



Cisco IP-telefon i 8800-serien – Administrationshandbok för Cisco Unified Communications Manager

Först publicerad: 2015-07-13

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 UNDERFÖRSTÄDD. 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 OVANNÄMNDNA LEVERANTÖRER FRÅNSÄGER SIG ALLA GARANTIER, UTTRYCKLIGA ELLER UNDERFÖRSTÄDDA, 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 ett partnerskap bildats mellan Cisco och något annat företag. (1721R)

© 2015–2023 Cisco Systems, Inc. Med ensamrätt.



INNEHÅLL

FÖRORD:

Förord	xiii
Översikt	xiii
Målgrupp	xiii
Konventioner för handböckerna	xiii
Relaterad dokumentation	xiv
Dokumentation för Cisco IP-telefon i 8800-serien	xiv
Dokumentation för Cisco Unified Communications Manager	xv
Dokumentation för Cisco Business Edition 6000	xv
Dokumentation, support och säkerhetsriktlinjer	xv
Översikt över Ciscos produktsäkerhet	xv

KAPITEL 1

Ny och ändrad information	1
Ny och ändrad information för den fasta programvaran 14.2(1)	1
Ny och ändrad information för version 14.1 (1) av den fasta programvaran	2
Ny och ändrad information för version 14.0 (1) av den fasta programvaran	2
Ny och ändrad information för version 12.8 (1) av den fasta programvaran	3
Ny och ändrad information för version 12.7 (1) av den fasta programvaran	3
Ny och ändrad information för version 12.6 (1) av den fasta programvaran	4
Ny information om version 12.5 (1) SR3 av den fasta programvaran	4
Ny information om version 12.5 (1) SR1 av den fasta programvaran	4
Ny information om version 12.1 (1) SR1 av den fasta programvaran	5
Ny information om version 12.1 (1) av den fasta programvaran	5
Ny information om version 12.0(1) av den fasta programvaran	6
Ny information om version 11.7 (1) av den fasta programvaran	6
Ny information om version 11.5 (1) SR1 av den fasta programvaran	6
Ny information om version 11.5 (1) av den fasta programvaran	7

Ny information om version 11.0 av den fasta programvaran 8

DEL I:**Om Cisco IP-telefon 11**

KAPITEL 2**Tekniska detaljer 13**

- Fysiska och driftsmiljörelaterade specifikationer 13
- Kabelspecifikationer 14
 - Nätverks- och datorportkontakt 14
 - Nätverksportkontakt 14
 - Datorportkontakt 15
- Telefonströmförsörjning 16
 - Strömavbrott 17
 - Energispar 17
 - Strömbalansering över LLDP 17
- Nätverksprotokoll 18
- Interaktion med VLAN 21
- Interaktion med Cisco Unified Communications Manager 21
- Interaktion med Cisco Unified Communications Manager Express 22
- Interaktion i röstmeddelandesystemet 23
- Telefonens startprocess – översikt 23
- Externa enheter 25
- Information om USB-port 25
- Telefonens konfigurationsfiler 26
- Telefonbeteende under överbelastning av nätverket 26
- Telefonbeteende i ett nätverk med två nätverksroutrar 27
- Programmeringsgränssnitt 27

KAPITEL 3**Maskinvara i Cisco IP-telefon 29**

- Översikt över telefon 29
- Cisco Wireless IP Phone 8811 31
 - Telefonanslutningar för 31
- Cisco IP-telefon 8841 och 8845 32
 - Telefonanslutningar 33
- Cisco IP-telefon 8851 och 8851NR 33

Telefonanslutningar för	34
Cisco IP-telefon 8851, 8865 och 8865NR	35
Telefonanslutningar	35
Knappar och maskinvara	36
Programstyrda knappar, linjeknappar och funktionsknappar	38
Skydda din telefons videokamera	39

DEL II:**Installation av Cisco IP-telefon 41****KAPITEL 4****Installation av Cisco IP-telefon 43**

Kontrollera nätverksinställningen	43
Aktiveringskod vid installation för telefoner på företaget	44
Aktiveringskodregistrering och mobilåtkomst och Remote Access	45
Aktivera autoregistrering för telefoner	45
Installera Cisco IP-telefon	47
Dela nätverksanslutning med din telefon och dator	48
Konfigurera telefonen från inställningsmenyerna	49
Använda ett telefonlösenord	50
Text och menyalternativ från telefon	50
Aktivera det trådlösa nätverket på telefonen	51
Konfigurera det trådlösa nätverket i Cisco Unified Communications Manager.	52
Ställa in trådlöst nätverk från telefonen	53
Ange antalet WLAN-autentiseringsförsök	54
Aktivera uppmaningsläge för WLAN	55
Ställa in en Wi-Fi-profil med hjälp av Cisco Unified Communications Manager	55
Ställa in en Wi-Fi-grupp med hjälp av Cisco Unified Communications Manager	57
Konfigurera nätverksinställningar	58
Fält för Ethernet-inställningar	58
IPv4-fält	60
IPv6-fält	61
Konfigurera telefonen för användning av DHCP	62
Konfigurera telefonen så att DHCP inte används	63
Laddningsserver	63
Verifiering vid telefonstart	64

Konfigurera telefontjänster för användare 64

Ändra en användares telefonmodell 65

KAPITEL 5**Telefoninställningar i Cisco Unified Communications Manager 67**

Konfigurera Cisco IP-telefon 67

Fastställ telefonens MAC-adress 70

Telefontilläggsmetoder 70

 Lägga till telefoner individuellt 71

 Lägga till telefoner med BAT-telefonmall 71

Lägga till användare i Cisco Unified Communications Manager 72

 Lägga till en användare från en extern LDAP-katalog 72

 Lägga till användare direkt i Cisco Unified Communications Manager 73

Lägga till en användare i en slutanvändargrupp 73

Associera telefoner med användare 74

Survivable Remote Site Telephony 74

Enhanced Survivable Remote Site Telephony 77

Programmets uppringningsregler 78

 Konfigurera programmets uppringningsregler 78

KAPITEL 6**Hantering av självbetjäningsportalen 79**

Översikt över självbetjäningsportalen 79

Konfigurera användaråtkomst till självbetjäningsportalen 79

Anpassa visningen av självbetjäningsportalen 80

DEL III:**Cisco IP-telefon – administration 81**

KAPITEL 7**Säkerhet i Cisco IP-telefon 83**

Säkerhetsförbättringar för telefonens nätverk 83

Säkerhetsfunktioner som stöds 84

 Konfigurera ett LSC-certifikat 89

 Aktivera FIPS-läge 90

 Säkerhet i telefonsamtal 90

 Identifiering för säkert konferenssamtal 91

 Identifiering för säkert telefonsamtal 92

Tillhandahålla kryptering för inbrytning	92
WLAN-säkerhet	93
Ställa in autentiseringsläget	96
Inloggningsuppgifter för säkerhet vid trådlöst	96
Ställa in användarnamn och lösenord	96
Förinställd delad nyckel	97
Trådlös kryptering	97
Exportera CA-certifikat från ACS med Microsoft Certificate Services	98
PEAP-inställning	103
Säkerhet för trådlöst LAN	104
Administrationssida för Cisco IP-telefon	104
SCEP-konfiguration	107
802.1X-autentisering	108
Åtkomst till 802.1X-autentisering	109
Ställa in fältet för autentisering av enhet	110

KAPITEL 8
Anpassning av Cisco IP-telefon 111

Anpassade telefonringsignaler	111
Anpassade bakgrundsbilder	111
Konfigurera bredbandskodning	113
Konfigurera viloläge	113
Anpassa kopplingstonen	114

KAPITEL 9
Telefonfunktioner och inställning 117

Översikt över telefonens funktioner och inställningar	117
Stöd för Cisco IP-telefon-användare	117
Telefonfunktioner	118
Funktionsknappar och programstyrda knappar	135
Telefonfunktionskonfiguration	137
Konfigurera telefonfunktioner som gäller alla telefoner	137
Konfigurera telefonfunktioner för en grupp av telefoner	138
Konfigurera telefonfunktioner för en enda telefon	138
Produktspecifik konfiguration	138
Bästa funktionskonfigurationerna	157

Miljöer med hög samtalsvolym	157
Multilinjemiljöer	158
Miljö för sessionslinjeläge	158
Fält: Använd alltid primär linje	159
Inaktivera Transport Layer Security-chiffer	159
Aktivera samtalshistorik för delad linje	160
Schemalägga energisparläge för Cisco IP-telefon	160
Schemalägga EnergyWise för Cisco IP-telefon	162
Konfigurera Stör ej	165
Aktivera agenthälsning	166
Konfigurera övervakning och registrering	167
Konfigurera meddelande om vidarekoppling av samtal	167
Aktivera BLF för samtalslistor	168
Ställa in Energy Efficient Ethernet för växel- och PC-port	169
Konfigurera RTP-/sRTP-portintervall	170
Mobil åtkomst och fjärråtkomst genom Expressway	170
Driftsättningsscenarier	171
Mediasökvägar och interaktiv etablering av anslutningar	172
Telefonfunktioner som är tillgängliga för Mobil åtkomst och fjärråtkomst genom Expressway	173
Konfigurera bestående inloggningsuppgifter för inloggning med Expressway	175
Generera en QR-kod för MRA-inloggning	175
Problemrapportverktyg	175
Konfigurera en uppladdnings-URL för kundsupport	176
Ställa in en etikett för en linje	177
Konfigurera dubbel bankinformation	177
Parkeringsövervakning	178
Ställa in timer för parkeringsövervakning	178
Ställa in parametrar för parkeringsövervakning för katalognummer	179
Ställa in parkeringsövervakning för svarslistor	180
Ställa in ljud- och videoportintervall	180
Konfigurera Cisco IP Manager Assistant	182
Konfigurera visuell inbox för röstbrevlåda	184
Konfigurera visuell inbox för röstbrevlåda för en viss användare	185
Visuell inbox för röstbrevlåda för en användargrupp	185

Säkra SIP-tjänster	185
Migration av din telefon till en multiplattformstelefon direkt	186
Prioritet och förtur på flera nivåer (MLPP)	186
Konfigurera mall för programstyrda knappar	187
Mallar för telefonknappar	189
Ändra mall för telefonknappar	189
Tilldela telefonknappmallen för alla samtal	190
Konfigurera adressboken eller kortnummer som IP-telefontjänst	190
Ändra telefonknappmallen för adressboken eller kortnummer	191
VPN-konfiguration	192
Ställa in ytterligare linjeknappar	193
Funktioner som är tillgängliga i förbättrat linjeläge	194
Ställa in timer för TLS-återupptagande	196
Aktivera intelligenta närhetstjänster	197
Ställa in upplösning för videosändning	197
Headsethantering på äldre versioner av Cisco Unified Communications Manager	199
Ladda ned standardkonfigurationsfilen för headset	199
Ändra standardkonfigurationsfilen för headset	200
Installera standardkonfigurationsfilen på Cisco Unified Communications Manager	202
Starta om Cisco TFTP-server	203

KAPITEL 10
Företagskatalog och den personliga katalogen 205

Inställning av företagskatalog	205
Inställning av personlig katalog	205
Inställning av användarens personliga telefonkatalog	206
Hämta Cisco IP-telefon synkroniserade adressbok	206
Användning av Cisco IP-telefon synkroniserade adressbok	207
Installera synkroniseringsprogrammet	207
Ställ in synkronisering	207

DEL IV:
Felsökning för Cisco IP-telefon 209

KAPITEL 11
Övervakning av telefonsystem 211

Status på Cisco IP-telefonen	211
------------------------------	-----

Visa telefoninformationsfönstret	211
Fälten för telefoninformation	212
Visa statusmenyn	212
Visa fönstret Statusmeddelanden	213
Visa skärmen Nätverksinformation	217
Visa skärmen Nätverksstatistik	217
Visa skärmen Trådlös statistik	220
Visa fönstret Samtalsstatistik	221
Visa fönstret Aktuell åtkomstpunkt	224
Webbsidan för Cisco IP-telefon	226
Åtkomst till webbsidan för telefonen	226
Enhetsinfo	227
Ställa in nätverk	229
Nätverksstatistik	234
Enhetsloggar	237
Direktspelningsstatistik	237
Begära information från telefonen i XML	241
Exempel på utdata från CallInfo	242
Exempel på utdata från LineInfo	242
Exempel på utdata från ModeInfo	243

KAPITEL 12**Felsökning 245**

Allmän felsökning	245
Startproblem	246
Cisco IP-telefon går inte igenom den normala startprocessen	247
Cisco IP-telefon registreras inte i Cisco Unified Communications Manager	247
Telefonen visar felmeddelanden	248
Telefonen kan inte ansluta till TFTP-servern eller till Cisco Unified Communications Manager	248
Telefonen kan inte ansluta till TFTP-servern	248
Telefonen kan inte ansluta till servern	248
Telefonen kan inte ansluta med DNS	249
Cisco Unified Communications Manager och TFTP-tjänsterna körs inte	249
Skadad konfigurationsfil	249

Telefonregistrering i Cisco Unified Communications Manager	249
Cisco IP-telefon kan inte hämta IP-adressen	250
Telefonen registrerar inte	250
Problem med telefonåterställning	250
Telefonen återställs på grund av intermittent nätverksfel	251
Telefonen återställs grund av DHCP-inställningsfel	251
Telefon återställs på grund av felaktig statisk IP-adress	251
Telefonen återställs vid kraftig nätverksanvändning	251
Telefonen återställs på grund av avsiktlig återställning	252
Telefon återställs på grund av DNS eller andra anslutningsproblem	252
Telefonen startar inte	252
Telefonen kan inte ansluta till LAN	252
Säkerhetsproblem med Cisco IP-telefon	253
Problem med CTL-filen	253
Autentiseringsfel, telefonen kan inte autentisera CTL-filen	253
Telefonen kan inte autentisera CTL-filen	253
CTL-filen autentiseras men andra konfigurationsfiler autentiseras inte	253
ITL-filen autentiseras men andra konfigurationsfiler autentiseras inte	254
TFTP-autentiseringen misslyckas	254
Telefonen registreras inte	254
Signerade konfigurationsfiler har inte begärts	255
Problem vid videosamtal	255
Ingen video mellan två Cisco IP-videotelefoner	255
Videon hackar eller hoppar över bilder	255
Jag kan inte överföra videosamtal	256
Ingen Video under konferenssamtal	256
Allmänna problem med samtal i telefonen	256
Telefonsamtal kan inte upprättas	256
Telefonen känner inte igen DTMF-siffror eller siffrorna fördröjs	257
Felsökningsförfaranden	257
Skapa en telefonproblemrapport från Cisco Unified Communications Manager	257
Skapa en konsollogg från din telefon	257
Kontrollera TFTP-inställningar	258
Fastställ DNS eller kopplingsproblem	258

Kontrollera DHCP-inställningar	259
Skapa en ny telefonkonfigurationsfil	259
Identifiera 802.1X-autentiseringsproblem	260
Verifiera DNS-inställningar	260
Starta tjänst	261
Kontrollera felsökningsinformationen från Cisco Unified Communications Manager	261
Ytterligare felsökningsinformation	262

KAPITEL 13**Underhåll 263**

Grundläggande återställning	263
Återställa telefonen till fabriksinställningarna från telefonens knappsats	263
Återställ alla inställningar från Telefon-menyn	264
Starta om telefonen från säkerhetskopian	264
Utföra återställning av nätverkskonfiguration	265
Utföra återställning av användarnätverkskonfiguration	265
Ta bort CTL-filen	265
Quality Report Tool	266
Röstkvalitetsövervakning	266
Tips för felsökning av röstkvalitet	266
Rengöring av Cisco IP-telefon	267

KAPITEL 14**Internationell användarsupport 269**

Språkinstallationsprogram för ändpunkter i Unified Communications Manager	269
Stöd för internationell samtalsloggning	269
Språkbegränsning	270



Förord

- [Översikt, på sidan xiii](#)
- [Målgrupp, på sidan xiii](#)
- [Konventioner för handböckerna, på sidan xiii](#)
- [Relaterad dokumentation, på sidan xiv](#)
- [Dokumentation, support och säkerhetsriktlinjer, på sidan xv](#)

Översikt

Cisco IP-telefon i 8800-serien – administrationshandbok till Cisco Unified Communications Manager innehåller den information du behöver för att förstå, installera, konfigurera, hantera och felsöka telefonerna i ett VoIP-nätverk.

På grund av komplexiteten i ett IP-telefonnät ger den här guiden inte fullständig och detaljerad information om procedurer som du behöver utföra i Cisco Unified Communications Manager eller andra nätverksenheter.

Målgrupp

Installation av Cisco IP-telefon De uppgifter som beskrivs i detta dokument omfattar konfiguration av nätverksinställningar som inte är avsedda för telefonanvändare. Uppgifterna i denna handbok kräver att användaren känner Cisco Unified Communications Manager.

Konventioner för handböckerna

I det här dokumentet används följande konventioner:

Konvention	Beskrivning
fet stil	Kommandon och nyckelord skrivs i fetstil .
<i>kursiv stil</i>	Argument som du anger värden för skrivs i <i>kursiv stil</i> .
[]	Element inom hakparentes är valfria.
{x y z}	Alternativa nyckelord grupperas inom klamrar och skiljs åt med vertikala linjer.

Konvention	Beskrivning
[x y z]	Valfria alternativa nyckelord grupperas inom klamrar och skiljs åt med vertikala linjer.
sträng	En teckenuppsättning utan citattecken. Använd inte citattecken runt strängen eftersom citattecken då ingår i själva strängen.
skärmteckensnitt	Terminalsessioner och den information som visas i systemet skrivs med skärmteckensnitt.
inmatningsteckensnitt	Informationen måste anges med inmatningsteckensnitt .
<i>skärmteckensnitt i kursiv stil</i>	Argument som du anger värden för skrivs med <i>skärmteckensnitt i kursiv stil</i> .
^	Symbolen ^ representerar nyckeln märkt Control – till exempel tangentkombinationen ^D på skärm betyder att du ska hålla ned Ctrl-tangenten samtidigt som du trycker på D-tangenten.
<>	Dolda tecken som lösenord visas inom vinkelparentes.



OBS! Betyder att *läsaren bör vara observant*. Anmärkningar innehåller praktiska förslag eller referenser till material som inte ingår i publikationen.



Försiktighet Betyder att *läsaren bör vara försiktig*. I den här situationen finns det risk för att du skulle kunna göra något som kan leda till att utrustningen skadas eller att information försvinner om du inte är försiktig.

Varningar har följande konvention:



Observera VIKTIGA SÄKERHETSANVISNINGAR

Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till hur du förebygger skador. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning. Statement 1071

SPARA DESSA ANVISNINGAR

Relaterad dokumentation

Läs följande avsnitt om du vill ha mer relevant information.

Dokumentation för Cisco IP-telefon i 8800-serien

Hitta dokumentation som är specifik för ditt språk, din telefonmodell och samtalskontrollsystem på sidan med [produktstöd](#) för Cisco IP-telefon i 7800-serien.

Implementeringsguiden finns på följande webbadress:

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

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 Business Edition 6000

Se *Cisco Business Edition 6000 Documentation Guide* och andra publikationer som är specifika för din utgåva av Cisco Business Edition 6000. Navigera från webbadressen som följer:

<https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/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/policiesandregulations/ear/index.htm>.



KAPITEL 1

Ny och ändrad information

- [Ny och ändrad information för den fasta programvaran 14.2\(1\), på sidan 1](#)
- [Ny och ändrad information för version 14.1 \(1\) av den fasta programvaran, på sidan 2](#)
- [Ny och ändrad information för version 14.0 \(1\) av den fasta programvaran, på sidan 2](#)
- [Ny och ändrad information för version 12.8 \(1\) av den fasta programvaran, på sidan 3](#)
- [Ny och ändrad information för version 12.7 \(1\) av den fasta programvaran, på sidan 3](#)
- [Ny och ändrad information för version 12.6 \(1\) av den fasta programvaran, på sidan 4](#)
- [Ny information om version 12.5 \(1\) SR3 av den fasta programvaran, på sidan 4](#)
- [Ny information om version 12.5 \(1\) SR1 av den fasta programvaran, på sidan 4](#)
- [Ny information om version 12.1 \(1\) SR1 av den fasta programvaran, på sidan 5](#)
- [Ny information om version 12.1 \(1\) av den fasta programvaran, på sidan 5](#)
- [Ny information om version 12.0\(1\) av den fasta programvaran, på sidan 6](#)
- [Ny information om version 11.7 \(1\) av den fasta programvaran, på sidan 6](#)
- [Ny information om version 11.5 \(1\) SR1 av den fasta programvaran, på sidan 6](#)
- [Ny information om version 11.5 \(1\) av den fasta programvaran, på sidan 7](#)
- [Ny information om version 11.0 av den fasta programvaran, på sidan 8](#)

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 83
Förenklad inloggning till Extension Mobility med Cisco-headset 730 USB-adapter	Telefonfunktioner, på sidan 118
Bluetooth-synkronisering av Ljud av för Cisco-Headset 700-serien	Telefonfunktioner, på sidan 118
Nya inställningar för Cisco-headset 500-serien: Docka händelse och läget Alltid på	Telefonfunktioner, på sidan 118

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 83
Förbättrad samtalsavisering för svarsgrupp	Telefonfunktioner, på sidan 118
Visning av konfigurerbart samtalsnummer för förbättrat linjeläge	Produktspecifik konfiguration
Konfigurerbar fördröjd PLAR	Telefonfunktioner, på sidan 118
MRA-stöd för Extension Mobility-inloggning med Cisco-headset	Telefonfunktioner, på sidan 118
Migrering av telefon utan övergångsladdning	Migration av din telefon till en multiplattformstelefon direkt, på sidan 186

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 138
Förbättringar av SIP OAuth	Säkerhetsförbättringar för telefonens nätverk, på sidan 83
Förbättrat användargränssnitt	Survivable Remote Site Telephony, på sidan 74 Telefonfunktioner, på sidan 118
Förbättringar av OAuth för MRA	Mobil åtkomst och fjärråtkomst genom Expressway, på sidan 170

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 65
Förbättringar i uppdatering av headset	Enhetsinfo, på sidan 227
Förenkla inloggningen till Extension Mobility med Cisco-headset	Telefonfunktioner, på sidan 118
Ändringar i funktionskontroll	Produktspecifik konfiguration, på sidan 138 , nya fält Sänk din röst varning och Markera samtal som skräp
Allmänna ändringar	Klargör trådlöst nätverk och PC-port: <ul style="list-style-type: none"> • Konfigurera telefonen från inställningsmenyerna, på sidan 49 • Aktivera det trådlösa nätverket på telefonen, på sidan 51
Lägga till ytterligare information om fältet för webbåtkomst	Produktspecifik konfiguration, på sidan 138
Ta bort funktion som inte stöds	Telefonfunktioner, på sidan 118

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

Tabell 2. Ändringar i administrationshandboken för Cisco IP-telefon 8800 för fasta programvaran version 12.1 (1).

Uppdatering	Uppdaterat avsnitt
Uppdaterat för stöd för bakgrund i moduler för nyckelexpansion.	Anpassade bakgrundsbilder, på sidan 111
Uppdaterad för stöd för Cisco-headset 730	Enhetsinfo, på sidan 227
Uppdaterad för Cisco-headset i 500-serien fast programvara version 2.0	Enhetsinfo, på sidan 227 Headsethantering på äldre versioner av Cisco Unified Communications Manager, på sidan 199
Uppdaterat för inkommande svarsgruppsamtal.	Telefonfunktioner, på sidan 118

Uppdatering	Uppdaterat avsnitt
Konfigurationsinformation om E-luren har tagits bort.	Produktspecifik konfiguration, på sidan 138

Ny och ändrad information för version 12.6 (1) 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 3. Ändringar i administrationshandbok för Cisco IP-telefon 8800 version 12.6 (1) av den fasta programvaran

Uppdatering	Uppdaterat avsnitt
Uppdaterat för att återgå till primär linje i sessionslinjeläge.	Produktspecifik konfiguration, på sidan 138 Miljö för sessionslinjeläge, på sidan 158

Ny information om 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 4. Administrationshandbok för Cisco IP-telefon 8800 – revideringar inför version 12.5 (1) SR3 av den fasta programvaran

Uppdatering	Uppdaterat avsnitt
Stöd för aktiveringskodregistrering och mobilåtkomst och Remote Access	Aktiveringskodregistrering och mobilåtkomst och Remote Access, på sidan 45
Stöd för användning av problemrappportverktyget från Cisco Unified Communications Manager.	Skapa en telefonproblemrappport från Cisco Unified Communications Manager, på sidan 257
Nytt ämne	Dela nätverksanslutning med din telefon och dator, på sidan 48
Nytt ämne	Skydda din telefons videokamera, på sidan 39

Ny information om version 12.5 (1) SR1 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 5. Administrationshandbok för Cisco IP-telefon 8800 – revideringar inför version 12.5 (1) SR1 av fasta programvara

Uppdatering	Uppdaterat avsnitt
Stöd för stöd av Elliptic Curve	Säkerhetsfunktioner som stöds, på sidan 84
Stöd för förbättringar i samtalshistorik för Avancerat linje-läge med rullningslinjer	Funktioner som är tillgängliga i förbättrat linjeläge, på sidan 194
Stöd för viskningssökning i Cisco Unified Communications Manager Express	Interaktion med Cisco Unified Communications Manager Express, på sidan 22
Stöd för kinesiska	Språkbegränsning, på sidan 270
Stöd för registrering via aktiveringskod	Aktiveringskod vid installation för telefoner på företaget, på sidan 44
Stöd för mediasökvägar och interaktiv etablering av anslutningar	Mediasökvägar och interaktiv etablering av anslutningar, på sidan 172
Stöd för inaktivering av TLS-chiffer	Produktspecifik konfiguration, på sidan 138
Stöd för inaktivering av handenhet så att ljudet går till headsetet	Produktspecifik konfiguration, på sidan 138
Stöd för fjärrkonfiguration av headsetparametrar	Headsethantering på äldre versioner av Cisco Unified Communications Manager, på sidan 199

Ny information om version 12.1 (1) SR1 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 6. Administrationshandbok för Cisco IP-telefon 8800 – revideringar inför version 11.5 (1) SR1 av den fasta programvaran

Uppdatering	Uppdaterat avsnitt
Enbloc-uppringning för Inter-Digit Timer T.302 Enhancement.	Produktspecifik konfiguration, på sidan 138

Ny information om version 12.1 (1) 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 7. Administrationshandbok för Cisco IP-telefon 8800 – revideringar inför version 12.1 (1) av den fasta programvaran

Uppdatering	Uppdaterat avsnitt
Mobilåtkomst och Remote Access via Expressway stöder nu förbättrat linjeläge.	Telefonfunktioner som är tillgängliga för Mobil åtkomst och fjärråtkomst genom Expressway, på sidan 173
	Mobil åtkomst och fjärråtkomst genom Expressway, på sidan 170
	Funktioner som är tillgängliga i förbättrat linjeläge, på sidan 194
Aktivering eller inaktivering av TLS 1.2 för åtkomst till webbservrar stöds nu.	Produktspecifik konfiguration, på sidan 138
Stöd för G722.2 AMR-WB-ljudcodec.	Översikt över telefon, på sidan 29
	Samtalsstatistikfält, på sidan 222

Ny information om version 12.0(1) av den fasta programvaran

Alla nya funktioner har lagts till i [Telefonfunktioner, på sidan 118](#).

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

Tabell 8. Administrationshandbok för Cisco IP-telefon 8800 – revideringar inför version 12.0 (1) av den fasta programvaran

Uppdatering	Uppdaterat avsnitt
Uppdaterad för samtalsparkering, samtalsparkering linjestatus, grupp hämtning och stöd för svarsgrupper i förbättrat linjeläge	Funktioner som är tillgängliga i förbättrat linjeläge, på sidan 194

Ny information om version 11.7 (1) av den fasta programvaran

Det behövdes inga administrativa uppdateringar inför firmware version 11.7 (1).

Ny information om version 11.5 (1) SR1 av den fasta programvaran

Alla nya funktioner har lagts till i [Telefonfunktioner, på sidan 118](#).

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

Tabell 9. Administrationshandbok för Cisco IP-telefon 8800 – revideringar inför version 11.5 (1) SR1 av den fasta programvaran

Uppdatering	Uppdaterat avsnitt
Uppdaterad för stöd av Cisco IP-telefon 8865NR	<ul style="list-style-type: none"> • Telefonströmförsörjning, på sidan 16 • Nätverksprotokoll, på sidan 18 • Översikt över telefon, på sidan 29 • Knappar och maskinvara, på sidan 36
Uppdaterad för stöd av inspelning och övervakning i förbättrat Linjeläge	Funktioner som är tillgängliga i förbättrat linjeläge , på sidan 194
Uppdaterad för stöd av WLAN skanninglista	Aktivera det trådlösa nätverket på telefonen , på sidan 51 Ställa in trådlöst nätverk från telefonen , på sidan 53 Konfigurera nätverksinställningar , på sidan 58
Uppdaterad för stöd av Stör ej med MLPP	Konfigurera Stör ej , på sidan 165
Uppdaterad för stöd av konfigurerbar ringning	Produktspecifik konfiguration , på sidan 138
Förbättrad säkerhet	Säkerhetsförbättringar för telefonens nätverk , på sidan 83
Allmänna ändringar	Uppdateringar av Webbsidan för Cisco IP-telefon , på sidan 226 Ny presentation av telefonfunktionskonfigurationen i Cisco Unified Communications Manager Telefonfunktionskonfiguration , på sidan 137

Ny information om version 11.5 (1) av den fasta programvaran

Tabell 10. Administrationshandbok för Cisco IP-telefon 8800 – revideringar inför version 11.5 (1) av den fasta programvaran.

Uppdatering	Uppdaterat avsnitt
Förbättrat linjeläge stöds.	Ställa in ytterligare linjeknappar , på sidan 193 Funktioner som är tillgängliga i förbättrat linjeläge , på sidan 194
Stör ej (DND) har uppdaterats för ny visning.	Konfigurera Stör ej , på sidan 165
Opus-kodning stöds.	Översikt över telefon , på sidan 29
FIPS-läge har lagts till.	Aktivera FIPS-läge , på sidan 90
WLAN-konfiguration har uppdaterats.	Ställa in trådlöst nätverk från telefonen , på sidan 53

Uppdatering	Uppdaterat avsnitt
WLAN-profil för Cisco IP-telefon 8861 och 8865 stöds.	Ställa in en Wi-Fi-profil med hjälp av Cisco Unified Communications Manager, på sidan 55
	Ställa in en Wi-Fi-grupp med hjälp av Cisco Unified Communications Manager, på sidan 57
Ange WLAN-autentiseringsförsök stöds.	Ange antalet WLAN-autentiseringsförsök, på sidan 54
Aktivera fråga WLAN-läge stöds.	Aktivera uppmaningsläge för WLAN, på sidan 55
Anpassa kopplingston stöds.	Anpassa kopplingstonen, på sidan 114
Visa skärmen Nätverksinformation stöds.	Visa skärmen Nätverksinformation, på sidan 217

Ny information om version 11.0 av den fasta programvaran

Alla nya funktioner har lagts till i [Telefonfunktioner](#), på sidan 118.

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

Tabell 11. Administrationshandbok för Cisco IP-telefon 8800 – revideringar inför version 11.0 av den fasta programvaran

Uppdatering	Uppdaterat avsnitt
Uppdaterat för förklaring och hantering av brister	<ul style="list-style-type: none"> • VPN-konfiguration, på sidan 192 • Konfigurera nätverksinställningar, på sidan 58 • Ställa in Energy Efficient Ethernet för växel- och PC-port, på sidan 169 • Ställa in upplösning för videosändning, på sidan 197 • Enhanced Survivable Remote Site Telephony, på sidan 77
Uppdaterat för bättre stöd av alternativet för sektionsvis felsökning av telefon	<ul style="list-style-type: none"> • Kontrollera felsökningsinformationen från Cisco Unified Communications Manager, på sidan 261.
Uppdaterat för bättre stöd av digitala certifikat för EAP-TLS + SCEP, PEAP GTC och X.509	<ul style="list-style-type: none"> • WLAN-säkerhet, på sidan 93. • Ställa in autentiseringsläget, på sidan 96 • Inloggningsuppgifter för säkerhet vid trådlöst, på sidan 96

Uppdatering	Uppdaterat avsnitt
Uppdaterat för bättre stöd av problemrapportverktyget (PRT)	<ul style="list-style-type: none">• Problemrapportverktyg, på sidan 175.• Konfigurera en uppladdnings-URL för kundsupport, på sidan 176.
Tillagt stöd för programmets uppringningsregel	<ul style="list-style-type: none">• Programmets uppringningsregler, på sidan 78
Tillagt för radtextetikett	<ul style="list-style-type: none">• Ställa in en etikett för en linje, på sidan 177.



DEL **I**

Om Cisco IP-telefon

- [Tekniska detaljer, på sidan 13](#)
- [Maskinvara i Cisco IP-telefon, på sidan 29](#)



KAPITEL 2

Tekniska detaljer

- Fysiska och driftsmiljörelaterade specifikationer, på sidan 13
- Kabelspecifikationer, på sidan 14
- Telefonströmförsörjning, på sidan 16
- Nätverksprotokoll, på sidan 18
- Interaktion med VLAN, på sidan 21
- Interaktion med Cisco Unified Communications Manager, på sidan 21
- Interaktion med Cisco Unified Communications Manager Express, på sidan 22
- Interaktion i röstmeddelandesystemet, på sidan 23
- Telefonens startprocess – översikt, på sidan 23
- Externa enheter, på sidan 25
- Information om USB-port, på sidan 25
- Telefonens konfigurationsfiler, på sidan 26
- Telefonbeteende under överbelastning av nätverket, på sidan 26
- Telefonbeteende i ett nätverk med två nätverksroutrar, på sidan 27
- Programmeringsgränssnitt, på sidan 27

Fysiska och driftsmiljörelaterade specifikationer

Följande tabell visar de fysiska och driftsmiljörelaterade specifikationer för Cisco IP-telefon i 8800-serien.

Tabell 12. Fysiska och driftsmässiga specifikationer

Specifikation	Värde eller Intervall
Driftstemperatur	0 ° till 40 °C
Relativ luftfuktighet	Drift: 10 % till 90 % (icke-kondenserande) Ej i drift: 10 % till 95 % (icke-kondenserande)
Förvaringstemperatur	-10 ° till 60 °C
Höjd	229,1 mm
Bredd	257,34 mm

Specifikation	Värde eller Intervall
Djup	40 mm
Vikt	1,19 kg
Ström	100-240 VAC, 50-60 Hz, 0,5 A när du använder nätadaptern 48 VDC, 0,2 A när du använder nätström i nätverkskabeln
Kablar	Kategori 3/5/5e/6 för 10-Mbps-kablar med 4 par Kategori 5/5e/6 för 100 Mbps-kablar med 4 par Kategori 5/5e/6 för 1000 Mbps-kablar med 4 par OBS! Kablarna har 4 ledarpar för totalt 8 ledare.
Distanskrav	Eftersom det stöds av Ethernet-specifikationen antas den maximala kabellängd varje Cisco IP-telefon och växel vara 100 meter.

Kabelfspecifikationer

Följande information avser kabelfspecifikationer:

- RJ-9-uttaget (4 ledare) för lur- och headsetanslutning
- RJ-45-uttag för LAN 10/100/1000BaseT-anslutning (nätverksport 10/100/1000 på telefonen)
- RJ-45-uttag för en andra 10/100/1000BaseT-kompatibel anslutning (datorport 10/100/1000 på telefonen)
- 3,5 mm kontakt för anslutning av högtalare (endast Cisco IP-telefon 8861)
- 48-volts strömkontakt
- USB-portar/-kontakt: en USB-port för Cisco IP-telefon 8851 och två USB-portar för Cisco IP-telefon 8861
- Anslutningar för tre expansionsmoduler som är avsedda för USB-kontakt för Cisco IP-telefon 8851 och 8861

Nätverks- och datorportkontakt

Även om både nätverkets och datorns åtkomstportar används för nätverksanslutning har de olika syften och olika portkontakt.

