv6 telefonen: Kontrollera nätverksanslutni IPv6 DNS-servern är nere: Kontrollera DNS-servern.
Okänd IPv4-värd för DNS	IPv4 DNS kunde inte lösa namnet på TFTP-servern eller Cisco Unified Communications Manager.	Kontrollera att värdnamn för TFTP-ser Communications Manager har konfigur Överväg att använda IPv4-adresser i st
Okänd IPv6-värd för DNS	IPv6 DNS kunde inte lösa namnet på TFTP-servern eller Cisco Unified Communications Manager.	Kontrollera att värdnamn för TFTP-ser Communications Manager har konfigur Överväg att använda IPv6-adresser i st

Meddelande	Beskrivning	Möjlig förklaring och åtgärd
Programvara förkastad HC	Programmet som hämtades är inte kompatibelt med telefonens maskinvara.	Detta inträffar om du försöker insta programvaran på den här telefonen maskinvaruförändringar. Kontrollera det last-ID som tilldelat Unified Communications Manager Registrera om lasten som visas på t
Ingen standardrouter	DHCP eller den statiska konfigurationen anger inte en standardrouter.	Om telefonen har en statisk IP-adre standardroutern är konfigurerad. Om du använder DHCP, har DHCP standardrouter. Kontrollera DHCP-
Ingen IPv4 DNS-server	Ett namn angavs men DHCP eller den statiska IP-konfigurationen anger inte en IPv4 DNS-serveradress.	Om telefonen har en statisk IP-adres DNS-servern är konfigurerad. Om du använder DHCP, har DHCP DNS-server. Kontrollera DHCP-ser
Ingen IPv6 DNS-server	Ett namn angavs men DHCP eller den statiska IP-konfigurationen anger inte en IPv6 DNS-serveradress.	Om telefonen har en statisk IP-adres DNS-servern är konfigurerad. Om du använder DHCP, har DHCP DNS-server. Kontrollera DHCP-ser
Ingen lista med pålitliga adresser installerad	CTL-filen eller ITL-filen är inte installerade på telefonen.	Listan över betrodda är inte konfigu Communications Manager, som int standard. Listan över betrodda är inte konfigu Mer information om listor över betro till din utgåva av Cisco Unified Co
Telefonen gick inte att registrera. Certnyckelstorleken är inte FIPS-kompatibel.	FIPS kräver att servercertifikat RSA är 2048 bitar eller mer.	Uppdatera certifikatet.
Omstart begärd av Cisco Unified Communications Manager	Telefonen startar om på grund av en begäran från Cisco Unified Communications Manager.	Konfigurationsändringar har troliget Unified Communications Manager så att ändringarna införts.
TFTP-åtkomstfel	TFTP-servern pekar på en katalog som inte finns.	Om du använder DHCP ska du kon pekar på rätt TFTP-server. Om du använder statiska IP-adresse konfigurationen av TFTP-servern.
TFTP-fel	Telefonen känner inte igen en felkod som TFTP-servern har angett.	Kontakta Cisco TAC.

Meddelande	Beskrivning	Möjlig förklaring och åtgärd
TFTP: Timeout	TFTP-servern svarade inte.	Nätverket är upptaget: Felen bör lösas n minskar. Ingen nätverksanslutning mellan TFTP Kontrollera nätverksanslutningarna. TFTP-servern är nere: Kontrollera kon TFTP-servern.
Tidsgränsen överskreds	Försök med supplikant för 802.1X-transaktionen men tidsgränsen nåddes eftersom en autentisering saknades.	Autentiseringens tidsgräns nås typiskt konfigurerats i växeln.
Uppdateringen av lista med pålitliga adresser misslyckades	Uppdatering av CTL- och ITL-filer misslyckades.	Telefonen har CTL- och ITL-filer som inte att uppdatera nya CTL- och ITL-fi Möjliga orsaker till underkännande: • Ett nätverksfel inträffade. • TFTP-servern var nere. • Den nya säkerhetstoken som anvä CTL-filen och TFTP-certifikatet s signera ITL-filen har införts, men aktuella CTL- och ITL-filer i telef • Internt telefonfel inträffade. Möjliga lösningar: • Kontrollera nätverksanslutningen. • Kontrollera om TFTP-servern är ak • Om TVS-servern stöds i Cisco Un Manager kontrollerar du om TVS- fungerar normalt. • Kontrollera om säkerhetstoken och Ta bort CTL- och ITL-filer manuellt or lösningarna misslyckas och återställ tel Mer information om listor över betrodda till din utgåva av Cisco Unified Comm
Lista med pålitliga adresser uppdaterad	CTL- eller ITL-filen eller båda filerna uppdateras.	Ingen. Detta meddelande är endast för Mer information om listor över betrodda till din utgåva av Cisco Unified Comm
Versionsfel	Namnet på telefonens inläsningsfil är fel.	Se till att telefonens lastfil har rätt nam
XmlDefault.cnf.xml eller .cnf.xml som motsvarar telefonens enhetsnamn	Namn på konfigurationsfilen.	Ingen. Detta meddelande anger namnet för telefonen.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Visa fönstret Nätverksstatistik

Arbetsordning

Steg 1 Tryck på **Inställningar** > **Status** > **Nätverksstatistik**.

Steg 2 Om du vill lämna menyn trycker du på **Avsluta**.

Nätverksstatistikfält

Följande tabell beskriver informationen i nätverket statistik skärmen.

Tabell 23. Nätverksstatistikfält

Objekt	Beskrivning
Tx Frames	Antalet paket som skickas från telefonen
Tx broadcast	Antal broadcast-paket som skickas från telefonen
Tx unicast	Totalt antal unicast paket som sänds av telefonen
Rx Frames	Antal paket som har mottagits av telefonen
Rx broadcast	Antal broadcastpaket som tas emot av telefonen
Rx unicast	Totalt antal unicastpaket som tas emot av telefonen
Enhets-ID för CDP-granne	Identifierare av en enhet som är ansluten till denna port upptäcktes av CDP-protokollet.
IP-adress för CDP-granne	Identifierare av en enhet som är ansluten till denna port upptäcktes av CDP-protokollet med IP.
Port för CDP-granne	Identifierare av en enhet som är ansluten till denna port upptäcktes av CDP-protokollet.
Omstartsorsak: Ett av dessa värden: • Maskinvaruåterställning (återställning vid uppstart) • Programvaruåterställning (minneskontroller återställs också) • Programvaruåterställning (minneskontroller återställs inte) • Övervakningsåterställning • Initialized • Okänt	Orsaken till den senaste återställningen av telefonen

Objekt	Beskrivning
Port 1	Länktillstånd och anslutning av nätverksporten (till exempel **`100 Full`** innebär att PC-porten är i ett länkat tillstånd och automatiskt har full duplex, anslutning med 100-Mbps)
IPv4	Information om DHCP-status. Detta omfattar följande lägen: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • DISABLED DUPLICATE IP • SET DHCP COLDBOOT • SET DHCP DISABLED • SET DHCP FAST

Objekt	Beskrivning
IPv6	Information om DHCP-status. Detta omfattar följande lägen: • CDP INIT • DHCP6 BOUND • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6-INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DISABLED DUPLICATE IPV6 • DHCP6 DECLINED DUPLICATE IP • ROUTER ADVERTISE • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT CANNOT RESTORE • IPV6 STACK TURNED OFF • ROUTER ADVERTISE • ROUTER ADVERTISE • UNRECOGNIZED MANAGED BY • ILLEGAL IPV6 STATE

Visa fönstret Samtalsstatistik

Arbetsordning

Steg 1 Tryck på **Inställningar** > **Status** > **Samtalsstatistik**.

Steg 2 Om du vill lämna menyn trycker du på **Avsluta**.

Samtalsstatistikfält

I följande tabell beskrivs alternativen på Samtalsstatistikskärmen.

Tabell 24. Alternativ för samtalsstatistik

Objekt	Beskrivning
Mottagarcodec	Typ av mottagen röstström (RTP-strömmande ljud från codec): • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
Avsändarkodning	Typ av överförd röstström (RTP-strömmande ljud från codec): • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
Mottagarstorlek	Storlek på röstpaket, i millisekunder, i den mottagande röstströmmen (RTP strömmande ljud).
Avsändarstorlek	Storlek på röstpaket, i millisekunder, i den sändande röstströmmen.

Objekt	Beskrivning
Mott. paket	Antal RTP-röstpaket som inkommit sedan röstströmmen öppnas. **OBS!** Detta nummer är inte nödvändigtvis identiskt med antalet RTP-röstpaket som mottogs sedan samtalet började eftersom samtalet kan ha parkerats.
Sänd. paket	Antal RTP-röstpaket som överförts sedan röstströmmen öppnades. **OBS!** Detta antal är inte nödvändigtvis identiskt med antalet RTP-röstpaket som sänts sedan samtalet började eftersom samtalet kan ha parkerats.
Genomsn. jitter	Uppskattat genomsnittligt RTP-paketjitter (dynamisk fördröjning för ett paket vid överföring via nätverket), i millisekunder, som observerats sedan den mottagande röstströmmen öppnades.
Max jitter	Max jitter i millisekunder som observerats sedan den mottagande röstströmmen öppnades.
Mottagare ignorerad	Antal RTP-paket i den mottagande röstströmmen som ignorerades (dåliga paket, för sent och så vidare). **OBS!** Telefonen ignorerar komfortbruspaket av nyttolasttyp 19 som genereras av Cisco-gateways eftersom de ökar denna räknare.
Mott. förlorade pkt	Saknade RTP-paket (förlorade i transit).
Röstkvalitetsmått	
Dolt förhållande kumulativt	Totalt antal dolda ramar dividerat med det totala antalet talramar som mottogs från början av röstströmmen.
Dolt förhållande intervall	Förhållandet mellan dolda ramar och talramar i föregående 3-sekundersintervall av aktivt tal. Om du använder talaktivitetsdetektering (VAD) kan ett längre intervall krävas för att samla in 3 sekunders aktivt tal.
Dolt förhållande max	Högst intervall av andel dolda från början av röstströmmen.
Dolt sekunder	Antal sekunder som har dolda händelser (förlorade ramar) från början av röstströmmen (med allvarligt dolda sekunder).
Allvarligt dolt sekunder	Antal sekunder som har mer än 5 procent dolda händelser (förlorade ramar) från början av röstströmmen.
Fördröjning	Uppskattning av nätverkslatensen, uttryckt i millisekunder. Representerar ett löpande medelvärde av rundtursfördröjningen som mätts upp när RTCP-mottagarrapportblocken togs emot.