- Nätverkporten är 10/100/1000 SW-porten på en Cisco IP-telefon.
- Datorporten är 10/100/1000 PC-porten på en Cisco IP-telefon.

Nätverksportkontakt

Följande tabell beskriver nätverksportens anslutningskontakt.

Tabell 13. Nätverksportens anslutningskontakt

Stiftnummer	Funktion
1	BI_DA +
2	BI_DA-
3	BI_DB +
4	BI_DC +
5	BI_DC-
6	BI_DB-
7	BI_DD +
8	BI_DD-
OBS!	BI står för dubbelriktad medan DA, DB, DC och DD står för Data A, Data B, Data C och Data D.

Datorportkontakt

Följande tabell beskriver uttag för anslutning i datorportar.

Tabell 14. Uttag för anslutning (åtkomst) i datorportar:

Stiftnummer	Funktion
1	BI_DB +
2	BI_DB-
3	BI_DA +
4	BI_DD +
5	BI_DD-
6	BI_DA-
7	BI_DC +
8	BI_DC-
OBS!	BI står för dubbelriktad medan DA, DB, DC och DD står för Data A, Data B, Data C och Data D.

Telefonströmförsörjning

Cisco IP-telefon kan drivas med extern ström eller med PoE. En separat strömförsörjning ger extern ström. Switchen kan ge PoE via telefonens Ethernet-kabel.

Cisco IP-telefon 8861 och 8865 är PoE-enheter i klass 4 och kräver ett kort för växel eller linje med klass 4-funktioner som stöder extrafunktioner.

Mer information om telefonens strömförsörjning finns på tillhörande datablad.

När du installerar en telefon som drivs med extern ström ska du ansluta strömförsörjningen innan du kopplar in Ethernet-kabeln till telefonen. När du tar bort en telefon som drivs med extern ström ska du koppla bort Ethernet-kabeln från telefonen innan du kopplar ur strömförsörjningen.

Tabell 15. Riktlinjer för ström till Cisco IP-telefon

Strömtyp	Riktlinjer
Extern ström: Tillhandahålls genom CP-PWR-CUBE-4 = extern strömförsörjning	Cisco IP-telefon använder CP-PWR-CUBE-4-strömförsörjning.
PoE power-Tillhandahålls av en omkopplare via Ethernet-kabel ansluten till telefonen.	Cisco IP-telefon 8851, 8851NR, 8861, 8865 och 8865NR stöder 802.3at PoE för anv av tillbehör. Mer information finns i databladet för din telefon. Växeln kräver en reservströmkälla för avbrottsfri drift av telefonen Se till att CatOS- eller IOS-versionen som körs i din omkopplare har stöd för distribu telefonen. I dokumentationen till din omkopplare står operativsystemets versionsinfo
UPoE (Universal Power over Ethernet)	Cisco IP-telefon 8865 och 8865NR har stöd för UPoE.

Dokumenterna i följande tabell innehåller mer information om följande ämnen:

- Cisco-switchar som arbetar med Cisco IP-telefon
- Cisco IOS-versioner som stöder dubbelriktad energibalansering
- Övriga krav och begränsningar om ström

Tabell 16. Ytterligare information

Ämnen i dokument	URL
PoE-lösningar	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
UPoE	http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe
Ciscos Catalyst-switchar	http://www.cisco.com/c/en/us/products/switches/index.html
Routrar för integrerade tjänster	http://www.cisco.com/c/en/us/products/routers/index.html
Cisco IOS-programvara	http://www.cisco.com/c/en/us/products/ios-nx-os-software/index

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 schemalagda tid eller tills användaren lyfter luren eller 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.

Strömbalansering över LLDP

Telefonen och växeln balanserar strömmen som telefonen använder. Cisco IP-telefon kan användas med flera ströminställningar, som sänker elförbrukningen när tillgången till ström är lägre.

När en telefon har startats om låser växeln och använder ett specifikt protokoll (CDP eller LLDP) för strömbalansering. Växeln använder det första protokollet (som innehåller en ström-TLV [Threshold Limit Value]) som telefonen sänder. Om systemadministratören har inaktiverat protokollet på telefonen kan den inte starta några tillbehör, eftersom växeln inte svarar på strömbegäranden i det andra protokollet.

Cisco rekommenderar att alltid aktivera strömbalansering (standard) vid koppling till en växel som stöder strömbalansering.

Om strömbalanseringen är inaktiverad kan växeln koppla bort strömmen till telefonen. Om växeln inte stöder strömbalansering måste du inaktivera den funktionen innan du slår på strömmen till tillbehör via PoE. När strömbalanseringsfunktionen är inaktiverad kan telefonen förse tillbehören med ström upp till den kapacitet som tillåts med IEEE 802.3af-2003.

**OBS!**

- När CDP och strömbalansering är inaktiverad kan telefonen förse tillbehören med ström upp till 15,4 W.

Nätverksprotokoll

Cisco IP-telefon i 8800-serien har stöd för flera av branschens standard- och Cisco-nätverksprotokoll som krävs för röstkommunikation. Följande tabell ger en översikt över de nätverksprotokoll som telefonerna stöder.

Tabell 17. Nätverksprotokoll som stöds på Cisco IP-telefon i 8800-serien

Nätverksprotokoll	Syfte	Att tänka på vid användning
Bluetooth	Bluetooth är ett WPAN (Personal Area Network)-protokoll som anger hur enheter kommunicerar över korta avstånd.	Cisco IP-telefon 8845, 8865 och 8851 har stöd för Bluetooth 4.1. Cisco IP-telefon 8861 har stöd för Bluetooth 4.0. Cisco IP-telefon 8811, 8841, 8851NR och 8865NR stöder inte Bluetooth.
BootP (Bootstrap Protocol)	BootP aktiverar en nätverksenhet, som en Cisco IP-telefon, för att kunna identifiera viss startinformation som till exempel IP-adressen.	—
CAST (Cisco Audio Session Tunnel)	CAST-protokollet tillåter telefonerna och tillhörande program att kommunicera med fjärranslutna IP-telefoner utan att signalsystemkomponenterna behöver ändras.	Cisco IP-telefon använder CAST som ett gränssnitt mellan CUVA och Cisco Unified Communications Manager, där Cisco IP-telefon används som en SIP-proxy.
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.	Cisco IP-telefon använder CDP för att kommunicera information om extra VLAN-ID, energispar detaljer per port och QoS-konfigurationsinformation (Quality of Service) med Cisco Catalyst-växeln.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP är ett tillverkarspecifikt Cisco-protokoll som används för att bilda en hierarki av peer-to-peer-enheter. Den här hierarkin används för att distribuera firmwarefiler från peer-enheter till deras närliggande enheter.	CPPDP används av funktionen för Peer-delning av firmware.
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 inaktiverat måste du manuellt konfigurera IP-adress, nätmask, gateway och en TFTP-server på varje telefon lokalt. Vi rekommenderar att du använder DHCP-anpassat alternativ 150. Med den här metoden konfigurerar du TFTP-serverns IP-adress som alternativvärdet. Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager. OBS! Om du inte kan använda alternativ 150 så kan du prova med DHCP-alternativ 66.

Nätverksprotokoll	Syfte	Att tänka på vid användning
HTTP (Hypertext Transfer Protocol)	HTTP är standardprotokoll vid överföring av information och flyttning av dokument över Internet och webben.	Cisco IP-telefon använder HTTP för XML-tjänster och felsökning.
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.	Webbapplikationer med både HTTP- och HTTPS-stöd har två konfigurerade URL:er. Cisco IP-telefon som stöder HTTPS väljer HTTPS-URL:en.
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 en Cisco IP-telefon implementeras IEEE 802.1X-standarden genom stöd för följande autentiseringsmetoder: EAP-FAST och EAP-TLS. När 802.1X-autentisering har aktiverats på telefonen bör du inaktivera PC-porten och röst-VLAN.
IEEE 802.11n/802.11ac	IEEE 802.11-standarden anger hur enheter kommunicerar över ett WLAN. 802.11n används med 2,4 GHz- och 5 GHz-band och 802.11ac används med 5 GHz-band.	802.11-gränssnittet är ett distributionsalternativ om Ethernet-kablage inte är tillgängligt eller oönskat. Endast Cisco IP-telefon 8861 och 8865 har stöd för WLAN.
IP (Internet Protocol)	IP är en meddelandeprotokoll som adresserar och skickar paket över nätverket.	För att kommunicera via IP måste nätverksenheter ha en tilldelad IP-adress, subnät och gateway. Identifiering av IP-adresser, undernät och gatewayer tilldelas automatiskt om du använder en Cisco IP-telefon med DHCP. Om du inte använder DHCP måste du manuellt tilldela dessa egenskaper till varje telefon lokalt. Cisco IP-telefon har stöd för IPv6-adresser. Mer information finns i dokumentationen till din version av Cisco Unified Communications Manager.
LLDP (Link Layer Discovery Protocol)	LLDP är ett standardiserat nätverksidentifieringsprotokoll (liknande CDP) som stöds på vissa Cisco-enheter och tredjepartsenheter.	Din Cisco IP-telefon har stöd för LLDP via PC-porten.
LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Devices)	LLDP-MED är en utökning av LLDP-standarden för röstprodukter.	Din Cisco IP-telefon har stöd för LLDP-MED via SW-porten för att kommunicera information som: <ul style="list-style-type: none"> • Konfiguration av röst-VLAN • Enhetsidentifiering • Energihantering • Lagerhantering

Nätverksprotokoll	Syfte	Att tänka på vid användning
RTP (Real-Time Transport Protocol)	RTP är ett standardprotokoll för att transportera realtidsdata, som interaktiv röst över datanät.	Cisco IP-telefon använder RTP-protokollet för att skicka och ta emot realtidsrösttrafik från andra telefoner och gateways.
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. Konferensamtal upprättas med hjälp av endast de SDP-funktioner som har stöd i alla ändpunkter i konferensen.	SDP-funktioner, till exempel kodektyper och identifiering av DTMF och komfortbrus, konfigureras vanligtvis globalt av Cisco Unified Communications Manager eller Media Gateway i drift. Vissa SIP-slutpunkter kan tillåta konfigurationen av dessa parametrar görs vid själva slutpunkten.
SIP (Session Initiation Protocol)	SIP är IETF-standarden (Internet Engineering Task Force) för multimediamkonferenser 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 används SIP i funktioner för signalering och sessionshantering i ett pakettelefoninätverk. Med signalering kan samtalsinformation transporteras över nätverksgränserna. Sessionshantering ger möjlighet att styra attribut för ett samtal från ändpunkt till ändpunkt. Cisco IP-telefoner stöder SIP-protokollet när telefonerna arbetar i endast IPv6 eller IPv4, eller i både IPv4 och IPv6.
TCP (Transmission Control Protocol)	TCP är ett anslutningsorienterat transportprotokoll.	Cisco IP-telefon använder TCP för att ansluta till Cisco Unified Communications Manager och få åtkomst till XML-tjänster.
TLS (Transport Layer Security)	TLS är ett standardprotokoll för att säkra och autentisera kommunikationer.	Vid säkerhetsimplemtering använder Cisco IP-telefon TLS-protokollet för säker registrering med Cisco Unified Communications Manager.
TFTP (Trivial File Transfer Protocol)	Med TFTP kan du överföra filer över nätverket. På din Cisco IP-telefon används TFTP till att hämta en konfigurationsfil som är specifik för telefonen.	TFTP kräver en TFTP-server i nätverket som kan identifieras automatiskt från DHCP-servern. Om du vill ha en telefon som använder en annan TFTP-server än den som anges av DHCP-servern måste du manuellt tilldela IP-adressen till TFTP-servern genom att använda meny Nätverkskonfiguration på telefonen. Mer information finns i dokumentationen till din version av Cisco Unified Communications Manager.
UDP (User Datagram Protocol)	UDP är ett anslutningslöst meddelandeprotokoll för leverans av datapaketer.	UDP används endast för RTP-strömmar. SIP-signalering på telefonerna stöder inte UDP.

Mer information om stöd för LLDP-MED finns i vitboken LLDP-MED and Cisco Discovery Protocol:

http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml

Relaterade ämnen

- [802.1X-autentisering](#), på sidan 108
- [Konfigurera nätverksinställningar](#)
- [Verifiering vid telefonstart](#), på sidan 64
- [Interaktion med VLAN](#), på sidan 21
- [Interaktion med Cisco Unified Communications Manager](#), på sidan 21
- [Interaktion med Cisco Unified Communications Manager Express](#), på sidan 22
- [Ställa in ljud- och videoportintervall](#), på sidan 180
- [Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Interaktion med VLAN

Cisco IP-telefonen innehåller en intern Ethernet-switch, som möjliggör vidarebefordran av paket till telefonen, till datorporten (åtkomst) och nätverksporten på telefonens baksida.

Om en dator är ansluten till datorns port (åtkomst) delar datorn och telefonen samma fysiska länk till växeln och delar samma port i växeln. Datatrafiken närvarande på VLAN stöd telefoner kan försämra kvaliteten på VoIP-trafik.

- De aktuella VLAN:erna kan konfigureras på ett IP-undernät. Däremot kan det hända att ytterligare IP-adresser inte är tillgängliga att tilldela telefonen till samma subnät som andra enheter som ansluter till samma port.
- Datatrafik i VLAN med stöd för telefoner kan ge sämre kvalitet på VoIP-trafik.
- Nätsäkerhet kan tyda på ett behov av att isolera VLAN-rösttrafiken från VLAN-datatrafiken.

Du kan lösa dessa problem genom att isolera rösttrafiken på ett separat VLAN. Växelporten som telefonen ansluter till konfigureras då för separata VLAN:

- Rösttrafik till och från IP-telefon (extra VLAN på Cisco Catalyst 6000-serien, till exempel)
- Datatrafik till och från datorn som ansluter till växeln genom porten dator (access) av IP-telefonen (native VLAN)

Isolera telefonerna på en separat, extra VLAN ökar kvaliteten på rösttrafik och tillåter ett stort antal telefoner som ska läggas till ett befintligt nätverk som inte har tillräckligt med IP-adresser för varje telefon.

För mer information, se dokumentationen som medföljer en Cisco switch. Du kan också få tillgång till kopplad information på denna URL:

<http://cisco.com/en/US/products/hw/switches/index.html>

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 telefonsystemet, 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 xv

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.

Både sessionslinjeläge och förbättrat linjeläge stöds i CME-läge.

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 startprocess – översikt

När du ansluter till VoIP-nätverket, går Cisco IP-telefon igenom en startprocess som standard. Beroende på din specifika nätverkskonfiguration kanske bara vissa av dessa steg genomförs på en Cisco IP Phone.

1. Få ström från växel. Om en telefon inte har extern strömförsörjning, ger växel ström via Ethernet-kabeln som är kopplad till telefonen.
2. (För Cisco IP-telefon 8861 och 8865 i ett trådlöst nätverk) Sök efter en åtkomstpunkt. Cisco IP-telefon 8861 och 8865 söker RF-täckningsområdet med radion. Telefonen söker i nätverksprofilerna och letar efter åtkomstpunkter som innehåller matchande SSID och autentiseringstyp. Telefonen kopplas till åtkomstpunkten med den högsta RSSI som matchar med nätverksprofilen.
3. (För Cisco IP-telefon 8861 och 8865 i ett trådlöst nätverk) Verifiera med åtkomstpunkten. En Cisco IP-telefon startar autentiseringsprocessen. I följande tabell beskrivs autentiseringsprocessen:

Autentiseringstyp	Alternativ för hantering av nycklar	Beskrivning
Öppen	Ingen	Alla enheter kan autentisera åtkomstpunkten. För ökad säkerhet kan du också använda statisk WEP-kryptering.

Autentiseringstyp	Alternativ för hantering av nycklar	Beskrivning
Delad nyckel	Ingen	Telefonen krypterar textsträngen med hjälp av WEP-nyckeln och åtkomstpunkten måste kontrollera WEP-nyckeln som användes för att kryptera textsträngen innan nätverksåtkomst är tillgänglig.
PEAP eller EAP-FAST	Ingen	RADIUS-servern autentiserar användarnamn och lösenord innan nätverksåtkomst är tillgänglig.

4. Läs in den lagrade telefonbilden. Vid start körs ett startprogram som läser in telefonens firmwarebild som lagras i telefonens flashminne. Med den här bilden kan telefonen initiera programvaran och maskinvaran.
5. Konfigurera VLAN. Om en Cisco IP-telefon är ansluten till en Cisco Catalyst-växel informerar den telefonen om det röst-VLAN som har definierats i växeln. Telefonen måste känna till VLAN-medlemskapet innan den kan fortsätta med begäran om DHCP (Dynamic Host Configuration Protocol) för en IP-adress.
6. Hämta en IP-adress. Om en Cisco IP-telefon använder DHCP för att hämta en IP-adress, gör telefonen en förfrågan om att få den från DHCP-servern. Om du inte använder DHCP i nätverket, måste du tilldela statiska IP-adresser till varje telefon lokalt.
7. Begär CTL-filen. TFTP-servern lagrar CTL-filen. Den här filen innehåller de certifikat som krävs för att upprätta en säker anslutning mellan telefonen och Cisco Unified Communications Manager.
Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.
8. Begär ITL-filen. Telefonen begär ITL-filen när den har begärt CTL-filen. ITL-filen innehåller certifikat för de enheter som är betrodda för telefonen. Certifikaten används för att autentisera en säker anslutning med servrarna eller för att autentisera en digital signatur som har signerats av servrarna. ITL-filen stöds i Cisco Unified Communications Manager 8.5 och senare.
9. Åtkomst till en TFTP-server. Förutom att tilldela IP-adress, dirigerar DHCP-servern en Cisco IP-telefon till en TFTP-server. Om telefonen har en statiskt definierad IP-adress måste du konfigurera TFTP-servern lokalt på telefonen. Telefonen kontaktar sedan TFTP-servern direkt.



OBS! Du kan även tilldela en alternativ TFTP-server i stället för den som DHCP tilldelar.

10. Begär konfigurationsfilen. TFTP-servern har konfigurationsfiler som styr parametrar för att ansluta till Cisco Unified Communications Manager och annan information för telefonen.
11. Kontakta Cisco Unified Communications Manager. Konfigurationsfilen definierar hur en Cisco IP-telefon kommunicerar med Cisco Unified Communications Manager och ger telefonen ett laddnings-ID. När den har hämtat filen från TFTP-servern, försöker telefonen ansluta till högst prioriterad Cisco Unified Communications Manager i listan.

Om säkerhetsprofilen på telefonen är konfigurerad för säker signalering (krypterad eller autentiserad) och Cisco Unified Communications Manager är inställd i säkerhetsläge, använder telefonen en TLS-anslutning. I annat fall gör telefonen en osäker TCP-anslutning.

Om telefonen har lagts till i databasen manuellt identifieras telefonen av Cisco Unified Communications Manager. Om telefonen inte har lagts till manuellt i databasen och autoregistrering är aktiverat i Cisco Unified Communications Manager, försöker telefonen automatisk registrera sig själv i Cisco Unified Communications Manager-databasen.



OBS! Autoregistrering är inaktiverad om du konfigurerar CTL-klienten. I så fall måste du lägga till telefonen i Cisco Unified Communications Manager-databasen manuellt.

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Externa enheter

Vi rekommenderar att du använder externa enheter av hög kvalitet som är avskärmade mot oönskade radiofrekvens- och tonfrekvenssignaler (RF respektive AF). Externa enheter kan vara headset, kablar och kontakter.

Beroende på enheternas kvalitet och närheten till andra enheter, till exempel mobiltelefoner eller radiosändare/-mottagare, kan vissa störningar förekomma. I dessa fall rekommenderar vi att du vidtar en eller flera av dessa åtgärder:

- Flytta bort den externa enheten från källan till radio- eller tonsignalerna.
- Led bort den externa enhetens kablar från källan till radio- eller tonsignalerna.
- Använd skärmade kablar till den externa enheten eller kablar med bättre avskärmning och kontakt.
- Minska längden på kabeln till den externa enheten.
- Använd ferrit eller liknande till den externa enhetens kablar.

Cisco kan inte garantera prestandan för externa enheter, kablar och kontakter.



Försiktighet Använd endast externa högtalare, mikrofoner och headset som uppfyller EMC-direktivet [89/336/EC] inom EU.

Information om USB-port

Cisco IP-telefon 8851, 8851NR, 8861, 8865 och 8865NR stöder upp till fem enheter som kan anslutas till varje USB-port. Varje enhet som ansluts till telefonen räknas när det gäller högsta antalet enheter. Telefonen kan till exempel ha upp till fem USB-enheter i sidoporten och fem ytterligare standard-USB-enheter i den bakre porten. Många USB-produkter från tredje parter räknas som flera USB-enheter. En enhet som består av en USB-hubb och ett headset kan till exempel räknas som två USB-enheter. Mer information finns i dokumentationen för USB-enheten.



- OBS!**
- Ej strömförsörjda hubbar stöds inte och strömförsörjda hubbar med fler än fyra portar stöds inte.
 - USB-headset som ansluts till telefonen via en USB-hubb stöds inte.

Varje knappexpansionsmodul som ansluts till telefonen räknas som en USB-enhet. Om tre knappexpansionsmoduler ansluts till telefonen räknas det som tre USB-enheter.

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

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Telefonbeteende under överbelastning av nätverket

Allt som försämrar nätverkets prestanda kan påverka telefonens ljud- och videokvalitet 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.

Telefonbeteende i ett nätverk med två nätverksroutrar

Cisco IP-telefon i 8800-serien använder en brandvägg för att tillhandahålla skydd mot cyberintrång, till exempel man-in-the-middle-attacker. Den här brandväggen kan inte inaktiveras. Men den kan stoppa trafiken i en telefon, om du konfigurerar ditt nätverk med två nätverksroutrar i samma subnät och IP-omdirigering.

Telefonens brandvägg stoppar trafik eftersom denna nätverksinställning liknar en man-in-the-middle-attack. Telefonen får omdirigeringspaket för olika destinations-IP-adresser i ett annat subnät från telefonen. Telefonen ingår i ett nätverk med fler än en router och standardroutern skickar trafik till en andra router.

Titta på telefonloggar om du misstänker att brandväggen stoppar trafik. Observera om ett meddelande med felkod 1 från operativsystemet visas vid försök att upprätta en anslutning. En av signaturerna är

```
sip_tcp_create_connection: socket connect failed cpr_errno: 1.
```

Ett nätverk med två nätverksroutrar i samma subnät och IP-omdirigering är inte en vanlig konfiguration. Om du använder den här nätverksinställningen, kan du överväga använda endast en router i ett subnät. Men om du behöver två nätverksroutrar i samma subnät kan du inaktivera IP-omdirigeringen i routern och starta om telefonen.

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](#).



KAPITEL 3

Maskinvara i Cisco IP-telefon

- [Översikt över telefon, på sidan 29](#)
- [Cisco Wireless IP Phone 8811, på sidan 31](#)
- [Cisco IP-telefon 8841 och 8845, på sidan 32](#)
- [Cisco IP-telefon 8851 och 8851NR, på sidan 33](#)
- [Cisco IP-telefon 8851, 8865 och 8865NR, på sidan 35](#)
- [Knappar och maskinvara, på sidan 36](#)
- [Skydda din telefons videokamera, på sidan 39](#)

Översikt över telefon

Cisco IP-telefon i 8800-serien tillhandahåller röstkommunikation över ett IP-nätverk. Cisco IP-telefonen fungerar ungefär som en digital företagstelefon, så att du kan ringa och ta emot telefonsamtal och använda funktioner som ljudavstängning, parkera samtal, överföra samtal och mycket mer. Eftersom telefonen ansluter till ditt datanätverk ger det dessutom förbättrade IP-telefonifunktioner, inklusive åtkomst till nätverksinformation och tjänster, och anpassningsbara funktioner och tjänster.

Cisco IP-telefon 8811 har en LCD-skärm i gråskala. Cisco IP-telefon 8841, 8845, 8851, 8851NR, 8861, 8865 och 8865NR har en 24-bitars färg-LCD-skärm.

Du är begränsad av antalet tillgängliga linjeknappar när du lägger till telefonfunktioner. Du kan inte lägga till flera funktioner än antalet linjeknappar på telefonen.

Cisco IP-telefoner har följande funktioner:

- Programmerbara funktionsknappar som stöder upp till fem linjer i sessionslinjeläge eller upp till tio linjer med förbättrat linjeläge
- Fullständiga videofunktioner (endast Cisco IP-telefon 8845, 8865 och 8865NR)
- Gigabit Ethernet-anslutning
- Bluetooth-stöd för trådlösa headset (endast Cisco IP-telefon 8845, 8851, 8861 och 8865. Den här funktionen stöds inte på Cisco IP-telefon 8811, 8841, 8851NR och 8865NR.)
- Stöd för en extern mikrofon och högtalare (endast Cisco IP-telefon 8861, 8865 och 8865NR)
- Anslutning till nätverket med Wi-Fi (endast Cisco IP-telefon 8861 och 8865. Wi-Fi stöds inte på Cisco IP-telefon 8865NR.)
- USB-portar:

- En USB-port för Cisco IP-telefon 8851 och 8851NR
- Två USB-portar för Cisco IP-telefon 8861, 8865 och 8865NR

Cisco IP-telefon 8845, 8865 och 8865NR har stöd för videosamtal med den inbyggda videokameran. Använd funktionen för att samarbeta med vänner och medarbetare eller för att hålla möten ansikte mot ansikte över telefonen.



OBS! Du bör spara kartongen och förpackningen för Cisco IP-telefon 8845, 8865 och 8865NR. Kamerorna på dessa telefoner är ömtåliga. Om du flyttar telefonen rekommenderar vi att du paketerar telefonen i originalkartongen för att skydda kameran. Mer information finns i [Skydda din telefons videokamera, på sidan 39](#).

Ett videosamtal inkluderar följande funktioner:

- PIP – Välj bland fyra lägen: Nere till höger, uppe till höger, uppe till vänster och nere till vänster. Du kan även slå av PIP.
- Växla – Växlar vyer i PIP-vyn. Den programstyrda knappen Växla är inaktiverat när PIP är av.
- Video av dig – Välj Video av dig för att se din bild som den visas på video.
- Start av videoanvändargränssnitt och konferens/överföring – Välj om du vill starta en konferens.

Mer information om videosamtal finns i *Cisco IP-telefon 8800-seriens användarhandbok för Cisco Unified Communications Manager* och dokumentationen till din utgåva av Cisco Unified Communications Manager.

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
- iSAC



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, konferensamtal 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 subnätinformation.

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.

Relaterade ämnen

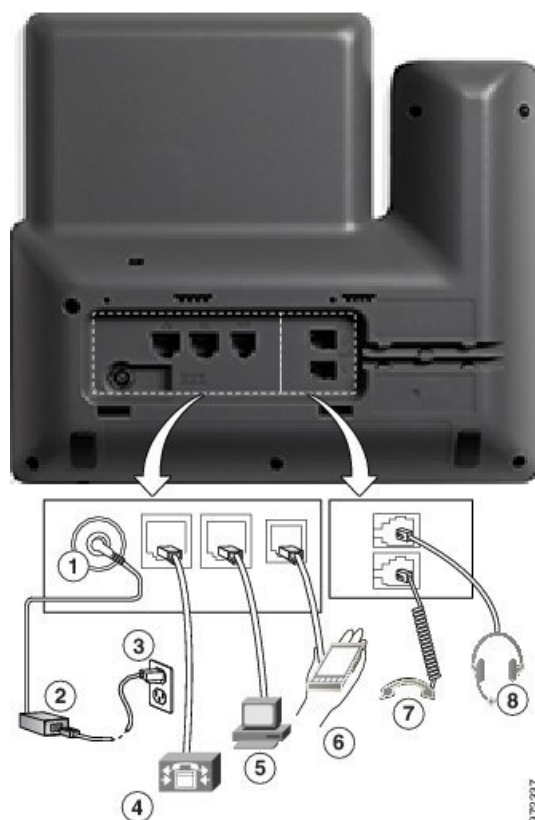
[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Cisco Wireless IP Phone 8811

I följande avsnitt beskrivs egenskaperna för Cisco Wireless IP Phone 8811.

Telefonanslutningar för

Anslut telefonen till företagets IP-telefonnätverk enligt följande diagram.



1	DC-adaptörport (DC48V).	5	Anslutning till åtkomstport (10/100/1000 PC).
2	Nättaggregat, växelström till likström (tillval).	6	Port :
3	Väggkontakt för nättaggregat (tillval).	7	Anslutning för lur.
4	Anslutning till nätverksport (10/100/1000 SW). IEEE 802.3at-effekt aktiverad.	8	Analog headset-anlutning (tillval).



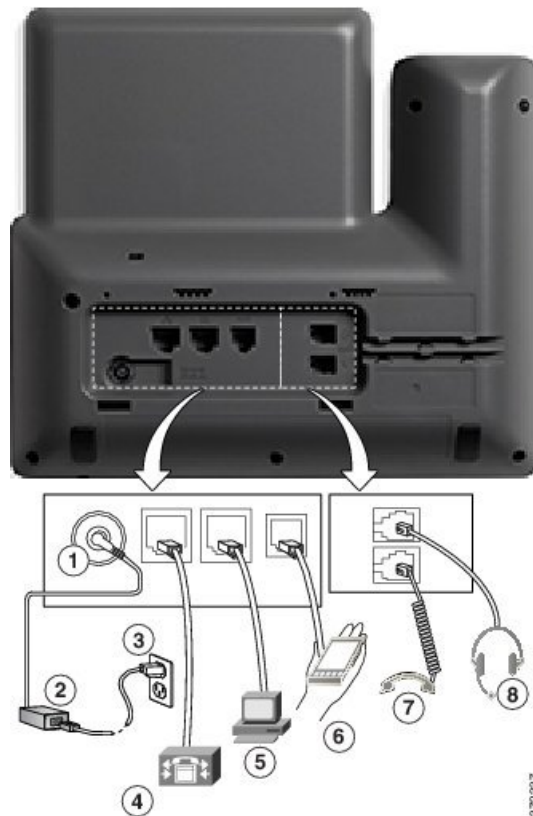
OBS! Cisco Wireless IP Phone 8811 har inte stöd för knappexpansionsmodul.

Cisco IP-telefon 8841 och 8845

I följande avsnitt beskrivs egenskaperna för Cisco IP-telefon 8841 och 8845.

Telefonanslutningar

Anslut telefonen till företagets IP-telefonnätverk med hjälp av följande diagram.



1	Likströmsadapterport (DC48V).	5	Anslutning till åtkomstport (10/100/1000 PC).
2	Nättaggregat, växelström till likström (tillval).	6	Port :
3	Väggkontakt för nättaggregat (tillval).	7	Anslutning för lur.
4	Anslutning till nätverksport (10/100/1000 SW). IEEE 802.3at-effekt aktiverad.	8	Analog headset-anslutning (tillval).



OBS! Cisco IP-telefon 8841 och 8845 har inte stöd för en knappexpansionsmodul.

Cisco IP-telefon 8851 och 8851NR

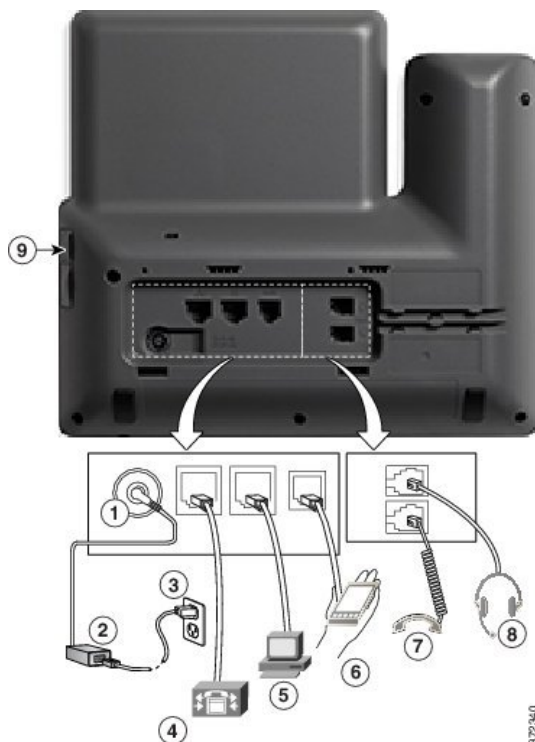
I följande avsnitt beskrivs egenskaperna för Cisco IP-telefon 8851 och 8851NR.



OBS! Cisco IP-telefon 8851NR stöder inte Bluetooth. I annat fall stöder Cisco IP-telefon 8851 och Cisco IP-telefon 8851NR samma funktioner.

Telefonanslutningar för

Anslut telefonen till företagets IP-telefonnätverk enligt följande diagram.



1	Likströmsadapterport (DC48V).	6	Port :
2	Nätaggreat, växelström till likström (tillval).	7	Anslutning för lur.
3	Väggkontakt för nätaggreat (tillval).	8	Analog headset-anslutning (tillval).
4	Anslutning till nätverksport (10/100/1000 SW). IEEE 802.3at-effekt aktiverad.	9	USB-port
5	Anslutning till åtkomstport (10/100/1000 PC).		



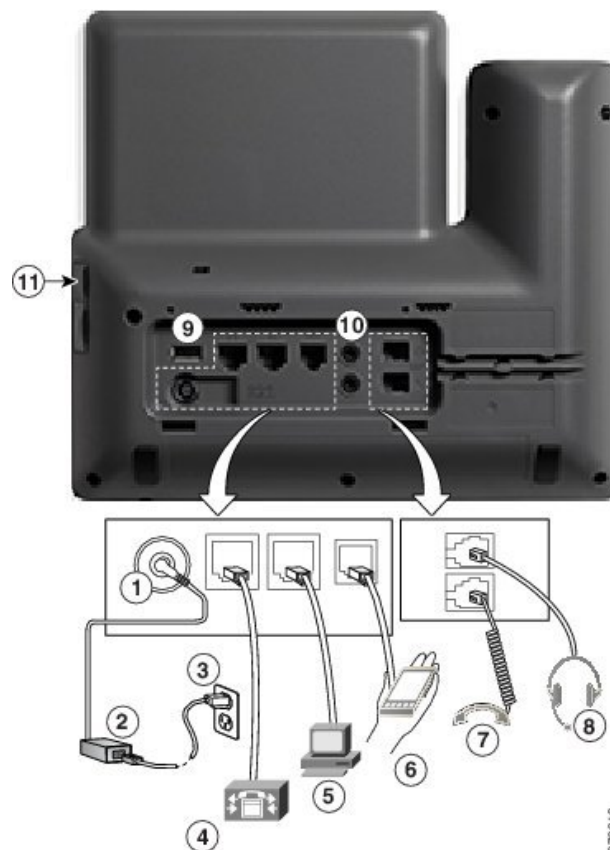
OBS! Varje USB-port stöder upp till fem anslutningar av enheter som stöds eller inte stöds. Varje ansluten enhet till telefonen räknas när det gäller högsta antalet enheter. Telefonen kan till exempel ha upp till fem USB-enheter (till exempel två knappexpansionsmoduler, ett headset, en hubb och en annan standard-USB-enhet) i sidoporten. Många USB-produkter från tredje parter räknas som flera USB-enheter. En enhet som består av en USB-hubb och ett headset kan till exempel räknas som två USB-enheter. Mer information finns i dokumentationen för USB-enheten.

Cisco IP-telefon 8851, 8865 och 8865NR

I följande avsnitt beskrivs egenskaperna för Cisco IP-telefon 8861, 8865 och 8865NR.

Telefonanslutningar

Anslut telefonen till företagets IP-telefonnätverk enligt följande diagram.



1	Likströmsadapterport (DC48V).	7	Anslutning för lur.
2	Nätaggregat, växelström till likström (tillval).	8	Analog headset-anslutning (tillval).

3	Väggkontakt för nätaggregat (tillval).	9	USB-port
4	Anslutning till nätverksport (10/100/1000 SW). IEEE 802.3at-effekt aktiverad.	10	Portar för ljud in/ut.
5	Anslutning till åtkomstport (10/100/1000 PC).	11	USB-port
6	Port :		



OBS! Varje USB-port stöder upp till fem anslutningar av enheter som stöds eller inte stöds. Varje ansluten enhet till telefonen räknas när det gäller högsta antalet enheter. Telefonen kan till exempel ha upp till fem USB-enheter (till exempel tre knappexpansionsmoduler, en hubb och en annan standard-USB-enhet) i sidoporten och fem ytterligare standard-USB-enheter i den bakre porten. Många USB-produkter från tredje parter räknas som flera USB-enheter. En enhet som består av en USB-hubb och ett headset kan till exempel räknas som två USB-enheter. Mer information finns i dokumentationen för USB-enheten.

Knappar och maskinvara

Cisco IP-telefon 8800-serien har två olika typer av maskinvara:

- Cisco IP-telefon 8811, 8841, 8851, 8851NR och 8861 har ingen kamera.
- Cisco IP-telefon 8845, 8865 och 8865NR har integrerad kamera.

På bilden nedan visas Cisco IP-telefon 8845.





Figur 1. Cisco IP-telefon 8845, knappar och maskinvara



I följande tabell beskrivs knapparna i Cisco IP-telefon i 8800-serien.

Tabell 18. Cisco IP-telefon i 8800-serien – knappar

1	Telefonlur med lamprad	Visar om du har ett inkommande samtal (blinkar rött) eller ett nytt röstmeddelande (lyser rött)
2	Kamera Endast Cisco IP-telefon 8845, 8865 och 8865NR	Använd kameran för videosamtal.
3	Programmerbara funktionsknappar och linjeknappar	 Kom åt telefonlinjer, funktioner och samtalsessioner. Du är begränsad av antalet tillgängliga linjeknappar när du lägger till telefonfunktioner. Du kan inte lägga till flera funktioner än antalet linjeknappar på telefonen. Mer information finns i avsnittet om programknappar, linjer och funktionsknappar i kapitlet "Maskinvara i Cisco IP-telefon".
4	Programstyrda knappar	 Kom åt funktioner och tjänster. Mer information finns i avsnittet om programknappar, linjer och funktionsknappar i kapitlet "Maskinvara i Cisco IP-telefon".
5	Tillbaka , navigeringshjul och Lägg på	Tillbaka  Gå tillbaka till föregående skärm eller meny. Navigeringskluster  Navigeringsring and Välj -knapp – bläddra i menyer, markera objekt och välj ett markerat objekt. Lägg på  Avsluta samtal eller en session.
6	Parkera/återuppta , Konferens och Överför	Parkera/återuppta  Parkera ett aktivt samtal och återuppta ett parkerat samtal. Konferens  Skapa ett konferenssamtal. Överför  Överför ett samtal.
7	Högtalartelefon , Ljud av och Headset	Högtalartelefon  Aktivera och inaktivera högtalartelefonen. När högtalartelefonen är aktiv är knappen tänd. Ljud av  Aktivera och inaktivera mikrofonen. När mikrofonen är tyst är knappen tänd. Headset  Aktivera headsetet. Knappen lyser när headsetet är aktivt. När du vill lämna headsetläge lyfter du på luren eller väljer Högtalartelefon  .






8	Kontakter, Program och Meddelanden	<p>Kontakter  Åtkomst till personlig katalog och företagskatalog.</p> <p>Program  Åtkomst till senaste samtal, användarinställningar, telefoninställningar och till telefonens modellinformation.</p> <p>Meddelanden  Ring upp ditt röstmeddelandesystem automatiskt.</p>
9	Volym-knapp	 Justera lurens, headsetets och högtalartelefonens volym (lur av) och ringsignalens volym (lur på).


Programstyrda knappar, linjeknappar och funktionsknappar

Du kan använda funktionerna på telefonen på flera olika sätt:

- Funktionsknappar, som finns underst på skärmen, ger dig tillgång till funktionen som visas på skärmen ovanför funktionsknappen. De programstyrda knapparna ändras beroende på vad du gör för tillfället. Den programstyrda knappen **Mer...** visar att det finns fler funktioner tillgängliga.
- Med funktions- och linjeknapparna på båda sidor av skärmen kommer du åt telefonfunktioner och telefonlinjer.
 - Funktionsknappar – Används för funktioner som **Kortnummer** och **Hämta samtal** och för att visa din status på en annan linje.
 - Linjeknappar – Används för att svara på ett samtal eller hämta ett parkerat samtal. När de inte används för ett aktivt samtal används de för att starta telefonfunktioner som till exempel att visa missade samtal.

Funktions- och linjeknapparna lyser för att visa status:

LED-färg och status	Normalinjeläge: Linjeknappar	Normalinjeläge: Funktionsknappar Förbättrat linjeläge
 Grön LED-lampa med fast sken	Aktivt samtal eller tvåvägs snabbtelefonsamtal, parkerat samtal, sekretessläge	Aktivt samtal eller tvåvägs snabbtelefonsamtal, sekretessläge
 Grön LED-lampa med blinkande sken	Ej tillämpligt	Parkerat samtal
 Gul LED-lampa med fast sken	Inkommande samtal, återställt samtal, envägs snabbtelefonsamtal, inloggad i svarsgrupp	Envägs snabbtelefonsamtal, inloggad i svarsgrupp
 Gul LED-lampa med blinkande sken	Ej tillämpligt	Inkommande samtal, återställt samtal
 Röd LED-lampa med fast sken	Fjärrlinje används, fjärrlinje parkerad, "stör ej" aktivt	Fjärrlinje används, "stör ej" aktivt

LED-färg och status	Normallinjeläge: Linjeknappar	Normallinjeläge: Funktionsknappar Förbättrat linjeläge
 Röd LED-lampa med blinkande sken	Ej tillämpligt	Fjärrlinje parkerad

Administratören kan ställa in vissa funktioner som programstyrda knappar eller som funktionsknappar. Du kan även komma åt vissa funktioner med programstyrda knappar eller motsvarande fast knapp.

Skydda din telefons videokamera

Kameran på din videotelefon är ömtålig och kan gå sönder under transport av telefonen.

Innan du börjar

Du behöver något av följande:

- Telefonens originalkartong och förpackningsmaterial
- Förpackningsmaterial, exempelvis skum eller bubbelwrap

Arbetsordning

-
- Steg 1** Om du har originalkartongen:
- Placera skummaterialet på kameran så att linsen är väl skyddad.
 - Lägg telefonen i sin originalkartong.
- Steg 2** Om du inte har kartongen ska du försiktigt paketera telefonen i skum eller bubbelwrap så att kameran skyddas. Se till att skummaterialet skyddar och omsluter kameran så att inget trycker mot kameran från något håll för att kameran inte ska skadas under transport.
-



DEL II

Installation av Cisco IP-telefon

- [Installation av Cisco IP-telefon, på sidan 43](#)
- [Telefoninställningar i Cisco Unified Communications Manager, på sidan 67](#)
- [Hantering av självbetjäningssportalen, på sidan 79](#)



KAPITEL 4

Installation av Cisco IP-telefon

- Kontrollera nätverksinställningen, på sidan 43
- Aktiveringskod vid installation för telefoner på företaget, på sidan 44
- Aktiveringskodregistrering och mobilåtkomst och Remote Access, på sidan 45
- Aktivera autoregistrering för telefoner, på sidan 45
- Installera Cisco IP-telefon, på sidan 47
- Konfigurera telefonen från inställningsmenyerna, på sidan 49
- Aktivera det trådlösa nätverket på telefonen, på sidan 51
- Konfigurera nätverksinställningar, på sidan 58
- Verifiering vid telefonstart, på sidan 64
- Konfigurera telefontjänster för användare, på sidan 64
- Ändra en användares telefonmodell, på sidan 65

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 xv

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 självbetjäningssportalen. 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 anknyningsnummer 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 anknyningsnummer**
 - **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**.

Installera Cisco IP-telefon

När telefonen ansluter till nätverket påbörjas telefonens startprocess och registreras i Cisco Unified Communications Manager. För att slutföra installationen av telefonen konfigurerar du nätverksinställningarna på telefonen beroende på om du aktiverar eller inaktiverar DHCP-tjänsten.

Om du har använt autoregistrering måste du uppdatera den specifika konfigurationsinformationen för telefonen som associerar telefonen med en användare, ändra knapptabellen eller katalognumret.



OBS! Innan du använder externa enheter ska du läsa [Externa enheter, på sidan 25](#).

Information om hur du installerar tillbehör finns i *Tillbehörshandboken för Cisco IP-telefon 7800- och 8800-serien för Cisco Unified Communications Manager*.

Om du bara har en LAN-kabel vid skrivbordet, kan du ansluta telefonen till LAN med SW-port och sedan ansluta datorn till PC-porten. Mer information finns i [Dela nätverksanslutning med din telefon och dator, på sidan 48](#).

Du kan också sammanlänka två telefoner tillsammans. Anslut PC-porten på den första telefonen till SW-porten på andra telefonen.



Försiktighet Anslut inte SW och PC-portar i LAN.

Arbetsordning

Steg 1 Välj kraftkällan för telefonen:

- Power over Ethernet (PoE)
- Extern strömförsörjning

Mer information finns i [Telefonströmförsörjning, på sidan 16](#).

Steg 2 Anslut luren till lurporten och tryck in kabeln i kanalen i telefonen.

Den bredbandskapabla telefonen är speciellt framtagen för att användas med en Cisco IP-telefon. Handenheten innehåller en ljusremsa som visar inkommande samtal och väntande röstmeddelanden.

Försiktighet Om du inte trycker in kabeln i telefonkanalen kan det orsaka skada på kretskortet. Kabelkanalen minskar belastningen på kontakten och kretskortet.

Steg 3 Anslut ett headset eller trådlöst headset. Du kan lägga till ett headset senare om du inte ansluter ett nu.

Tryck in kabeln i kabelspåret.

Försiktighet Om du inte trycker in kabeln i telefonkanalen kan det orsaka skada på kretskortet som finns i telefonen. Kabelkanalen minskar belastningen på kontakten och kretskortet.

- Steg 4** Anslut en rak Ethernet-kabel från växeln till nätverksporten märkt 10/100/1000 SW på en Cisco IP-telefon. Varje Cisco IP-telefon levereras med en Ethernet-kabel i lådan.
- Använd kablar i kategori 3, 5, 5e eller 6 för 10 anslutningar på Mbit/s, kategori 5, 5e eller 6 för anslutningar på 100 Mbit/s och kategori 5e eller 6 för anslutningar på 1 000 Mbit/s. Mer information och riktlinjer finns i [Nätverks- och datorportkontakt, på sidan 14](#).
- Steg 5** Anslut en rak Ethernet-kabel från en annan nätverksenhet, till exempel en stationär dator till dator-porten på en Cisco IP-telefon. Du kan ansluta en annan nätverksenhet senare om du inte ansluter en nu.
- Använd kablar i kategori 3, 5, 5e eller 6 för 10 anslutningar på Mbit/s, kategori 5, 5e eller 6 för anslutningar på 100 Mbit/s och kategori 5e eller 6 för anslutningar på 1 000 Mbit/s. Mer information och riktlinjer finns i [Nätverks- och datorportkontakt, på sidan 14](#).
- Steg 6** Om telefonen är på ett skrivbord justerar du basstället. Med en väggmonterad telefon, kan du behöva justera telefonlurshållaren för att säkerställa att mottagaren inte kan glida ut ur hållaren.
- Steg 7** Övervaka telefonens startprocess. I det här steget läggs primära och sekundära katalognummer och funktioner till som är associerade med katalognummer till telefonen och verifierar att telefonen är korrekt konfigurerad.
- Steg 8** Om du konfigurerar nätverksinställningarna på telefonen, kan du ställa in en IP-adress för telefonen genom att antingen använda DHCP eller manuellt ange en IP-adress.
- Se [Konfigurera nätverksinställningar, på sidan 58](#) och [Ställa in nätverk, på sidan 229](#).
- Steg 9** Uppgradera telefonen till den aktuella firmwarebilden.
- Firmwareuppgraderingar över WLAN-gränssnittet kan ta längre tid än att uppdatera över det trådbundna gränssnittet beroende på kvaliteten och bandbredden i den trådlösa anslutningen. Vissa uppgraderingar kan ta mer än en timme.
- Steg 10** Ring samtal med en Cisco IP-telefon för att kontrollera att telefonen och funktionerna fungerar korrekt.
- Se *Användarhandbok för Cisco IP-telefon 8800-serien*.
- Steg 11** Tillhandahåll information till slutanvändare 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 IP-telefoner.

Dela nätverksanslutning med din telefon och dator

Både telefonen och datorn måste anslutas till nätverket för att fungera. Om du bara har en Ethernet-port kan dina enheter dela nätverksanslutning.

Innan du börjar

Administratören måste aktivera PC-porten i Cisco Unified Communications Manager innan du kan använda den.

Arbetsordning

- Steg 1** Anslut telefonens SW-port till LAN med en Ethernet-kabel.
- Steg 2** Anslut datorn till telefonens PC-port med en Ethernet-kabel.
-

Konfigurera telefonen från inställningsmenyerna

Cisco IP-telefon innehåller följande konfigurationsmenyer:

- **Nätverksinställning:** Här finns det alternativ för visning och konfiguration av nätverksinställningar som endast IPv4 och endast IPv6, WLAN och Ethernet.
- **Ethernet-inställning:** Menyalternativen i denna undermeny ger alternativ för att konfigurera Cisco IP-telefon över ett Ethernet-nätverk.
- **Wi-Fi-klientens inställningar:** Menyalternativen i denna undermeny ger alternativ för att konfigurera Cisco IP-telefon med det trådlösa lokala nätverket (WLAN). Wi-Fi stöds endast på Cisco IP-telefon 8861 och 8865.



OBS! Telefonens PC-port är inaktiverad när wifi är aktiverat på din telefon.

- **IPv4-inställning och IPv6-inställning:** Dessa undermenyer på menyn Ethernet-inställning och menyn Wi-Fi-klientens inställningar ger ytterligare nätverksalternativ.
- **Säkerhetsinställning:** Här finns det alternativ för visning och konfiguration av säkerhetsinställningar som säkerhetsläge, listan över betrodda och 802.1X-autentisering.

Innan du kan ändra alternativinställningar på menyn Nätverksinställning, måste du låsa upp alternativ för redigering.





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

- **Aktiverat:** Ger tillgång till inställningsmenyn.
- **Inaktiverat:** Förhindrar åtkomst till inställningsmenyn.
- **Begränsat:** Ger tillgång till menyn med användarinställningar och tillåter att volymändringar sparas. Förhindrar åtkomst till andra alternativ på menyn Inställningar.

Om du inte kan få tillgång till ett alternativ på menyn Admin.inställningar kontrollerar du fältet Inställningsåtkomst.

Arbetsordning

- Steg 1** Tryck på **Program** .
- Steg 2** Välj **Admin-inställningar**.
- Steg 3** Välj **Nätverksinställning** eller **Säkerhetsinställning**.
- Steg 4** Ange ditt användar-ID och lösenord (om det behövs) och klicka på **Logga in**.
- 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 stänga en meny, trycker du på **Avsluta** eller på bakåtpilen .
-

Använda ett telefonlösenord


Du kan använda ett lösenord till telefonen. Då kan inga ändringar göras av de administrativa alternativen på telefonen utan att ange lösenord på skärmen Administratörsinställningar på telefonen.

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 telefon

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

- Använd pilarna på navigeringsknappsatsen för att markera det fält som du vill redigera och tryck sedan på **Välj** på navigeringsknappsatsen 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 pilknappen  om du gör fel. Denna funktionsknapp raderar tecknet till vänster om markören.
- Tryck på **Avbryt** innan du trycker på **Spara** för att ignorera eventuella ändringar som du har gjort.

- Om du vill ange en IP-adress, anger du värden i fyra segment som redan är uppdelade åt dig. När du har angett siffrorna längst till vänster före den första punkten, använder du högerpilen för att flytta till nästa segment. Punkten efter siffrorna längst till vänster infogas automatiskt.
- 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.

Relaterade ämnen

[Grundläggande återställning](#), på sidan 263

[Använda ett telefonlösenord](#), på sidan 50

Aktivera det trådlösa nätverket på telefonen

Kontrollera att din telefon har stöd för trådlös kommunikation innan du konfigurerar ett trådlöst nätverk. Cisco IP-telefon 8861 och 8865 har stöd för implementering av trådlöst nätverk. Cisco IP-telefon 8865NR har inte stöd för trådlöst nätverk.

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

Om du har aktiverat Wi-Fi-anslutningen för röst och använder EAP-FAST- eller PEAP-säkerhetsläge, behöver Wi-Fi-nätverket autentiseras med programmet för WLAN-inloggning. WEP, PSK och öppna säkerhetslägen autentiserar i Wi-Fi-nätverket.

En fast och säker roamingmetod rekommenderas för Wi-Fi-användare.



OBS! Telefonens PC-port är inaktiverad när wifi är aktiverat på din telefon.

Fullständig konfigurationsinformation finns i *Driftsättningsguide för Cisco IP-telefon 8800 trådlöst nätverk* på den här platsen:

<http://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 8800 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 **Program** .
- Steg 2** Gå till **Admin.inställningar > Nätverksinställning > Wi-Fi-klientinställning > Nätverksnamn**. Du kan se en lista över tillgänglig trådlös åtkomst som du kan ansluta till.
- Steg 3** Aktivera det trådlösa nätverket.
-

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 den trådlösa Cisco IP-telefonen.



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:
- Välj **Enhet > Telefon**.
 - Leta reda på telefonen.
 - Välj inställningen **Aktiverad** för Wi-Fi-parametern i avsnittet Produktspecifik konfigurationslayout.
 - Markera kryssrutan **Åsidosätt allmänna inställningar**.
- Steg 2** Så här aktiverar du trådlöst nätverk för en grupp av telefoner:
- Välj **Enhet > Enhetsinställningar > Allmän telefonprofil**.
 - 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.
- Markera kryssrutan **Åsidosätt allmänna inställningar**.
 - Associera telefonerna med den allmänna telefonprofilen i **Enhet > Telefon**.
- Steg 3** Så här aktiverar du trådlöst nätverk för alla WLAN-kompatibla telefoner i nätverket:
- Välj **System > Företagstelefonkonfiguration**.
 - 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! Telefonens PC-port är inaktiverad när wifi är aktiverat på din telefon.



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-telefon 8800-seriens implementeringsguide 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>.

Fältet **Kan ändras av användaren** i den trådlösa LAN-profilen styr användarens möjlighet att konfigurera säkerhetslägen på telefonen. När en användare inte kan ändra vissa fält visas de fälten i grått.

Innan du börjar

Konfigurera det trådlösa nätverket från Cisco Unified Communications Manager.

Arbetsordning

- Steg 1** Tryck **Program** .
- Steg 2** Välj **Admininställningar > Nätverksinställning > Wi-Fi-klientinställning**.
- Steg 3** Ställ in den trådlösa konfigurationen enligt beskrivningen i tabellen nedan.

Tabell 19. Menyalternativ för Wi-Fi-klientinställning

Alternativ	Beskrivning	Om du vill ändra
Nätverksnamn	Anger Service Set Identifier, en unik identifierare för att komma åt trådlösa åtkomstpunkter. Visar en lista över tillgängliga trådlösa åtkomstpunkter.	Se Konfigurera nätverksinställning 58 .

Alternativ	Beskrivning	Om du vill ändra
Endast IPv4-inställning	<p>På undermenyn för konfiguration av IPv4-installation kan du göra följande:</p> <ul style="list-style-type: none"> • 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. <p>Mer information om fälten för IPv4-adress finns i IPv4-fält, på sidan 60.</p>	Bläddra till IPv4-inställning och tryck
Endast IPv6-inställning	<p>På undermenyn för konfiguration av IPv6-installation kan du göra följande:</p> <ul style="list-style-type: none"> • 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. <p>Mer information om fälten för IPv6-adress finns i IPv6-fält, på sidan 61.</p>	Bläddra till IPv6-inställning och tryck
MAC-adress	Unik MAC-adress (Media Access Control) för telefonen.	Endast visning. Kan inte konfigurera.
Domännamn	Namn på DNS-domän där telefonen befinner sig.	Se Konfigurera nätverksinställningar, 58 .

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.



OBS! Telefoner med mobilåtkomst och Remote Access via Expressway som används för att ansluta till Cisco Unified Communications Manager kan inte ha en Wi-Fi-profil. Eftersom du inte har samma SSID, autentiseringsläge och inloggningsuppgifter som användarens telefon, kan du inte konfigurera en trådlös LAN-profil för telefonen.

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.

OBS! Fältet **Åtkomstprofil för nätverk** stöds inte av Cisco IP-telefon 8861 och 8865.

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**.

Konfigurera nätverksinställningar

Arbetsordning

- Steg 1** Tryck på **Program** .
- Steg 2** Öppna menyn Nätverksinställningar genom att välja **Admininställningar > Ethernet-inställning**.
- Steg 3** Ange fälten enligt beskrivningen i [Fält för Ethernet-inställningar, på sidan 58](#).
- Steg 4** När du har angett fälten trycker du på **Använd** och **Spara**.
- Steg 5** Starta om telefonen.

Fält för Ethernet-inställningar

Menyn Nätverksinställning innehåller fält och undermenyer för IPv4 och IPv6. Om du vill ändra vissa fält måste du först inaktivera DHCP.

När en VPN-anslutning upprättas skrivs Ethernet-datafälten över.

Tabell 20. Menyalternativ för Ethernet-inställning

Post	Typ	Beskrivning
Ställa in IPv4	Meny	Se avsnittet med IPv4-fält. Det här alternativet visas bara när telefonen är konfigurerad i endast IPv4- eller IPv6-läget.
Ställa in IPv6	Meny	Se avsnittet med IPv6-fält.
MAC-adress	Sträng	Unik MAC-adress (Media Access Control) för telefonen. Endast visning. Kan inte konfigurera.
Domännamn	Sträng	Namn på DNS-domän där telefonen befinner sig. Om du vill ändra det här fältet måste du inaktivera DHCP.
Operativt VLAN-ID		Extra VLAN som är konfigurerat i en Cisco Catalyst-växel där telefonen är ansluten. Den här inställningen är tom om extra-VLAN eller administrativt VLAN är konfigurerat. Om telefonen inte har tilldelats ett extra VLAN, anger det här alternativet administrativt VLAN. Telefonen använder inte operativt VLAN från administrativt VLAN om Cisco Discovery Protocol (CDP) eller LLDP-MED (Link Level Discovery Protocol Media Endpoint Discovery) är konfigurerat. Om du vill tilldela ett VLAN-ID manuellt använder du alternativet Administrativt VLAN-ID.

Post	Typ	Beskrivning
Administrativt VLAN-ID		Extra-VLAN där telefonen är medlem. Används endast om telefonen inte tilldelas ett extra VLAN från växelvärdet.
PC VLAN		Gör att telefonen kan samverka med tredjepartsväxlar som inte stöder PC VLAN-ID måste anges innan du kan ändra det här alternativet.
Ställa in SW-port	Autoförhandla 1000 Full 100 Halv 10 Halv 10 Full	Hastighet och duplex i nätverksporten. Giltiga värden anger: <ul style="list-style-type: none"> • Autoförhandla (standard) • 1000 full: 1000-BaseT/full duplex • 100 halv: 100-BaseT/halv duplex • 100 full: 100-BaseT/full duplex • 10 halv: 10-BaseT/halv duplex • 10 full: 10-BaseT/full duplex <p>Om telefonen är ansluten till en växel konfigurerar du porten i växelns telefonen har, eller konfigurerar båda för autobalansering.</p> <p>Lås upp alternativen för nätverkskonfiguration om du vill redigera de ändrar inställningen av det här alternativet måste du ändra alternativets samma inställning.</p>
Ställa in PC-port	Autoförhandla 1000 Full 100 Halv 10 Halv 10 Full	Datorportens hastighet och duplex. Giltiga värden: <ul style="list-style-type: none"> • Autoförhandla (standard) • 1000 full: 1000-BaseT/full duplex • 100 halv: 100-BaseT/halv duplex • 100 full: 100-BaseT/full duplex • 10 halv: 10-BaseT/halv duplex • 10 full: 10-BaseT/full duplex <p>Om telefonen är ansluten till en växel konfigurerar du porten i växelns telefonen har, eller konfigurerar båda för autobalansering.</p> <p>Lås upp alternativen för nätverkskonfiguration om du vill ändra det h inställningen måste du ändra alternativet SW-portkonfiguration till sa</p> <p>Om du vill konfigurera inställningen för flera telefoner samtidigt, aktiv i fönstret Företagstelefonkonfiguration (System > Företagstelefonko</p> <p>Om portarna är konfigurerade för fjärrportkonfiguration i Cisco Unified Administration kan data inte ändras i telefonen.</p>

IPv4-fält

Tabell 21. Menyalternativ för IPv4-inställning

Post	Beskrivning
DHCP aktiverad	<p>Anger om telefonen har DHCP aktiverat eller inaktiverat.</p> <p>Om DHCP har aktiverats tilldelar DHCP-servern telefonen en IP-adress. Om DHCP är inaktiverat måste administratören manuellt tilldela en IP-adress till telefonen.</p> <p>Mer information finns i Konfigurera telefonen för användning av DHCP, på sidan 62 och Konfigurera telefonen så att DHCP inte används, på sidan 63.</p>
IP-adress	<p>IP-adress till telefonen.</p> <p>Om du tilldelar en IP-adress med det här alternativet måste du också tilldela en nätmask och standardrouter. Se alternativen nätmask och standardrouter i den här tabellen.</p>
Nätmask	Nätmask som används av telefonen.
Standardrouter	Standardrouter som används av telefonen.
DNS-server 1 DNS-server 2 DNS-server 3	Primär DNS-server (DNS-server 1) och valfria DNS-reservservrar (DNS-server 2 och 3) som telefonen använder.
Alt. TFTP	Anger om telefonen använder en alternativ TFTP-server.
TFTP-server 1	<p>Primär TFTP-server som telefonen använder. Om du inte använder DHCP i nätverket och du vill ändra den här servern, måste du använda alternativet TFTP-server 1.</p> <p>Om du anger På för Alternativ TFTP måste du ange ett annat värde än noll för TFTP-server 1.</p> <p>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.</p> <p>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:</p> <ol style="list-style-type: none"> 1. Alla manuellt tilldelade IPv4 TFTP-servrar 2. Alla manuellt tilldelade IPv6-servrar 3. DHCP-tilldelade TFTP-servrar 4. DHCPv6-tilldelade TFTP-servrar <p>OBS! Information om CTL- och ITL-filer finns i <i>Säkerhetshandboken till Cisco Unified Communications Manager</i>.</p>

Post	Beskrivning
TFTP-server 2	<p>Valfri TFTP-reservserver som telefonen använder om den primära TFTP-servern inte är tillgänglig.</p> <p>Om varken den primära TFTP-servern eller reserv-TFTP-servern finns i CTL- eller ITL-filen på telefonen, måste du låsa upp en av filerna innan du kan spara ändringar i alternativet för TFTP-server 2. I så fall tas en av filerna bort 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.</p> <p>Om du glömmet att låsa upp CTL- eller ITL-filen kan du ändra TFTP-server 2-adressen i endera fil och sedan radera dem genom att trycka på Radera på menyn Säkerhetskfiguration. En ny CTL- eller ITL-fil hämtas från den nya adressen för TFTP-server 2.</p> <p>När telefonen söker efter TFTP-servern prioriteras 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:</p> <ol style="list-style-type: none"> 1. Alla manuellt tilldelade IPv4 TFTP-servrar 2. Alla manuellt tilldelade IPv6-servrar 3. DHCP-tilldelade TFTP-servrar 4. DHCPv6-tilldelade TFTP-servrar <p>OBS! Information om CTL- och ITL-filer finns i Säkerhetshandboken till Cisco Unified Communications Manager.</p>
BOOTP-server	Anger om telefonen tog emot IP-adressen från en BOOTP-server i stället för från en DHCP-server.
DHCP-adressen släppt	Släpper de IP-adresser som tilldelats av DHCP. Det här fältet kan redigeras om DHCP har aktiverats. Om du vill ta bort telefonen från VLAN och släppa IP-adressen för omtilldelning, anger du alternativet med Ja och trycker på Använd.

IPv6-fält

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-distribution finns i [IPv6-driftsättningsguide för Cisco Collaboration Systems version 12.0](#).

Ställ in IPv6 från en av följande menyer:

- Om Wi-Fi är inaktiverat: **Ethernet-inställning > IPv6-inställning**

- Om Wi-Fi är aktiverat: **Wi-Fi-klientinställning > IPv6-inställning**

Använd knappsatsen för att ange eller redigera en IPv6-adress. Om du vill ange kolon (:) trycker du på asterisk (*) på knappsatsen. Om du vill ange hexadecimala tecken a, b och c, trycker du på 2 på knappsatsen, bläddrar till önskat tecken och trycker på **RETUR**. Om du vill ange hexadecimala tecken d, e och f, trycker du på 3 på knappsatsen, bläddrar till önskat tecken och trycker på **RETUR**.

I följande tabell beskrivs IPv6-relaterad information som finns på IPv6-menyn.


Tabell 22. Menyalternativ för IPv6-inställning

Post	Standardvärde	Beskrivning
DHCPv6 aktiverad	Ja	Anger den metod som telefonen använder för att hämta IP-adresser. När DHCPv6 aktiveras hämtar telefonen IP-adresser från den IPv6-aktiverade routern. Och om DHCPv6 är inaktiverad hämtar telefonen IP-adresser från tillståndslös (från SLAAC) IPv6-adresser.
IPv6-adress	::	Visar aktuell endast IPv6-adress på telefonen. En giltig IPv6-adress är 128 bitar i längd. <ul style="list-style-type: none"> • Åtta grupper med hexadecimala siffror • Komprimerat format som döljer flera nollor Om IP-adressen har tilldelats med det här formatet, kan du använda :: för att skriva ut de återstående siffrorna.
IPv6-prefixlängd	0	Visar aktuell prefixlängd för undernätet. Prefixlängd för subnätet är ett decimaltal mellan 1 och 64.
IPv6-standardrouter	::	Visar standardrouter som används av telefonen.
IPv6 DNS-server 1	::	Visar den primära DNSv6-server som används av telefonen.
IPv6 DNS-server 2	::	Visar den sekundära DNSv6-server som används av telefonen. DNSv6-server.
Alternativ IPv6 TFTP	Nej	Tillåter användaren att möjliggöra användning av alternativ IPv6 TFTP-server.
IPv6 TFTP-server 1	::	Visar den primära IPv6 TFTP-server som används av telefonen. TFTP-server.
IPv6 TFTP-server 2	::	(Valfritt) Visar den sekundära IPv6 TFTP-server som används av telefonen. Tillåter användaren att ställa in en ny sekundär IPv6 TFTP-server.
IPv6-adressen släppt	Nej	Tillåter användaren att släppa IPv6-relaterad information.

Konfigurera telefonen för användning av DHCP

Om du vill aktivera DHCP och tillåta att DHCP-servern automatiskt tilldelar IP-adress till en Cisco IP-telefon och dirigerar telefonen till en TFTP-server gör du så här:


Arbetsordning

- Steg 1** Tryck på **programknappen** .
- Steg 2** Välj **Admin.inställningar > Nätverksinställning > Ethernet-inställning > IPv4-inställning**.
- Steg 3** Om du vill aktivera DHCP ställer du in DHCP-aktiverad med **Ja**. DHCP är aktiverat som standard.
- Steg 4** Om du vill använda en alternativ TFTP-server ställer du in Alternativ TFTP-server med **Ja** och anger IP-adressen för TFTP-servern.
- OBS!** Kontakta nätverksadministratören för att fastställa om du måste tilldela en alternativ TFTP-server istället för att använda den TFTP-server som tilldelas i DHCP.
- Steg 5** Tryck på **Använd**.
-

Konfigurera telefonen så att DHCP inte används

När du inte använder DHCP måste du konfigurera IP-adressen, subnätmask, TFTP-server och standardrouter lokalt på telefonen.

Arbetsordning

- Steg 1** Tryck på **programknappen** .
- Steg 2** Välj **Admin.inställningar > Nätverksinställning > Ethernet-inställning > IPv4-inställning**.
- Steg 3** Inaktivera DHCP och ange en IP-adress manuellt:
- Ange DHCP-aktiverat till **Nej**.
 - Ange den statiska IP-adressen för telefonen.
 - Ange subnätmasken.
 - Ange IP-adresser för standardroutern.
 - Ställ in alternativ TFTP-Server till **Ja** och ange IP-adressen för TFTP-server 1.
- Steg 4** Tryck på **Använd**.
-

Laddningsserver

Laddningsservern används för att optimera installationstiden vid uppgradering av telefonens fasta programvara och avlasta WAN genom att lagra bilder lokalt för att eliminera behovet att korsa WAN-länken för varje telefons uppgradering.

Du kan ställa in laddningsservern till en annan IP-adress för TFTP-servern eller ange det namn (annat än TFTP Server 1 eller TFTP Server 2) som telefonens inbyggda programvara kan hämtas från för uppgraderingar av telefonen. När alternativet Laddningsserver är inställt kontakter telefonen angiven server för uppgradering av den fasta programvaran.



OBS! Med alternativet Laddningsserver kan du ange en alternativ TFTP-server som gäller endast för telefonuppdateringar. Telefonen fortsätter att använda TFTP Server 1 eller TFTP Server 2 för att få konfigurationsfiler. Alternativet Laddningsserver tillhandahåller inte hantering av processen och filerna, till exempel filöverföring, komprimering eller borttagning.

Laddningsservern konfigureras i fönstret Företagstelefonkonfiguration. Öppna Cisco Unified Communications Manager Administration och välj **Enhet > Telefon > Företagstelefonkonfiguration**.

Verifiering vid telefonstart

När Cisco IP-telefon har ström börjar telefonens startdiagnostikprocess som innehåller följande steg.

1. Funktions- och sessionsknapparna blinkar gult och sedan grönt i turordning under de olika stegen vid uppstart då telefonen kontrollerar maskinvaran.
2. Huvudskärmen visar `Registreras i Cisco Unified Communications Manager`.

När telefonen har slutfört alla steg har den startat korrekt och knappen **Välj** lyser tills användaren har valt den.

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. Tjänsterna består av XML-program och Cisco-signerade Java-midletar som möjliggör visningen av interaktivt innehåll med text och bilder på telefonen. IP-telefonen hanterar varje tjänst som ett separat program. Exempel på tjänster inbegriper lokala filmvisningar, börskurser och väderleksrapporter.

Innan en användare kan få tillgång till alla tjänster:

- Använd alltid Administration av Cisco Unified Communications Manager om du vill 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** I Administration av Cisco Unified Communications Manager, välj **Enhet > Enhetsinställningar > Telefontjänster**

- Steg 2** Kontrollera att dina användare kan få åtkomst till Cisco Unified Communications självbetjäningsportal där de kan välja och prenumerera på konfigurerade tjänster.
- I [Hantering av självbetjäningsportalen, på sidan 79](#) finns det en sammanfattning av den information som du måste lämna till slutanvändarna.