Webbsidan för Cisco IP-telefon

Varje Cisco IP-telefon har en webbsida där du kan se en mängd information om telefonen, inklusive:

- Enhetsinformation: Visar enhetsinställningar och relaterad information för telefonen.
- Nätverksinställning: Visar nätverksinställningsinformation och information om andra telefoninställningar.
- Nätverksstatistik: Visar hyperlänkar som ger information om nätverkstrafiken.
- Enhetsloggar: Visar hyperlänkar som ger information som du kan använda för felsökning.
- Strömningsstatistik: Visar hyperlänkar till en mängd olika strömmande statistik.

Detta avsnitt beskriver den information som du kan få från telefonen webbsida. Du kan använda denna information för att fjärrövervaka driften av en telefon och för att hjälpa till med felsökning.

Du kan också få en stor del av denna information direkt från en telefon.

Åtkomst till webbsidan för telefonen

OBS! Om du inte kan få tillgång till webbsidan, kan det vara inaktiverad som standard.

Arbetsordning

Steg 1 Skaffa IP-adressen för Cisco IP-telefon genom att använda någon av följande metoder:

a) Sök efter telefonen i Cisco Unified Communications Manager Administration genom att välja **Enhet** > **Telefon**. Telefoner som registrerar med Cisco Unified Communications Manager visar IP-adressen i fönstret Sök och lista telefoner och högst upp i fönstret Telefonkonfiguration.

b) Tryck på **Inställningar på telefonen och välj** > **Systeminformation**. Bläddra sedan till fältet IPv4-adress.

Steg 2 Öppna en webbläsare och ange följande URL, där *IP_address* är IP-adressen till Cisco IP-telefon:

http://<IP_address>

Webbsida med enhetsinformation

Området Enhetsinformation på en telefonwebbsida visar enhetsinställningar och relaterad information om telefonen. Följande tabell beskriver dessa poster.

Om du vill visa området med enhetsinformation öppnar du webbsidan för telefonen och klickar på hyperlänken **Enhetsinformation**.

Tabell 25. Webbsidans fält med enhetsinformation

Fält	Beskrivning
Tjänsteläge	Telefonens tjänsteläge.
Tjänstdomän	Domän för tjänsten.
Tjänstetillstånd	Aktuell status på tjänsten.
MAC-adress	MAC-adress till telefonen.
Värdnamn	Unikt, fast namn som tilldelas automatiskt till telefonen baserat på MAC-adressen.
Telefonnummer	Katalognummer som tilldelats till telefonen.
Programvaru-ID	Identifierar programladdningsversionen.
Bootladdnings-ID	Anger startladdningsversionen.
Version	ID på den fasta programvaran som körs i telefonen.
Maskinvaruversion	Mindre revisionsnummer på telefonens maskinvara.
Serienummer	Unikt serienummer på telefonen.
Modellnummer	Modellnummer på telefonen.
Meddelande väntar	Anger om ett röstmeddelande väntar på den primära linjen i den här telefonen.
UDI	Visar följande UDI-information (Cisco Unique Device Identifier) om telefonen: • Typ av maskinvara • Telefonmodell • Produkt-ID • Versions-ID (VID) – Anger det större versionsnumret för maskinvaran. • Serienummer
Tid	Tid i datum/tid-gruppen som telefonen tillhör. Denna information kommer från Cisco Unified Communications Manager.
Tidszon	Tidszon i datum/tid-gruppen som telefonen tillhör. Denna information kommer från Cisco Unified Communications Manager.
Datum	Datum i datum/tid-gruppen som telefonen tillhör. Denna information kommer från Cisco Unified Communications Manager.
Ledigt systemminne	Mängden tillgängligt systemminne.
Ledigt Java-heapminne	Mängden ledigt minne för Java-heapen.
Ledigt Java-poolminne	Mängden ledigt minne för Java-poolen.

Fält	Beskrivning
FIPS-läge aktiverat	Anger om FIPS-läge (Federal Information Processing Standard) har aktiverats.

Webbsida för nätverksinställning

I området Nätverksinställning på en telefonwebbsida visas nätverksinställningsinformation och information om andra telefoninställningar. Följande tabell beskriver dessa poster.

Du kan visa och ställa in många av dessa alternativ från menyn Nätverksinställning på Cisco IP-telefon.

Om du vill visa området Nätverksinställning öppnar du webbsidan för telefonen och klickar sedan på hyperlänken **Nätverksinställning**.

Tabell 26. Alternativ i området Nätverksinställning

Objekt	Beskrivning
MAC-adress	MAC-adress till telefonen.
Värdnamn	Värdnamn som DHCP-servern tilldelat till telefonen.
Domännamn	Namn på DNS-domän där telefonen befinner sig.
DHCP-server	IP-adress till DHCP-servern där telefonen erhåller IP-adressen.
BOOTP-server	Anger om telefonen hämtar sin konfiguration från en BOOTP-server.
DHCP	Anger om telefonen använder DHCP.
IP-adress	IP-adress till telefonen.
Nätmask	Nätmask som telefonen använder.
Standardrouter 1	Standardrouter som telefonen använder.
DNS-server 1–3	Primär DNS-server (DNS-server 1) och valfria DNS-reservservrar (DNS-server 2 och 3) som t använder.
Alt. TFTP	Anger om telefonen använder en alternativ TFTP-server.
TFTP-server 1	Primär TFTP-server som telefonen använder.
TFTP-server 2	TFTP-reservserver som telefonen använder.
DHCP-adressen släppt	Anger inställningen av alternativet DHCP-adressen släppt.
Operativt VLAN-ID	Operativt VLAN som är konfigurerat i en Cisco Catalyst-växel där telefonen är medlem.
Administrativt VLAN-ID	Extra-VLAN där telefonen är medlem.

Objekt	Beskrivning
Unified CM 1–5	Värdnamn eller IP-adresser, i prioriterad ordning, för Cisco Unified Communications Man som telefonen kan registrera. Ett alternativ kan också visa IP-adressen för en SRST-router begränsad Cisco Unified Communications Manager-funktion, om en sådan router är tillgä För en tillgänglig server visar ett alternativ Cisco Unified Communications Manager-server och ett av följande tillstånd: • Aktivt: Cisco Unified Communications Manager-server där telefonen för närvarande samtalsbehandlingstjänster • Standby: Cisco Unified Communications Manager-server som telefonen växlar över aktuella servern blir otillgänglig • Tomt: Ingen aktuell anslutning till denna Cisco Unified Communications Manager-s Ett alternativ kan även omfatta en SRST-beteckning som identifierar en SRST-router för C Communications Manager med en begränsad uppsättning funktioner. Denna router förutsä av samtalsbehandlingen om alla andra Cisco Unified Communications Manager-servrar b SRST Cisco Unified Communications Manager visas alltid visas sist i listan över servrar, ä är aktiv. Du kan konfigurera SRST-routeradressen i avsnittet Enhetsgrupp i fönstret Cisco Communications Manager Configuration.
Info URL	URL till hjälptexten som visas på telefonen.
Katalog URL	URL till den server där telefonen hämtar kataloginformation.
Medd. URL	URL till den server där telefonen hämtar meddelandetjänster.
Tjänster URL	URL till den server där telefonen hämtar Cisco IP-telefon-tjänster.
Passiv URL	URL som visas på telefonen när telefonen är i viloläge under den tid som anges i fältet In ingen meny är öppen.
Passiv URL-timer	Antal sekunder som telefonen är i viloläge och ingen meny är öppen innan XML-tjänsten i URL för inaktivitet aktiveras.
Proxyserver-URL	URL till proxyservern som gör HTTP-begäranden till icke-lokala värdadresser på uppdrag a HTTP-klient och ger svar från den icke-lokala värden till telefonens HTTP-klient.
URL för verifiering	URL som telefonen använder för att validera förfrågningar som görs till telefonens webbs
SWport-inställning	Hastighet och duplex i växelporten, där: • A = Autobalansering • 10H = 10-BaseT/halv duplex • 10F = 10-BaseT/full duplex • 100H = 100-BaseT/halv duplex • 100F = 100-BaseT/full duplex • 1000F = 1000-BaseT/full duplex • Ingen länk = Ingen anslutning till växelporten
Användarspråk	Användarspråk som associeras med telefonanvändaren. Identifierar en uppsättning detaljera för att stödja användare, inklusive språk, teckensnitt, datum- och tidsformat och textinfor alfanumeriskt tangentbord.