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager, på sidan xv](#)

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.

Om du ändrar en gammal telefon med den fasta programvaran SCCP till en modell i Cisco IP-telefon i 8800-serien konfigureras den nya telefonen för läget sessionslinje.

Om den gamla telefonen har en knappexpansionsmodul konfigurerad kopierar Unified CM samtidigt informationen om expansionsmodulen till den nya telefonen. När användaren ansluter en kompatibel knappexpansionsmodul till den nya telefonen får den nya expansionsmodulen information om den migrerade expansionsmodulen.

Om den gamla telefonen har en knappexpansionsmodul konfigurerad och den nya telefonen inte har stöd för en expansionsmodul, kopierar inte Unified CM informationen om expansionsmodulen.

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

Telefoninställningar i Cisco Unified Communications Manager

- Konfigurera Cisco IP-telefon, på sidan 67
- Fastställ telefonens MAC-adress, på sidan 70
- Telefontilläggsmetoder, på sidan 70
- Lägg till användare i Cisco Unified Communications Manager, på sidan 72
- Lägg till en användare i en slutanvändargrupp, på sidan 73
- Associera telefoner med användare , på sidan 74
- Survivable Remote Site Telephony, på sidan 74
- Enhanced Survivable Remote Site Telephony, på sidan 77
- Programmets uppringningsregler, på sidan 78

Konfigurera Cisco IP-telefon

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

Mer information om Cisco Unified Communications Manager Administration 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
- Fysiska platsen för telefonen
- Namn eller användar-ID för telefonanvändaren
- Enhetsgrupp

- Partition, samtalssöksområde och platsinformation
- Antal linjer och tillhörande katalognummer (DNS) att tilldela till telefonen
- Cisco Unified Communications Manager-användaren som ska associeras med telefonen
- Telefonanvändningsinformation som påverkar telefonknappmallen, telefonens funktioner, IP-telefon tjänster eller telefonprogram

Informationen visas en lista över konfigurationskrav för att ställa in telefoner och identifierar preliminär konfiguration som du behöver göra innan du konfigurerar enskilda telefoner, till exempel telefonknappmallar.

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

Steg 3 Anpassa telefonknappmallar (om det behövs) genom att ändra antalet linjeknappar, kortnummerknappar eller tjänst-URL-knappar. Välj **Enhet > Enhetsinställningar > Telefonknappmall** för att skapa och uppdatera mallarna.

Du kan lägga till en knapp för sekretess, alla samtal eller mobilitet för att uppfylla användarnas behov.

Mer information finns i [Mallar för telefonknappar, på sidan 189](#).

Steg 4 Definiera Enhetsgrupper. Välj **System > Enhetsgrupp**.

Enhetsgrupper definierar gemensamma egenskaper för enheter, till exempel region, datum-/tidgrupp, funktionsknappmall och MLPP-information.

Steg 5 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 6 Definiera ett söksområde för samtal. Gå till Cisco Unified Communications Manager Administration och klicka på **Samtalsroutning > Kontrollklass > Söksområde för samtal**.

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

Steg 7 Konfigurera en säkerhetsprofil för enhetstyp och protokoll. Välj **System > Säkerhet > Telefonsäkerhetsprofil**.

Steg 8 Lägg till och konfigurera telefonen genom att fylla i de obligatoriska fälten i fönstret Telefonkonfiguration. En asterisk (*) bredvid fältnamnet anger ett obligatoriskt fält, till exempel MAC-adress och enhetspool.

I det här steget läggs enheten till med standardinställningarna i Cisco Unified Communications Manager-databasen.

Mer information om produktspecifika konfigurationsfält finns i "???" Knappjälpe i fönstret Telefonkonfiguration.

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.

Steg 9 Lägg till och konfigurera katalognummer (linjer) på telefonen genom att fylla i de obligatoriska fälten i fönstret Katalognummerkonfiguration. En asterisk (*) bredvid fältnamnet anger ett obligatoriskt fält, till exempel katalognummer och närvarogrupp.

Det här steget lägger till primära och sekundära katalognummer och funktioner som är kopplade till katalognummer i telefonen.

OBS! Om du inte konfigurerar det primära katalognumret visas meddelandet `Odelad` på telefonen.

- Steg 10** Konfigurera kortnummerknappar och tilldela kortnummer.
Användare kan ändra inställningarna för kortnummer på sina telefoner via självbetjäningssportalen för Cisco Unified Communications.
- Steg 11** Konfigurera Cisco Unified IP-telefon-tjänster och tilldela tjänster (valfritt) för att ange IP-telefon-tjänster.
Användare kan lägga till eller ändra tjänster på sina telefoner via självbetjäningssportalen för Cisco Unified Communications.
- OBS!** Användare kan prenumerera på IP-telefon-tjänsten endast om kryssrutan Företagsprenumeration är avmarkerad när IP-telefon-tjänsten konfigureras första gången i Cisco Unified Communications Manager Administration.
- OBS!** Vissa standardtjänster från Cisco klassificeras som företagsprenumerationer och då kan användaren inte lägga till dem via självbetjäningssportalen. Sådana tjänster finns på telefonen som standard, och de kan bara tas bort från telefonen om du inaktiverar dem i Cisco Unified Communications Manager Administration.
- Steg 12** Tilldela tjänster till programmerbara knappar (valfritt) som ger åtkomst till en IP-telefon-tjänst eller webbadress.
- Steg 13** Lägg till användarinformation genom att konfigurera obligatoriska fält. En asterisk (*) bredvid fältnamnet visar ett obligatoriskt fält, till exempel användar-ID och efternamn. Med det här steget lägger du till användarinformation i den globala katalogen för Cisco Unified Communications Manager.
- OBS!** Tilldela ett lösenord (för självbetjäningssportalen) och PIN-kod (för Cisco Extension Mobility och den personliga katalogen).
- OBS!** Om ditt företag använder en LDAP-katalog för att lagra information om användare kan du installera och konfigurera Cisco Unified Communications för användning av din befintliga LDAP-katalog.
- 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.
- Steg 14** Associera en användare till en användargrupp. I det här steget tilldelas 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. Du måste till exempel lägga till användare i standardanvändargruppen i CCM så att användare har åtkomst till självbetjäningssportan i Cisco Unified Communications Manager.
- Steg 15** Associera en användare med en telefon (valfritt). I det här steget ges användare kontroll över sin telefon med vidarekoppling av samtal eller tillägg av kortnummer eller tjänster.
Vissa telefoner, till exempel i konferensrum, har inte någon associerad användare.
- Steg 16** Om fönstret Slut användarkonfiguration inte visas kan du välja **Användarhantering > Slut användare** för att utföra vissa slutgiltiga åtgärder i konfigurationen. Använd sökfälten och **Sök** för att hitta användaren (till exempel Johan Svensson). Klicka på användar-ID:t för att öppna fönstret Slut användarkonfiguration för användaren.
- Steg 17** Gå till området Katalognummerassociationer på skärmen och ställ in den primära anslutningen i listrutan.
- Steg 18** Gå till området Mobilitetsinformation och markera rutan Aktivera mobilitet.

- Steg 19** I området med behörighetsinformation kan du använda knapparna Användargrupp 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.
- Steg 20** Visa alla konfigurerade användargrupper genom att välja **Användarhantering > Användargrupp**.
- Steg 21** Gå till området Extension Mobility och markera kryssrutan Aktivera Extension Mobility Cross Cluster om användaren tillåts använda tjänsten Extension Mobility Cross Cluster.
- Steg 22** Välj **Spara**.

Relaterade ämnen


[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

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:

- Tryck på **Program**  på telefonen, välj **Telefoninformation** 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.

- Lägg till telefoner individuellt med hjälp av Cisco Unified Communications Manager Administration
- Lägg 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 70](#).

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

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 xv

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 xv

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 73.
- 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 xv

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. Slut användare 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-slut användargruppen 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 användargrupskonfigurationen 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 Slut användare i Cisco Unified Communications Manager.

Arbetsordning

- Steg 1** Utgå från Cisco Unified Communications Manager Administration och välj **Användarhantering > Slut användare**.
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

Survivable Remote Site Telephony (SRST) säkerställer att de grundläggande telefonfunktionerna är tillgängliga om WAN-anslutningen 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.

Mer information om inbyggd programvara som stöds och Survivable Remote Site Telephony finns på sidan *Cisco Unified Survivable Remote Site Telephony Compatibility Information* på Cisco.com (<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html>).

Följande tabell beskriver tillgängliga funktioner under felväxlingen.

Tabell 23. Stöd för SRST-funktioner

Funktion	Stöds	Anteckningar
Nytt samtal	Ja	
Avsluta samtal	Ja	
Ring igen	Ja	
Svara	Ja	
Parkera	Ja	
Återuppta	Ja	
Konferenssamtal	Ja	
Konferens till aktiva samtal (delta)	Nej	Den programstyrda knappen för aktiva samtal visas inte.
Konferenslista	Nej	
Överföring	Ja	
Överföring till aktiva samtal (direktöverföring)	Nej	
Autosvar	Ja	
Samtal väntar	Ja	
Samtals-ID	Ja	
Ljudsignal för meddelande som väntar	Ja	
Programmerbar linjeknapp för alla samtal	Ja	
Programmerbar linjeknapp för att svara	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.

Funktion	Stöds	Anteckningar
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	
Programmerbar linjeknapp för IRL-tjänst	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.
BrytIn	Nej	Den programstyrda knappen Bryt in visas inte.
Förbättrad indikation för meddelande väntar	Nej	Indikator för antalet meddelanden visas inte på telefonskärmen. Endast ikonerna för Meddelande väntar visas.
Dirigerad parkering av samtal	Nej	Den programstyrda knappen visas inte.
Lampfältet för Upptagen	Delvis	BLF-funktionsknappen fungerar som kortnummerknappar.
Återställning från förfrågan	Nej	Samtal förblir parkerade på obestämd tid.
Fjärrparkering	Nej	Samtal visas som lokalt parkerade samtal.
Meet me	Nej	Den programstyrda knappen för Meet Me visas inte.
Hämta	Nej	Den programstyrda knappen kräver ingen åtgärd.
Hämta grupp	Nej	Den programstyrda knappen kräver ingen åtgärd.

Funktion	Stöds	Anteckningar
Hämta annan	Nej	Den programstyrda knappen kräver ingen åtgärd.
Hotsamtals-ID	Nej	Den programstyrda knappen kräver ingen åtgärd.
QRT	Nej	Den programstyrda knappen kräver ingen åtgärd.
Svarsgrupp	Nej	Den programstyrda knappen kräver ingen åtgärd.
Snabbtelefon	Nej	Den programstyrda knappen kräver ingen åtgärd.
Mobilitet	Nej	Den programstyrda knappen kräver ingen åtgärd.
Funktionen Privat	Nej	Den programstyrda knappen kräver ingen åtgärd.
Ring igen	Nej	Den programstyrda knappen för att ringa tillbaka visas inte.
Video	Ja	Videokonferens stöds inte.
Video	Ja	Videokonferens stöds inte.
Delad linje	Nej	
ÖF-kortnummer	Ja	

Enhanced Survivable Remote Site Telephony

Förbättrad E-SRST (Survivable Remote Site Telephony) säkerställer att det finns ytterligare funktioner tillgängliga om WAN-anslutningen bryts. Förutom de funktioner som stöds av SRST (Survivable Remote Site Telephony) har E-SRST stöd för följande:

- Delad linje
- Fältet för upptagetlampa (BLF)
- Videosamtal

Mer information om inbyggd programvara som stöds och Survivable Remote Site Telephony finns på sidan *Cisco Unified Survivable Remote Site Telephony Compatibility Information* på Cisco.com (<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html>).

Programmets uppringningsregler

Programmets uppringningsregler används för att omvandla nummer för delade mobilkontakter till uppringningsbara nätverksnummer. Programmets uppringningsregler gäller inte när användaren slår ett nummer manuellt eller om numret redigeras innan användaren ringer.

Programmets uppringningsregler anges i Cisco Unified Communications Manager.

Mer information om uppringningsregler finns i *Systemkonfigurationshandbok för Cisco Unified Communications Manager*, i kapitlet ”Konfigurera uppringningsregler”.

Konfigurera programmets uppringningsregler

Arbetsordning

- Steg 1** I Cisco Unified Communications Manager Administration, gå till **vidarekoppling av samtal > uppringningsregler > programmets uppringningsregler**.
- Steg 2** Välj **Lägg till ny** för att skapa en ny uppringningsregel för programmet eller välj en befintlig uppringningsregel som du kan redigera.
- Steg 3** Fyll i följande fält:
- **Namn** Det här fältet består av ett unikt namn för uppringningsregeln som kan innehålla upp till 20 alfanumeriska tecken och en kombination av blanksteg, punkter (.), bindestreck (-) och understreck (_).
 - **Beskrivning** Det här fältet utgör en kort beskrivning som du anger för uppringningsregeln.
 - **Numret börjar med** Det här fältet utgör de första siffrorna i de katalognummer som du vill använda för programmets uppringningsregel.
 - **Antal siffror** Det här obligatoriska fältet utgör de första siffrorna i de katalognummer som du vill använda för programmets uppringningsregel.
 - **Totalt antal siffror som ska tas bort** Det här obligatoriska fältet består av antalet siffror som du vill att Cisco Unified Communications Manager ska ta bort från katalognummer som avser den här uppringningsregeln.
 - **Prefix med mönster** Det här obligatoriska fältet utgör mönstret som läggs till de katalognummer som gäller för programmets uppringningsregel.
 - **Prioritet för programmets uppringningsregel** Det här fältet visas när du anger information för Prefix med mönster. I fältet kan du ange prioritetsordningen för programmets uppringningsregler.
- Steg 4** Starta om Cisco Unified Communications Manager.
-



KAPITEL 6

Hantering av självbetjäningsportalen

- [Översikt över självbetjäningsportalen, på sidan 79](#)
- [Konfigurera användaråtkomst till självbetjäningsportalen, på sidan 79](#)
- [Anpassa visningen av självbetjäningsportalen, på sidan 80](#)

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 användare 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 värdet där webbservern finns installerad och `portnumber` är portnumret på den värdet.
- 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 xv

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 självbetjäningssportalen

De flesta alternativ visas i självbetjäningssportalen. 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 självbetjäningssportalsidor på din webbplats.

Arbetsordning

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



DEL III

Cisco IP-telefon – administration

- [Säkerhet i Cisco IP-telefon, på sidan 83](#)
- [Anpassning av Cisco IP-telefon, på sidan 111](#)
- [Telefonfunktioner och inställning, på sidan 117](#)
- [Företagskatalog och den personliga katalogen, på sidan 205](#)



KAPITEL 7

Säkerhet i Cisco IP-telefon

- Säkerhetsförbättringar för telefonens nätverk, på sidan 83
- Säkerhetsfunktioner som stöds, på sidan 84

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>).

- *Säkerhetsöversikt för Cisco IP-telefon 7800- och 8800-serien* (<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.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>)



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 medieströmmmanipulering.

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.

Cisco IP-telefon i 8800-serien uppfyller FIPS. För att fungera korrekt kräver FIPS-läget en nyckelstorlek på 2048 bitar eller mer. Om certifikatet inte är 2048 bitar eller mer kan telefonen inte registreras i Cisco Unified Communications Manager och -telefonen misslyckas med registreringen. Cert-nyckelstorleken är inte FIPS-kompatibel visas på telefonen.

Om telefonen har en LSC, måste du uppdatera LSC-nyckelstorleken till 2048 bitar eller mer innan du aktiverar FIPS.

Följande tabell ger en översikt över de säkerhetsfunktioner som telefonerna stöder. Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Visa aktuella säkerhetsinställningar på en telefon, inklusive säkerhetsläge, listan över betrodda och 802.1X-autentisering genom att trycka på **Program**  och välja **Admin.inställningar > Säkerhetsinställning**.

Tabell 24. Översikt över säkerhetsfunktioner

Funktion	Beskrivning
Bildautentisering	Signerade binära filer (med tillägget .sbn) förhindrar att firmware-avbilden manipuleras innan den läses in på en telefon. Manipulering av bilden orsakar att en telefon inte godkänns i autentiseringsprocessen och avvisar den nya bilden.
Bildkryptering	Krypterade binära filer (med tillägget .sebn) förhindrar att firmware-avbilden manipuleras innan den läses in på en telefon. Manipulering av bilden orsakar att en telefon inte godkänns i autentiseringsprocessen och avvisar den nya bilden.
Installation av kundens arbetsplatscertifikat	Varje Cisco IP-telefon kräver ett unikt certifikat för enhetsverifiering. Telefoner har ett fabriksinstallerat certifikat (MIC), men för extra säkerhet kan du gå till Cisco Unified Communications Manager Administration och göra en certifikatinstallation genom att använda CAPF (Certificate Authority Proxy Function). Eller så kan du installera ett LSC-certifikat (Locally Significant Certificate) från säkerhetskonnfigurationsmenyn i telefonen.
Enhetsautentisering	Skер mellan Cisco Unified Communications Manager-servern och telefonen när en enhet accepterar certifikatet för den andra enheten. Fastställer om en säker anslutning mellan telefonen och en Cisco Unified Communications Manager inträffar och skapar en säker signaleringssökväg om det behövs mellan dessa enheter med hjälp av TLS-protokollet. Cisco Unified Communications Manager registrerar endast telefoner som kan autentiseras.
Filautentisering	Validerar digitalt signerade filer som telefonen hämtar. Telefonen validerar signaturen för att se till att filmanipulering inte har inträffat efter att filen skapades. Filer som inte godkänns vid autentisering skrivs inte till Flash-minnet i telefonen. Telefonen avvisar sådana filer utan vidare bearbetning.

Funktion	Beskrivning
Kryptering	Kryptering förhindrar att känslig information visas när filen är på väg till telefonen. Telefonen validerar dessutom signaturen för att se till att filmanipulering inte har inträffat efter att filen skapades. Filer som inte godkänns vid autentisering skrivs inte till Flash-minnet i telefonen. Telefonen avvisar sådana filer utan vidare bearbetning.
Signaleringsautentisering	Använder TLS-protokollet för att validera att ingen manipulering skett till signaleringspaket under sändning.
Fabriksinstallerade certifikat	Varje Cisco IP-telefon innehåller ett unikt fabriksinstallerat certifikat (MIC) som används för enhetsautentisering. MIC ger ett permanent unikt identitetsbevis för telefonen och gör det möjligt för Cisco Unified Communications Manager att autentisera telefonen.
Mediakryptering	Använder SRTP för att säkerställa att mediaströmmarna mellan enheter som stöds är säkra och att endast den avsedda enheten tar emot och läser data. Här skapas även ett par primärt medianyckelpar för enheterna som levereras till enheterna och skyddas under transporten.
CAPF (Certificate Authority Proxy funktion)	Implementerar delar av certifikatgenereringsförloppet som är för processkrävande för telefonen och samverkar med telefonen vid nyckelgenereringen och certifikatinstallationen. CAPF kan konfigureras för att begära certifikat från kundspecifika certifikatutfärdare till telefonen eller konfigureras för att generera certifikat lokalt.
Säkerhetsprofil	Anger om telefonen är osäker, autentiserad, krypterad eller skyddad. Övriga poster i den här tabellen beskriver säkerhetsfunktioner.
Krypterade konfigurationsfiler	Låter du säkerställa integriteten i telefonens konfigurationsfiler.
Valfri webbserver inaktiverar en telefon	Av säkerhetsskäl kan du förhindra åtkomst till webbsidor för en telefon (som visar olika driftstatistik för telefonen) och självbetjäningssportalen.
Telefonhärdning	Ytterligare säkerhetsalternativ, som du styr från Cisco Unified Communications Manager Administration: <ul style="list-style-type: none"> • Inaktivera PC-porten • Inaktivera GARP (Gratuitous ARP) • Inaktivera åtkomst till PC-röst-VLAN • Inaktivera åtkomst till inställningsmenyer, eller ge begränsad åtkomst som ger åtkomst till meny Inställningar och sparar endast volymändringar • Inaktivera åtkomst till webbsidor för en telefon • Inaktivera port för Bluetooth-tillbehör • Begränsa TLS-chiffer
802.1X-autentisering	Cisco IP-telefon kan använda 802.1X-autentisering för att begära och få tillgång till nätverket. Mer information finns i 802.1X-autentisering, på sidan 108 .
Säker SIP-växling för SRST	När du har konfigurerat en SRST-referens (Survivable Remote Site Telephony) för säkerhet och sedan återställer de beroende enheterna i Cisco Unified Communications Manager Administration lägger TFTP-servern till SRST-certifikatet i telefonens cnf.xml-fil och skickar filen till telefonen. En säker telefon använder sedan en TLS-anslutning för att interagera med den SRST-aktiverade routern.

Funktion	Beskrivning
Signaleringskryptering	Säkerställer att alla SIP-signalingsmeddelanden som skickas mellan enheten och Cisco Unified Communications Manager-servern är krypterade.
Uppdateringslarm för lista över betrodda adresser	När listan över betrodda adresser uppdateras på telefonen, får Cisco Unified Communications Manager ett larm som indikerar genomförd eller misslyckad uppdatering. Mer information finns i följande tabell.
AES 256-kryptering	<p>Om du är ansluten till Cisco Unified Communications Manager Release 10.5 (2) och senare har telefonerna stöd för AES 256-kryptering för TLS och SIP för signalering och mediakryptering. Då kan telefoner initiera och få stöd för TLS 1.2-anslutningar med AES-256-baserade chiffer som uppfyller SHA-2-standarder (Secure Hash Algorithm) och är FIPS-kompatibla. Chiffren omfattar:</p> <ul style="list-style-type: none"> • För TLS-anslutningar: <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • För SRTP: <ul style="list-style-type: none"> • AEAD_AES_256_GCM • AEAD_AES_128_GCM <p>Mer information finns i dokumentationen till Cisco Unified Communications Manager.</p>
ECDSA (Elliptic Curve Digital Signature Algorithm)-certifikat	Lade till ECDSA-certifikat i version 11.0 för Cisco Unified Communications Manager enligt CC-certifieringen (Common Criteria). Det här påverkar alla Voice Operating System (VOS)-produkter från version CUCM 11.5 och senare.

Följande tabell innehåller meddelanden och innebörd av uppdateringslarm för listan över betrodda adresser. Mer information finns i dokumentationen till Cisco Unified Communications Manager.

Tabell 25. Meddelanden för uppdateringslarm för lista över betrodda adresser

Kod och meddelande	Beskrivning
1 – TL_SUCCESS	Mottagen ny CTL och/eller ITL
2 - CTL_INITIAL_SUCCESS	Mottagen ny CTL, ingen befintlig TL
3 - ITL_INITIAL_SUCCESS	Mottagen ny ITL, ingen befintlig TL
4 – ITL_INITIAL_SUCCESS	Mottagen ny CTL och ITL, ingen befintlig TL
5 – TL_FAILED_OLD_CTL	Uppdatering av ny CTL misslyckades, men har tidigare TL
6 – TL_FAILED_NO_TL	Uppdatering av ny TL misslyckades och har ingen tidigare TL
7 – TL_FAILED	Allmänt fel
8 – TL_FAILED_OLD_ITL	Uppdatering av ny ITL misslyckades, men har tidigare TL
9 – TL_FAILED_OLD_TL	Uppdatering av ny TL misslyckades, men har tidigare TL

Menyn Säkerhetsinställning ger information om olika säkerhetsinställningar. Menyn ger även åtkomst till menyn Lista över betrodda adresser och anger om CTL- eller ITL-filen är installerad på telefonen.

I följande tabell beskrivs menyalternativen för Säkerhetsinställning.

Tabell 26. Menyn Säkerhetsinställning

Alternativ	Beskrivning	Om du vill ändra
Säkerhetsläge	Visar säkerhetsläge som är inställt för telefonen.	Utgå från Cisco Unified Communications Manager Administration och välj Enhet > Telefon . Inställningen visas under Protokollspecifik information i fönstret Telefonkonfiguration.
LSC	Anger om ett LSC-certifikat som används för säkerhetsfunktioner finns installerat i telefonen (Ja) eller inte (Nej).	Mer information om hur du hanterar LSC för telefonen finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.
Lista med pålitliga adresser	Listan över betrodda adresser har undermenyer för CTL- och ITL-filer samt signerade konfigurationsfiler. På undermenyn CTL-filen visas innehållet i CTL-filen. På undermenyn ITL-filen visas innehållet i ITL-filen. På menyn Lista över betrodda adresser visas också följande information: <ul style="list-style-type: none"> • CTL-signatur: SHA1-hash i CTL-filen • Unified CM/TFTP-Server: namnet på den Cisco Unified Communications Manager och TFTP-server som telefonen använder. Visar en certifikatikon om ett certifikat har installerats på servern. • CAPF-server: namnet på CAPF-servern som telefonen använder. Visar en certifikatikon om ett certifikat har installerats på servern. • SRST-router: IP-adressen för betrodd SRST-router som telefonen kan använda. Visar en certifikatikon om ett certifikat har installerats på servern. 	Mer information finns i Konfigurera ett LSC-certifikat, på sidan 89 .
802.1X-autentisering	Här kan du aktivera 802.1X-autentisering för telefonen.	Se 802.1X-autentisering, på sidan 108 .

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

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 säkerhetskfiguration 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 trycker du på **Program** .
- 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 säkerhetskfigurationsmenyn 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.
-

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! Säkra samtal stöds bara för anslutningar mellan endast två telefoner. Vissa funktioner, som konferenssamtal och delade linjer, är inte tillgängliga när säkert samtal har konfigurerats.


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 27. 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 Uppfyll säkerhetsnivå, samtal avvisa
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 (spärerton) 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. Både PEAP-MSCHAPV2 och PEAP-GTC autentiseringsmetoder stöds.

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 28. Autentiserings- och krypteringsscheman

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

Ställa in autentiseringsläget

Om du vill välja autentiseringsläget för den här profilen, gör du så här:

Arbetsordning

Steg 1 Välj den nätverksprofil som du vill konfigurera.

Steg 2 Välj autentiseringsläget.

OBS! Beroende på vad du har valt, måste du konfigurera ytterligare alternativ för säkerhet vid trådlöst eller trådlös kryptering. Mer information finns i [WLAN-säkerhet, på sidan 93](#).

Steg 3 Klicka på **Spara** för att genomföra ändringen.

Inloggningsuppgifter för säkerhet vid trådlöst

När ditt nätverk använder EAP-FAST och PEAP vid användarautentisering, måste du konfigurera både användarnamn och lösenord om det behövs på RADIUS (Remote Authentication Dial-in User Service) och på telefonen.



OBS! Om du använder domäner i nätverket måste du ange användarnamn med namnet på domänen i formatet *domän\användarnamn*.

Följande åtgärder kan leda till att det befintliga Wi-Fi-lösenordet försvinner:

- Om du anger ett ogiltigt användar-id eller lösenord.
- Om du installerar en ogiltig eller utgången rotcertifikatutfärdare och EAP-typen är inställd på PEAP-MSCHAPV2 eller PEAP GTC.
- Om du inaktiverar EAP-typen på RADIUS-servern som används av telefonen innan du ändrar en telefon till den nya EAP-typen.

Om du vill ändra EAP-typer gör du följande i den angivna ordningen:

- Aktivera de nya EAP-typerna på RADIUS.
- Ändra EAP-typen på en telefon till den nya EAP-typen.

Behåll den aktuella EAP-typen som har konfigurerats i telefonen tills den nya EAP-typen har aktiverats på RADIUS-servern. När den nya EP-typen har aktiverats på RADIUS-servern kan du ändra telefonens EAP-typ. När alla telefoner har ändrats till den nya EAP-typen kan du inaktivera den tidigare EAP-typen om du vill.

Ställa in användarnamn och lösenord

Om du vill ange eller ändra användarnamn och lösenord för nätverksprofilen, måste du använda samma användarnamn och samma lösenord som har konfigurerats i RADIUS-servern. Den maximala längden för användarnamn och lösenord är 64 tecken.

Om du vill ställa in användarnamnet och lösenordet i inloggningsuppgifter för säkerhet vid trådlöst gör du så här:

Arbetsordning

- Steg 1** Välj nätverksprofil.
 - Steg 2** Ange användarnamnet för nätverk för den här profilen i fältet Användarnamn.
 - Steg 3** Ange lösenordet för nätverk för den här profilen i fältet Lösenord.
 - Steg 4** Klicka på **Spara** för att genomföra ändringen.
-

Förinställd delad nyckel

Följande avsnitt hjälper dig när du ställer in i förväg delade nycklar.

Format för förinställd delad nyckel

Cisco IP-telefon har stöd för ASCII- och hexadecimala format. Du måste använda något av dessa format när du konfigurerar en förinställd delad WPA-nyckel:

Hexadecimal

För hexadecimala nycklar, anger du 64 hexadecimala tecken (0-9 och A-F). till exempel
AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C

ASCII

För ASCII-nycklar anger du en teckensträng med 0-9, A-Z (versaler och gemener), inklusive symboler och som har en längd på 8 till 63 tecken. till exempel GREG12356789ZXYW

Ställa in PSK

Om du vill konfigurera en PSK i området Inloggningsuppgifter för trådlöst gör du så här:

Arbetsordning

- Steg 1** Välj den nätverksprofil som använder i förväg delad WPA-nyckel eller WPA2-nyckel.
 - Steg 2** Ange lämplig nyckel i området för nyckeltypen.
 - Steg 3** Ange en ASCII-sträng eller hexadecimala siffror i fältet Lösenkod/i förväg delad nyckel.
 - Steg 4** Klicka på **Spara** för att genomföra ändringen.
-

Trådlös kryptering

Om det trådlösa nätverket använder WEP-kryptering och du ställer in autentiseringsläget som Öppet + WEP, måste du ange en ASCII- eller hexadecimal WEP-nyckel.

WEP-knapparna för telefonen måste matcha de WEP-nycklar som tilldelats åtkomstpunkten. Cisco IP-telefon och Cisco Aironets-åtkomstpunkter stöder både 40-bitars och 128-bitars krypteringsnycklar.

WEP-nyckelformat

Du måste använda något av dessa format när du konfigurerar en WEP-nyckel:

Hexadecimal

Använd någon av följande nyckelstorlekar för hexadecimala nycklar:

40-bitars

Du anger en 10-siffrig krypteringssträng som använder hexadecimala tecken (0-9 och A-F), till exempel ABCD123456.

128-bitars

Du anger en 26-siffrig krypteringssträng som använder hexadecimala tecken (0-9 och A-F), till exempel AB123456789CD01234567890EF.

ASCII

För ASCII-nycklar anger du en teckensträng som använder 0-9, A-Z (versaler och gemener) och alla symboler, i en av följande nyckelstorlekar:

40-bitars

Du anger en 5-teckensträng, till exempel GREG5.

128-bitars

Du anger en 13-teckensträng, till exempel GREGSSECRET13.

Ställa in WEP-nycklar

Följ dessa steg när du vill konfigurera WEP-nycklar.

Arbetsordning

-
- Steg 1** Välj den nätverksprofil som använder Öppna + WEP eller Delade + WEP.
 - Steg 2** Ange lämplig nyckel i området för nyckeltypen.
 - Steg 3** Välj en av dessa teckenstränglängder i området Nyckelstorlek:
 - 40
 - 128
 - Steg 4** Ange lämplig nyckelsträngen baserat på vald nyckeltyp och nyckelstorlek i fältet Krypteringsnyckel. Se [WEP-nyckelformat, på sidan 98](#).
 - Steg 5** Klicka på **Spara** för att genomföra ändringen.
-

Exportera CA-certifikat från ACS med Microsoft Certificate Services

Exportera rotcertifikatutfärdarcertifikatet från ACS-servern. Ytterligare information finns i dokumentationen för certifikatutfärdaren eller RADIUS.

Fabriksinstallerade certifikat

Cisco har inkluderat ett fabriksinstallerat certifikat (MIC) i telefonen vid tillverkningen.

Vid EAP-TLS-autentiseringen måste ACS-servern kontrollera betrodd relation till telefonen och telefonen måste kontrollera betrodd relation till ACS-servern.

För att kontrollera MIC måste rotcertifikatet och CA-certifikatet exporteras från en Cisco IP-telefon och installerats på Cisco ACS-servern. Dessa båda certifikat ingår i den betrodda certifikatkedjan som används för att kontrollera MIC via Cisco ACS-servern.

För att kontrollera Cisco ACS-certifikatet måste eventuellt betrodd underordnat certifikat och rotcertifikatet (skapas från CA) på Cisco ACS-servern exporteras och installeras på telefonen. Dessa certifikat ingår i den betrodda certifikatkedjan som används för att kontrollera betrodda certifikat från ACS-servern.

Användarinstallerat certifikat

Om du vill använda ett användarinstallerat certifikat genereras ett CSR (Certificate Signing Request) och skickas till certifikatutfärdaren (CA) för godkännande. Ett certifikat kan också genereras av certifikatutfärdaren utan CSR.

Vid EAP-TLS-autentiseringen måste ACS-servern kontrollera betrodd relation till telefonen och telefonen måste kontrollera betrodd relation till ACS-servern.

Om du vill kontrollera att användarinstallerat certifikat är äkta måste du installera ett underordnat betrodd certifikat (om det finns) och rotcertifikatet från certifikatutfärdaren som godkände användarcertifikatet på Cisco ACS-servern. Dessa certifikat ingår i den betrodda certifikatkedjan som används för att kontrollera att användarinstallerat certifikat är tillförlitligt.

För att kontrollera Cisco ACS-certifikatet måste du exportera eventuellt betrodd underordnat certifikat och rotcertifikatet (skapas från CA) på Cisco ACS-servern så att exporterade certifikat installeras på telefonen. Dessa certifikat ingår i den betrodda certifikatkedjan som används för att kontrollera betrodda certifikat från ACS-servern.

Installera certifikat för EAP-TLS-autentisering

Gör följande om du vill installera autentiseringscertifikat för EAP-TLS.

Arbetsordning

-
- Steg 1** Ställ in Cisco Unified Communications Manager datum och tid på telefonen via webbsidan för telefonen.
- Steg 2** Om du använder fabriksinstallerat certifikat (MIC):
- Exportera rot-CA-certifikatet och tillverknings-CA-certifikatet från telefonens webbsida.
 - Installera certifikaten på Cisco ACS-servern från Internet Explorer och redigera listan med betrodda anslutningar.
 - Importera rot-CA till telefonen.
- Mer information finns i:
- [Exportera och installera certifikat på ACS, på sidan 100](#)
 - [Exportera CA-certifikat från ISE med Microsoft Certificate Services, på sidan 101](#)
- Steg 3** Använd ACS-konfigurationsverktyget för att ställa in användarkontot.

Mer information finns i:

- [Ställa in ACS-användarkonto och installera certifikat, på sidan 102](#)
- *Användarhandbok för Cisco säker ACS för Windows*(<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>)

Ställa in datum och klockslag

EAP-TLS använder certifikatbaserad autentisering som kräver att den interna klockan i Cisco IP-telefon ställs in korrekt. Datum och tid på telefonen kan ändras när den är registrerad i Cisco Unified Communications Manager.



OBS! Om ett nytt servercertifikat för autentisering begärs och den lokala tiden är efter GMT (Greenwich Mean Time), kan autentiseringens certifikatvalidering misslyckas. Cisco rekommenderar att du ställer in lokalt datum och tid före GMT.

Följ dessa steg om du vill ställa in telefonen med rätt lokalt datum och tid.