Objekt	Beskrivning
Nätverksspråk	Nätverksspråk som associeras med telefonanvändaren. Identifierar en uppsättning detaljerade u till stöd för telefonen i ett visst läge, inklusive definitioner av toner och kadenser som telefonen a
Användarspråkversion	Version av användarens språk som laddas på telefonen.
Version av nätverksspråk	Version av nätverksspråk som laddas på telefonen.
Högtalare aktiverad	Anger om högtalartelefonen är aktiverad på telefonen.
Grupplyssna	Anger om grupplyssningsfunktionen är aktiverad på telefonen. Med grupplyssning kan du pr mobiltelefonen och lyssna i högtalartelefonen samtidigt.
GARP aktiverat	Anger om telefonen lär in MAC-adresser från svar på opåkallad ARP.
Autom. linjeval aktiverat	Anger om telefonen skiftar samtalsfokus mot inkommande samtal på alla linjer.
DSCP för samtalskontroll	DSCP IP-klassificering för samtalsstyrsignalering.
DSCP för konfiguration	DSCP IP-klass för alla telefonkonfigurationsöverföringar.
DSCP för tjänster	DSCP IP-klass för telefonbaserade tjänster.
Säkerhetsläge	Säkerhetsläge som är inställt för telefonen.
Webbåtkomst aktiverad	Anger om webbåtkomst är aktiverad (Ja) eller inaktiverad (Nej) för telefonen.
SSH-åtkomst aktiverad	Anger om telefonen accepterar eller blockerar SSH-anslutningar.
CDP: SW-port	Anger om CDP-stöd finns i väljarporten (aktiverat som standard). Aktivera CDP-växelporten för VLAN-tilldelning till telefonen, strömbalansering, QoS-hante 802.1X-säkerhet. Aktivera CDP i växelporten när telefonen ansluts till en Cisco-växel. När CDP är inaktiverat i Cisco Unified Communications Manager visas en varning som indi CDP endast ska inaktiveras i väljarporten om telefonen är ansluten till en annan växel än Cis CDP-värden för nuvarande PC- och växelport visas på inställningsmenyn.
LLDP-MED: SW-port	Anger om LLDP-MED har aktiverats i väljarporten.
LLDP-kraftsprioritet	Annonserar telefonströmprioriteringar till växeln så att växeln kan fördela ström till telefone Inställningar: • Okänt: Detta är standardvärdet. • Låg • hög • Kritiskt
LLDP tillgångs-ID	Identifierar resurs-ID som tilldelas till telefonen för lagerhantering.
CTL-fil	Identifierar CTL-filen.
ITL-fil	ITL-filen innehåller den initiala listan över betrodda anslutningar.

Objekt	Beskrivning
ITL-signatur	Ökar säkerheten med hjälp av säker hash-algoritm (SHA-1) i CTL- och ITL-filer.
CAPF-server	Namnet på CAPF-servern som används av telefonen.
TVS	Den viktigaste komponenten i Säkerhet som standard. Med TVS kan Cisco Unified IP-telefo programservrar som EM-tjänster, katalogen och MIDlet:ar under HTTPS-etableringen.
TFTP-server	Namnet på den TFTP-server som används av telefonen.
Automatisk portsynkronisering	Synkroniserar portar till den lägre hastigheten som eliminerar paketförluster.
Fjärrkonfiguration för växelport	Låter administratören fjärrkonfigurera hastighet och funktion i Cisco Desktop Collaborat Experience-tabellporten med hjälp av Cisco Unified Communications Manager Administ
Fjärrkonfiguration för PC-port	Anger om fjärrportkonfiguration av hastigheten och duplexläget för PC-porten är aktivera inaktiverad.
IP-adresseringsläge	Visar IP-adresseringsläget som finns i telefonen.
IP-inställningsläge	Anger IP-adressversion som telefonen använder under signalering med Cisco Unified Com Manager när både IPv4 och IPv6 är tillgängliga på telefonen.
IP-inställningsläge för media	Anger att enheten använder en IPv4-adress vid anslutning till Cisco Unified Communicatio
Automatisk IPv6-konfiguration	Visar om automatisk konfiguration aktiverats eller inaktiverats på telefonen.
IPv6 DAD	Verifierar att nya unicast IPv6-adresser är unika innan adresserna tilldelas till gränssnitter
IPv6-godkänd omdirigering av meddelanden	Anger om telefonen accepterar omdirigeringsmeddelanden från samma router som använ destinationsnummer.
IPv6-svar på begäran om multicast-eko	Anger att telefonen skickar ett Echo Reply-meddelande som svar på ett Echo Request-med skickats till en IPv6-adress.
IPv6-laddningsserver	Används för att optimera installationstiden för uppgradering av telefonens fasta programvar WAN genom att lagra bilder lokalt för att eliminera behovet att korsa WAN-länken för va uppgradering.
IPv6-loggserver	Anger IP-adress och port till fjärrloggningsdatorn dit telefonen skickar loggmeddelanden
IPv6-CAPF-server	Vanligt namn (från Cisco Unified Communications Manager-certifikatet) i CAPF som an telefonen.
DHCPv6	DHCP tilldelar automatiskt IPv6-adressen till enheter när du ansluter dem till nätverket. C IP-telefon aktiverar DHCP som standard.
IPv6-adress	Visar aktuell IPv6-adress på telefonen eller tillåter användaren att ange en ny IPv6-adress
IPv6-prefixlängd	Visar aktuell prefixlängd för undernätet eller tillåter användaren att ange en ny prefixläng

Objekt	Beskrivning
IPv6-standardrouter 1	Visar standardrouter som används av telefonen eller tillåter användaren att ange en ny IPv6-standardrouter.
IPv6 DNS-server 1	Visar den primära DNSv6-server som används av telefonen eller tillåter användaren att ange server.
IPv6 DNS-server 2	Visar den sekundära DNSv6-server som används av telefonen eller tillåter användaren att stä ny sekundär DNSv6-server.
Alternativ IPv6 TFTP	Tillåter användaren att möjliggöra användningen av en alternativ (sekundär) IPv6 TFTP-serv
IPv6 TFTP-server 1	Visar den primära IPv6 TFTP-server som används av telefonen eller tillåter användaren att stä ny primär TFTP-server.
IPv6 TFTP-server 2	Visar den sekundära IPv6 TFTP-server som används om den primära IPv6 TFTP-servern int tillgänglig eller tillåter användaren att ställa in en ny sekundär TFTP-server.
IPv6-adressen släppt	Tillåter användaren att släppa IPv6-relaterad information.
Energywise-strömnivå	Ett mått på den energi som förbrukas av enheter i ett EnergyWise-nätverk.
EnergyWise-domän	En administrativ gruppering av enheter i syfte att effektivisera strömövervakning och kontrol

Webbsida med Ethernet-information

Följande tabell beskriver innehållet på webbsidan med Ethernet-Information.

Tabell 27. Alternativ för Ethernet-information

Objekt	Beskrivning
Tx Frames	Totalt antal paket som telefonen sänder.
Tx broadcast	Totalt antal broadcastpaket som telefonen sänder.
Tx multicast	Totalt antal multicastpaket som telefonen sänder.
Tx unicast	Totalt antal unicastpaket som telefonen sänder.
Rx Frames	Totalt antalet paket som tas emot av telefonen.
Rx broadcast	Totalt antal broadcastpaket som telefonen tar emot.
Rx multicast	Totalt antalet multicastpaket som telefonen tar emot.
Rx unicast	Totalt antal unicastpaket som telefonen tar emot.
Rx PacketNoDes	Totalt antal distributionspaket som genererats av en DMA-beskrivning (Direct Memory Access).

Webbsidor för nätverket

I följande tabell beskrivs informationen på webbsidor för nätverksområdet.

OBS! När du klickar på länken till **Nätverk** under Nätverksstatistik öppnas sidan ”Portinformation”.

Tabell 28. Alternativ i nätverksområdet

Objekt	Beskrivning
Rx totalPkt	Totalt antal paket som telefonen tagit emot.
Rx multicast	Totalt antal multicastpaket som telefonen tagit emot.
Rx broadcast	Totalt antal sändningspaket som telefonen tagit emot.
Rx unicast	Totalt antal unicastpaket som telefonen tagit emot.
Rx tokenDrop	Totalt antal paket som tagits bort på grund av resursbrist (till exempel FIFO Overflow).
Tx totalGoodPkt	Totalt antal godtagna paket (multicast, broadcast och unicast) som telefonen tagit emot.
Tx broadcast	Totalt antal broadcastpaket som telefonen överfört.
Tx multicast	Totalt antal multicastpaket som telefonen överfört.
LLDP FramesOutTotal	Totalt antal LLDP-ramar som telefonen skickat ut.
LLDP AgeoutsTotal	Totalt antal LLDP-ramar som nådde tidsgränsen i cacheminnet.
LLDP FramesDiscardedTotal	Totalt antal LLDP-ramar som ignorerats när någon obligatorisk TLV saknats, varit utanför intervall eller haft för lång stränglängd.
LLDP FramesInErrorsTotal	Totalt antal LLDP-ramar som tagits emot med ett eller flera detekterbara fel.
LLDP FramesInTotal	Totalt antal LLDP-ramar som telefonen tagit emot.
LLDP TLVDiscardedTotal	Totalt antal LLDP TLV som ignorerats.
LLDP TLVUnrecognizedTotal	Totalt antal LLDP TLV som inte kunnat identifieras i telefonen.
Enhets-ID för CDP-granne	Ett ID på en enhet som är ansluten till denna port som identifierats av CDP.
IP-adress för CDP-granne	IP-adress till närliggande enhet har identifierats under CDP-protokollidentifieringen.
IPv6-adress för CDP-granne	IPv6-adress till närliggande enhet har identifierats under CDP-protokollidentifieringen.

Objekt	Beskrivning
Port för CDP-granne	Port till närliggande enhet som telefonen är ansluten till har identifierats av CDP-protokollet.
Enhets-ID för LLDP-granne	Ett ID på en enhet som är ansluten till denna port som identifierats av LLDP.
IP-adress för LLDP-granne	IP-adress till närliggande enhet har identifierats av LLDP-protokollet.
Iv6P-adress för LLDP-granne	IPv6-adress till närliggande enhet har identifierats av CDP-protokollet.
Port för LLDP-granne	Port till närliggande enhet som telefonen är ansluten till har identifierats av LLDP-protokollet.
Portinformation	Hastighet och duplexinformation.

Webbsidor för konsolloggar, kärndumpar, statusmeddelanden och felsökningsvy

Under rubriken Enhetsloggar visas hyperlänkar till konsolloggar, kärndumpar, statusmeddelanden och felsökningsvyn som ger information och hjälp vid övervakning och felsökning av telefonen.

- Konsolloggarna: Innehåller hyperlänkar till enskilda loggfiler. Konsolloggfilerna innehåller felsökningar och felmeddelanden som telefonen tagit emot.
- Kärndumpar: Innehåller hyperlänkar till enskilda dumpfiler. Kärndumpfiler inkluderar data från en telefonkrasch.
- Statusmeddelanden: Visar de tio senaste statusmeddelanden som telefonen har genererat sedan den senast startades. Du hittar även den här informationen på telefonens statusmeddelandeskärm.
- Visa felsökning: Visar felsökningsmeddelanden som kan vara till nytta för Cisco TAC om du behöver hjälp med felsökning.

Webbsida för direktspelningsstatistik

Cisco IP-telefon kan strömma information till och från upp till fem enheter samtidigt. En telefon strömmar information när det är på ett samtal eller kör en tjänst som skickar eller tar emot ljud eller data.

Det finns områden med strömningsstatistik på telefonens webbsida som ger information om strömmarna.

Om du vill visa ett område med strömningsstatistik öppnar du webbsidan för telefonen och klickar på en **strömningshyperlänk**.

Följande tabell beskriver postern i strömningsstatistikområdena.

Tabell 29. Fält för direktspelningsstatistik

Objekt	Beskrivning
Fjärradress	IP-adress och UDP-port för strömningsdestinationen.

Objekt	Beskrivning
Lokal adress	IP-adress och UPD-port på telefonen.
Starttid	En intern tidsstämpel visar när Cisco Unified Communications Manager begärde at skulle börja sända paket.
Strömstatus	Indikering om strömning är aktiverat eller inte.
Värdnamn	Unikt, fast namn som tilldelas automatiskt till telefonen baserat på MAC-adressen.
Sänd. paket	Totalt antal RTP-datapaket som telefonen överfört sedan starten av denna anslutnin är 0 om anslutningen är inställd på endast mottagning (skyddat läge).
Sänd. oktetter	Totalt antal lastoktetter av standardnyttolast som telefonen överfört i RTP-datapake starten av denna anslutning. Värdet är 0 om anslutningen är inställd på endast motta (skyddat läge).
Avsändarkodning	Typ av ljudkodning som används för den överförda strömmen.
Avsändarrapporter sända (se not)	Antal gånger RTCP-avsändarrapporten har skickats.
Avsändarrapport sänd tid (se not)	Intern tidsstämpel indikation på när den sista RTCP Sender Rapporten skickades.
Mott. förlorade pkt	Totalt antal RTP datapaket som har gått förlorade sedan datamottagning startade de sammanhang. Definieras som antalet förväntade paket mindre antalet paket faktiskt antalet mottagna paket omfattar alla som är sent eller är dubbletter. Värdet visas so anslutningen var inställd på skicka skyddat läge.
Genomsn. jitter	Uppskattning av medelavvikelse för RTP-datapaketet interarrival tid, mätt i millisel Värdet visas som 0 om anslutningen var inställd på skicka skyddat läge.
Mottagarcodec	Typ av ljudkodning som används för den mottagna strömmen.
Mottagarrapporter sända (se not)	Antal gånger RTCP mottagare Rapporter har skickats.
Mottagarrapport sänd tid (se not)	Intern tidsstämpel indikation om när en RTCP mottagare rapport har skickats.
Mott. paket	Totalt antal RTP datapaket som telefonen har fått sedan datamottagning startade de sammanhang. Inkluderar paket som mottogs från olika källor om det här samtalet är e samtal. Värdet visas som 0 om anslutningen var inställd på skicka skyddat läge.
Mott. oktetter	Totalt antal lastoktetter att enheten fått i RTP datapaket sedan mottagning började p anslutningen. Inkluderar paket som mottogs från olika källor om det här samtalet är e samtal. Värdet visas som 0 om anslutningen var inställd på skicka skyddat läge.
Dolt förhållande kumulativt	Totalt antal hemlighållande ramar dividerat med totala antalet talramar som mottogs av röstströmmen.

Objekt	Beskrivning
Dolt förhållande intervall	Förhållandet mellan hemlighållande ramar till talramar i föregående 3-sekundersinterva aktivt tal. Om röstaktivitetsdetektering (VAD) är i bruk, kan ett längre intervall krävas samla tre sekunder aktivt tal.
Dolt förhållande max	Högsta intervall dölja förhållandet från början av röstströmmen.
Dolt sekunder	Antal sekunder som har dolda händelser (förlorade ramar) från början av röstströmmen allvarligt dolda sekunder).
Allvarligt dolt sekunder	Antal sekunder som har mer än fem procent döljande händelser (förlorade ramar) från av röstströmmen.
Fördröjning (se not)	Uppskattning av nätverkslatensen, uttryckt i millisekunder. Representerar ett löpande med av rundtursfördröjningen som mätts upp när RTCP-mottagarrapportblocken togs emot.
Max jitter	Maximalt värde av momentant jitter, i millisekunder.
Avsändarstorlek	RTP-paketstorleken, i millisekunder, för den översända strömmen.
Avsändarrapporter mottagna (se not)	Antal gånger RTCP-avsändarrapporter har mottagits.
Avsändarrapport mottagen tid (se not)	Senaste gången en RTCP-avsändarrapport mottogs.
Mottagarstorlek	RTP-paketstorleken, i millisekunder, för den mottagna strömmen.
Mottagare ignorerad	RTP-paket som tagits emot från nätet men ignorerats av jitterbuffertarna.
Mottagarrapporter mottagna (se not)	Antal gånger RTCP-mottagarerapporter togs emot.
Mottagarrapport mottagen tid (se not)	Senaste gången en RTCP-mottagarrapport mottogs.

OBS! När RTP-kontrollprotokollet har inaktiverats genereras inga data för detta fält så då visas det som 0.

Begära information från telefonen i XML

För felsökning kan du begära information från telefonen. Den resulterande informationen är i XML-format. Följande information finns tillgänglig:

- Samtalsinfo är samtalssessionsinformation för en viss linje.
- Linjeinfo är linjekonfigurationsinformation för telefonen.

- Lägesinfo är telefonlägesinformation.

Innan du börjar

Webbåtkomst måste vara aktiverat för att få information.

Telefonen måste vara associerad med en användare.

Arbetsordning

Steg 1 För samtalsinfo anges följande URL i en webbläsare: **http://<phone ip address>/CGI/Java/CallInfo<x>**

där

- <*phone ip address*> är telefonens IP-adress
- <*x*> är linjenumret som informationen avser.

Kommandot returnerar ett XML-dokument.

Steg 2 För linjeinfo anges följande URL i en webbläsare: **http://<phone ip address>/CGI/Java/LineInfo**

där

- <*phone ip address*> är telefonens IP-adress

Kommandot returnerar ett XML-dokument.

Steg 3 För modellinfo anges följande URL i en webbläsare: **http://<phone ip address>/CGI/Java/ModeInfo**

där

- <*phone ip address*> är telefonens IP-adress

Kommandot returnerar ett XML-dokument.

Exempel på utdata från CallInfo

Följande XML-kod är ett exempel på utdata från kommandot CallInfo.

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneCallLineInfo>
  <Prompt/>
  <Notify/>
  <Status/>
  <LineDirNum>1030</LineDirNum>
  <LineState>CONNECTED</LineState>
  <CiscoIPPhoneCallInfo>
     <CallState>CONNECTED</CallState>
     <CallType>INBOUND</CallType>
     <CallingPartyName/>
```

```
      <CallingPartyDirNum>9700</CallingPartyDirNum>
      <CalledPartyName/>
      <CalledPartyDirNum>1030</CalledPartyDirNum>
      <HuntPilotName/>
      <CallReference>30303060</CallReference>
      <CallDuration>12835</CallDuration>
      <CallStatus>null</CallStatus>
      <CallSecurity>UNAUTHENTICATED</CallSecurity>
      <CallPrecedence>ROUTINE</CallPrecedence>
      <FeatureList/>
    </CiscoIPPhoneCallInfo>
    <VisibleFeatureList>
      <Feature Position="1" Enabled="true" Label="End Call"/>
      <Feature Position="2" Enabled="true" Label="Show Detail"/>
    </VisibleFeatureList>
</CiscoIPPhoneCallLineInfo>
```

Exempel på utdata från LineInfo

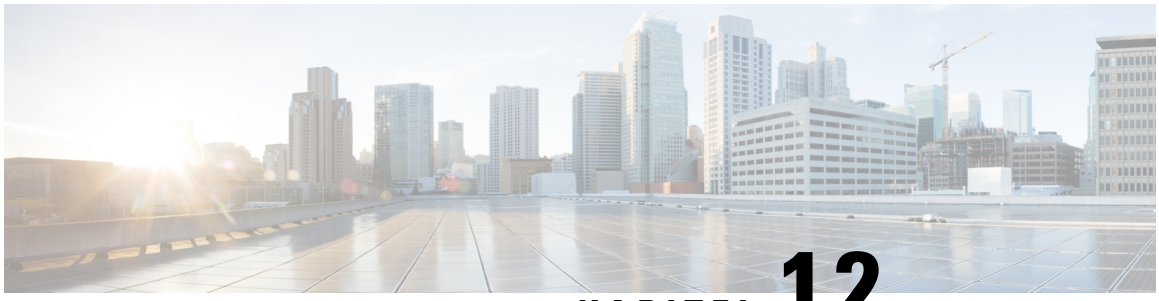
Följande XML-koden är ett exempel på utdata från kommandot LineInfo.