Arbetsordning

- Steg 1** Välj **Datum och tid** i navigeringspanelen till vänster.
- Steg 2** Om inställningen i fältet Telefonens aktuella datum och tid skiljer sig från fältet Lokalt datum och tid, klickar du på **Ställ in telefonen på lokalt datum och tid**.
- Steg 3** Klicka på **Telefonstart** och klicka sedan på **OK**.

Exportera och installera certifikat på ACS

Om du vill använda MIC exporterar du rotcertifikatet och CA-certifikatet och installerar dem på Cisco ACS-servern.

Så här exporterar du rotcertifikatet och CA-certifikatet till ACS-servern:

Arbetsordning

- Steg 1** Välj **Certifikat** på telefonwebbsidan.
- Steg 2** Klicka på **Exportera** bredvid rotcertifikatet.
- Steg 3** Spara certifikatet och kopierar det till ACS-servern.
- Steg 4** Upprepa steg 1 och 2 för CA-certifikatet.
- Steg 5** Ange sökvägen till varje certifikat på systemkonfigurationssidan för ACS-servern och installera certifikaten.

OBS! Mer information om hur du använder ACS-konfigurationsverktyget finns i direkthjälpen för ACS eller i *Användarhandbok för Cisco säker ACS för Windows*(<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>).

- Steg 6** Använd sidan Redigera lista över betrodda certifikat (CTL) för att lägga till certifikat som är betrodda av ACS.
-

Exportmetoder för ACS-certifikat

Beroende på vilken typ av certifikat du exporterar från ACS, använder du någon av följande metoder:

- Om du vill exportera CA-certifikatet från ACS-servern som kvitterade det användarinstallerade certifikatet eller ACS-certifikatet, se [Exportera CA-certifikat från ISE med Microsoft Certificate Services, på sidan 101](#).
- Om du vill exportera CA-certifikatet från ACS-servern som använder ett självsignerat certifikat, se [Exportera CA-certifikat från ACS via Internet Explorer, på sidan 101](#).

Exportera CA-certifikat från ISE med Microsoft Certificate Services

Använd den här metoden för att exportera CA-certifikatet från ISE-servern som kvitterade det användarinstallerade certifikatet eller ISE-certifikatet.

Följ dessa steg om du vill exportera CA-certifikatet via webbsidan Microsoft Certificate Services.

Arbetsordning

- Steg 1** Välj **Hämta ett CA-certifikat, certifikatkedja eller CRL** på webbsidan Microsoft Certificate Services.
- Steg 2** På nästa sida markerar du det aktuella CA-certifikatet i textrutan, väljer DER under kodningsmetod och klickar på **Hämta CA-certifikat**.
- Steg 3** Spara CA-certifikatet.
-

Exportera CA-certifikat från ACS via Internet Explorer

Använd den här metoden om du vill exportera CA-certifikatet från ACS-servern som använder ett självsignerat certifikat.

Följ dessa steg om du vill exportera certifikat från ACS-servern via Internet Explorer.

Arbetsordning

- Steg 1** I Internet Explorer väljer du **Verktyg > Internet-alternativ** och klickar sedan på fliken Innehåll.
- Steg 2** Under certifikat klickar du på **Certifikat**. Klicka sedan på fliken Betrodda rotcertifikatutfärdare.
- Steg 3** Markera rotcertifikatet och klicka på **Exportera**. Guiden Exportera certifikat öppnas.
- Steg 4** Klicka på **Nästa**.
- Steg 5** I nästa fönster väljer du **DER-kodad binär X.509 (.CER)** och klickar på **Nästa**.
- Steg 6** Ange ett namn för certifikatet och klicka på **Nästa**.
- Steg 7** Spara CA-certifikatet som ska installeras på telefonen.
-

Begära och importera användarinstallerat certifikat

Följ dessa steg om du vill begära och installera certifikat på telefonen.

Arbetsordning

-
- Steg 1** Välj nätverksprofilen med EAP-TLS på webbsidan för telefonen och välj Användarinstallerat i fältet för EAP-TLS-certifikat.
- Steg 2** Klicka på **Certifikat**.
På sidan Installation av användarcertifikat måste fältet Vanligt namn matcha användarnamnet i ACS-servern.
- OBS!** Du kan redigera fältet Vanligt namn om du vill. Se till att det matchar användarnamnet i ACS-servern. Se [Ställa in ACS-användarkonto och installera certifikat, på sidan 102](#).
- Steg 3** Ange informationen som du vill ska visas på certifikatet och klicka på **Skicka** för att generera CSR (Certificate Signing Request).
-

Installera rotcertifikat för autentiseringsservern

Följ dessa steg om du vill installera rotcertifikat för autentiseringsservern på telefonen.

Arbetsordning

-
- Steg 1** Exportera rotcertifikatet för autentiseringsservern från ACS. Se [Exportmetoder för ACS-certifikat, på sidan 101](#).
- Steg 2** Öppna telefonwebbsidan och välj **Certifikat**.
- Steg 3** Klicka på **Importera** bredvid rotcertifikatet för autentiseringsservern.
- Steg 4** Starta om telefonen.
-

Ställa in ACS-användarkonto och installera certifikat

Följ dessa steg om du vill ställa in namnet på användarkontot och installera MIC-rotcertifikatet för telefonen på ACS.



-
- OBS!** Mer information om hur du använder ACS-konfigurationsverktyget finns i direkthjälpen för ACS eller i *Användarhandbok för Cisco säker ACS för Windows*.
-

Arbetsordning

-
- Steg 1** Skapa ett användarkonto för telefonen på sidan för användarinställningar i ACS-konfigurationsverktyget, om det inte redan har konfigurerats.
Användarnamnet innehåller vanligtvis telefonens MAC-adress i slutet. Det krävs inget lösenord för EAP-TLS.

OBS! Kontrollera att användarnamnet matchar fältet Vanligt namn på sidan Installation av användarcertifikat. Se [Begära och importera användarinstallerat certifikat, på sidan 102](#).

Steg 2 Aktivera följande fält i avsnittet EAP-TLS på sidan Systemkonfiguration:

- **Tillåt EAP-TLS**
- **CN-jämförelse av certifikat**

Steg 3 Lägg till rotcertifikatet och CA-certifikatet i ACS-servern på sidan Inställningar för certifikatutfärdare.

Steg 4 Aktivera både rotcertifikatet och CA-certifikatet i listan över betrodda certifikat för ACS.

PEAP-inställning

Skyddat PEAP (Extensible Authentication Protocol) använder offentliga nyckelcertifikat på serversidan för att autentisera klienter genom att skapa en krypterad SSL/TLS-tunnel mellan klienten och autentiseringsservern.

Cisco IP-telefon 8865 har stöd för endast ett servercertifikat som kan installeras via SCEP eller manuellt, men inte båda metoderna. Telefonen stöder inte TFTP-metoden för installation av certifikat.



OBS! Valideringen i autentiseringsservern kan aktiveras genom att importera certifikatet för autentiseringsservern.

Innan du börjar

Innan du konfigurerar PEAP-autentisering för telefonen ska du se till att de här förutsättningarna för Cisco säker ACS är uppfyllda:

- ACS-rotcertifikatet måste vara installerat.
- Ett certifikat kan också installeras för att aktivera Server-validering för PEAP. Men om ett servercertifikat installeras aktiveras servervalidering.
- Inställningen Tillåt EAP-MSCHAPv2 måste vara aktiverad.
- Användarnamn och lösenord måste vara konfigurerade.
- Du kan använda den lokala ACS-databasen eller en extern databas (till exempel Windows eller LDAP) för autentisering av lösenord.

Aktivera PEAP-autentisering

Arbetsordning

Steg 1 Välj PEAP som autentiseringsläge på webbsidan för telefonkonfigurationen.

Steg 2 Ange användarnamn och lösenord.

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, nätverkskonfiguration, loggar och statistisk information.

Relaterade ämnen

[Webbsidan för Cisco IP-telefon](#), på sidan 226

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**.
- Tryck på **Program**  på telefonen, välj **Telefoninformation** och bläddra sedan till IPv4-adressfältet.

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 Leta reda på fältet Användarinstallerat och klicka på **Installera**.

Steg 3 Bläddra till certifikatet på datorn.

Steg 4 Ange certifikatets extraheringslösenord i fältet **Extraheringslösenord**.

Steg 5 Klicka på **Överför**.

Steg 6 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 servers 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-telefon och Cisco Catalyst-växlar använder traditionellt Ciscos CDP-protokoll för att identifiera varandra och fastställa parametrar som VLAN-tilldelning och interna strömbehov. CDP identifierar inte lokalt anslutna arbetsstationer. Cisco IP-telefon har en EAPOL-överföringsmekanism. Denna mekanism medger att en arbetsstation som är ansluten till Cisco IP-telefon kan överföra EAPOL-meddelanden till 802.1X-autentiseraren på LAN. Överföringsmekanismen säkerställer att IP-telefonen inte agerar som LAN-växel för autentisering av en dataändpunkt innan åtkomsten till nätverket.

Cisco IP-telefon har också en EAPOL-utloggningmekanism via proxy. Om den lokalt anslutna datorn kopplas bort från IP-telefonen kan LAN-växeln inte tolka att den fysiska länken brutits eftersom länken mellan LAN-växeln och IP-telefonen bibehålls. För att undvika att äventyra nätverksintegriteten sänder IP-telefonen ett EAPOL-utloggningssmeddelande till växeln från datorn nedströms, vilket utlöser att LAN-växeln börjar rensa autentiseringsposten för datorn nedströms.

Stödet för 802.1X-autentisering kräver flera komponenter:

- Cisco IP-telefon: Telefonen initierar begäran om att få tillgång till nätverket. Cisco IP-telefon 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 ACS-server (eller annan autentiseringsserver från tredje part): Autentiseringsservern och telefonen måste båda konfigureras med delad hemlighet som autentiserar telefonen.
- 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 PC-porten: 802.1X-standarden använder inte VLAN och föreslår därför att en enda enhet ska autentiseras för en specifik växelport. Men vissa växlar (inklusive Cisco Catalyst-växlar) stödjer multidomänautentisering. Växelkonfigurationen avgör om du kan ansluta en dator till PC-porten på telefonen.
 - Aktiverat: Om du använder en växel som stöder multidomänautentisering, kan du aktivera PC-porten och ansluta en dator till den. I det här fallet har Cisco IP-telefon stöd för EAPOL-proxyutloggning för att övervaka autentiseringsutväxlingen mellan växeln och en ansluten dator. Mer information om stöd för IEEE 802.1X i Cisco Catalyst-växlar finns i Cisco Catalyst-växelkonfigurationshandböcker på: http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
 - Inaktiverat: Om växeln inte stöder flera 802.1X-kompatibla enheter i samma port, bör du inaktivera PC-porten när 802.1X-autentisering har aktiverats. Om du inte inaktiverar denna port och därefter försöka att fästa en dator till det, förnekar omkopplaren nätverksåtkomst till både telefonen och datorn.
- 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 multidomänaутentisering kan du fortsätta att använda röst-VLAN.
- Inaktiverat: Om växeln inte stöder multidomänaутentisering inaktiverar du röst-VLAN och överväg sedan att tilldela porten till det inbyggda VLAN-nätet.

Åtkomst till 802.1X-autentisering

Du kan visa 802.1X-autentiseringsinställningarna på följande sätt:

Arbetsordning

-
- Steg 1** Tryck på **programknappen** .
- Steg 2** Välj **Admin.inställningar > Säkerhetsinställning > 802.1X-autentisering**.
- Steg 3** Konfigurera alternativen enligt [Alternativ för 802.1X-autentisering, på sidan 109](#).
- Steg 4** Om du vill avsluta menyn trycker du på **Avsluta**.
-

Alternativ för 802.1X-autentisering


I följande tabell beskrivs alternativen för 802.1X-autentisering.

Tabell 29. 802.1X-autentiseringsinställningar

Alternativ	Beskrivning	Om du vill ändra
Enhetsautentisering	Anger om 802.1X-autentisering är aktiverad: <ul style="list-style-type: none"> • Aktiverat: Telefonen använder 802.1X-autentisering för att begära åtkomst till nätverket. • Inaktiverat: Standardinställningen. Telefonen använder CDP för att få åtkomst till VLAN och nätverk. 	Se Ställa in fältet för autentisering på sidan 110 .
Transaktionsstatus	Status: Visar status på 802.1X-autentisering: <ul style="list-style-type: none"> • Frånkopplad: Anger att 802.1X-autentisering inte är konfigurerad på telefonen. • Autentiserad: Anger att telefonen är autentiserad. • Under förfrågan: Anger att autentiseringsprocessen pågår. Protokoll: Visar den EAP-metod som används för 802.1X-autentisering (kan vara EAP-FAST eller EAP-TLS).	Endast visning. Kan inte konfigurera.

Ställa in fältet för autentisering av enhet

Arbetsordning

- Steg 1** Tryck på **programknappen** .
- Steg 2** Välj **Admin.inställningar > Säkerhetsinställning > 802.1X-autentisering**
- Steg 3** Ställ in alternativet Enhetsautentisering:
- Ja
 - Nej
- Steg 4** Tryck på **Använd**.
-



KAPITEL 8

Anpassning av Cisco IP-telefon

- Anpassade telefonringsignaler, på sidan 111
- Anpassade bakgrundsbilder, på sidan 111
- Konfigurera bredbandskodning, på sidan 113
- Konfigurera viloläge, på sidan 113
- Anpassa kopplingstonen, på sidan 114

Anpassade telefonringsignaler

Telefonen levereras med tre ringsignaler som implementerats i maskinvaran: Sunshine, Chirp och Chirp1.

Cisco Unified Communications Manager ger också en standarduppsättning av ytterligare telefoner ringer ljud som genomförs i mjukvaran som pulskodmodulering (PCM) filer. PCM-filer, tillsammans med en XML-fil (som heter Ringlist-wb.xml) 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 använder Ringlist-wb.xml som filnamn kommer telefonen inte att tillämpa ändringarna.

Mer information finns i kapitlet ”Anpassade ringsignaler och bakgrunder” i [Konfigurationshandbok för funktioner i Cisco Unified Communications Manager](#) för Cisco Unified Communications Manager version 12.0 (1) eller senare.

Anpassade bakgrundsbilder

Du kan anpassa en Cisco IP-telefon med bakgrundsbild eller bakgrund. Anpassade bakgrunder är ett vanligt sätt att visa företagets logotyp eller bild, och många organisationer använder bakgrunder för att få sina telefoner att synas.

Från version 12.7 (1) den fasta programvaran kan du anpassa bakgrunder på både telefoner och moduler för nycklexpansion. Men du behöver en bild för en telefon och en bild för modulen expansion.

Telefonen analyserar bakgrundens färg och ändrar färg på teckensnitt och ikoner så att de är läsbara. Om din bakgrund är mörk ändrar telefonen teckensnitt och ikoner till vitt. Om bakgrunden är ljus visas teckensnitt och ikoner som svarta på telefonen.

Det är bäst att välja en enkel bild, exempelvis en solid färg eller ett mönster för bakgrunden. Undvik bilder med hög kontrast.

Du lägger till anpassade bakgrunder på ett av följande två sätt:

- Med hjälp av listfilen
- Med hjälp av en allmän telefonprofil

Om du vill att användaren ska kunna välja din bild bland olika bakgrunder som finns tillgängliga på telefonen ska du modifiera listfilen. Om du i stället vill skicka filen till telefonen skapar eller modifierar du en befintlig allmän telefonprofil.

Oavsett hur du gör ska du tänka på följande:

- Bilderna måste vara i PNG-format och bildens hela storlek måste vara inom följande mått:
 - Miniaturbilder – 139 pixlar (bredd) x 109 pixlar (höjd).
 - Cisco IP-telefon i 8800-serien – 800 pixlar x 480 pixlar
 - Cisco IP-telefon 8851 och 8861 modul för nyckelexpansion med dubbel LCD-skärm – 320 x 480 pixlar
 - Cisco IP-telefon 8865 modul för nyckelexpansion med dubbel LCD-skärm – 320 x 480 pixlar
 - Cisco IP-telefon 8800 modul för nyckelexpansion med en LCD-skärm – 272 x 480 pixlar
- Ladda upp bilderna, miniaturbilderna och listfilen till din TFTP-server. Katalogen är:
 - Cisco IP-telefon i 8800-serien – Desktops/800x480x24
 - Cisco IP-telefon 8851 och 8861 modul för nyckelexpansion med dubbel LCD-skärm – Desktops/320x480x24
 - Cisco IP-telefon 8865 modul för nyckelexpansion med dubbel LCD-skärm – Desktops/320x480x24
 - Cisco IP-telefon 8800 modul för nyckelexpansion med en LCD-skärm – Desktops/272x480x24

Starta om TFTP-servern när överföringen är klar.

- Om du inte vill att användaren ska kunna välja sin egen bakgrund inaktiverar du **Aktivera användaråtkomst till telefonens bakgrundsbild**. Spara och använd telefonprofilen. Starta om telefonerna så att ändringarna börjar gälla.



OBS! Du kan använda telefonens bakgrundsbilder i bulk med den **allmänna telefonprofilen**. Men masskonfigurationen kräver att du inaktiverar **Aktivera användaråtkomst till telefonens bakgrundsbild**. Mer information om masskonfiguration av bakgrundsbilder finns i kapitlet ”Konfigurera den allmänna telefonprofilen” i [Bästa metoder för anpassade bakgrunder Cisco IP-telefon i 8800-serien](#).)

Mer information om att anpassa bakgrunder finns i följande dokumentation:

- [Bästa metoder för anpassade bakgrunder Cisco IP-telefon i 8800-serien](#)).

- ”Anpassade ringsignaler och bakgrunder” i [Konfigurationshandbok för funktioner i Cisco Unified Communications Manager](#) för Cisco Unified Communications Manager version 12.0 (1) eller senare.
- Se kapitlet ”Inställningar” i *Cisco IP-telefon 8800-seriens användarhandbok*.

Konfigurera bredbandskodning

Som standard är G.722-kodek aktiverat för Cisco IP-telefon. Om Cisco Unified Communications Manager är konfigurerat för att använda G.722 och om den sista slutpunkten stöder G.722 kopplas samtalet med G.722-kodek i stället för G.711.

Denna situation uppstår oavsett om användaren har aktiverat ett bredbandsheadset eller en bredbandslur, men om antingen headsetet eller telefonen är aktiverad kan användaren märka en större ljudkänslighet under samtalet. Ökad känslighet innebär förbättrad klart ljud, men också att långväga ändpunkter kan höra mer bakgrundsljud: brus som prasslande papper eller konversationer i närheten. Även utan bredbandsheadset eller lur kan vissa användare tycka att den extra känsligheten i G.722 är störande. Andra användare kanske föredrar den extra känsligheten i G.722.

Serviceparametern för Annonsera G.722- och iSAC-kodek fastställer om det finns bredbandsstöd för alla enheter som registreras med denna Cisco Unified Communications Manager-server eller en viss telefon, beroende på fönstret Cisco Unified Communications Manager Administration där parametern är konfigurerad.

Arbetsordning

Steg 1

Så här konfigurerar du bredbands stöd för alla enheter:

- Öppna Cisco Unified Communications Manager Administration och välj **System > Företagsparametrar**.
- Ställa in fältet Annonsera G.722- och iSAC-kodek.

Standardvärdet för denna företagsparameter är **Sant**, vilket innebär att alla Cisco IP-telefon-modeller som registreras i Cisco Unified Communications Manager annonserar G.722 till Cisco Unified Communications Manager. Om varje ändpunkt i samtalsförsöket har stöd för G.722 i de inställda alternativen väljer Cisco Unified Communications Manager den här kodeken för samtalet när det är möjligt.

Steg 2

Så här konfigurerar du bredbandsstöd för en specifik enhet:

- Utgå från Cisco Unified Communications Manager Administration och välj **Enhet > Telefon**.
- Ange parametern Annonsera G.722- och iSAC-kodek i området Produktspecifik konfiguration.

Standardvärdet för den här produktspecifika parametern är att använda det värde som företagsparametern anger. Om du vill åsidosätta värdet på en telefon väljer du **Aktiverat** eller **Inaktiverat**.

Konfigurera viloläge

Du kan ange en vilolägeskärm (endast text och textfilstorleken bör inte överstiga 1 MB) som visas på telefonens skärm. Vilolägeskärmen är en XML-tjänst som telefonen anropar när telefonen är i viloläge (ej i bruk) under en bestämd tid och ingen funktionsmeny är öppen.

Detaljerade instruktioner om hur du skapar och visar vilolägeskärmen finns i avsnittet om att *Skapa URL-grafik för viloläge på Cisco IP-telefon* som öppnas med denna URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml

Följande information finns dessutom i dokumentationen till din utgåva av Cisco Unified Communications Manager:

- Ange URL till XML-tjänsten för vilolägeskärmen:
 - För en enskild telefon: Vilolägesfältet i telefonkonfigurationsfönstret i Cisco Unified Communications Manager Administration.
 - För flera telefoner samtidigt: URL-vilolägesfältet i företagsparameterkonfigurationsfönstret eller vilolägesfältet i BAT-verktyget för massadministration
- Specificera tidslängd utan användning av telefonen innan XML-tjänsten för vilolägeskärm anropas:
 - För en enskild telefon: Vilolägestimerfältet i telefonkonfigurationsfönstret i Cisco Unified Communications Manager Administration.
 - För flera telefoner samtidigt: URL-vilolägestidsfältet i företagsparameterkonfigurationsfönstret eller vilolägestimerfältet i BAT-verktyget för massadministration

Arbetsordning

- Steg 1** Utgå från Cisco Unified Communications Manager Administration och välj **Enhet > Telefon**.
 - Steg 2** Gå till vilolägesfältet och ange URL till XML-tjänsten för vilolägeskärm.
 - Steg 3** I fältet Vilolägestimer anger du tidslängd utan användning av telefonen innan XML-tjänsten för vilolägeskärm ska aktiveras.
 - Steg 4** Välj **Spara**.
-

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

Telefonfunktioner och inställning

- [Översikt över telefonens funktioner och inställningar, på sidan 117](#)
- [Stöd för Cisco IP-telefon-användare, på sidan 117](#)
- [Telefonfunktioner, på sidan 118](#)
- [Funktionsknappar och programstyrda knappar, på sidan 135](#)
- [Telefonfunktionskonfiguration, på sidan 137](#)
- [Konfigurera mall för programstyrda knappar, på sidan 187](#)
- [Mallar för telefonknappar, på sidan 189](#)
- [VPN-konfiguration, på sidan 192](#)
- [Ställa in ytterligare linjeknappar, på sidan 193](#)
- [Ställa in timer för TLS-återupptagande, på sidan 196](#)
- [Aktivera intelligenta närhetstjänster, på sidan 197](#)
- [Ställa in upplösning för videosändning, på sidan 197](#)
- [Headsethantering på äldre versioner av Cisco Unified Communications Manager, på sidan 199](#)

Översikt över telefonens funktioner och inställningar

När du har installerat Cisco IP-telefon i ditt nätverk, konfigurerat nätverksinställningar och lagt till dem i Cisco Unified Communications Manager måste du använda programmet Cisco Unified Communications Manager Administration för att konfigurera telefonifunktioner, eventuellt ändra telefonmallarna, ställa in tjänster och tilldela användare.

Du kan ändra ytterligare inställningar för Cisco IP-telefon från Cisco Unified Communications Manager Administration. Använd detta webbaserade program för att ställa upp kriterier för telefonregistrering och samtalssökutrymmen, konfigurera företagskataloger och tjänster och för att ändra telefonknappsmallar, bland annat.

Du är begränsad av antalet tillgängliga linjeknappar när du lägger till telefonfunktioner. Du kan inte lägga till flera funktioner än antalet linjeknappar på telefonen.

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

Telefonfunktioner

När du lägger till Cisco IP-telefon i Cisco Unified Communications Manager kan du lägga till funktioner för telefonerna. Följande tabell innehåller en lista över vilka telefonifunktioner. Många kan du konfigurera med hjälp av Cisco Unified Communications Manager Administration.

Mer information om att använda de flesta av dessa funktioner på telefonen finns i *Användarhandboken till Cisco IP-telefon i 8800-serien*. I [Funktionsknappar och programstyrda knappar, på sidan 135](#) finns det en lista över funktioner som kan konfigureras som programmerbara knappar och dedikerade funktionstangenter och funktionsknappar.



OBS! Cisco Unified Communications Manager Administration tillhandahåller också flera tjänsteparametrar som du kan använda för att utföra olika telefonifunktioner. Mer information om hur du öppnar och konfigurerar tjänsteparametrar finns i dokumentationen om din utgåva av Cisco Unified Communications Manager.

Mer information om funktionerna i en tjänst visas när du markerar namnet på parametern eller trycker på **hjälpknappen med frågetecknet (?)** i fönstret [Produktspecifik konfiguration](#).

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

Funktion	Beskrivning och mer information
Förkortat nummer	Låter användare snabbbringa ett telefonnummer genom att ange en tilldelad indexkod (1-199) på telefonens knappsats. OBS! Du kan använda kortnummer både när luren är på och av. Användare tilldelar indexkoder från självbetjäningsportalen.
Avisering om inkommande samtal med åtgärder	Ger olika alternativ för att styra aviseringar om inkommande samtal. Du kan aktivera eller inaktivera samtalsaviseringar. Du kan också aktivera eller inaktivera nummerpresentation. Mer information finns i Avisering om inkommande samtal med åtgärder, Produktspecifik konfiguration, på sidan 138 .

Funktion	Beskrivning och mer information
AES 256-krypteringsstöd för telefoner	Ökar säkerheten genom att stödja TLS 1.2 och nya chiffer. Mer information finns i Säkerhetsfunktioner som stöds, på sidan 84 .
Agents hälsningsfras	Låter en agent skapa och uppdatera en förinspelad hälsning som spelas upp i början av ett samtal, som ett kundsamtal, innan agenten börjar samtalet med den som ringer. Agenten kan förinspela en enda hälsning eller flera hälsningar, efter behov. Se Aktivera agenthälsning, på sidan 166 .
Samtalshämtning	Låter användare plocka upp ett samtal på en linje i sin svarsgrupp, oavsett hur samtalet kopplas till telefonen. Mer information om samtalshämtning finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.
Programmets uppringningsregler	Omvandla nummer för delade mobilkontakter till uppringningsbara nätverksnummer. Se Programmets uppringningsregler, på sidan 78 .
Assisterad dirigerad parkering av samtal	Möjliggör för användare att parkera ett samtal genom att bara trycka på en knapp med direktparkeringsfunktionen. Administratörer måste konfigurera en knapp för BLF-dirigerad parkering av samtal. När användare trycker på en ledig knapp för BLF-dirigerad parkering av samtal för ett aktivt samtal parkeras det aktiva samtalet på direktparkeringsplatsen som har associerats med knappen BLF-dirigerad parkering av samtal. Se avsnittet om assisterad parkering av dirigerat samtal i dokumentationen till din utgåva av Cisco Unified Communications Manager.
Indikator på att ljudmeddelande väntar (AMWI)	En avbruten ton från telefonluren, headsetet eller högtalartelefonen anger att en användare har ett eller flera nya röstmeddelanden på en linje. OBS! Den oregelbundna tonen är linjespecifik. Du hör det bara när du använder linjen med de väntande meddelandena.
Autosvar	Kopplar inkommande samtal automatiskt efter en ringning eller två. Autosvar fungerar med antingen högtalartelefon eller headset. Se katalognummerinformationen i dokumentationen till din utgåva av Cisco Unified Communications Manager.
Automatisk portsynkronisering	Synkroniserar portar till den lägsta hastigheten mellan portar i en telefon för att eliminera paketförluster. Se Automatisk portsynkronisering, Produktspecifik konfiguration, på sidan 138 .
Autohämta	Låter en användare hämta samtal med en enda knapptryckning för alla funktioner. Mer information om samtalshämtning finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.
BrytIn	Låter en användare bryta in i ett samtal genom att upprätta ett trevägskonferenssamtal med den inbyggda konferensbryggan i måltelefonen. Se ”BrytInKF” i tabellen.

Funktion	Beskrivning och mer information
Blockera överföring från extern till extern	Hindrar användare från att överföra ett externt samtal till ett annat externt nummer. Se avsnittet om extern samtalsöverföring i dokumentationen till din utgåva av Cisco Unified Communications Manager.
Bluetooth-multianslutning	Gör att användaren kan parkoppla flera enheter till telefonen. Användaren kan sedan ansluta en mobilenhet med Bluetooth och ett Bluetooth-headset samtidigt. Cisco IP-telefon 8851NR stöder inte Bluetooth.
Fältet för upptagetlampa (BLF)	Tillåter en användare att övervaka samtalsstatus av ett katalognummer som associerats med en kortnummerknapp på telefonen. Se närvaroinformationen i dokumentationen till din utgåva av Cisco Unified Communications Manager.
Fältet för upptagetlampa (BLF), hämta	Ger förbättringar för BLF-kortnummer. Här kan du konfigurera ett katalognummer (DN) där en användare kan övervaka inkommande samtal. När DN tar emot ett inkommande samtal varnar systemet övervakningsanvändaren, som sedan kan plocka upp samtalet. Mer information om samtalshämtning finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.
Ring igen	Ger användarna en ljud- och visuell varning på telefonen när en upptagen eller otillgänglig part blir tillgänglig. Se avsnittet om återuppringning i dokumentationen till din utgåva av Cisco Unified Communications Manager.
Begränsningar för visning av samtal	Fastställer den information som ska visas för samtals- eller anslutna linjer, beroende vilka parter som är inblandade i samtalet. Se avsnittet om routningsplaner och begränsad samtalsvisning i dokumentationen till din utgåva av Cisco Unified Communications Manager.
Vidarebefordra	Låter användare omdirigera inkommande samtal till ett annat nummer. Vidarekopplingsalternativen inkluderar vidarekoppling av alla, vidarekoppling vid upptaget, vidarekoppling vid inget svar och vidarekoppling vid ingen täckning. Se informationen om katalognummer i dokumentationen till din utgåva av Cisco Unified Communications Manager och i Anpassa visningen av självbetjäningssportalen, på sidan 80 .
Avbryt vidarekoppling av alla i slingor	Upptäcker och förhindrar vidarekoppling av alla slingor. Om en vidarekoppling av alla i slinga upptäcks ignoreras inställningen av vidarekoppling för alla och samtalen rings.
Förhindra vidarekoppling av alla i slingor	Upptäcker och förhindrar vidarekoppling av alla slingor. Om en vidarekoppling av alla i slinga upptäcks ignoreras inställningen av vidarekoppling för alla och samtalen rings.

Funktion	Beskrivning och mer information
Konfigurerbar visning av vidarekoppling	<p>Förhindrar en användare från att konfigurera en vidarekoppling av alla destinationer direkt på telefonen som skapar en vidarekoppling av alla i slinga eller vidarekoppling av alla i kedja med fler hopp än vad som tillåts i den befintliga tjänstparametern för max antal hopp i vidarekoppling.</p> <p>Se katalognummerinformationen i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Åsidosättning av destination vid vidarekoppling	<p>Gör det möjligt att åsidosätta vidarekoppling av alla (CFA) i de fall då CFA-målet kopplar ett samtal till CFA-initiatorn. Den här funktionen gör det möjligt för CFA-målet att nå CFA-initiatorn vid viktiga samtal. Åsidosättningen sker oavsett om CFA-måltelefonnumret är internt eller externt.</p> <p>Se katalognummerinformationen i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Meddelande för vidarebefordra samtal	<p>Här kan du konfigurera den information som användaren ser när du tar emot ett vidarekopplat samtal.</p> <p>Se Konfigurera meddelande om vidarekoppling av samtal, på sidan 167.</p>
Samtalshistorik för delad linje	<p>Låter dig visa aktivitet på en delad linjen i telefonens samtalshistorik. Med denna funktion kan du göra följande:</p> <ul style="list-style-type: none"> • Logga missade samtal för en delad linje • Logga alla besvarade och kopplade samtal för en delad linje
Parkera samtal	<p>Låter användare parkera (tillfälligt lagra) ett samtal och sedan hämta samtalet med en annan telefon i Cisco Unified Communications Manager.</p> <p>Du kan konfigurera fältet Dedikera en linje för samtalsparkering i panelen Produktspecifik konfigurationslayout om du vill parkera samtalet till den ursprungliga linjen eller en annan linje.</p> <p>När fältet är aktiverat fortsätter det parkerade samtalet på användarens linje och användaren kan plocka upp samtalet med den programstyrda knappen Återuppta. Användaren ser det parkerade samtalets anknyningsnummer på telefonens skärm.</p> <p>När fältet är inaktiverat överförs det parkerade samtalet till linjen för samtalsparkering. Användarens linje återgår till det inaktiva tillståndet och användaren ser anknyningen för parkerade samtal i ett popupfönster. Användaren kan plocka upp samtalet genom att ringa anknyningen.</p> <p>Se avsnittet om samtalsparkering i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Hämta samtal	<p>Låter användare vidarekoppla ett samtal som ringer på en annan telefon i sin hämtningsgrupp till sin telefon.</p> <p>Du kan konfigurera ett ljud och visuell varning för den primära linjen på telefonen. Denna varning meddelar användarna att ett samtal ringer i deras svarsgrupp.</p> <p>Mer information om samtalshämtning finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>

Funktion	Beskrivning och mer information
Samtalsinspelning	<p>Låter en handledare registrera ett pågående samtal. Användaren kan höra en varningston under samtal när samtalet spelas in.</p> <p>När ett samtal är säkrat visas säkerhetsstatusen för samtalet som en låsikon på Cisco IP-telefonen. De anslutna parterna kan också höra en varningston som indikerar samtalet är säkert och spelas in.</p> <p>OBS! Även om ett aktivt samtal övervakas eller spelas in kan användaren ta emot och koppla snabbtelefonsamtal, men om användaren kopplar ett snabbtelefonsamtal parkeras det aktiva samtalet vilket medför att inspelningen avslutas och övervakningssessionen avbryts. För att återgå till övervakningssessionen måste parten i det övervakade samtalet återuppta samtalet.</p> <p>Se information om övervakning och inspelning i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Samtal väntar	<p>Indikerar (och gör det möjligt för användare att svara på) ett inkommande samtal som ringer under ett pågående samtal. Information om inkommande samtal visas på telefonens skärm.</p> <p>Se katalognummerinformationen i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Rington för väntande samtal	<p>Ger användare av funktionen Samtal väntar ett alternativ att välja en ringsignal i stället för standardpipet.</p> <p>Alternativen är Ring och Ring en gång.</p> <p>Se katalognummerinformationen i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Samtals-ID	<p>Nummerpresentation med telefonnummer, namn eller annan beskrivande text visas på telefonens skärm.</p> <p>Se avsnittet om planer, begränsad samtalsvisning och katalognummer i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Blockering av samtals-ID	<p>Tillåter en användare att blockera sitt telefonnummer eller sin e-postadress i telefoner som har nummerpresentation.</p> <p>Se informationen om routningsplan och katalognummer i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Normalisering av uppringare	<p>Vid normalisering av uppringaren presenteras telefonsamtalet för användaren med ett telefonnummer som kan ringas upp. Alla escape-koder läggs till i numret så att användaren enkelt kan kopplas till den som ringer igen. Det uppringningsbara numret sparas i samtalshistoriken och kan sparas i den personliga adressboken.</p>
CAST för SIP	<p>Upprättar kommunikation mellan Cisco Unified Video Advantage (CUVA) och Cisco IP-telefoner för att få stöd för video på datorn, även om IP-telefonen inte har videofunktion.</p>

Funktion	Beskrivning och mer information
BrytInKf	<p>Tillåter en användare att ansluta sig till ett ickeprivat samtal på en delad telefonlinje. Med BrytInKf kan en användare läggas till i ett samtal och samtalet omvandlas till en konferens, så att användaren och andra parter kan få tillgång till konferensfunktioner. Konferenssamtalet skapas med hjälp av funktionen för konferensbrygga i Cisco Unified Communications Manager.</p> <p>Du måste aktivera både den programstyrda knappen och funktionen för konferensbrygga för BrytInKf ska fungera korrekt.</p> <p>I Firmware version 10.2 (2) och senare används funktionen BrytInKf med den programstyrda knappen Bryt in.</p> <p>Mer information finns i kapitlet ”Bryt in” i Konfigurationshandbok för funktioner i Cisco Unified Communications Manager.</p>
Ladda en mobilenhet	<p>Tillåter en användare att ladda en mobilenhet genom att ansluta den till USB-porten på Cisco IP-telefonen.</p> <p>Se <i>Användarhandbok för Cisco IP-telefon i 8800-serien</i>.</p>
Cisco Extension Mobility	<p>Ger användare åtkomst till sin konfiguration av Cisco IP-telefonen, som utseende för linjer, tjänster och kortnummer från en delad Cisco IP-telefon.</p> <p>Cisco Extension Mobility kan vara användbart för personer som arbetar från flera olika platser inom företaget eller om de delar en arbetsyta med medarbetare.</p>
Cisco Extension Mobility Cross Cluster (EMCC)	<p>Låter en användare som konfigurerats i ett kluster logga in på en Cisco IP-telefon i ett annat kluster. Användare från ett hemkluster loggar in på en Cisco IP-telefon i ett gästkluster.</p> <p>OBS! Konfigurera Cisco Extension Mobility på Cisco IP-telefoner innan du konfigurerar EMCC.</p>
Cisco IP Manager Assistant (IPMA)	<p>Hanterar samtalsroutning och innehåller andra funktioner som hjälper chefer och assistanter att hantera samtal effektivare.</p> <p>Se Konfigurera Cisco IP Manager Assistant, på sidan 182 .</p>
<p>Expansionsmodul för Cisco IP Phone 8800</p> <p>Expansionsmodul för Cisco IP Phone 8851/8861</p> <p>Expansionsmodul för Cisco IP Phone 8865</p>	<p>Ger ytterligare nycklar genom att lägga till en expansionsmodul till telefonen.</p> <p>Mer information finns i <i>Tillbehörshandboken för Cisco IP-telefon 7800- och 8800-serien för Cisco Unified Communications Manager</i>.</p>
Cisco Wireless IP Phone 8811 Support	Ger stöd för Cisco Wireless IP Phone 8811.
Stöd för Cisco IP-telefon 8851NR	Ger stöd för Cisco IP-telefon 8851NR.