```
<CiscoIPPhoneLineInfo>
   <Prompt/>
   <Notify/>
   <Status>null</Status>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1028</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1029</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>  <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1030</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>CONNECTED</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>2</LineType>
     <lineDirNum>9700</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <LineLabel>SD9700</LineLabel>
     <LineIconState>ON</LineIconState>
  </CiscoIPPhoneLines>
</CiscoIPPhoneLineInfo>
```

Exempel på utdata från ModeInfo

Följande XML-kod är ett exempel på utdata från kommandot ModeInfo.

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
   <PlaneTitle>Applications</PlaneTitle>
   <PlaneFieldCount>12</PlaneFieldCount>
   <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
   <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
   <Prompt></Prompt>
   <Notify></Notify>
   <Status></Status>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Call History</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Preferences</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   ...
</CiscoIPPhoneModeInfo>
```



KAPITEL 12

Felsökning av telefonen

Allmän felsökning

Följande tabell innehåller allmän information om felsökning för Cisco IP-telefon.

Tabell 30. Felsökning för Cisco IP-telefon

Sammanfattning	Förklaring
Vid långvariga sändningsstormar kan IP-telefonerna återställas eller så kanske det inte går att ringa eller ta emot samtal	En långvarig lager 2-sändningsstorm (under flera minuter) i röst-VLAN k att IP-telefoner återställas eller ett aktivt samtal bryts, eller så går det in eller svara på samtal. Telefonerna kanske inte fungerar igen förrän sändn slutar.
Flytta en nätverksanslutning från telefonen till en arbetsstation	Om du startar din telefon via nätverksanslutningen måste du vara försil sedan väljer att koppla från nätverksanslutningen på telefonen och anslu en stationär dator. **Försiktighet** Nätverkskortet i datorn kan inte få ström genom nätverksanslutningen. Om anslutningen är strömförande k nätverkskortet förstöras. För att skydda nätverkskortet ska sekunder eller längre efter att du kopplat loss kabeln från tele du ansluter den till en dator. Denna fördröjning ger omkop tillräckligt med tid att inse att det inte längre finns en telef och sluta ge ström till kabeln.

Sammanfattning	Förklaring
Ändra telefonkonfigurationen	Som standard är administratörslösenordsinställningarna låsta för att hindra a från att göra ändringar som kan påverka deras nätverksanslutning. Du måste administratörslösenordsinställningarna innan du kan konfigurera dem. Mer information finns i Använda ett telefonlösenord, på sidan 41. **OBS!** Om administratörslösenordet inte är inställt i en allmän telefon kan användaren ändra nätverksinställningarna.
Kodfelmatchning mellan telefonen och en annan enhet	Statistik om RxType och TxType visar koden som används för samtal mell Cisco IP-telefon och den andra enheten. Värdena i statistiken måste match inte gör det ska du kontrollera att den andra enheten kan hantera kodsamtal det finns en transkoder för att hantera tjänsten. Mer information finns i Vis Samtalsstatistik, på sidan 134.
Ljudfelmatchning mellan telefonen och en annan enhet	Statistik om RxSize och TxSize visar storleken på röstpaketet som används i mellan denna Cisco IP-telefon och den andra enheten. Värdena i statistiken matcha. Mer information finns i Visa fönstret Samtalsstatistik, på sidan 13
Loopback	En loopback kan inträffa under följande förutsättningar: • SW-portkonfigurationen i telefonen är 10 halv (10-BaseT/halv duplex • Telefonen får ström från en extern strömkälla. • Telefonen är avstängd (strömförsörjningen är frånkopplad). I detta fall kan växelporten på telefonen inaktiveras och följande meddelar i växelkonsolloggen: HALF_DUX_COLLISION_EXCEED_THRESHOLD För att lösa detta problem måste du återaktivera porten från växeln.

Startproblem

När du har installerat en telefon i nätverket och lagt till den i Cisco Unified Communications Manager, bör telefonen startas så som beskrivs i det relaterade ämnet nedan.

Om telefonen inte startar på rätt sätt läser du följande avsnitt för information om felsökning.

Relaterade ämnen

Kontrollera att telefonen startar, på sidan 52

Cisco IP-telefon går inte igenom den normala startprocessen

Problem

När du ansluter en Cisco IP-telefon i nätverksporten går inte telefonen igenom den normala startprocessen som beskrivs i det relaterade ämnet och telefonens skärm visar ingen information.

Orsak

Om telefonen inte går igenom startprocessen kan det bero på dåliga kablar, dåliga anslutningar, nätverksfel, strömbrist eller att telefonen inte fungerar.

Lösning

Kontrollera att telefonen är fungerar med hjälp av följande förslag, för att eliminera andra möjliga problem.

- Byt ut Ethernet-kablar mot kablar som du vet fungerar.
    - Byt ut Ethernet-kablar mot kablar som du vet fungerar.
    - Koppla ur en fungerande Cisco IP-telefon från en annan port och anslut den till den här nätverksporten för att kontrollera om porten är aktiv.
    - Anslut den Cisco IP-telefon som inte startar till en annan nätverksport som du vet fungerar.
    - Anslut den Cisco IP-telefon som inte startar direkt till porten på växeln. Detta eliminerar anslutningen till kopplingspanelen på kontoret.
- Kontrollera att telefonen får ström:
    - Om du använder en extern strömkälla så kontrollera att eluttaget fungerar.
    - Om du använder ett vägguttag ska du prova en extern strömkälla i stället.
    - Om du använder extern strömförsörjning ska du byta till en enhet som du vet fungerar.
- Om telefonen fortfarande inte startar ordentligt ska du prova att starta telefonen från programvaruavbildningen från en säkerhetskopia.
- Om telefonen fortfarande inte startar på rätt sätt gör du en fabriksåterställning av telefonen.
- Om du försökt med dessa lösningar och telefonens skärm på Cisco IP-telefon inte visar några tecken efter minst fem minuter kontaktar du en Cisco-supportrepresentant för att få ytterligare hjälp.

Relaterade ämnen

Kontrollera att telefonen startar, på sidan 52

Cisco IP-telefon registreras inte i Cisco Unified Communications Manager

Om telefonen fortsätter förbi första steget i startprocessen (LED-knappar blinkar på och av) men fortsätter att gå igenom de meddelanden som visas på telefonens skärm har telefonen inte startats på rätt sätt. Telefonen kan inte starta om den ansluts till Ethernet-nätverk och den registreras på en Cisco Unified Communications Manager-server.

Dessutom kan problem med säkerhet förhindra att telefonen startar ordentligt. Mer information finns i Felsökningsförfaranden, på sidan 162.

Telefonen visar felmeddelanden

Problem

Statusmeddelanden visar fel vid start.

Lösning

När telefonen går igenom startprocessen, kan du komma åt statusmeddelanden som kan ge dig information om orsaken till ett problem. Se avsnittet i ”fönstret Visa statusmeddelanden” för att visa instruktioner om åtkomst till statusmeddelanden och för en lista över potentiella fel, förklaringar och lösningar.

Relaterade ämnen

Visa fönstret Statusmeddelanden, på sidan 126

Telefonen kan inte ansluta till TFTP-servern eller till Cisco Unified Communications Manager

Problem

Om nätverket är nere mellan telefonen och antingen TFTP-servern eller Cisco Unified Communications Manager, kan telefonen inte starta på rätt sätt.

Lösning

Se till att nätverket är igång.

Telefonen kan inte ansluta till TFTP-servern

Problem

TFTP-serverinställningarna kanske inte är rätt.

Lösning

Kontrollera TFTP-inställningarna.

Relaterade ämnen

Kontrollera TFTP-inställningar, på sidan 163

Telefonen kan inte ansluta till servern

Problem

IP-adresserings- och routningsfälten kan inte konfigureras korrekt.

Lösning

Du bör kontrollera IP-adresserings- och routningsinställningarna på telefonen. Om du använder DHCP bör DHCP-servern tillhandahålla dessa värden. Om du har tilldelat en statisk IP-adress till telefonen måste du ange dessa värden manuellt.

Relaterade ämnen

Kontrollera DHCP-inställningar, på sidan 164

Telefonen kan inte ansluta med DNS

Problem

DNS-inställningarna kan vara felaktiga.

Lösning

Om du använder DNS för att få tillgång till TFTP-servern eller Cisco Unified Communications Manager måste du se till att du anger en DNS-server.

Relaterade ämnen

Verifiera DNS-inställningar, på sidan 165

Cisco Unified Communications Manager och TFTP-tjänsterna körs inte

Problem

Om Cisco Unified Communications Manager eller TFTP-tjänster inte körs, kan telefoner inte att kunna starta ordentligt. I en sådan situation, är det troligt att du upplever en hela systemet som fel och andra telefoner och enheter kan inte starta ordentligt.

Lösning

Om Cisco Unified Communications Manager-tjänsten inte körs påverkas alla enheter i nätverket som är beroende av den för att ringa samtal. Om TFTP tjänsten inte är igång, kan många enheter inte starta. Mer information finns i Starta tjänst, på sidan 165.

Skadad konfigurationsfil

Problem

Om du fortsätter att ha problem med ett visst telefonnummer som andra förslag i detta kapitel inte lösa, kan konfigurationsfilen vara skadad.

Lösning

Skapa en ny telefonkonfigurationsfil.

Relaterade ämnen

Skapa en ny telefonkonfigurationsfil, på sidan 164

Telefonregistrering i Cisco Unified Communications Manager

Problem

Telefonen är inte registrerad i Cisco Unified Communications Manager

Lösning

En Cisco IP-telefon kan endast registreras på en Cisco Unified Communications Manager-server om telefonen läggs till på servern eller om automatisk registrering har aktiverats. Granska information och förfaranden i Telefontilläggsmetoder, på sidan 60 för att säkerställa att telefonen lagts till i Cisco Unified Communications Manager-databasen.

Om du vill kontrollera att telefonen finns i Cisco Unified Communications Manager-databasen väljer du **Enhet** > **Telefon** från Cisco Unified Communications Manager Administration. Klicka på **Sök** och sök efter telefonen

baserat på MAC-adressen. Mer information om att fastställa en MAC-adress finns i Fastställ telefonens MAC-adress, på sidan 59.

Om telefonen redan finns i Cisco Unified Communications Manager-databasen kan konfigurationsfilen vara skadad. I Skadad konfigurationsfil, på sidan 155 finns det mer information.