Funktion	Beskrivning och mer information
Versionsintegrering med Cisco Unified Communications Manager Express (Unified CME)	<p>I Cisco Unified Communications Manager Express används en särskild tagg i den information som skickas till telefonen för att identifiera den. Med den här taggen kan telefonen tillhandahålla tjänster för användaren som växeln stöder.</p> <p>Se:</p> <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Express System Administrator Guide</i> • Interaktion med Cisco Unified Communications Manager Express, på sidan 22
Cisco Unified Video Advantage (CUVA)	<p>Låter användare ringa videosamtal med hjälp av en Cisco IP-telefon, en personlig dator och en videokamera.</p> <p>OBS! Konfigurera videofunktionsparametern i det produktspecifika konfigurationslayoutområdet i telefonkonfigurationen.</p> <p>Mer information finns i dokumentationen om Cisco Unified Video Advantage.</p>
Cisco WebDialer	Låter användare ringa från webb- och skrivbordsprogram.
Klassisk ringsignal	<p>Stöd för ringsignaler som är inbäddade i telefonens inbyggda programvara eller hämtas från Cisco Unified Communications Manager. Funktionen gör tillgängliga ringsignaler allmänna för andra Cisco IP-telefoner.</p> <p>Se Anpassade telefonringsignaler, på sidan 111 .</p>
Konferenssamtal	<p>Låter en användare tala samtidigt med flera parter genom att ringa varje deltagare individuellt. I konferensfunktionerna ingår konferens och Meet Me.</p> <p>Låter en ickeinitiator i en (tillfällig) standardkonferens lägga till eller ta bort deltagare och låter även alla konferensdeltagare koppla ihop två standardkonferenser på samma linje.</p> <p>Parametern för avancerad tillfällig konferenstjänst är inaktiverad som standard i Cisco Unified Communications Manager Administration men du kan aktivera dessa funktioner.</p> <p>OBS! Var noga med att informera användarna om dessa funktioner är aktiverade.</p>
Konfigurerbar EEE (Energy Efficient Ethernet) för PC- och växelport	<p>Tillhandahåller en metod för att styra EEE-funktioner i datorporten och växelporten genom att aktivera eller inaktivera EEE. Funktionen kontrollerar båda typerna av portar individuellt. Standardvärdet är Aktiverat.</p> <p>Se Ställa in Energy Efficient Ethernet för växel- och PC-port, på sidan 169 .</p>
Konfigurerbar teckenstorlek	<p>Låter användare öka eller minska det maximala antalet tecken som IP-telefonen visar på skärmen Samtalshistorik och Ringa samtal genom att ändra teckenstorleken.</p> <p>Ett teckensnitt som är mindre ökar det maximala antalet tecken, och ett teckensnitt som är större minskar det maximala antalet tecken.</p>
CTI-program	En CTI-målpunkt (Computer Telephony Integration) kan utse en virtuell enhet för att ta emot flera simultana samtal för programstyrd omdirigering.

Funktion	Beskrivning och mer information
Avböj alla	<p>Tillåter en användare att överföra en ringsignal, ett kopplat samtal eller ett parkerat samtal direkt till ett röstmeddelandesystem. När ett samtal avvisas blir linjen ledig för att ringa samtal eller ta emot nya samtal.</p> <p>Se information om omedelbar vidarekoppling i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Enhetsanropad inspelning	<p>Ger slutanvändarna möjligheten att spela in sina telefonsamtal via en funktionsknapp.</p> <p>Dessutom kan administratörer fortsätta att spela in telefonsamtal via CTI-användargränssnittet.</p> <p>Se information om övervakning och inspelning i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Dirigerad parkering av samtal	<p>Tillåter en användare att överföra ett pågående samtal till ett tillgängligt riktad samtalsparkeringsnummer som användaren ringer eller kortnummer. En BLF-dirigerad parkeringsknapp indikerar om ett nummer för dirigerad parkering av samtal är upptaget och ger kortnummeråtkomst till numret för dirigerad parkering av samtal.</p> <p>OBS! Om du implementerar dirigerad parkering av samtal ska du undvika att konfigurera parkeringsfunktionsknappen. Då undviker du att användare blandar ihop de två samtalsparkeringsfunktionerna.</p> <p>Se avsnittet om samtalsparkering i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Visar ikoner för batterinivå och signalstyrka	<p>Visar batterinivå och signalstyrka för mobiltelefonen på IP-telefonen när mobiltelefonen är ansluten till IP-telefonen via Bluetooth.</p> <p>Cisco IP-telefon 8851NR stöder inte Bluetooth.</p>
Olika ringsignaler	<p>Användare kan anpassa hur telefonen indikerar ett inkommande samtal och ett nytt röstmeddelande.</p> <p>Mer information om samtalshämtning finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Stör ej (DND)	<p>När Stör ej (DND) är aktiverat hörs ingen ringning när ett samtal kommer in och inga ljud eller aviseringar visas.</p> <p>Telefonens fönsterhuvud blir röd och Stör ej visas på telefonen.</p> <p>Om prioritet och förtur på flera nivåer (MLPP) har konfigurerats och användaren får ett prioriterat samtal ringer telefonen med en speciell ringsignal.</p> <p>Se Konfigurera Stör ej, på sidan 165 .</p>
Aktivera/inaktivera JAL/TAL	<p>Gör att administratören kan kontrollera funktionerna Delta över linjer (JAL) och Direktöverföring över linjer (TAL).</p> <p>Se policyn för koppling och direktöverföring, Produktspecifik konfiguration, på sidan 138.</p>

Funktion	Beskrivning och mer information
EnergyWise	<p>Aktiverar en funktion i IP-telefonen förviloläge (avstängning) och uppvakning (slås på) vid förutbestämda tidpunkter, för att ge energibesparingar.</p> <p>Se Schemalägga EnergyWise för Cisco IP-telefon, på sidan 162 .</p>
Förbättrat linjeläge	<p>Aktivera Förbättrat linjeläge för att använda knapparna på båda sidorna om telefonskärmen som linjeknappar.</p> <p>Se Ställa in ytterligare linjeknappar, på sidan 193</p>
Secure Extension Mobility Cross Cluster (EMCC)	<p>Förbättrar EMCC-funktionen genom att bevara nätverks- och säkerhetskonfigurationer på inloggningstelefonen. Då kan säkerhetsreglerna följas, bandbredden bevaras och nätfel undviks i gästklustret (VC).</p>
Kortnummer	<p>Tillåter användaren att ange ett kortnummer för att ringa ett samtal. Kortnummer kan tilldelas till telefonnummer eller hela poster i den personliga adressboken. Se ”Tjänster” i tabellen.</p> <p>Se Ändra telefonknappmallen för adressboken eller kortnummer, på sidan 191 .</p>
Hämta grupp	<p>Tillåter en användare att svara på ett samtal som ringer upp ett katalognummer i en annan grupp.</p> <p>Mer information om samtalshämtning finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Kontroll av sidoton i headset	<p>Låter en administratör ställa in sidotonsnivån för ett trådbundet headset.</p>
Återställning från förfrågan	<p>Begränsar den tid som ett samtal kan vara parkerat innan det återgår till den telefon som kopplade samtalet och varnar användaren.</p> <p>Återställda samtal skiljer sig från inkommande samtal genom en enda ringning (eller ljudsignal, beroende på den nya samtalsindikatorinställningen för linjen). Denna avisering upprepas i intervall om samtalet inte återupptas.</p> <p>Ett samtal som utlöser Återställ parkering visar också en animerad ikon i samtalsbubblan. Du kan konfigurera prioritet på samtalsfokus genom att gynna inkommande eller återställda samtal.</p>
Parkeringsstatus	<p>Aktiverar en funktion för telefoner med en delad linje så att det går att skilja mellan lokala linjer och fjärrlinjer med parkerade samtal.</p>
Parkerat/Återuppta	<p>Låter användaren flytta ett anslutet samtal från ett aktivt tillstånd till parkerat tillstånd.</p> <ul style="list-style-type: none"> • Ingen konfiguration krävs om du vill använda Musik vid parkerat samtal. Se ”Musik vid parkerat samtal” i den här tabellen för mer information. • Se ”Återställning från parkerat” i tabellen.
HTTP-hämtning	<p>Förbättrar filhämtningsprocessen i telefonen med användning av HTTP som standard. Om HTTP-hämtningen misslyckas, återgår telefonen till att använda TFTP-hämtning.</p>

Funktion	Beskrivning och mer information
Svarsgrupp	<p>Ger lastdelning för samtal till ett huvudkatalognummer. En samtalsgrupp innehåller en rad katalognummer som kan svara på inkommande samtal. Om det första katalognumret i samtalsgruppen är upptaget jagar systemet vidare i en bestämd ordning efter nästa tillgängliga katalognummer i gruppen och dirigerar samtalet till den telefonen.</p> <p>Du kan få Samtals-ID (om samtals-ID har konfigurerats), katalognummer och svarsgruppens pilotnummer visat på avisering om inkommande samtal för samtalet i svarsgrupp. Svarsgruppsnumret visas efter etiketten "Svarsgrupp".</p> <p>Se information om svarsgrupper och routningsplaner i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Popup-meddelandetimer för inkommande samtal	<p>Låter dig ställa in hur lång tid ett popup-meddelande för inkommande samtal visas på telefonens skärm.</p> <p>Se Popup-meddelandetimer för inkommande samtal, Produktspecifik konfiguration, på sidan 138.</p>
Intelligenta närhetstjänster	<p>Gör att användare kan parkoppla en mobilenhet till telefonen via Bluetooth och använda telefonen för att ringa och ta emot mobila samtal.</p> <p>Se Aktivera intelligenta närhetstjänster, på sidan 197.</p> <p>Cisco IP-telefon 8811, 8841 och 8851NR stöder varken Bluetooth eller intelligenta närhetstjänster.</p>
Snabbtelefon	<p>Låter användare ringa och ta emot internsamtal med hjälp av programmerbara knappar på telefonen. Du kan konfigurera linjeknappar för snabbtelefon och göra detta:</p> <ul style="list-style-type: none"> • Ring upp en anknytning direkt med snabbtelefonval. • Initiera ett internsamtal och uppmana användaren att ange ett giltigt snabbtelefonnummer. <p>OBS! Om användaren loggar in på samma telefon på daglig basis med sin Cisco Extension Mobility-profil kan du tilldela telefonknappsmallen som innehåller snabbtelefoninformation till deras profil och tilldela telefonen som standardsnabbtelefon för snabbtelefonlinjen.</p>
Endast IPv6-stöd	<p>Ger stöd för utökad IP-adressering på Cisco IP-telefoner. IPv4- och IPv6-konfigurering rekommenderas och har fullständigt stöd. Vissa funktioner stöds inte i en fristående konfiguration. Bara IPv6-adress tilldelas.</p> <p>Se Konfigurera nätverksinställningar, på sidan 58.</p>
Jitterbuffert	<p>Jitterbuffertfunktionen hanterar jitter från 10 millisekunder (ms) till 1000 ms för ljudströmmar.</p> <p>Det körs i ett anpassningsbart läge och justerar dynamiskt mängden jitter.</p>
Delta	<p>Låter användare kombinera två samtal på samma linje för att skapa ett konferenssamtal och stanna kvar i samtalet.</p>

Funktion	Beskrivning och mer information
Linjestatus för samtalslistor	<p>Låter användaren se tillgänglighetsstatus för linjestatusen på övervakade linjenummer i listan Samtalshistorik. Linjestatusen har följande lägen</p> <ul style="list-style-type: none"> • Frånkopplad • Tillgänglig • Används • Stör ej <p>Se Aktivera BLF för samtalslistor, på sidan 168 .</p>
Linjestatus i företagskatalogen	<p>Gör det möjligt att visa status för en kontakt i företagskatalogen.</p> <ul style="list-style-type: none"> • Frånkopplad • Tillgänglig • Används • Stör ej <p>Se Aktivera BLF för samtalslistor, på sidan 168 .</p>
Linjetextetikett	<p>Ställer in en textetikett för en telefonlinje istället för katalognummer.</p> <p>Se Ställa in en etikett för en linje, på sidan 177 .</p>
Logga ut från samtalsgrupper	<p>Låter användare logga ut från en svarsgrupp och tillfälligt blockera samtal från att ringa upp deras telefon när de inte kan ta emot samtal. Utloggningen ur svarsgrupperna hindrar inte gruppsamtal från andra grupper än svarsgrupper att ringa upp telefonen.</p> <p>Se informationen om routningsplan i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Skadlig nummerpresentation (MCID)	<p>Låter användare meddela systemadministratören om misstänkta samtal som tas emot.</p>
Meet Me-konferens	<p>Låter en användare vara värd för en Meet Me-konferens där övriga deltagare ringer ett förutbestämt nummer vid en schemalagd tidpunkt.</p>
Meddelande väntar	<p>Definierar katalognummer för på- och av-indikatorer för väntande meddelanden. Ett direktanslutet röstmeddelandesystem använder det angivna katalognumret för att ställa in eller ta bort en indikering på att meddelande väntar för en viss Cisco IP-telefon.</p> <p>Se informationen om väntande meddelanden och röstbrevlådan i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Meddelande väntar-indikator	<p>En lampa på luren som tyder på att en användare har ett eller flera nya röstmeddelanden.</p> <p>Se informationen om väntande meddelanden och röstbrevlådan i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Minsta ringvolym	<p>Ställer in minsta ringvolym för en IP-telefon.</p>

Funktion	Beskrivning och mer information
Loggning av missade samtal	<p>Låter en användare ange om missade samtal loggas i katalogen med missade samtal för en viss linje.</p> <p>Se katalognummerinformationen i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Mobile Connect	<p>Låter användare hantera affärssamtal med hjälp av ett enda telefonnummer och plocka upp pågående samtal på sin bordstelefon och en fjärrenhet som en mobiltelefon. Användare kan begränsa gruppen av uppringare efter telefonnummer och tid på dagen.</p> <p>Mer information om Cisco Unified Mobility finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Mobil åtkomst och fjärråtkomst genom Expressway	<p>Låter fjärrarbetare ansluta till företagets nätverk enkelt och säkert utan att använda en VPN-klienttunnel.</p> <p>Se Mobil åtkomst och fjärråtkomst genom Expressway, på sidan 170</p>
Mobilröståtkomst	<p>Utökar funktionerna i Mobile Connect genom att låta användare få åtkomst till ett interaktivt röstvarssystem (IVR) för att initiera ett samtal från en fjärrenhet, till exempel en mobiltelefon.</p> <p>Mer information om Cisco Unified Mobility finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Övervakning och inspelning	<p>Låter en handledare göra en tyst övervakning av ett pågående samtal. Ingen av parterna i samtalet kan höra handledaren. Användaren kan höra en varningston under samtal när samtalet spelas in.</p> <p>När ett samtal är säkrat visas säkerhetsstatusen för samtalet som en låsikon på Cisco IP-telefonen. De anslutna parterna kan också få en ljudsignal som indikerar att samtalet är säkert och övervakas.</p> <p>OBS! Även om ett aktivt samtal övervakas eller spelas in kan användaren ta emot och koppla snabbtelefonsamtal, men om användaren kopplar ett snabbtelefonsamtal parkeras det aktiva samtalet vilket medför att inspelningen avslutas och övervakningssessionen avbryts. För att återgå till övervakningssessionen måste parten i det övervakade samtalet återuppta samtalet.</p>
Prioritet och förtur på flera nivåer (MLPP)	<p>Gör det möjligt för användaren att ringa och ta emot brådskande samtal i vissa miljöer, som militära eller myndigheter.</p> <p>Se Prioritet och förtur på flera nivåer (MLPP), på sidan 186 .</p>
Flera samtal per linje	<p>Varje linje kan hantera flera samtal. Som standard stöder telefonen två aktiva samtal per linje, och högst sex aktiva samtal per linje. Endast ett samtal kan kopplas när som helst. Andra samtal parkeras automatiskt.</p> <p>I systemet kan du konfigurera max antal samtal/upptagetton högst 6/6. Konfiguration med mer än 6/6 stöds inte officiellt.</p> <p>Se katalognummerinformationen i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>

Funktion	Beskrivning och mer information
Musik i vänteläge	Spelar musik medan samtal är parkerat.
Ljud av	Stänger av luren eller headsetets mikrofon.
Ingen varning	Gör det lättare för slutanvändare att identifiera överförda samtal genom att visa den ursprungliga uppringarens telefonnummer. Samtalet visas som ett varningssamtal följt av uppringarens telefonnummer.
Ringa med luren på	Tillåter en användare att ringa ett nummer utan att lyfta luren. Användaren kan sedan antingen plocka upp luren eller trycka på Ring.
Samtalshämtning från annan grupp	Låter användare svara på ett samtal som ringer på en telefon i en annan grupp som är associerad med användarens grupp. Mer information om samtalshämtning finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.
Meddelande för Extension Mobility-användare på telefonskärmen	Denna funktion förbättrar telefongränssnittet för Extension Mobility-användare med vänliga meddelanden.
Telefonens meddelande för lista över betrodda adresser i Cisco Unified Communications Manager	Aktiverar telefonen för att skicka ett larm till Cisco Unified Communications Manager när listan över betrodda adresser uppdateras. Se Säkerhetsfunktioner som stöds, på sidan 84 .
PLK-stöd för köstatistik	Funktionen med PLK-stöd för köstatistik låter användare söka efter samtalsköstatistik för svarspiloter. Informationen visas sedan på telefonens skärm.
Ringa med plustecken	Låter användare ringa E.164-nummer som inleds med ett plustecken (+). För att ringa plustecknet + måste användaren trycka på och hålla ned knappen med en stjärna (*) i minst en sekund. Då slås den första siffran för samtal med eller utan lur (inklusive redigeringsläge).
Strömbalansering över LLDP	Ger funktion för strömbalansering i telefonen med LLDP- och CDP-protokoll. Se Strömbalansering, Produktspecifik konfiguration, på sidan 138 .
Prognostiserad uppringning	Gör det enklare att ringa ett samtal. Listan Senaste ändras och visar endast telefonnummer som liknar numret som rings upp. Prognostiserad uppringning är aktiverad när förbättrat linjeläge har aktiverats. Förenklat användargränssnitt för nytt samtal måste inaktiveras för att prognostiserad uppringning ska fungera.
Funktionen Privat	Hindrar användare som delar en linje från att lägga till sig själva i ett samtal och från att visa information på sin telefonskärm om samtalet hos den andra användaren. Se informationen om inbrytning och sekretess i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Funktion	Beskrivning och mer information
PLAR (Private Line Automated Ringdown)	<p>Cisco Unified Communications Manager-administratören kan konfigurera ett telefonnummer som Cisco IP-telefonen ringer upp så snart som luren lyfts. Detta kan vara praktiskt för telefoner som är avsedda för akutsamtal eller ”hotline”.</p> <p>Administratören kan konfigurera en fördröjning på upp till 15 sekunder. Det gör att användaren kan ringa ett samtal innan telefonen återställs till hotlinenumret. Timern går att konfigurera med parametern Timer för luren av till första siffra under Enhet > Enhetsinställningar > SIP-profil.</p> <p>Mer information finns i <i>Guide till funktionskonfiguration i Cisco Unified Communications Manager</i>.</p>
Problemrapportverktyget (PRT)	<p>Skicka telefonloggar eller rapportera problem till en administratör.</p> <p>Se Problemrapportverktyg, på sidan 175.</p>
Programmerbara funktionsknappar	<p>Du kan tilldela funktioner, till exempel Nytt samtal, Ring tillbaka och Vidarekoppla alla, till linjeknapparna.</p> <p>Se informationen om telefonknappmallar i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Kvalitetsrapporterings- verktyg (QRT)	<p>Låter användare lämna information om problem med telefonsamtal genom att trycka på en knapp. QRT kan konfigureras för endera av två användarlägen, beroende på mängden av användarinteraktion som önskas med QRT.</p>
Senaste	<p>Låter användare se de 150 senaste enskilda samtalen och samtalsgrupperna. Du kan se senast uppringda nummer, missade samtal och ta bort en post.</p>
Ring igen	<p>Låter användare ringa det senast slagna telefonnumret genom att trycka på en knapp eller återuppringningsfunktionsknappen.</p>
Fjärrportskonfiguration	<p>Här kan du konfigurera hastigheten och duplexfunktion telefonens Ethernet-portar på distans med hjälp av Cisco Unified Communications Manager Administration. Detta förbättrar prestanda för stora installationer med särskilda portinställningar.</p> <p>OBS! Om portarna är konfigurerade för fjärrportkonfiguration i Cisco Unified Communications Manager kan inte data ändras i telefonen.</p> <p>Se Fjärrportkonfiguration, Produktspecifik konfiguration, på sidan 138.</p>
Omdirigera direktsamtal till fjärrdestination till företagsnummer	<p>Omdirigerar ett direktsamtal till användarens mobiltelefon till företagets nummer (bordstelefon). För ett inkommande samtal till fjärrdestination (mobil), endast fjärrdestinationering. Bordstelefonen rings inte upp. När samtalet besvaras på deras mobiltelefon visar bordstelefonen ett meddelande om fjärranvändningen. Under dessa samtal kan användarna utnyttja olika funktioner i sin mobiltelefon.</p> <p>Mer information om Cisco Unified Mobility finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Ta bort timer för meddelande om avslutat samtal	<p>Förbättrar svarstiden för Avsluta samtal genom att ta bort meddelandet <code>Samtal avslutat</code> som visas på telefonens skärm.</p>

Funktion	Beskrivning och mer information
Ringsignalinställning	<p>Identifierar ringningstypen för en linje när en telefon har ett annat pågående samtal.</p> <p>Se informationen om katalognummer i dokumentationen till din utgåva av Cisco Unified Communications Manager och i Anpassade telefonringssignaler, på sidan 111.</p>
RTCP-vänteläge för SIP	<p>Säkerställer att parkerade samtal inte ignoreras av gatewayen. Gatewayen kontrollerar status på RTCP-porten för att fastställa om ett samtal är aktivt eller inte. Genom att hålla telefonporten öppen kommer gatewayen inte att avsluta parkerade samtal.</p>
Säker konferens	<p>Tillåter säkra telefoner att koppla konferenssamtal med hjälp av en säker konferensbrygga. När nya deltagare läggs till med hjälp av funktionsknapparna Konf, Delta, Bryt in eller i MeetMe-konferenser visas ikonen för säkra samtal så länge alla deltagare använder säkra telefoner.</p> <p>i konferenslistan visas säkerhetsnivån för varje konferensdeltagare. Initiatorer kan ta bort osäkra deltagare från konferenslistan. Andra deltagare än initiatorer kan lägga till eller ta bort konferensdeltagare om parametern för avancerad tillfällig konferenstjänst är aktiverad.</p> <p>Se information om konferensbrygga i dokumentationen till din utgåva av Cisco Unified Communications Manager och Säkerhetsfunktioner som stöds, på sidan 84.</p>
Säker EMCC	<p>Förbättrar EMCC-funktionen genom att tillhandahålla ökad säkerhet för en användare som loggar in på sin telefon från en fjärranslutning.</p>
Tjänster	<p>Låter dig använda Cisco IP-telefonens tjänstekonfigurationsmenyn i Cisco Unified Communications Manager Administration för att definiera och underhålla listan över telefontjänster som användarna kan prenumerera på.</p> <p>Se information om tjänster i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Tjänste-URL-knappen	<p>Låter användare få åtkomst till tjänster från en programmerbar knapp i stället för att använda menyn Tjänster på en telefon.</p> <p>Se information om tjänster i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Visa uppringarens ID och uppringarens nummer	<p>Telefonerna kan visa både uppringarens ID och uppringarens nummer för inkommande samtal. IP-telefonens LCD-skärmstorlek begränsar längden på uppringarens ID och uppringarens nummer som kan visas.</p> <p>Funktionen för att visa uppringarens ID och uppringarens nummer används endast för avisering av inkommande samtal och ändrar inte funktionerna Vidarekoppling och Svarsgrupp.</p> <p>Se ”Nummerpresentation” i tabellen.</p>

Funktion	Beskrivning och mer information
Förenkla inloggningen till Extension Mobility med Cisco-headset	<p>Gör att användare kan logga in till Extension Mobility med sina Cisco-headset.</p> <p>När telefonen är i MRA-läge kan användaren logga in på telefonen via headsetet.</p> <p>Funktionen kräver Cisco Unified Communications Manager (UCM) version 11.5 (1) SU8, 11.5 (1) SU.9, 12.5 (1) SU3 eller senare.</p> <p>Mer information finns i <i>Funktionskonfigurationshandbok för Cisco Unified Communications Manager</i>, version 11.5 (1) SU8 eller senare, eller version 12.5 (1) SU3 eller senare.</p>
Stöd för förenklad surfplatta	<p>Låter användare av Android- eller iOS-surfplattor parkoppla surfplattan till telefonen via Bluetooth och sedan använda telefonen för ljudet vid samtal på surfplattan.</p> <p>Se Aktivera intelligenta närhetstjänster, på sidan 197.</p> <p>Cisco IP-telefon 8851NR stöder inte Bluetooth.</p>
Snabbval	<p>Ringer upp ett visst nummer som har lagrats i förväg.</p>
SSH-åtkomst	<p>Här kan du aktivera eller inaktivera SSH-åtkomstinställningen med Cisco Unified Communications Manager Administration. Om du aktiverar SSH-servern kan telefonen acceptera SSH-anslutningar. Om SSH-serverfunktionen inaktiveras i telefonen blockeras all SSH-åtkomst till telefonen.</p> <p>Se SSH-åtkomst, Produktspecifik konfiguration, på sidan 138.</p>
Routning på klockslag	<p>Begränsar tillgången till specificerade telefonifunktioner under en tidsperiod.</p> <p>Se information om tidsperiod- och tidsroutning i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Tidszonsuppdatering	<p>Uppdaterar Cisco IP-telefonen med tidszonsändringar.</p> <p>Se information om tid och datum i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>
Överföring	<p>Låter användare omdirigera anslutna samtal från sina telefoner till ett annat nummer.</p>
Överföring – direktöverföring	<p>Överföring: Den första anropade överföringen kommer alltid att initiera ett nytt samtal genom att använda samma katalognummer efter parkering av det aktiva samtalet.</p> <p>Användaren kan direkt överföra samtal med funktioner för överföring av aktiva samtal.</p> <p>Vissa JTAPI-/TAPI-program är inte kompatibla med kopplings- och direktöverföringsfunktionen på Cisco IP-telefonen och du kan behöva konfigurera policyn för koppling och direktöverföring för att inaktivera koppling och direktöverföring på samma linje eller möjligen på flera linjer.</p> <p>Se katalognummerinformationen i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p>

Funktion	Beskrivning och mer information
TVS	<p>Med TVS (Trust Verification Services) kan telefoner autentisera signerade konfigurationer och autentisera andra servrar eller enheter utan att öka storleken på listan över betrodda certifikat (CTL) eller kräva hämtning av en uppdaterad CTL-fil till telefonen. TVS är aktiverat som standard.</p> <p>Säkerhetsinställningsmenyn på telefonen visar TVS-information.</p>
UCR 2013	<p>Cisco IP-telefoner stöder UCR (Unified Capabilities Requirements) 2013 genom att tillhandahålla följande funktioner:</p> <ul style="list-style-type: none"> • Stöd för FIPS (Federal Information Processing Standard) 140-2 • Stöd för 80-bitars SRTCP-tagging <p>Som IP-telefonadministratör måste du ställa in specifika parametrar i Cisco Unified Communications Manager Administration.</p>
Meddelande om ej konfigurerad primär linje	<p>Meddelar användaren om den primära linjen inte är konfigurerad. Användaren ser meddelandet <code>Odelad</code> på telefonens skärm.</p>
Uppdateringar av användargränssnittet för lista, varning och visuell inbox för röstbrevlåda.	<p>Ökar storleken på programfönstret för att minimera trunkerade strängar.</p>
Videoläge	<p>Tillåter en användare att välja videovisningsläge för att visa en videokonferens, beroende på konfigurerade lägen i systemet.</p> <p>Se informationen om video i dokumentationen till din utgåva av Cisco Unified Communications Manager.</p> <p>Tillgängliga på Cisco IP-telefon 8845, 8865 och 8865NR.</p>
Stöd för video	<p>Ger stöd för video på telefonen. Parametern för videofunktioner måste vara aktiverad för videosamtal på fönstret Telefonkonfiguration i Cisco Unified Communications Manager. Det är aktiverat som standard.</p> <p>Tillgängliga på Cisco IP-telefon 8845, 8865 och 8865NR.</p>
Video via dator	<p>Låter användare ringa videosamtal med hjälp av deras Cisco Unified IP-telefon, dator och en extern videokamera.</p> <p>Funktionen låter även användare ringa videosamtal med Cisco Jabber eller Cisco Unified Video Advantage-produkter.</p>
Visuella röstmeddelanden	<p>Ersätter de inspelade instruktionerna för röstmeddelanden med ett grafiskt gränssnitt.</p> <p>Se <i>Installations- och konfigurationshandbok för visuell röstbrevlåda</i> på http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3.</p>
Röstmeddelandesystem	<p>Låter uppringaren lämna ett meddelande om samtalen är obesvarade.</p> <p>Se information om röstbrevlåda i dokumentationen till din utgåva av Cisco Unified Communications Manager och i Konfigurera visuell inbox för röstbrevlåda, på sidan 184.</p>

Funktion	Beskrivning och mer information
VPN	Tillhandahåller VPN-anslutning (virtuellt privat nätverk) via SSL på Cisco Unified IP-telefonen när den är placerad utanför ett betrodd nätverk eller när nätverkstrafik mellan telefonen och Unified Communications Manager måste passera betrodda nätverk.
Webbåtkomst inaktiverad som standard	Ökar säkerheten genom att inaktivera åtkomst till alla webbtjänster, som HTTP. Användare kan bara komma åt webbtjänster om du aktiverar åtkomst till webben.

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Funktionsknappar och programstyrda knappar

Följande tabell innehåller information om funktioner som finns på funktionsknappar, funktioner som finns på dedikerade funktionsknappar och funktioner som du behöver för att konfigurera som programmerbara funktionsknappar. En post i tabellen som ”stöds” indikerar att funktionen stöds för motsvarande knapptyp eller funktionsknapp. Av de två knapp typerna och funktionsknapparna är det endast programmerbara funktionsknappar som kräver konfiguration i Cisco IP-telefon.

Mer information om hur du konfigurerar programmerbara funktionsknappar finns i [Mallar för telefonknappar](#), på sidan 189.

Tabell 30. Funktioner med motsvarande knappar och funktionsknappar

Funktionens namn	Dedikerad funktionsknapp	Programmerbar funktionsknapp	Programstyrd knapp
Aviseringssamtal	Stöds inte	Stöds	Stöds inte
Alla samtal	Stöds inte	Stöds	Stöds inte
Svara	Stöds inte	Stöds	Stöds
BrytInKf	Stöds inte	Stöds inte	Stöds
Ring igen	Stöds inte	Stöds	Stöds
Vidarebefordra alla samtal	Stöds inte	Stöds inte	Stöds
Parkera samtal	Stöds inte	Stöds	Stöds
Samtalsparkering linjestatus	Stöds inte	Stöds	Stöds inte
Hämta samtal	Stöds inte	Stöds	Stöds
Hämta samtal linjestatus	Stöds inte	Stöds	Stöds inte
Konferens	Stöds	Stöds inte	Stöds

Funktionens namn	Dedikerad funktionsknapp	Programmerbar funktionsknapp	Programstyrd knapp
vidarekoppla	Stöds inte	Stöds inte	Stöds
Stör ej	Stöds inte	Stöds	Stöds
Hämta grupp	Stöds inte	Stöds	Stöds
Parkera	Stöds	Stöds inte	Stöds
Svarsgrupper	Stöds inte	Stöds	Stöds inte
Snabbtelefon	Stöds inte	Stöds	Stöds inte
SpårID	Stöds inte	Stöds	Stöds
Meet me	Stöds inte	Stöds	Stöds
Koppla	Stöds inte	Stöds inte	Stöds
Mobile Connect (Mobility)	Stöds inte	Stöds	Stöds
Ljud av	Stöds	Stöds inte	Stöds inte
Hämta annan	Stöds inte	Stöds	Stöds
PLK-stöd för kösamtal	Stöds inte	Stöds inte	Stöds
Funktionen Privat	Stöds inte	Stöds	Stöds inte
Köstatus	Stöds inte	Stöds	Stöds inte
Kvalitetsrapporteringsverktyg (QRT)	Stöds inte	Stöds	Stöds
Spela in	Stöds inte	Stöds inte	Stöds
Ring igen	Stöds inte	Stöds	Stöds
Snabbval	Stöds inte	Stöds	Stöds inte
Kortnummer linjestatus	Stöds inte	Stöds	Stöds inte
Stöd för parkeringsknapp på USB-headset	Stöds inte	Stöds inte	Stöds
Överföra	Stöds	Stöds inte	Stöds

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.

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.

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.
-

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.
-

Produktspecifik konfiguration

I följande tabell beskrivs fälten i rutan med den produktspecifika konfigurationslayouten.