Cisco IP-telefon kan inte hämta IP-adressen

Problem

Om en telefon inte kan hämta en IP-adress när den startas kanske den inte är i samma nätverk eller VLAN som DHCP-servern, eller växelport som telefonen ansluter till kan ha inaktiverats.

Lösning

Se till att nätverket eller VLAN som telefonen ansluter till har åtkomst till DHCP-servern och se till att växelporten är aktiverad.

Problem med telefonåterställning

Om användarna rapporterar att deras telefoner återställs under samtal eller när telefonerna är inaktiva, bör du undersöka orsaken. Om nätverksanslutningen och Cisco Unified Communications Manager-anslutningen är stabila, bör en telefon inte återställas.

En telefon återställs typiskt om den har problem med att ansluta till nätverket eller Cisco Unified Communications Manager.

Telefonen återställs på grund av intermittent nätverksfel

Problem

Nätverket kan ha intermittenta avbrott.

Lösning

Periodiska driftsstopp i nätverket påverkar data- och rösttrafik på olika sätt. Ditt nätverk kan ha drabbats av återkommande avbrott utan att det upptäckts. I så fall kan datatrafiken skicka om tappade paket och också verifiera att paketen tas emot och överförs. Rösttrafiken kan dock inte skicka om förlorade paket. Snarare än att återsända en förlorad nätverksanslutning försöker telefonen återställa sig och ansluta till nätverket igen. Kontakta systemadministratören för information om kända problem i röstnätverket.

Telefonen återställs grund av DHCP-inställningsfel

Problem

DHCP-inställningarna kan vara felaktiga.

Lösning

Kontrollera att du har konfigurerat telefonen för användning av DHCP. Kontrollera att DHCP-servern är rätt inställd. Kontrollera att DHCP-lånetiden. Vi rekommenderar att du ställer lånetiden till 8 dagar.

Relaterade ämnen

Kontrollera DHCP-inställningar, på sidan 164

Telefon återställs på grund av felaktig statisk IP-adress

Problem

Den statiska IP-adress som tilldelats telefonen kan vara felaktig.

Lösning

Om telefonen har tilldelats en statisk IP-adress, kontrollera att du har angett rätt inställningar.

Telefonen återställs vid kraftig nätverksanvändning

Problem

Om telefonen verkar återställas vid kraftig nätverksanvändning, är det troligt att du inte har konfigurerat röst-VLAN.

Lösning

Isolera telefonerna på ett separat extra-VLAN om du vill öka kvaliteten på rösttrafiken.

Telefonen återställs på grund av avsiktlig återställning

Problem

Om du inte är den enda administratören med tillgång till Cisco Unified Communications Manager bör du kontrollera att ingen annan medvetet har återställt telefonerna.

Lösning

Du kan kontrollera om en Cisco IP-telefon har tagit emot ett kommando från Cisco Unified Communications Manager för återställning genom att trycka på **Inställningar** på telefonen och välja **Admin.inställningar** > **Status** > **Nätverksstatistik**.

- Om fältet Startorsak visar texten `Reset-Reset` tar telefonen emot en återställning från Cisco Unified Communications Manager Administration.
- Om fältet Startorsak visar texten `Reset-Restart` har telefonen stängts av eftersom den fick en begäran om återställning/omstart från Cisco Unified Communications Manager Administration.

Telefon återställs på grund av DNS eller andra anslutningsproblem

Problem

Återställningen av telefonen fortsätter och du misstänker DNS eller andra anslutningsproblem.

Lösning

Om telefonen fortsätter att återställas kan du eliminera DNS eller andra anslutningsfel genom att följa proceduren i Fastställ DNS eller kopplingsproblem, på sidan 163.

Telefonen startar inte

Problem

Telefonen verkar inte starta.

Lösning

I de flesta fall startas en telefon om ifall den slås på med hjälp av en extern strömkälla men anslutningen bryts och den växlar över till PoE. På samma sätt kan en telefon starta om ifall slås på med hjälp av PoE och sedan ansluts till en extern strömkälla.

Telefonen kan inte ansluta till LAN

Problem

Den fysiska anslutningen till LAN kan brytas.

Lösning

Kontrollera att Ethernet-anslutningen som Cisco IP-telefon ansluter till är uppe. Kontrollera till exempel om en viss port eller växel som telefonen ansluter till är nere och att växeln inte startas om. Se också till att inga kabelbrott föreligger.

Säkerhetsproblem med Cisco IP-telefon

Följande avsnitt innehåller felsökningsinformation för säkerhetsfunktioner på Cisco IP-telefon. Mer information om lösningar på sådana problem och ytterligare information om felsökning av säkerheten finns i *Cisco Unified Communications Manager Security Guide*.

Problem med CTL-filen

Följande avsnitt beskriver felsökning av problem med CTL-filen.

Autentiseringsfel, telefonen kan inte autentisera CTL-filen

Problem

En enhetsverifiering inträffar.

Orsak

CTL-filen inte har ett Cisco Unified Communications Manager-certifikat eller har ett felaktigt certifikat.

Lösning

Installera rätt certifikat.

Telefonen kan inte autentisera CTL-filen

Problem

Telefonen kan inte autentisera CTL-filen.

Orsak

Säkerhetstoken som kvitterade den uppdaterade CTL-filen finns inte i CTL-filen på telefonen.

Lösning

Ändra säkerhetstoken i CTL-filen och installera den nya filen på telefonen.

CTL-filen autentiseras men andra konfigurationsfiler autentiseras inte

Problem

Telefonen kan inte autentisera några konfigurationsfiler utöver CTL-filen.

Orsak

Det finns en skadad TFTP-post eller så kanske konfigurationsfilen inte kan signeras med motsvarande certifikat i telefonens lista med betrodda adresser.

Lösning

Kontrollera TFTP rekord och certifikatet i Trust listan.

ITL-filen autentiseras men andra konfigurationsfiler autentiseras inte

Problem

Telefonen kan inte autentisera några konfigurationsfiler utöver ITL-filen.

Orsak

Konfigurationsfilen kan inte undertecknas av motsvarande certifikat på telefonen Förtroende listan.

Lösning

Signera konfigurationsfilen igen genom att använda rätt certifikat.

TFTP-autentiseringen misslyckas

Problem

Telefonen rapporterar att TFTP-autentiseringen misslyckas.

Orsak

TFTP-adressen från telefonen finns inte i CTL-filen.

Om du har skapat en ny CTL-fil med en ny TFTP-post kanske den befintliga CTL-filen på telefonen inte innehåller en post för den nya TFTP-servern.

Lösning

Kontrollera konfigurationen av TFTP-adressen i telefonens CTL-fil.

Telefonen registreras inte

Problem

Telefonen registreras inte i Cisco Unified Communications Manager.

Orsak

Ändra serverinformationen för Cisco Unified Communications Manager i CTL-filen.

Lösning

Ändra serverinformation för Cisco Unified Communications Manager i CTL-filen.

Signerade konfigurationsfiler har inte begärts

Problem

Telefonen kräver inte några signerade konfigurationsfiler.

Orsak

CTL-filen innehåller inga TFTP-poster med certifikat.

Lösning

Konfigurera TFTP-poster med certifikat i CTL-filen.

Ljudproblem

Följande avsnitt beskriver hur du löser ljudproblem.

Ingen talsökväg

Problem

En eller flera personer på ett samtal inte hör något ljud.

Lösning

När minst en person inte får ljud har inte IP-anslutningen mellan telefonerna etablerats. Kontrollera konfigurationen av routrar och växlar för att säkerställa att IP-anslutningen är rätt konfigurerad.

Hackigt tal

Problem

En användare klagar över hackigt tal på ett samtal.

Orsak

Det kan finnas en obalans i jitterkonfigurationen.

Lösning

Kontrollera statistiken för AvgJtr och MaxJtr. En stor variation i denna statistik kan tyda på ett problem med jitter i nätverket eller återkommande hög nätverksaktivitet.

En telefon i kedjekopplingsläge fungerar inte

Problem

En av konferenstelefonerna fungerar inte i kedjekopplingsläge.

Lösning

Kontrollera att kablarna som anslutits till smartadaptern är korrekt. Det är de båda kraftigare kablarna som kopplar samman telefonerna till smartadaptern. Den tunnare kabeln kopplar samman smartadaptern till strömadaptern.

Relaterade ämnen

Sammanlänkningsläge, på sidan 31
Installera konferenstelefonen i kedjekopplingsläge, på sidan 38

Allmänna problem med samtal i telefonen

Följande avsnitt hjälper dig att felsöka allmänna problem med telefonsamtal.

Telefonsamtal kan inte upprättas

Problem

En användare klagar över att inte kunna ringa ett samtal.

Orsak

Telefonen har inte en DHCP IP-adress och kan inte registreras i Cisco Unified Communications Manager. Telefoner med en LCD-skärm visar meddelandet `Konfigurera IP` eller `Registrering`. Telefoner utan en LCD-skärm spelar upp en felton (i stället för kopplingston) i mobiltelefonen när användaren försöker ringa ett samtal.

Lösning

1. Kontrollera följande:
    1. Ethernet-kabeln är ansluten.
    2. Cisco CallManager-tjänsten körs på Cisco Unified Communications Manager-server.
    3. Båda telefonerna är registrerade på samma Cisco Unified Communications Manager.
2. Ljudserverfelsökning och insamling av loggar har aktiverats för båda telefonerna. Om det behövs kan du aktivera Java-felsökning.

Telefonen känner inte igen DTMF-siffror eller siffrorna fördröjs

Problem

Användaren klagar över att siffror saknas eller är fördröjda när knappsatsen används.

Orsak

Genom att trycka på knapparna för snabbt kan siffror missas eller fördröjas.

Lösning

Tryck inte för snabbt på knapparna.

Felsökningsförfaranden

Dessa förfaranden kan användas för att identifiera och åtgärda problem.