Tabell 31. Produktspecifika konfigurationsfält

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Inaktivera högtalartelefonen	Kryssruta	Omarkerad	Stänger av högtalarfunktionen i telefonen.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Inaktivera högtalartelefon och headset	Kryssruta	Omarkerad	Stänger av högtalartelefonen och headsetfunktionen i telefonen.
Inaktivera handhetheten	Kryssruta	Omarkerad	Stänger av handhethetsfunktionen i telefonen.
PC-port	Aktiverad Inaktiverad	Aktiverad	Styr möjligheten att använda PC-porten för att ansluta en dator till LAN.
Åtkomst till inställningar	Inaktiverad Aktiverad Begränsad	Aktiverad	Aktiverar, inaktiverar eller begränsar åtkomsten till lokala telefonkonfigurationsinställningar i appen Inställningar. <ul style="list-style-type: none"> • Inaktiverat – Inställningsmenyn visar inte några alternativ. • Aktiverat – Alla alternativ på inställningsmenyn är tillgängliga. • Begränsat – Endast menyn Telefoninställningar är tillgänglig.
Datoråtkomst till röst-VLAN	Aktiverad Inaktiverad	Aktiverad	Anger om telefonen ska tillåta en enhet som är ansluten till PC-porten för att få åtkomst till röst-VLAN. <ul style="list-style-type: none"> • Inaktiverad – Datorn kan inte skicka och ta emot data i röst-VLAN eller från telefonen. • Aktiverad – Datorn kan skicka och ta emot data från röst-VLAN eller från telefonen. Ställ in detta fält som Aktiverad om ett program som körs på datorn ska övervaka telefontrafiken. Dessa program kan omfatta övervakning och inspelning, och användning av nätverksövervakningsprogramvara för analys.
Videofunktioner	Aktiverad Inaktiverad	8845, 8865 och 8865NR: aktiverad 8811, 8851, 8851NR, 8861: inaktiverad	Låter användare ringa videosamtal med hjälp av en Cisco IP-telefon, en personlig dator och en videokamera.
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.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Inaktivera TLS 1.0 och TLS 1.1 för webbåtkomst	Inaktiverad Aktiverad	Inaktiverad	<p>Styr användningen av TLS 1.2 för en webserveranslutning.</p> <ul style="list-style-type: none"> • 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	<p>Styr vilken uppringningsmetod.</p> <ul style="list-style-type: none"> • Inaktiverad – Cisco Unified Communications Manager väntar på att siffterimern 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. <p>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.</p>
Visning av dagar ej aktiverat	Dagar i veckan		<p>Definierar de dagar som skärmen inte slås på automatiskt vid den tid som anges i fältet Display på-tid.</p> <p>Välj dagar från listrutan. Om du vill välja mer än en dag Ctrl-klickar du på varje dag som du vill välja.</p>
Display på-tid	hh:mm		<p>Anger vid vilken tidpunkt varje dag som skärmen slås på automatiskt (utom på de dagar som anges i fältet Visning av dagar ej aktiverat).</p> <p>Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt.</p> <p>Om du till exempel vill stänga av bakgrundsbelysningen automatiskt vid 07:00 (0700), ange 07:00. Om du vill stänga av skärmen vid 14:00 anger du 14:00 .</p> <p>Om detta fält är tomt, slås skärmen automatiskt på 00:00.</p>

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Display på-varaktighet	hh:mm		<p>Definierar den tid som skärmen är tänd efter att den slagits på vid den tid som anges i fältet Display på-tid.</p> <p>Om du till exempel vill ha skärmen tänd i 4 timmar och 30 minuter efter att den slås på automatiskt, anger du 4:30.</p> <p>Om detta fält är tomt stängs telefonen av vid slutet av dagen (0:00).</p> <p>Om Display på-tid 0:00 och skärmens varaktighet för påslagen är tom (eller 24:00) släcks inte skärmen.</p>
Visa timeout för ledig	hh:mm	01:00	<p>Definierar den tid 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).</p> <p>Ange värdet i fältet i formatet timmar:minuter.</p> <p>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.</p> <p>Mer information finns i Konfigurera viloläge, på sidan 113.</p>
Visa På vid inkommande samtal	Inaktiverad Aktiverad	Aktiverad	Slår på passiv skärm när det kommer ett inkommande samtal.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Aktivera Energisparplus	Dagar i veckan		<p>Definierar schema med dagar då telefonen ska stängas av.</p> <p>Välj dagar från listrutan. Om du vill välja mer än en dag Ctrl-klickar du på varje dag som du vill välja.</p> <p>När Aktivera energispar Plus är på visas ett meddelande som varnar om nödfall (E911).</p> <p>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.</p> <p>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.</p>
Påslagningstid för telefon	hh:mm		<p>Bestämmer när telefonen slås på automatiskt för de dagar som anges i fältet Aktivera energispar plus.</p> <p>Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt.</p> <p>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 .</p> <p>Standardvärdet är tomt, vilket betyder 00:00.</p> <p>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.</p>

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Avstängningstid för telefon	hh:mm		<p>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.</p> <p>Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt.</p> <p>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 .</p> <p>Standardvärdet är tomt, vilket betyder 00:00.</p> <p>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.</p>
Tidsgräns för telefon av vid inaktivitet	20 till 1 440 minuter	60	<p>Anger hur lång tid telefonen måste vara inaktiv innan telefonen stängs av.</p> <p>Tidsgränsen inträffar under följande förhållanden:</p> <ul style="list-style-type: none"> 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.
Aktivera varningsignal	Kryssruta	Omarkerad	<p>När detta är aktiverat instrueras telefonen att spela upp en ljudsignal som startar 10 minuter innan tiden i fältet Avstängningstid för telefon.</p> <p>Den här kryssrutan används endast om listrutan Aktivera energisparläge plus har en eller flera dagar utvalda.</p>
EnergyWise-domän	Högst 127 tecken.		Identifierar EnergyWise-domänen som telefonen är i.
EnergyWise Secret	Högst 127 tecken.		Identifierar det hemliga säkerhetslösenordet som används för att kommunicera med ändpunkterna i EnergyWise-domänen.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Tillåt åsidosättning av EnergyWise	Kryssruta	Omarkerad	<p>Avgör om du tillåter EnergyWise-domänkontrollantpolicyn att skicka uppdateringar av strömnivån till telefonerna. Följande villkor gäller:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • Om EnergyWise styr telefonen att stängas av vid 20:00 (8:00), kvarstår direktivet i praktiken (förutsatt att inga telefonanvändarändringar 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. <p>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.</p>
Policy för koppling och direktöverföring	<p>Aktivering samma linje, mellan linjer</p> <p>Aktivera endast samma linje</p> <p>Inaktivering samma linje, mellan linjer</p>	Aktivering samma linje, mellan linjer	<p>Styr förmågan hos en användare att koppla och överföra samtal. \$\$\$</p> <ul style="list-style-type: none"> • Aktivering samma linje, mellan linjer – Användare kan direkt överföra eller koppla ihop ett samtal på nuvarande linje till ett annat samtal på en annan linje. • Aktivera endast samma linje – Användare kan bara direkt överföra eller koppla ihop samtal när båda samtalen är på samma linje. • Inaktivering samma linje, mellan linjer – Användare kan inte koppla eller vidarekoppla samtal på samma linje. Kopplings- och överföringsfunktioner är inaktiverade och användaren kan inte göra någon direkt överföring eller koppla ihop samtal.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Vidarebefordra till PC-port	Inaktiverad Aktiverad	Inaktiverad	Anger om telefonen vidarebefordrar paket som sänds och tas emot på nätverksporten till åtkomstporten.
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>
CDP (Cisco Discovery Protocol): Växelport	Inaktiverad Aktiverad	Aktiverad	Styr CDP-protokollet i SW-porten på telefonen.
CDP (Cisco Discovery Protocol): PC-port	Inaktiverad Aktiverad	Aktiverad	Styr CDP-protokollet i PC-porten på telefonen.
LLDP-protokoll – Media Endpoint Discover (LLDP-MED): Växelport	Inaktiverad Aktiverad	Aktiverad	Aktiverar LLDP-MED i SW-porten.
LLDP (Link Layer Discovery Protocol): PC-port	Inaktiverad Aktiverad	Aktiverad	Aktiverar LLDP i PC-porten.
LLDP tillgångs-ID	Sträng, upp till 32 tecken		Identifierar resurs-ID som tilldelas till telefonen för lagerhantering.
LLDP-kraftsprioritet	Okänt Låg hög Kritiskt	Okänt	Tilldelar en telefonströmprioritet till växeln så att växeln kan ge rätt ström till telefonerna.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
802.1x-autentisering	Användarkontrollerad Aktiverad Inaktiverad	Användarkontrollerad	Anger status på 802.1X-autentiseringsfunktionen. <ul style="list-style-type: none"> 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.
Automatisk portsynkronisering	Inaktiverad Aktiverad	Inaktiverad	Synkroniserar portar till den lägsta hastigheten mellan portar i en telefon för att eliminera paketförluster.
Fjärrkonfiguration för växelport	Inaktiverad Aktiverad	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.
Fjärrkonfiguration för PC-port	Inaktiverad Aktiverad	Inaktiverad	Här kan du konfigurera hastigheten och duplexfunktionen i telefonens PC-port fjärranslutet. Detta förbättrar prestanda för stora installationer med särskilda portinställningar. Om 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.
Popup-meddelandetimer för inkommande samtal	0, 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, 60	5	Anges tid, i sekunder, som visas i popup-meddelanden. Tiden inkluderar toningseffekter när fönstret öppnas och stängs. 0 betyder att meddelande om senaste inkommande samtal är inaktiverat.
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.

Fältnamn	Fältyp eller val	Standard	Beskrivning och bruksanvisningar
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. Du kan ställa in en telefon så att ringsignalen inte kan stängas av.
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: <ul style="list-style-type: none"> • Begränsar trängsel vid TFTP-överföringar till centraliserade TFTP-fjärrservrar. • Elimineras 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 bandbredds begränsade WAN-länkar.
Laddningsserver	Sträng på upp till 256 tecken		Identifierar den alternativa IPv4-server som telefonen använder för att få firmware och uppgraderingar. Formatet på adressen är: adress : <port>@<base=<0-7>;pfs=<0-1>
IPv6-laddningsserver	Sträng på upp till 256 tecken		Identifierar den alternativa IPv6-server som telefonen använder för att få firmware och uppgraderingar. Adressformatet är: [adress] : <port>@<base=<0-7>;pfs=<0-1>
UI-kontroll för bredband-headset	Inaktiverad Aktiverad	Aktiverad	Tillåter användaren att använda bredbandskodek för ett analogt headset.
HD-headset	Inaktiverad Aktiverad	Aktiverad	Aktiverar eller inaktiverar användningen av ett bredbandsheadset på telefonen. Används i samband med bredbandsheadset för användarkontroll. Mer information finns i Konfigurera bredbandskodning, på sidan 113 .

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Wi-Fi	Inaktiverad Aktiverad	Aktiverad	Gör att Cisco IP-telefon 8861 och 8865 kan ansluta till Wi-Fi-nätverket. Fältet visas inte i telefoner som inte stöder den här funktionen.
Bakre USB-port	Inaktiverad Aktiverad	8861, 8865 och 8865NR: aktiverad	Styr möjligheten att använda USB-porten på baksidan av Cisco IP-telefon 8861 och 8865. Fältet visas inte i telefoner som inte stöder den här funktionen.
USB-port på sidan	Inaktiverad Aktiverad	Aktiverad	Styr möjligheten att använda USB-porten på sidan av Cisco IP-telefon 8861, 8851NR, 8861, 8865 och 8865NR. Fältet visas inte i telefoner som inte stöder den här funktionen.
Konsolåtkomst	Inaktiverad Aktiverad	Inaktiverad	Anger om seriekonsolen är aktiverad eller inaktiverad.
Bluetooth	Inaktiverad Aktiverad	Aktiverad	Aktiverar eller inaktiverar Bluetooth-alternativet på telefonen. Om det är inaktiverad kan användaren inte aktivera Bluetooth på telefonen. Stöds på Cisco IP-telefon 8845, 8851, 8861 och 8865. Fältet visas inte i telefoner som inte stöder den här funktionen.
Tillåta import av Bluetooth-kontakter	Inaktiverad Aktiverad	Aktiverad	Gör att användaren kan importera kontakter från sin anslutna mobilenhet via Bluetooth. När alternativet är inaktiverad kan användaren inte importera kontakter från ansluten mobilenhet på telefonen. Stöds på Cisco IP-telefon 8845, 8851, 8861 och 8865. Fältet visas inte i telefoner som inte stöder den här funktionen.
Tillåta Bluetooth-mobilt Handsfree-läge	Inaktiverad Aktiverad	Aktiverad	Gör att användare kan dra nytta av telefonens akustiska egenskaper med mobilenheten eller surfplattan. Användaren parkopplar den mobila enheten eller surfplattan till telefonen via Bluetooth. Om funktionen är inaktiverad kan användaren inte parkoppla den mobila enheten eller surfplatta med sin telefon. När den mobila enheten är parkopplad kan användaren ringa och ta emot mobilsamtal på telefonen. Med hjälp av en surfplatta kan användaren dirigera ljudet från surfplattan till telefonen. Användare kan parkoppla flera mobila enheter, surfplattor och ett Bluetooth-headset till telefonen. Men bara en enhet och ett headset kan anslutas samtidigt. Fältet visas inte i telefoner som inte stöder den här funktionen.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Bluetooth-profiler	Handsfree Gränssnittsenhet	Handsfree	Anger vilka Bluetooth-profiler på telefonen som är aktiverade eller inaktiverade. Fältet visas inte i telefoner som inte stöder den här funktionen.
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.
Visa alla samtal på den primära linjen	Inaktiverad Aktiverad	Inaktiverad	Anger om alla samtal som presenterats för den här telefonen visas på den primära linjen eller inte. Syftet med det här fältet är att göra det enklare för användare att överskådligt visa alla samtal på alla linjer i stället för att behöva välja en linje för att se samtalen på den linjen. Om flera linjer är konfigurerade på telefonen är det vanligtvis logiskt att vilja se alla samtal på alla linjer i en och samma bildskärm. När den här funktionen är aktiverad visas alla samtal på den primära linjen, men du kan fortfarande välja en viss linje för att filtrera visningen om du vill visa bara samtalen för den specifika linjen.
HTTPS-server	HTTP och HTTPS aktiverat HTTPS endast	HTTP och HTTPS aktiverat	Kontrollerar typen av kommunikation till telefonen. Om du bara väljer HTTPS är telefonkommunikationen säkrare.
IPv6-loggserver	Sträng på upp till 256 tecken		Identifierar IPv6-loggservern. Adressformatet 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 och bruksanvisningar
Loggprofil	Standard Förinställd Telefoni SIP UI Nätverk Media Uppgradera Tillbehör Säkerhet Wi-Fi VPN EnergyWise MobileRemoteAc	Förinställd	<p>Anger den fördefinierade loggningsprofilen.</p> <ul style="list-style-type: none"> • 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 • Wi-Fi – Loggar Wi-Fi-information • VPN – Loggar information om VPN-nätverk • Energywise – Loggar information om energibesparingar • MobileRemoteAC – Loggar informationen om mobilåtkomst och Remote Access via Expressway
Annonsera G.722- och iSAC-kodek	Använd systemstandard Inaktiverad Aktiverad	Använd systemstandard	<p>Anger om telefonen annonserar G.722- och iSAC-kodek till Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> • Använd systemstandard – skiljer sig mot den inställning som anges i företagsparametern Annonsera G.722-kodek. • Inaktiverat – G.722 annonseras inte till Cisco Unified Communications Manager. • Aktiverat – G.722 annonseras till Cisco Unified Communications Manager. <p>Mer information finns i anmärkningen under tabellen.</p>

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Identifiera anslutningsfel för Unified CM	Normal Försenat	Normal	<p>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.</p> <ul style="list-style-type: none"> • Normal – Detektering av ett Unified CM-anslutningsfel görs med standardsystemhastigheten. Välj detta värde för snabbare identifiering av ett Unified CM-anslutningsfel. • Fördröjd – Detektering av ett Unified CM-anslutningsfel görs ungefär fyra gånger långsammare än normalt. Välj detta värde om du föredrar att felövertäckningen försenas något för att se om anslutningen kan återupprättas <p>Den exakta tidsskillnaden mellan Normal och Fördröjd anslutning vid fel-detektering beror på många variabler som ständigt förändras.</p> <p>Det här fältet avser bara kabelansluten Ethernet-anslutning.</p>
Strömförhandling	Inaktiverad Aktiverad	Aktiverad	<p>Ger funktion för strömbalansering i telefonen med LLDP- och CDP-protokoll.</p> <p>Energibalansering bör inte inaktiveras när telefonen är ansluten till en omkopplare som stöder energibalansering. Om det inaktiveras kan omkopplaren stänga av strömmen till telefonen.</p>
Ge kopplingston från knappen Frisläpp	Inaktiverad Aktiverad	Inaktiverad	<p>Anger om användaren hör en kopplingston när han/hon trycker på knappen Frisläpp.</p> <ul style="list-style-type: none"> • Inaktiverat – användaren hör ingen kopplingston. • Aktiverat – användaren hör en kopplingston.
Bakgrundsbild	Sträng upp till 64 tecken		<p>Anger fil för standardbakgrund. När en standardbakgrund är inställd kan användaren inte ändra bakgrunden på telefonskärmen.</p>
Förenklat användargränssnitt vid nytt samtal	Inaktiverad Aktiverad	Inaktiverad	<p>Anger användargränssnittet för uppringning med luren av. När detta är aktiverat kan användaren inte välja ett nummer från listan med senaste samtal.</p> <p>När detta är aktiverat öppnar fältet ett förenklat fönster så att användaren kan ringa ett samtal. Användaren ser inte popup-fönstret med samtalshistorik som visas när telefonen är av. Popup-fönstret betraktas som användbart och förenklat användargränssnitt för nya samtal är inaktiverat som standard.</p>
Återgå till Alla samtal	Inaktiverad Aktiverad	Inaktiverad	<p>Anger om telefonen återställs till Alla samtal när ett samtal avslutas eller inte om samtalet har ett annat filter än Primär linje, Alla samtal eller Aviseringssamtal.</p>

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Visa samtalshistorik för endast vald linje	Inaktiverad Aktiverad	Inaktiverad	Styr visningen av listan med senaste samtal. <ul style="list-style-type: none"> • Inaktiverat – listan över senaste samtal visar samtalshistoriken för alla linjer. • Aktiverat – listan över senaste samtal visar samtalshistoriken för vald linje.
Avisering om inkommande samtal med åtgärder	Inaktiverad Visa för alla inkommande samtal Visa för osynliga inkommande samtal	Visa för alla inkommande samtal	Kontrollerar den typ av inkommande samtal som visas på telefonens skärm. Syftet med det här fältet är att minska antalet knapptryckningar som användaren behöver göra för att besvara ett samtal. <ul style="list-style-type: none"> • Inaktiverat – Aviseringen om inkommande samtal inaktiveras och användaren ser den traditionella popup-varningen om inkommande samtal. • Visa för alla inkommande samtal – Aviseringen om inkommande samtal visas för alla samtal oavsett synlighet. • Visa för osynliga inkommande samtal – Aviseringen om inkommande samtal visas för samtal som inte visas på telefonen. Denna parameter fungerar på liknande sätt som popup-meddelandet om inkommande samtal.
DF-bit	0 1	0	Styr hur nätverkpaket skickas. Paket kan skickas i bitar (fragment) i olika storlekar. När DF-biten är inställd på 1 i pakethuvudet fragmenteras inte i nätverkets nyttolast vid överföring via nätverksenheter, till exempel växlar och routrar. Om fragmenteringen tas bort undviker man felaktig analys på den mottagande sidan, men det medför något långsammare hastigheter. Inställningen av DF-bit gäller inte för ICMP-, VPN-, VXC VPN- eller DHCP-trafik.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Standardlinjefilter	Lista över kommaavgränsade telefonenhetsnamn		<p>Anger listan över telefoner som finns i standardfiltret.</p> <p>När linjens standardfilter har konfigurerats ser användare ett filter som heter <code>Dagligt schema</code> i Samtalsmeddelanden på menyn Inställningar > Inställningar på telefonen. Det här filtret för dagligt schema används utöver det förinställda filtret för Alla samtal.</p> <p>Om standardlinjefiltret inte konfigureras kontrollerar telefonen alla tillhandhållna linjer. Om alternativet konfigureras kontrollerar telefonen linjerna som har ställts in i Cisco Unified Communications Manager om användaren väljer standardfiltret som aktivt filter, eller om det inte finns några anpassade filter.</p> <p>Med anpassade linjefilter kan du filtrera högprioriterade linjer för minskad aviseringssamtal på en del linjer som omfattas av ett aviseringfilter. Det anpassade filtret skapar antingen traditionella popup-varningar eller aviseringar som kan åtgärdas för inkommande samtal på de valda linjerna. För varje filter skapas en avisering endast för den uppsättning linjer som omfattas av filtret. Den här funktionen är ett sätt för användare med flera linjer att minska aviseringssamtal genom att filtrera och visa aviseringar endast från högprioriterade linjer. Användarna kan själva konfigurera det här. Du kan också programmera standardlinjefiltret och överföra det till telefonen.</p>
Lägsta prioritet för aviserande linjestatus	Inaktiverad Aktiverad	Inaktiverad	<p>Anger aviseringsstatus när du använder delade linjer.</p> <ul style="list-style-type: none"> • Inaktiverat – när det finns ett inkommande samtal som aviseras på den delade linjen, indikeras aktuell aviseringsstatus av LED/linjens statusikon istället för fjärranvändning. • Aktiverat – när det finns ett inkommande samtal med avisering på den delade linjen, ser användaren ikonen för fjärranvändning.
Visning i en kolumn för KEM	Inaktiverad Aktiverad	Inaktiverad	<p>Styr visningen på expansionsmodulen.</p> <ul style="list-style-type: none"> • Inaktiverat – expansionsmodulen använder läget med två kolumner. • Aktiverat – expansionsmodulen använder läget med en kolumn. <p>Fältet visas inte i telefoner som inte stöder den här funktionen.</p>
EEE (Energy Efficient Ethernet): PC-port	Inaktiverad Aktiverad	Inaktiverad	Styr EEE på PC-porten.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
EEE (Energy Efficient Ethernet): SW-port	Inaktiverad Aktiverad	Inaktiverad	Styr EEE i växelporten.
Startar videoport			Definierar början på portintervallet för videosamtal. Fältet visas inte i telefoner som inte stöder den här funktionen.
Stoppar videoport			Definierar slutet på portintervallet för videosamtal. Fältet visas inte i telefoner som inte stöder den här funktionen.
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 användare 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 kontoret) är inloggningsinformationen förhandsfylld på inloggningsskärmen. Mer information finns i Mobil åtkomst och fjärråtkomst genom Expressway, på sidan 170 .
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 Mobil åtkomst och fjärråtkomst genom Expressway, på sidan 170 .
Webbadmin	Inaktiverad Aktiverad	Inaktiverad	Aktiverar eller inaktiverar administratörens tillgång till telefonens webbsidor via en webbläsare. Mer information finns i Konfigurera administrationssidan för telefon, på sidan 104 . Fältet visas inte i telefoner som inte stöder den här funktionen.
Adminlösenord	Sträng med 8-127 tecken		Definierar administratörlösenordet när du öppnar telefonens webbsidor som administratör. Fältet visas inte i telefoner som inte stöder den här funktionen.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
WLAN SCEP-server	Sträng på upp till 256 tecken		Anger den SCEP-server som telefonen använder för att få certifikat för WLAN-autentisering. Ange värddnamnet eller IP-adressen (med hjälp av IP-adressering i standardformat) på servern. Fältet visas inte i telefoner som inte stöder den här funktionen.
WLAN rot-CA-fingeravtryck (SHA256 eller SHA1)	Sträng på upp till 95 tecken		Anger SHA256- eller SHA1-fingeravtrycket i rot-CA som ska användas vid validering under SCEP-processen när certifikat för WLAN-autentisering utfärdas. Vi rekommenderar att du använder SHA256-fingeravtryck, som kan erhållas via OpenSSL (t.ex. openssl x509 -in rootca.cer -noout -sha256 -fingerprint) eller med en webbläsare för att granska certifikatuppgifterna. Anger det 64-hexadecimala teckenvärdet för SHA256-fingeravtrycket eller det 40-hexadecimala teckenvärdet för SHA1-fingeravtrycket med vanligt skiljetecken (kolon, streck, punkt, blanksteg) eller utan avgränsare. Om du använder avgränsare ska skiljetecknet placeras konsekvent efter varje 2, 4, 8, 16 eller 32 hexadecimala tecken för ett SHA256-fingeravtryck eller varje 2, 4 eller 8 hexadecimala tecken för ett SHA1-fingeravtryck. Fältet visas inte i telefoner som inte stöder den här funktionen.
WLAN-autentiseringsförsök			Fältet visas inte i telefoner som inte stöder den här funktionen.
Uppmaningsläge för WLAN-profil 1	Inaktiverad Aktiverad	Inaktiverad	Fältet visas inte i telefoner som inte stöder den här funktionen.
Linje-läge	Sessionslinjeläge Förbättrat linjeläge	Sessionslinjeläge	Styr linjevisningen på telefonen. <ul style="list-style-type: none"> • Sessionslinjeläge – knapparna på ena sidan av skärmen är linjeknappar. • Förbättrat linjeläge – knapparna på båda sidor av telefonskärmen är linjeknappar. Aviseringar om prognostiserad uppringning och inkommande samtal med åtgärder aktiveras som standard i förbättrat linjeläge.
Adminkonfigurerbar ringning	Inaktiverad Soluppgång Chirp1 Chirp2	Inaktiverad	Styr ringsignal och möjligheten för användarna att ställa in ringsignal. <ul style="list-style-type: none"> • Om du väljer Inaktiverad kan användarna konfigurera standardringsignaler på sina telefoner. • För alla andra värden, kan användarna inte ändra ringsignal. Menyalternativet Ringsignal på menyn Inställningar är nedtonat (grå).

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Användning av kundsupport	Sträng på upp till 64 tecken	Tom	Används endast för Cisco TAC.
Inaktivera TLS-chiffer	Se Inaktivera Transport Layer Security-chiffer, på sidan 159 .	Ingen	Inaktiverar valt TLS-chiffer. 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.
Sänk din röst-varning	Aktiverad Inaktiverad	Aktiverad	Styr funktionen som sänker din röst. <ul style="list-style-type: none"> • Inaktiverad: <ul style="list-style-type: none"> • Telefonen visar inte menyalternativet Sänk din röst i menyn Inställningar. • Användare får inte se meddelandet på skärmen när de talar högt. • Aktiverad: <ul style="list-style-type: none"> • Användare styr funktionen med menyalternativet Sänk din röst i menyn Inställningar. Fältet är som standard inställt som På.
Markera samtal som skräp	Aktiverad Inaktiverad	Aktiverad	Styr funktionen för att markera samtal som skräp. <ul style="list-style-type: none"> • Inaktiverad: <ul style="list-style-type: none"> • Telefonen visar inte programstyrda knappen för Markera skräp. • Objektet Skräplista i menyn Inställningar visas inte. • Om det fanns en skräplista är den raderad och kan inte återställas. • Aktiverad: <ul style="list-style-type: none"> • Telefonen visar programstyrda knappen Markera skräp. • Objektet Skräplista i menyn Inställningar visas.
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.

Fältnamn	Fälttyp eller val	Standard	Beskrivning och bruksanvisningar
Linjetextetikett i ELM	Inaktiverad Aktiverad	Aktiverad	<p>Kontrollerar visning av linjeetikett under ett samtal när Förbättrat linjeläge har konfigurerats</p> <ul style="list-style-type: none"> • Aktiverad <ul style="list-style-type: none"> • Om uppringarens namn har konfigurerats visas namnet på den första raden i samtalet och den lokala linjeetiketten på den andra raden. • Om uppringarens namn inte har konfigurerats visas fjärnumret på den första raden och den lokala linjeetiketten på den andra raden. • Inaktiverad <ul style="list-style-type: none"> • Om uppringarens namn har konfigurerats visas namnet på den första raden i samtalet och numret på den andra raden. • Om uppringarens namn inte är konfigurerat visas bara fjärnumret. <p>Det här fältet är obligatoriskt.</p>



OBS! Kodekhantering omfattar två steg:

1. Telefonen annonserar kodek som stöds till Cisco Unified Communications Manager. Alla ändpunkter har inte stöd för samma kodek uppsättning.
2. När Cisco Unified Communications Manager får lista över codec från alla telefoner som deltar i uppringningen väljs en codec med allmänt stöd baserat på olika faktorer, bland annat regionparinställningen.

Bästa funktionskonfigurationerna

Du kan ställa in telefonens funktioner för att passa användarnas behov. Men vi har några rekommendationer för vissa situationer och installationer som kan hjälpa dig.

Miljöer med hög samtalsvolym

I en miljö med hög samtalsvolym rekommenderas du ställa in en del funktioner på ett visst sätt.

Fält	Området Administration	Rekommenderad inställning
Använd alltid primär linje	Enhetsinfo	Av eller På Mer information finns i Fält: Använd alltid primär linje, på sidan 159 .
Avisering om inkommande samtal med åtgärder	Produktspecifik konfigurationslayout	Visa för alla inkommande samtal
Visa alla samtal på den primära linjen	Produktspecifik konfigurationslayout	Aktiverad
Återgå till Alla samtal	Produktspecifik konfigurationslayout	Aktiverad

Multilinjemiljöer

I multilinjemiljö rekommenderas du ställa in en del funktioner på ett visst sätt.

Fält	Området Administration	Rekommenderad inställning
Använd alltid primär linje	Enhetsinfo	Av Mer information finns i Fält: Använd alltid primär linje, på sidan 159 .
Avisering om inkommande samtal med åtgärder	Produktspecifik konfigurationslayout	Visa för alla inkommande samtal
Visa alla samtal på den primära linjen	Produktspecifik konfigurationslayout	Aktiverad
Återgå till Alla samtal	Produktspecifik konfigurationslayout	Aktiverad

Miljö för sessionslinjeläge

Förbättrat linjeläge är det rekommenderade verktyget för hantering av de flesta samtalsmiljöer. Om förbättrat linjeläge inte passar dina behov kan du dock använda sessionslinjeläge.

Fält	Området Administration	Rekommenderad inställning för sessionslinjeläge
Visa alla samtal på den primära linjen	Produktspecifik konfigurationslayout	Inaktiverad
Återgå till Alla samtal	Produktspecifik konfigurationslayout	Inaktiverad

Fält	Området Administration	Rekommenderad inställning för sessionslinjeläge
Avisering om inkommande samtal med åtgärder	Produktspecifik konfigurationslayout	Aktiverat som standard (fast programvara version 11.5 (1) och senare).

Relaterade ämnen

[Ställa in ytterligare linjeknappar](#), på sidan 193

[Funktioner som är tillgängliga i förbättrat linjeläge](#), på sidan 194

Fält: Använd alltid primär linje

Detta fält anger om den primära linjen på en IP-telefon väljs när en användare lägger av luren. Om denna parameter är Sant när en telefon har luren av är den primära linjen vald och blir den aktiva linjen. Även om ett samtal ringer på den andra linjen hos användaren med telefonluren av är bara den första linjen aktiv. Det går inte att svara på inkommande samtal på den andra linjen. I detta fall måste användaren välja den andra linjen för att besvara samtalet. Standardvärdet är Falskt.

Fältet Använd alltid primär linje används av samma skäl som kombinationen av Visa alla samtal på den primära linjen och Återgå till alla samtal när båda dessa två funktioner är aktiverade. Men den största skillnaden är att när Använd alltid primär linje är aktiverat kan inkommande samtal inte besvaras på den andra linjen. Endast kopplingston hörs på den primära linjen. Det finns vissa miljöer med hög samtalsvolym där detta är den önskade användarupplevelsen. I allmänhet är det bäst att lämna det här fältet inaktiverat förutom i miljöer med hög samtalsvolym som kräver den här funktionen.

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>).

Aktivera samtalshistorik för delad linje

Låter dig visa aktivitet på en delad linjen i samtalshistoriken. Den här funktionen:

- Loggar missade samtal för en delad linje.
- Loggar alla besvarade och kopplade samtal för en delad linje.

Innan du börjar

Inaktivera sekretess innan du aktiverar samtalshistorik för delad linje. Annars visar inte samtalshistoriken de samtal som andra användare besvarar.

Arbetsordning

-
- Steg 1** Utgå från Cisco Unified Communications Manager Administration och välj **Enhet > Telefon**.
 - Steg 2** Lokalisera telefonen som ska konfigureras.
 - Steg 3** Gå till listrutan Spela in samtalslogg från delad linje i det produktspecifika konfigurationsområdet.
 - Steg 4** Välj **Aktiverat** i listrutan.
 - Steg 5** Välj **Spara**.
-

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.

För mer information, se [Produktspecifik konfiguration, på sidan 138](#)

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 32. 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 <i>timmar:minuter</i> . 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 <i>timmar:minuter</i> . 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.

För mer information, se [Produktspecifik konfiguration, på sidan 138](#)

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 33. Konfigurationsfält för EnergyWise

Fält	Beskrivning
Aktivera Energisparplus	<p>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.</p> <p>Inga dagar väljs som standard.</p> <p>När Aktivera energispar Plus är markerat visas ett meddelande som varnar vid nödfall (E911).</p> <p>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.</p> <p>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.</p>
Påslagningstid för telefon	<p>Bestämmer när telefonen slås på automatiskt för de dagar som anges i fältet Aktivera energispar plus.</p> <p>Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt.</p> <p>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 .</p> <p>Standardvärdet är tomt, vilket betyder 00:00.</p> <p>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.</p>
Avstängningstid för telefon	<p>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.</p> <p>Ange tiden i detta fält i 24-timmarsformat, där 00:00 är midnatt.</p> <p>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 .</p> <p>Standardvärdet är tomt, vilket betyder 00:00.</p> <p>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.</p>

Fält	Beskrivning
Tidsgräns för telefon av vid inaktivitet	<p>Hur lång tid telefonen måste vara inaktiv innan telefonen stängs av.</p> <p>Tidsgränsen inträffar under följande förhållanden:</p> <ul style="list-style-type: none"> 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. <p>Fältintervallet är 20 till 1 440 minuter.</p> <p>Standardvärdet är 60 minuter.</p>
Aktivera varningsignal	<p>När detta är aktiverat instrueras telefonen att spela upp en ljudsignal som startar 10 minuter innan tiden i fältet Avstängningstid för telefon.</p> <p>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:</p> <ul style="list-style-type: none"> 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. <p>Den här kryssrutan används endast om listrutan Aktivera energisparläge plus har en eller flera dagar utvalda.</p>
EnergyWise-domän	<p>EnergyWise-domänen som telefonen finns i.</p> <p>Fältets maximala längd är 127 tecken.</p>
EnergyWise Secret	<p>Det hemliga säkerhetslösenordet som används för att kommunicera med ändpunkterna i EnergyWise-domänen.</p> <p>Fältets maximala längd är 127 tecken.</p>

Fält	Beskrivning
Tillåt åsidosättning av EnergyWise	<p>Kryssrutan anger om du tillåter EnergyWise-domänkontrollantpolicyn att skicka uppdateringar av strömnivån till telefonerna. Följande villkor gäller:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • 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. <p>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.</p>

- Steg 4** Välj **Spara**.
- Steg 5** Välj **Använd konfig**.
- Steg 6** Starta om telefonen.

Konfigurera Stör ej

När Stör ej (DND) är aktiverat hörs ingen ringning när ett samtal kommer in och inga ljud eller notiser visas.

När Stör ej (DND) har aktiverats ändras färgen högst upp på telefonens skärm och Stör ej visas på telefonen.