Skapa en telefonproblemrapport från Cisco Unified Communications Manager

Du kan skapa en telefonproblemrapport för telefonerna från Cisco Unified Communications Manager. Åtgärden ger samma information som problemrapportverktyget (PRT) genererar på telefonen.

Problemrapporten innehåller information om telefonen och headseten.

Arbetsordning

Steg 1 I Cisco Unified CM Administration väljer du **Enhet** > **Telefon**.

Steg 2 Klicka på **Sök** och välj en eller flera Cisco IP-telefoner.

Steg 3 Klicka på **Skapa PRT för valda** om du vill samla in PRT-loggar för de headset som används på valda Cisco IP-telefoner.

Kontrollera TFTP-inställningar

Arbetsordning

Steg 1 Kontrollera fältet TFTP-server 1.

Om du har tilldelat en statisk IP-adress till telefonen, måste du manuellt ange en inställning för TFTP-server 1.

Om du använder DHCP hämtar telefonen adressen för TFTP-servern från DHCP-servern. Kontrollera att IP-adressen har konfigurerats i Alternativ 150.

Steg 2 Du kan också aktivera användning av en alternativ TFTP-server i telefonen. En sådan inställning är särskilt användbar om telefonen nyligen flyttat från en plats till en annan.

Steg 3 Om en lokal DHCP inte erbjuder rätt TFTP-adress kan du aktivera användning av en alternativ TFTP-server i telefonen.

Detta behövs ofta i VPN-scenarier.

Fastställ DNS eller kopplingsproblem

Arbetsordning

Steg 1 Använd Återställ inställningar-menyn för att återställa telefonens inställningar till fabriksvärden.

Steg 2 Ändra DHCP och IP-inställningar:

a) Inaktivera DHCP.
b) Tilldela statiska IP-värden till telefonen. Använd samma standardrouterinställning som andra fungerande telefoner använder.
c) Tilldela en TFTP-server. Använd samma TFTP-server som andra fungerande telefoner använder.

Steg 3 Gå till Cisco Unified Communications Manager-servern och kontrollera att de lokala värdfilerna har rätt Cisco Unified Communications Manager-servernamn mappade till rätt IP-adress.

Steg 4 Gå till Cisco Unified Communications Manager, välj **System** > **Server** och kontrollera att referensen till servern görs av IP-adressen och inte av DNS-namnet.

Steg 5 Gå till Cisco Unified Communications Manager och välj **Enhet** > **Telefon**. Klicka på **Sök** för att söka efter den här telefonen. Kontrollera att du har tilldelat rätt MAC-adress till denna Cisco IP-telefon.

Steg 6 Slå av telefonen.

Relaterade ämnen

Fastställ telefonens MAC-adress, på sidan 59
Starta om eller återställa konferenstelefonen, på sidan 169

Kontrollera DHCP-inställningar

Arbetsordning

Steg 1 På telefonen trycker du på **Inställningar**.

Steg 2 Välj **Admininställningar** > **Ethernet-inställning** > **IPv4-inställning**.

Steg 3 Kontrollera fältet DHCP-server.

Om du har tilldelat en statisk IP-adress till telefonen, behöver du inte ange ett värde för alternativet DHCP-server. Men om du använder en DHCP-server, måste det här alternativet har ett värde. Om det inte går värde, kontrollera din IP-routing och VLAN-konfiguration. Se dokumentet om att *Felsöka växelporten och gränssnittsproblem* på denna webbadress:

https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

Steg 4 Kontrollera fälten IP-adress, nätmask och standardrouter.

Om du tilldelar en statisk IP-adress till telefonen måste du ange inställningarna för dessa alternativ manuellt.

Steg 5 Om du använder DHCP, kontrollera IP-adresser som DHCP-servern distribuerar.

Se dokumentet om att *Förstå och felsöka DHCP i Catalyst-växeln eller företagsnätverk* på denna webbadress:

https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Skapa en ny telefonkonfigurationsfil

När du tar bort en telefon från Cisco Unified Communications Manager-databasen tas konfigurationsfilen bort från Cisco Unified Communications Manager TFTP-servern. Numren i telefonkatalogen finns kvar i Cisco Unified Communications Manager-databasen. De kallas otilldelade DN:ar och kan användas för andra enheter. Om otilldelade DN:ar inte används av andra enheter kan du ta bort dessa DN:ar från Cisco Unified Communications Manager-databasen. Du kan använda nummerplanrapporten om du vill visa och ta bort otilldelade referensnummer. Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Om du ändrar knapparna i en telefonknappsmall eller tilldelar en annan telefonknappsmall till en telefon kanske katalognummer inte längre är tillgängliga från telefonen. Katalognummer tilldelas fortfarande till telefonen i Cisco Unified Communications Manager-databasen, men det finns ingen knapp på telefonen att besvara samtal med. Dessa katalognummer bör tas bort från telefonen.

Arbetsordning

Steg 1 Utgå från Cisco Unified Communications Manager, välj **Enhet** > **Telefon** och klicka på **Sök** för att lokalisera telefonen som har problem.

Steg 2 Välj **Ta bort** om du vill ta bort telefonen från Cisco Unified Communications Manager-databasen.

OBS! När du tar bort en telefon från Cisco Unified Communications Manager-databasen tas konfigurationsfilen bort från Cisco Unified Communications Manager TFTP-servern. Numren i telefonkatalogen finns kvar i Cisco Unified Communications Manager-databasen. De kallas otilldelade DN:ar och kan användas för andra enheter. Om otilldelade DN:ar inte används av andra enheter kan du ta bort dessa DN:ar från Cisco Unified Communications Manager-databasen. Du kan använda nummerplanrapporten om du vill visa och ta bort otilldelade referensnummer.

Steg 3 Lägg tillbaka telefonen i Cisco Unified Communications Manager-databasen.

Steg 4 Slå av telefonen.

Relaterade ämnen

Telefontilläggsmetoder, på sidan 60
Dokumentation för Cisco Unified Communications Manager, på sidan 14

Verifiera DNS-inställningar

Arbetsordning

Steg 1 På telefonen trycker du på **Inställningar**.

Steg 2 Välj **Admininställningar** > **Ethernet-inställning** > **IPv4-inställning**.

Steg 3 Kontrollera att fältet DNS-Server 1 är korrekt.

Steg 4 Du bör också kontrollera att en CNAME-post har skapats på DNS-servern för TFTP-servern och för Cisco Unified Communications Manager-systemet.

Du måste också se till att DNS är konfigurerat för omvänd sökning.

Starta tjänst

En tjänst måste aktiveras innan den kan startas eller stoppas.

Arbetsordning

Steg 1 Gå till Cisco Unified Communications Manager Administration och välj **Cisco Unified Serviceability** i navigationslistrutan och klicka på **Kör**.

Steg 2 Välj **Verktyg** > **Kontrollcenter – servicetjänster**.

Steg 3 Välj den primära Cisco Unified Communications Manager-servern i listrutan Server.

Fönstret visar servicenamn för den server som du väljer, status för tjänster och en tjänstestyrpanelen för att starta eller stoppa en tjänst.

Steg 4 Om en tjänst har stoppats klickar du på knappen som motsvarar tjänsten och klickar sedan på **Starta**.

Service Status symbol förändras från en ruta till en pil.

Kontrollera felsökningsinformationen från Cisco Unified Communications Manager

Om du upplever telefonproblem som du inte kan lösa, kan Cisco TAC hjälpa dig. Du kommer att behöva aktivera felsökning för telefonen, återskapa problemet, slå av felsökning och skicka loggarna till TAC för analys.

Eftersom felsökningen samlas in detaljerad information kan kommunikationstrafiken sakta ner telefonen så att den svarar sämre. När du samlar in loggar bör du slå av felsökningen för att säkerställa att telefonen kan användas normalt.

Felsökningsinformationen kan innehålla en ensiffrig kod som återspeglar allvaret i situationen. Situationerna graderas enligt följande:

- 0 – Nödfall
- 1 – Varning
- 2 – Kritiskt
- 3 – Fel
- 4 – Varna
- 5 – Avisering
- 6 – Information
- 7 – Felsökning

Kontakta Cisco TAC för mer information och hjälp.

Arbetsordning

Steg 1 Gå till Cisco Unified Communications Manager Administration och välj ett av följande fönster:

- **Enhet** > **Enhetsinställningar** > **Allmän telefonprofil**
- **System** > **Företagstelefonkonfiguration**
- **Enhet** > **Telefon**

Steg 2 Ställ in följande parametrar:

- Loggprofil – värden: Förinställd (standard), Standard, Telefoni, SIP, UI, Nätverk, Media, Uppgradering, Tillbehör, Säkerhet, Energywise, MobileRemoteAccess
- Fjärrlogg – värden: Inaktivera (standard), Aktivera
- IPv6-loggserver eller loggserver – IP-adress (IPv4- eller IPv6-adress)

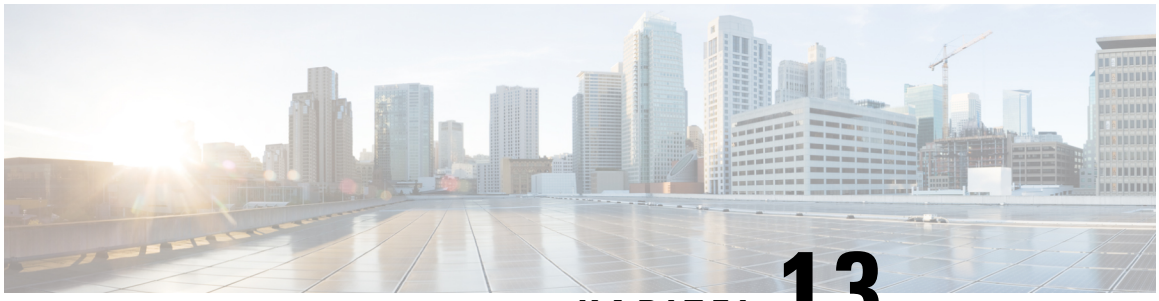
OBS! När loggservern inte kan nås slutar telefonen att skicka felsökningsmeddelanden.

- Formatet för IPv4-loggserveradressen är **`address:<port>@@base=<0-7>;pfs=<0-1>`**
- Formatet för IPv6-loggserveradressen är **`[adress]:<port>@@base=<0-7>;pfs=<0-1>`**
- Där:
  - IPv4-adressen avgränsas med punkt (.)
  - IPv6-adressen avgränsas med kolon (:)

Ytterligare felsökningsinformation

Om du har ytterligare frågor om felsökning telefonen gå till följande Cisco hemsida och navigera till den önskade telefonmodell:

https://www.cisco.com/cisco/web/psa/troubleshoot.html



KAPITEL 13

Underhåll

Starta om eller återställa konferenstelefonen

Du kan utföra en grundläggande återställning av en telefon som återskapar funktioner om telefonen får ett fel. Du kan också återställa konfiguration och säkerhetsinställningar till fabriksinställningarna.

Starta om konferenstelefonen

När du startar om telefonen försvinner ändringar som användare har gjort och ändrade nätverksinställningar som inte har allokerats till telefonens flashminne.

Arbetsordning

Tryck på **Inställningar** > **Admininställningar** > **Återställ inställningar** > **Återställ enhet**.

Relaterade ämnen

Text och menyalternativ från telefonen, på sidan 41

Återställa konferenstelefonens inställningar från telefonmenyn

Arbetsordning

Steg 1 Tryck på **Inställningar**.

Steg 2 Välj **Admininställningar** > **Återställ inställningar**.

Steg 3 Välj typ av återställning.

- **Alla** – återställer fabriksinställningarna.
- **Återställ enhet** – återställer enheten. De befintliga inställningarna ändras inte.

- **Nätverk** – återställer nätverkskonfigurationen med standardinställningar.
- **Tjänsteläge** – rensar det aktuella tjänsteläget, inaktiverar VPN och startar sedan om telefonen.
- **Säkerhet** – återställer säkerhetskonfigurationen med standardinställningar. Det här alternativet tar bort CTL-filen.

Steg 4 Tryck på **Återställ** eller **Avbryt**.

Relaterade ämnen

Text och menyalternativ från telefonen, på sidan 41

Återställa konferenstelefonen till fabriksinställningarna via knappsatsen

När du återställer telefonen via knappsatsen återgår telefonen till fabriksinställningarna.

Arbetsordning

Steg 1 Koppla ur telefonen:

- Om du använder PoE drar du ut nätverkskabeln.
- Om du använder en strömadapter tar du ut adaptern ur uttaget.

Steg 2 Vänta 5 sekunder.

Steg 3 Tryck och håll ned **#**. Anslut sedan telefonen igen.

Steg 4 När telefonen startar tänds lysdioden. Så snart lysdioden tänds ska du trycka **123456789*0#** i följd.

När du trycker på dessa knappar går telefonen igenom fabriksåterställningsprocessen.

Om du trycker på knapparna i fel ordning slå telefonen på normalt.

Försiktighet Stäng inte av telefonen förrän den är klar med fabriksåterställningen och huvudskärmen visas.

Relaterade ämnen

Text och menyalternativ från telefonen, på sidan 41

Röstkvalitetsövervakning

För att mäta röstkvalitet samtal som skickas och tas emot inom nätverket, Cisco IP-telefoner använder dessa statistiska mått som bygger på döljande händelser. DSP spelar upp dolda ramar på grund av förlorade ramar i röstpaketströmmen.

- Dolt antal – Visar andelen dolda ramar av det totala antalet talramar. Ett intervall med andel dolda ramar beräknas var 3 sekund.
- Antal dolda sekunder – Visar antalet sekunder då DSP spelar upp dolda ramar på grund av förlorade ramar. En gravt ”dold sekund” är en sekund där DSP spelar upp mer än fem procent dolda ramar.

OBS! Dolt antal och dolda sekunder är primära mätningar baserade på ramförlust. En Dölja Förhållandet mellan noll indikerar att IP-nätverket levererar ramar och paket i tid utan att förlora.

Du kan komma åt röstkvalitetsmått från Cisco IP-telefon med hjälp av samtalsstatistik skärmen eller på distans med hjälp av Streaming statistik.

Tips för felsökning av röstkvalitet

När du ser betydande och ihållande förändringar till mått, använd följande tabell för allmän information om felsökning.

Tabell 31. Ändringar i röst kvalitetsmetrik

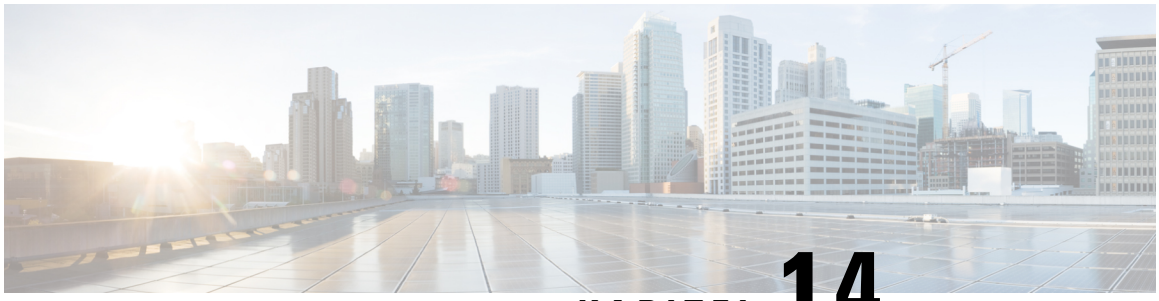
Metrisk förändring	Villkor
Dolt förhållande och dolda sekunder ökar avsevärt	Försämrad nätverksfunktion från paketförluster eller hög jitter.
Dolt förhållande är nära eller på noll, men röstkvaliteten är dålig.	• Brus eller distorsion i ljudkanal såsom eko eller ljudnivåer. • Tandemsamtal som genomgår flera kodningar/avkodningar, som samtal till ett mobilnät eller telefonkortsnät. • Akustiska problem som kommer från en högtalartelefon, mobiltelefon med handsfree eller trådlöst headset. Kontrollera räknare för paketsändningen (TxCnt) och paketmottagningen (RxCnt) för att kontrollera att röstpaketen flödar.
MOS LQK-poäng minskar kraftigt	Försämrad nätverksfunktion från paketförluster eller höga jitternivåer: • En minskad genomsnittlig MOS LQK kan tyda på en utbredd och jämn försämring. • Enskilda MOS LQK-minskningar kan tyda på tillfällig försämring. Dubbelkontrollera om dolt förhållande och dolda sekunder beror på paketförlust och jitter.
MOS LQK-poäng ökar kraftigt	• Kontrollera om telefonen använder en annan kodning än väntat (RxType och TxType). • Kontrollera om MOS LQK-versionen ändras efter en uppgradering av firmware.

OBS! Röstkvalitetsmått tar inte hänsyn till brus eller förvrängning utan endast ramförlust.

Rengöring av Cisco IP-telefon

För att rengöra din Cisco IP-telefon, använder endast en torr, mjuk trasa för att försiktigt torka av telefonen och telefonens skärm. Gäller inte vätskor eller pulver direkt till telefonen. Som med alla icke-väder elektronik, vätskor och pulver kan skada komponenterna och orsaka fel.

När telefonen är i strömsparläge är skärmen tom och knappen Välj lyser inte. När telefonen är i det här tillståndet kan du rengöra skärmen så länge du vet att telefonen är i strömsparläge tills du är klar med rengöringen.



KAPITEL 14

Internationell användarsupport

Språkinstallationsprogram för ändpunkter i Unified Communications Manager

Som standard är Cisco IP-telefon inställd med engelska (USA) som språk. Om du vill använda Cisco IP-telefon på andra språk måste du installera den språkspecifika versionen av Unified Communications Manager Endpoints Locale Installer på alla Cisco Unified Communications Manager-servrar i klustret. Med språkinstallationsprogrammet installeras den senast översatta texten för telefonanvändargränssnittet och landsspecifika telefonsignaler i ditt system så att de är tillgängliga för Cisco IP-telefon.

När du vill använda språkinstallationsprogrammet som krävs för en utgåva kan du gå till sidan Hämta programvara, navigera till din telefonmodell och välja länken Unified Communications Manager Endpoints Locale Installer.

Mer information finns i dokumentationen till din version av Cisco Unified Communications Manager.

OBS! Det senaste språkinstallationsprogrammet kanske inte finns tillgängligt direkt, så fortsätt att kontrollera webbplatsen för uppdateringar.

Relaterade ämnen

Dokumentation för Cisco Unified Communications Manager, på sidan 14

Stöd för internationell samtalsloggning

Om telefonsystemet är konfigurerat för loggning av utlandssamtal (normalisering av uppringaren) kan samtalsloggar, återuppringningar eller samtalskatalogposter visa ett plustecken (+) för att representera den internationella koden för din plats. Beroende på konfiguration av telefonsystemet, kan + ersättas med rätt landsnummer, eller så kan du behöva redigera numret innan du ringer för att manuellt ersätta + med den internationella koden för din plats. Medan samtalsloggen eller katalogposten kan visa hela internationella

nummer för mottagna samtal kan telefonens skärm visar den förkortade lokala versionen av numret, utan internationell symbol eller landsnummer.

Språkbegränsning

Det finns ingen lokaliserad KATE-support (Keyboard Alphnumeric Text Entry) för följande asiatiska språk:

- Kinesiska (Kina)
- Kinesiska (Hongkong)
- Kinesiska (Taiwan)
- Japanska (Japan)
- Koreanska (Sydkorea)

Engelska (USA) som standard-KATE presenteras för användaren i stället.

Till exempel visas texten på telefonskärmen på koreanska, men knappen **2** på knappsatsen visar **a b c 2 A B C**.