Du kan konfigurera telefonen med en telefonknappsmall med DND som en av de valda funktionerna.

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.
Välj inte att avvisa samtal om du vill prioritera MLPP-samtal för uppringning av den här telefonen när DND är aktiverat.
 - 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 xv

Aktivera agenthälsning

Med agenthälsningsfunktionen kan en agent skapa och uppdatera en förinspelad hälsning som spelas upp i början av ett samtal, som ett kundsamtal, innan agenten börjar samtalet med den som ringer. Agenten kan förinspela en enda hälsning eller flera hälsningar, efter behov, och skapa och uppdatera dessa hälsningar.

När en kund ringer kan både agenten och den som ringer höra den förinspelade hälsningen. Agenten kan ha avstängt ljud tills hälsningen är klar eller så kan agenten besvara samtalet samtidigt som hälsningen.

Alla koder som stöds för telefonen stöds för agenthälsningssamtal.

Mer information finns i inbrytnings- och sekretessinformationen 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** Leta reda på den IP-telefon du vill konfigurera.
- Steg 3** Rulla till panelen med enhetsinformationslayout och ange **Inbyggd brygga** som På eller Standard.
- Steg 4** Välj **Spara**.
- Steg 5** Kontrollera inställningen av bryggan:
 - a) Välj **System > Tjänstparametrar**.
 - b) Välj lämplig server och tjänst.
 - c) Rulla till rutan med klusterparameter (Enhet – Telefon) och ange **Inbyggd brygga – aktivera** som På.
 - d) Välj **Spara**.

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Konfigurera övervakning och registrering

Med övervaknings och registreringsfunktionen kan en handledare göra en tyst övervakning av ett pågående samtal. Ingen av parterna i samtalet kan höra handledaren. Användaren kan få en ljudsignal under ett samtal när det övervakas.

När ett samtal är säkert visas en låsikon. Uppringaren kan också få en ljudsignal som indikerar att samtalet övervakas. De anslutna parterna kan också få en ljudsignal som indikerar att samtalet är säkert och övervakas.

När ett aktivt samtal övervakas eller spelas in kan användaren ta emot eller koppla snabbtelefonsamtal, men om användaren kopplar ett snabbtelefonsamtal parkeras det aktiva samtalet. Denna åtgärd medför att inspelningen avslutas och övervakningssessionen avbryts. För att återgå till övervakningssessionen måste parten i det övervakade samtalet återuppta samtalet.

Mer information finns i avsnittet om övervakning och registrering av uppgifter i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Med följande procedur lägger du till en användare i standardövervakningsanvändargrupperna.

Innan du börjar

Cisco Unified Communications Manager måste konfigureras för att stödja övervakning och registrering.

Arbetsordning

-
- Steg 1** Utgå från Cisco Unified Communications Manager Administration och välj **Användarhantering > Programanvändare**.
 - Steg 2** Markera användargrupperna Standard CTI – Tillåt samtalsövervakning och Standard CTI – Tillåt inspelning av samtal.
 - Steg 3** Klicka på **Lägg till markerade**.
 - Steg 4** Klicka på **Lägg till användargrupp**.
 - Steg 5** Lägg till användarnas telefoner i listan över kontrollerade enheter hos programanvändare.
 - Steg 6** Välj **Spara**.

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

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**.

Aktivera BLF för samtalslistor

Fältet BLF för samtalslistor styr även linjestatus för företagskatalogfunktionen.

Arbetsordning

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

Steg 2 Gå till fältet BLF för samtalslistor och aktivera eller inaktivera funktionen.

Som standard är funktionen inaktiverad.

Parametrar som du anger i det produktspecifika konfigurationsområdet kan också visas i enhetskonfigurationsfönstret för olika enheter och i företagstelefonkonfigurationsfönstret. Om du ställer in samma parametrar i dessa fönster prioriteras inställningarna så här:

1. Inställningar i fönstret Enhetskonfiguration
2. Inställningar i fönstret Allmän telefonprofil
3. Inställningar i fönstret Företagstelefonkonfiguration

Steg 3 Välj **Spara**.

Ställa in Energy Efficient Ethernet för växel- och PC-port

IEEE 802.3az Energy Efficient Ethernet (EEE) är en utökning av befintlig IEEE 802.3-standard som tillhandahåller en metod för minskad energiförbrukning utan försämrad funktion i nätverksgränssnitt. Konfigurerbar EEE gör att administratören kan styra EEE-funktioner i datorporten och växelporten.



OBS! Administratörer måste kontrollera att kryssrutan Åsidosätt är markerad på alla tillämpliga UCM-sidor, annars fungerar inte EEE.

Administratören styr EEE-funktioner med följande två parametrar:

- **Energy Efficient Ethernet:** PC-porten: ger sömlös anslutning med persondatorer. Administratören kan välja alternativen Aktiverad och Inaktiverad för att styra funktionen.
- **Energy Efficient Ethernet:** växelport: ger sömlös anslutning

Mer information finns i: [Produktspecifik konfiguration, på sidan 138](#)

Arbetsordning

Steg 1 Gå till Cisco Unified Communications Manager Administration och välj ett av följande fönster:

- **Enhet > Telefon**
- **Enhet > Enhetsinställningar > Allmän telefonprofil**
- **System > Företagstelefonkonfigurationer**

Om du konfigurerar parametern i flera fönster är prioritetsordningen:

1. **Enhet > Telefon**
2. **Enhet > Enhetsinställningar > Allmän telefonprofil**
3. **System > Företagstelefonkonfigurationer**

Steg 2 Leta reda på telefonen om det behövs.

Steg 3 Ange värden i fälten **Energy Efficient Ethernet: PC-port** och **Energy Efficient Ethernet: växelport**.

- Energy Efficient Ethernet: PC-port
- Energy Efficient Ethernet: växelport

Steg 4 Välj **Spara**.

Steg 5 Välj **Använd konfig**.

Steg 6 Starta om telefonen.

Konfigurera RTP-/sRTP-portintervall

Du konfigurerar RTP- och sSRTP-portvärden i SIP-profilen. RTP- och sRTP-portvärden sträcker sig från 2048 till 65535, med standardintervallet 16384 till 32764. En del portvärden inom portintervallet RTP och sRTP är avsedda för andra telefontjänster. Du kan inte konfigurera dessa portar för RTP och SRTP.

För mer information, se SIP-profilinformationen i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Arbetsordning

Steg 1 Välj **Enhet > Enhetsinställningar > SIP-profil**

Steg 2 Välj sökkriterier att använda och klicka på **Sök**.

Steg 3 Välj den profil som du vill ändra.

Steg 4 Ställ in Start Media Port och Stoppmedieport för att generera början och slutet på portintervallet.

Följande lista identifierar UDP-portar som används för andra telefontjänster och därmed inte tillgängliga för RTP och sRTP:

port 4051

används för PFS

port 5060

används för SIP över UDP-transport

portintervall 49152-53247

används för lokala tillfälliga portar

portintervall 53248-65535

används för VPN-funktion med en VXC-tunnel

Steg 5 Klicka på **Spara**.

Steg 6 Klicka på **Använd konfig**.

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

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).

Mobil åtkomst och fjärråtkomst genom Expressway stöder förbättrat linjeläge.

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.

Driftsättningsscenarioer

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

Lokala användare loggar in i företagets nätverk

När Mobil åtkomst och fjärråtkomst genom Expressway har distribuerats loggar du in i företagets nätverk på plats. Företagets nätverk identifieras och telefonen registreras med Cisco Unified Communications Manager.

Externa användare loggar in i företagets nätverk

När du inte är på kontoret känner telefonen av att den är i läget för distansarbete. Inloggningsfönstret Mobil åtkomst och fjärråtkomst genom Expressway öppnas och du ansluts till företagets nätverk.

Notera följande:

- Du måste ha en giltig tjänstdomän och ett giltigt användarnamn och lösenord för att ansluta till nätverket.
- Återställ tjänsteläget för att rensa de alternativa TFTP-inställningarna innan du får tillgång till företagets nätverk. Då rensas inställningen för alternativ TFTP-server så att telefonen identifierar nätverket för distansarbete och förhindrar telefonen från att upprätta en VPN-anslutning. Hoppa över det här steget om en telefon ska användas för första gången.
- Om du DHCP-alternativ 150 eller 66 har aktiverats i nätverksroutern kanske du inte kan logga in på företagets nätverk. Återställ tjänsteläget för att använda MRA-läge.

Externa användare loggar in i företagets nätverk med VPN.

Om du arbetar på distans loggar du in i företagets nätverk med VPN efter distributionen av Mobil åtkomst och fjärråtkomst genom Expressway.

Utför en grundläggande återställning för att återställa dina telefonkonfigurationer om telefonen får ett fel.

Du måste konfigurera alternativ TFTP-inställning i (**Admin.inställningar > Nätverksinställningar > IPv4**, fältet **Alternativ TFTP-server 1**).

Relaterade ämnen

[Grundläggande återställning](#), på sidan 263

Mediasökvägar och interaktiv etablering av anslutningar

Du kan distribuera ICE (Interactive Connectivity Establishment) för att förbättra tillförlitligheten med MRA (Mobile and Remote Access)-samtal som går via en brandvägg eller NAT (Network Address Translation). ICE är en valfri distribution som används med tjänster för Serial Tunneling and Traversal Using Relays around NAT för att välja bästa mediasökvägen till ett samtal.

Sekundär Turn Server och Turn Server Failover stöds inte.

Mer information om MRA och ICE finns i *Systemkonfigurationshandbok för Cisco Unified Communications Manager, version 12.0 (1)* eller senare. Det finns även ytterligare information genom begäran i Internet Engineering Task Force (IETF) för kommentarsdokument:

- *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*(RFC 5766)
- *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols* (RFC 5245)

Telefonfunktioner som är tillgängliga för Mobil åtkomst och fjärråtkomst genom Expressway

Mobil åtkomst och fjärråtkomst genom Expressway erbjuder säker åtkomst utan VPN till samarbets tjänster för Ciscos mobil- och fjärranvändare. Men för att bevara nätverkets säkerhet begränsar den åtkomst till vissa telefonfunktioner.

Följande lista visar tillgängliga telefonfunktioner med Mobil åtkomst och fjärråtkomst genom Expressway.

Tabell 34. Stöd för funktioner och Mobil åtkomst och fjärråtkomst genom Expressway

Telefonfunktion	Version av den fasta programvaran för telefoner
Förkortat nummer	10.3 (1) och senare
Besvara äldsta	11.5 (1) SR1 och senare
Assisterad dirigerad parkering av samtal	10.3 (1) och senare
Autosvar	11.5 (1) SR1 och senare
Bryt in och cBarge (BrytInKonf)	11.5 (1) SR1 och senare
Fältet för upptagetlampa (BLF)	10.3 (1) och senare
Fältet för upptagetlampa (BLF), hämta	10.3 (1) och senare
Upptagetfält (BLF), kortnummer	10.3 (1) och senare
Ring igen	10.3 (1) och senare
Vidarebefordra samtal	10.3 (1) och senare
Meddelande för vidarebefordra samtal	10.3 (1) och senare
Parkera samtal	10.3 (1) och senare
Hämta samtal	10.3 (1) och senare
Cisco Unified Serviceability	11.5 (1) SR1 och senare
CAL (Client Access License)	11.5 (1) SR1 och senare
Konferens	10.3 (1) och senare
Konferenslista/Ta bort deltagare	11.5 (1) SR1 och senare
Företagskatalog	11.5 (1) SR1 och senare
CTI-program (CTI-kontrollerad)	11.5 (1) SR1 och senare
Direktöverföring	10.3 (1) och senare
Dirigerad parkering av samtal	10.3 (1) och senare
Olika ringsignaler	11.5 (1) SR1 och senare
vidarekoppla	10.3 (1) och senare

Telefonfunktion	Version av den fasta programvaran för telefoner
Förbättrat linjeläge	12.1 (1) och senare
vidarekoppla	10.3 (1) och senare
Obligatoriska åtkomstkoder och ärendekoder	11.5 (1) SR1 och senare
Hämta grupp	10.3 (1) och senare
Förfrågan/Åter	10.3 (1) och senare
Återställning från förfrågan	10.3 (1) och senare
Omedelbar vidarekoppling	10.3 (1) och senare
Delta	10.3 (1) och senare
Skadlig nummerpresentation (MCID)	11.5 (1) SR1 och senare
Meet Me-konferens	10.3 (1) och senare
Meddelande väntar-indikator	10.3 (1) och senare
Mobile Connect	10.3 (1) och senare
Mobilröståtkomst	10.3 (1) och senare
Prioritet och förtur på flera nivåer (MLPP)	11.5 (1) SR1 och senare
Multilinje	11.5 (1) SR1 och senare
Musik i vänteläge	10.3 (1) och senare
Ljud av	10.3 (1) och senare
Nätverksprofiler (automatiskt)	11.5 (1) SR1 och senare
Ringa med luren av	10.3 (1) och senare
Ringa med luren på	10.3 (1) och senare
Ringa med plustecken	10.3 (1) och senare
Funktionen Privat	11.5 (1) SR1 och senare
PLAR (Private Line Automated Ringdown)	11.5 (1) SR1 och senare
Ring igen	10.3 (1) och senare
Kortnummer (har inte stöd för paus)	10.3 (1) och senare
Tjänste-URL-knappen	11.5 (1) SR1 och senare
Överföra	10.3 (1) och senare
Samtal med URI (Uniform Resource Identifier)	10.3 (1) och senare

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 tjänstomän, 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 137

[Produktspecifik konfiguration](#), på sidan 138

Generera en QR-kod för MRA-inloggning

Användare som har en telefon med kamera kan skanna en QR-kod för att logga in på MRA, i stället för att ange tjänstomän och användarnamn manuellt.

Arbetsordning

-
- Steg 1** Använd en QR-kodgenerator som skapar en QR-kod med antingen tjänstomän eller tjänstomän och användarnamn åtskiljda med kommatecken. Till exempel: mra.exempel.com eller mra.exempel.com,användarnamn.
- Steg 2** Skriv ut QR-koden och ge den till användaren.
-

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**.
-

Konfigurera dubbel bankinformation

Om du vill konfigurera dubbel bankinformation gör du så här:

Arbetsordning

- Steg 1** Utgå från Cisco Unified Communications Manager Administration och välj **Enhet > Standardinställningar**.
- Steg 2** Markera Läs in informationen i fältet Inaktiv laddningsinformation.

- Steg 3** Välj **Massadministration > Import/Export > Exportera > Standardinställningar** och schemalägg ett exportjobb.
- Steg 4** Hämta den exporterade .tar-filen och ta bort .tar-formatet.
- Steg 5** Kontrollera filformatet i den exporterade CSV-filen och kontrollera att CSV-filen har en kolumn för Inaktiv laddningsinformation med rätt värde.
- OBS!** Värdet CSV-filen måste matcha värdet för standardinställningar i fönstret Cisco Unified Communications Manager Administration.

Parkeringsövervakning

Parkeringsövervakning stöds endast när en Cisco IP-telefon parkerar ett samtal. Parkeringsövervakning övervakar sedan statusen för ett parkerat samtal. Samtalsbubblan för parkeringsövervakningen rensas inte förrän det parkerade samtalet hämtas eller avbryts av det parkerade samtalet. Det parkerade samtalet kan hämtas genom att använda samma samtalsbubblan i telefonen som parkerade samtalet.

Ställa in timer för parkeringsövervakning

Cisco Unified Communications Manager Administration tillhandahåller tre klusterparametrar för tjänstetimer för parkeringsövervakning: Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer och Park Monitoring Forward No Retrieve Timer. Varje tjänsteparameter innehåller ett standardvärde och kräver ingen särskild konfiguration. Dessa timerparametrar avser endast övervakning av parkerade samtal; Call Park Display Timer och Call Park Reversion Timer används inte för parkeringsövervakning. Se tabellen nedan för beskrivningar av dessa parametrar.

Konfigurera timer på sidan Cisco Unified Communications Manager – serviceparametrar.

Arbetsordning

- Steg 1** Gå till Cisco Unified Communications Manager Administration och välj **System > Tjänsteparametrar**.
- Steg 2** Uppdatera fälten Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer och Park Monitoring Forward No Retrieve Timer i panelen Klusterparametrar (allmän funktion).

Tabell 35. Tjänsteparametrar för parkeringsövervakning

Fält	Beskrivning
Park Monitoring Reversion Timer	Standard är 60 sekunder. Den här parametern avgör hur många sekunder som Cisco Unified Communications Manager ska vänta innan användaren uppmanas att besvara ett samtal som han/hon har parkerat. Timern börjar när användaren trycker på Parkera på telefonen och en påminnelse utfärdas när tiden börjar att gälla. Du kan åsidosätta det värde som den här tjänsteparametern anger för önskad linje i avsnittet Parkeringsovervakning i fönstret Katalognummerkonfiguration (öppna Cisco Unified Communications Manager Administration och välj Samtalsdirigering > Katalognummer). Ange ett värde på 0 för att direkt använda regelbundet återställningsintervall som tjänsteparametern Park Monitoring Periodic Reversion Timer anger. (Se beskrivningen som följer.) Om den här parametern till exempel anges till 15 och Park Monitoring Periodic Reversion Timer är inställt på 15, uppmanas användaren direkt om det parkerade samtalet och var 15:e sekund därefter tills Park Monitoring Forward No Retrieve Timer (se beskrivningen som följer) upphör att gälla.
Park Monitoring Periodic Reversion Timer	Standard är 30 sekunder. Den här parametern anger intervallet (i sekunder) som Cisco Unified Communications Manager ska vänta innan användaren uppmanas igen om att besvara ett parkerat samtal. För att ansluta till det parkerade samtalet behöver användaren bara lyfta luren under en av dessa sekunder. Cisco Unified Communications Manager fortsätter att uppmana användaren om det parkerade samtalet så länge det är parkerat och fram tills angiven tid enligt Park Monitoring Forward No Retrieve Timer (se beskrivningen som följer) upphör att gälla. Ange ett värde på 0 om du vill inaktivera regelbundet återställningsintervall och uppmaningar om det parkerade samtalet.
Park Monitoring Forward No Retrieve Timer	Standard är 300 sekunder. Den här parametern avgör hur många sekunder som parkeringspåminnelse visas innan det parkerade samtalet vidarekopplas till mottagaren i Park Monitoring Forward No Retrieve Timer (se beskrivningen som följer) som anges i fönstret Katalognummerkonfiguration. (Om ingen vidarekopplingsdestination anges i Cisco Unified Communications Manager Administration, returneras samtalet till samma linje som den som användes för att parkera samtalet.) Den här parametern börjar när angiven tidpunkt enligt tjänsteparametern Park Monitoring Periodic Reversion Timer upphör att gälla. När Park Monitoring Forward No Retrieve Timer förfaller bort från parkeringen och vidarekopplas till angiven mottagare eller återgår till parkeringslinjen.

Ställa in parametrar för parkeringsövervakning för katalognummer

I fönstret Katalognummerkonfiguration finns området Parkeringsövervakning där du kan konfigurera tre parametrar.

Arbetsordning

- Steg 1** Utgå från Cisco Unified Communications Manager Administration och välj **Samtalsroutning > Katalognummer**.
- Steg 2** Ställ in fälten Parkeringsövervakning som beskrivs i tabellen nedan.

Tabell 36. Parametrar för parkeringsövervakning

Fält	Beskrivning
Parkeringsövervakning vidarekopplar ingen hämtning vid extern mottagare	När parkerad part är en extern person vidarekopplas samtalet till angiven mottagare i parametern Parkeringsövervakning vidarekopplar ingen hämtning vid extern mottagare. Om fältvärdet för Parkeringsövervakning vidarekopplar ingen hämtning är tomt dirigeras parkerad part till parkeringslinjen.
Parkeringsövervakning vidarekopplar ingen hämtning vid intern mottagare	När parkerad part är en intern person vidarekopplas samtalet till angiven mottagare i parametern Parkeringsövervakning vidarekopplar ingen hämtning vid intern mottagare. Om fältvärdet för Parkeringsövervakning vidarekopplar ingen hämtning vid intern mottagare är tomt dirigeras parkerad part till parkeringslinjen.
Park Monitoring Reversion Timer	Den här parametern avgör hur många sekunder som Cisco Unified Communications Manager ska vänta innan användaren uppmanas att besvara ett samtal som han/hon har parkerat. Det här timern börjar när användaren trycker på Parkera på telefonen och en påminnelse utfärdas när timern upphör att gälla. Standard: 60 sekunder Om du konfigurerar ett annat värde än noll åsidosätter värdet för den här parametern som anges i fönstret Tjänsteparametrar. Men om du konfigurerar ett värde på 0 används värdet i fönstret Tjänsteparametrar.

Ställa in parkeringsövervakning för svarslistor

När ett samtal som har dirigerats via svarsgrupplistan är parkerat, används parametervärdet Hunt Pilot Park Monitoring Forward No Retrieve Destination (om det inte är tomt) när Park Monitoring Forward No Retrieve Timer löper ut.

Arbetsordning

-
- Steg 1** Öppna Cisco Unified Communications Manager Administration och välj **Samtalsroutning > Rutt/Målgrupp > Anropsnummer för svarsgrupp**.
- Steg 2** Ställ in parametern Hunt Pilot Park Monitoring Forward No Retrieve Destination.
- Om parametervärdet för Hunt Pilot Park Monitoring Forward No Retrieve Destination är tomt, vidarekopplas samtalet till den mottagare som har konfigurerats i fönstret Katalognummerkonfiguration när Park Monitoring Forward No Retrieve Timer löper ut.
-

Ställa in ljud- och videoportintervall

Ljud- och videotrafiken kan skickas till olika RTP-portintervaller för förbättrad Quality of Service (QoS). Följande fält anger portintervallen i Cisco Unified Communications Manager Administration:

- Ljudportar
 - Starta medieport (standard: 16384)
 - Stoppa medieport (standard: 32766)
- Videoportar
 - Starta videon (för att ställa in videostartporten).
 - Minst: 2048
 - Högst: 65535
 - Stoppa videon (för att ställa in videostoppporten).
 - Minst: 2048
 - Högst: 65535

Följande regler gäller när du konfigurerar fälten för videoport:

När Starta video-RTP-port och Stoppa video-RTP-port har konfigurerats använder telefonen portar inom videoportintervall för videotrafik. Ljudtrafiken använder medieportarna.

Om ljud- och videoportintervallen överlappar varandra, används de överlappande portarna för både ljud- och videotrafik. Om videoportintervallet inte har konfigurerats på rätt sätt, använder telefonen de konfigurerade ljudportarna för både ljud- och videotrafik.

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

Arbetsordning

- Steg 1** Öppna Cisco Unified Communications Manager Administration och välj **Enhet > Enhetsinställningar > SIP-profil**.
- Steg 2** Ange värden i fälten Starta medieport och Stoppa medieport för ljudportintervallet.
- Steg 3** Välj **Spara**.
- Steg 4** Välj ett av följande fönster:
- **System > Företagstelefonkonfiguration**
 - **Enhet > Enhetsinställningar > Allmän telefonprofil**
 - **Enhet > Enhetsinställningar > Telefonkonfiguration**
- Steg 5** Ställ in fälten Starta video-RTP-Port och Stoppa video-RTP-port med det portintervall som krävs.
- Följande regler gäller när du konfigurerar fälten för videoport:
- Värdet i fältet Stoppa video-RTP-port måste vara större än värdet i fältet Starta video-RTP-port.
 - Skillnaden mellan fälten Starta video-RTP-port och Stoppa video-RTP-port måste vara minst 16.

Steg 6 Välj **Spara**.**Relaterade ämnen**

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Konfigurera Cisco IP Manager Assistant

Cisco IPMA (Cisco IP Manager Assistant) hanterar samtalsroutning och innehåller andra funktioner som hjälper chefer och assistanter att hantera samtal effektivare.

IPMA-tjänsterna måste vara konfigurerade i Cisco Unified Communications Manager innan du kan använda dem. Mer information om hur du konfigurerar IPMA finns i *Handbok om konfiguration av funktioner i Cisco Unified Communications Manager*.

IPMA har tre viktiga komponenter:

Handläggare

En chef har samtal som fångas upp av tjänsten för samtalsroutning.

Assistent

En assistent hanterar samtal åt en chef.

Assistent Console

Assistent Console är ett datorprogram som assistanter kan använda för att utföra uppgifter och hantera de flesta funktionerna.

IPMA stöder två olika lägen: support för proxylinje och support för delad linje. Båda lägena stöder flera samtal per linje för chefen. Tjänsten IPMA har stöd för både proxylinje och stöd för delad linje i ett kluster.

I delad linje-läget delar chefen och assistenten ett katalognummer och samtal hanteras på den delade linjen. Både chefstelefonen och assistanttelefonen ringer när ett samtal tas emot på den delade linjen. Delad linje-läget har inte stöd för standardassistentval, assistantövervakning, samtalsfiltrering och vidarekoppling av alla samtal.

Om du konfigurerar Cisco IPMA i delad linje-läget så delar chefen och assistenten ett katalognummer, till exempel 1701. Sekreteraren hanterar samtal för en chef för det delade katalognumret. När en chef får ett samtal på katalognummer 1701 ringer både chefens och assistentens telefon.

Alla IPMA-funktionerna är inte tillgängliga i delad linje-läge, vilket inbegriper standardassistentval, assistantövervakning, samtalsfiltrering och vidarekoppling av alla samtal. En sekreterare kan inte se eller komma åt de här funktionerna i programmet Assistant Console. Assistentens telefon har inte någon programstyrd knapp för vidarekoppling av alla samtal. Chefens telefon saknar programstyrda knappar för assistantövervakning, samtalsinbrytning och vidarekoppling av alla samtal.

För att kunna använda stöd för delad linje på en användarenhet, måste du först använda Cisco Unified Communications Manager Administration för att konfigurera och starta tjänsten Cisco IP Manager Assistant.

I proxy-line-läget hanterar assistenten samtal åt en chef och använder ett proxynummer. Proxy-line-läge har stöd för alla IPMA-funktioner.

Om du konfigurerar Cisco IPMA i proxy-line-läget kan chefen och assistenten inte dela ett katalognummer. Sekreteraren hanterar chefens samtal med hjälp av ett proxynummer. Proxynumret är inte katalognumret för chefen. Det är ett alternativt nummer som har valts i systemet och kan användas av en assistent som hanterar chefens samtal. I proxy-line-läget har en chef och en assistent tillgång till alla funktioner i IPMA, inklusive standardassistentval, assistantövervakning, samtalsfiltrering och vidarekoppling av alla samtal.

För att kunna använda stöd för proxy-line på en användarenhet, måste du först använda Cisco Unified Communications Manager Administration för att konfigurera och starta tjänsten Cisco IP Manager Assistant.

Du får tillgång till IPMA-funktioner med programstyrda knappar och via telefontjänster. Mallen för programstyrda knappar är konfigurerad i Cisco Unified Communications Manager. IPMA har stöd för följande standardmallar för programstyrda knappar:

Standard Manager

Stöder administratör för proxyläget.

Standard Shared Mode Manager

Stöder administratör för delat läge.

Standard Assistant

Stöder assistant i proxyläge eller i delat läge.

I följande tabell beskrivs de programstyrda knappar som är tillgängliga i mallarna för programstyrda knappar.

Tabell 37. IPMA-programstyrda knappar

Programstyrd knapp	Samtalsstatus	Beskrivning
Omdirigera	Ringer, Ansluten, Väntkopplad	Vidarekoppling av valt samtal till ett förkonfigurerat mål.
Ta över	Alla lägen	Vidarekoppla ett samtal från assistantens telefon till chefens telefon och svara automatiskt.
Visa info.	Alla lägen	Visa status för samtal som hanterats av en assistant.
TransVM	Ringer, Ansluten, Väntkopplad	Vidarebefordra det markerade samtalet till chefens röstmeddelande.
Vidarekoppla alla	Alla lägen	Vidarekoppling av alla samtal som dirigeras till chefen till en förkonfigurerad mottagare.



OBS! Inbrytning, Visa info. och Vidarekoppla alla bör endast konfigureras för en chefstelefon i proxylinjeläget.

Nedan visas en översikt över de steg som krävs.

Arbetsordning

- Steg 1** Konfigurera telefoner och användare.
- Steg 2** Associera telefoner till användarna.
- Steg 3** Aktivera tjänsten Cisco IP Manager Assistant i fönstret för aktivering av tjänst.
- Steg 4** Konfigurera parametrar för systemadministration.

- Steg 5** Om det behövs kan du konfigurera parametrar för IPMA Clusterwide-tjänster.
- Steg 6** (Valfritt) Konfigurera användarens CAPF-profil
- Steg 7** (Valfritt) Konfigurera IPMA-serviceparametrar för säkerhet
- Steg 8** Stoppa och starta om IPMA-tjänsten.
- Steg 9** Konfigurera telefonparametern, chefs- och assistantinställningar, inklusive mallar för programstyrda knappar.
- Steg 10** Konfigurera programmet Cisco Unified Communications Manager Assistant.
- Steg 11** Konfigurera uppringningsregler.
- Steg 12** Installera programmet Assistant Console.
- Steg 13** Konfigurera programmen för chefs- och assistantkonsolen.

Konfigurera visuell inbox för röstbrevlåda

Visuell röstbrevlåda är konfigurerad för alla Cisco IP-telefoner eller till en enskild användare eller grupp av användare från Cisco Unified Communications Manager Administration.



OBS! Information om konfiguration finns i dokumentationen om Ciscos visuella inbox för röstbrevlåda på <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

Klienten för visuell inbox för röstbrevlåda stöds inte som en midlet på någon av Cisco IP-telefon 8800.

Arbetsordning

- Steg 1** Öppna Cisco Unified Communications Manager Administration och välj **Enhet > Enhetsinställningar > Telefontjänster**.
- Steg 2** Välj **Lägg till ny** så här skapar du en ny tjänst för visuell inbox för röstbrevlåda.
- Steg 3** Ange följande information i respektive fält i konfigurationsfönstret för IP-telefontjänst:
 - Tjänstnamn – ange **VisualVoiceMail**.
 - ASCII-tjänstnamn – ange **VisualVoiceMail**.
 - Tjänst-URL – ange som **program: Cisco/VisualVoiceMail**.
 - Tjänstkategori – välj **XML-tjänsten** i listrutan.
 - Tjänstetyp – välj **meddelanden** i listrutan.
- Steg 4** Markera **Aktivera** och klicka på **Spara**.

OBS! Se till att du inte markerar **Företagsabonnemang**.
- Steg 5** I fönstret Information om tjänsteparameter klickar du på **Ny parameter** och anger följande information i respektive fält:
 - Parameternamn. Ange voicemail_server.
 - Visningsnamn för parametern. Ange voicemail_server.
 - Standardvärde. Ange värde för den primära Unity-servern.
 - Parameterbeskrivning

- Steg 6** Markera **Parametern är obligatorisk** och klicka på **Spara**.
OBS! Se till att du inte markerar **Parametern är ett lösenord (maskinnehåll)**.
- Steg 7** Stäng fönstret och välj **Spara** igen i fönstret Telefonens tjänstekonfiguration.

Konfigurera visuell inbox för röstbrevlåda för en viss användare

Använd följande procedur för att konfigurera visuell inbox för röstbrevlåda för en specifik användare.



OBS! Information om konfiguration finns i dokumentationen om Ciscos visuella inbox för röstbrevlåda på <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

Arbetsordning

- Steg 1** Utgå från Cisco Unified Communications Manager Administration och välj **Enhet > Telefon**.
- Steg 2** Välj den enhet som är kopplad till den användare som du söker efter.
- Steg 3** Välj i listrutan Relaterade länkar **Prenumerera på eller avbryta prenumerationstjänster** och klicka på **Kör**.
- Steg 4** Välj den VisualVoiceMail-tjänst som du har skapat och välj sedan **Nästa > Prenumerera**.
-

Visuell inbox för röstbrevlåda för en användargrupp

Om du vill lägga till en grupp med Cisco IP-telefoner i Cisco Unified Communications Manager med den visuella inbox för röstbrevlåda som du prenumererar på, skapar du en telefonmall i BAT-verktyget för varje typ av telefon och i varje telefonmall. Du kan sedan prenumerera på tjänsten för visuell inbox för röstbrevlåda och använda mallen för att infoga telefonerna.

Om du redan har registrerat dina Cisco IP-telefoner och vill ha telefoner som prenumererar på tjänsten Visuell inbox för röstbrevlåda, skapar du en telefonmall i BAT, prenumererar på tjänsten Visuell inbox för röstbrevlåda i mallen och använder sedan BAT-verktyget för att uppdatera telefoner.

Mer information finns i <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

Säkra SIP-tjänster

AS-SIP (Assured Services SIP) är en samling funktioner och protokoll som ger ett mycket säkert samtalsflöde för Cisco IP-telefoner och telefoner från tredje part. Följande funktioner benämns gemensamt som AS-SIP:

- Prioritet och förtur på flera nivåer (MLPP)
- DSCP (Differentiated Services Code Point)
- TLS (Transport Layer Security) och SRTP (Secure Real-time Transport Protocol)

- IPv6 (Internet Protocol version 6)

AS-SIP används ofta med MLPP (Multilevel Precedence and Preemption) för att prioritera samtal i en nödsituation. Med MLPP tilldelar du prioritetsnivå för utgående samtal, från 1 (låg) till 5 (hög). När du tar emot ett samtal visas en ikon för prioriterat samtal och nivån på telefonen.

Om du vill konfigurera AS-SIP gör du följande i Cisco Unified Communications Manager:

- Konfigurera en sammanfattningsanvändare – konfigurera användaren för att använda sammanfattad autentisering vid SIP-begäranden.
- Konfigurera säker port för SIP-telefon – Cisco Unified Communications Manager använder denna port för att avlyssna SIP-telefoner för SIP-linjeregistreringar över TLS.
- Starta om tjänsterna – när du har konfigurerat en säker port, startar du om Cisco Unified Communications Manager- och Cisco CTL-providertjänster. Konfigurera SIP-profil för AS-SIP-konfigurera en SIP-profil med SIP-inställningar för dina AS-SIP-slutpunkter och för SIP-trunkar. Telefonspecifika parametrar hämtas inte till AS-SIP-telefoner från tredje part. De används endast av Cisco Unified Manager. Telefoner från tredje part måste lokalt konfigurera samma inställningar.
- Konfigurera profil för telefonsäkerhet för AS-SIP – du kan använda telefonsäkerhetsprofilen för att tilldela säkerhetsinställningar, till exempel TLS, SRTP och digest-autentisering.
- Konfigurera AS-SIP-slutpunkt – konfigurera en Cisco IP-telefon eller en slutpunkt från tredje part med AS-SIP-support.
- Associera enheten med slutlig användning – koppla ändpunkten till en användare.
- Konfigurera säkerhetsprofil för SIP-trunk för AS-SIP – du kan använda säkerhetsprofilen för SIP om du vill tilldela säkerhetsfunktioner som till exempel TLS eller digest-autentisering.
- Konfigurera SIP-trunk för AS-SIP – konfigurera en SIP-trunk med AS-SIP-support.
- Konfigurera AS-SIP-funktioner – konfigurera ytterligare AS-SIP-funktioner som MLPP, TLS, V.150 och IPv6.

Mer information om hur du konfigurerar AS-SIP finns i kapitlet Configure AS-SIP Endpoints i *System Configuration Guide for Cisco Unified Communications Manager*.

Migration av din telefon till en multiplattformstelefon direkt

Du kan enkelt migrera din företagstelefon 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

Prioritet och förtur på flera nivåer (MLPP)

Med MLPP (Multilevel Precedence and Preemption) kan du prioritera samtal vid nödsituationer. Du tilldelar en prioritet till dina utgående samtal som sträcker sig från 1 till 5. Inkommande samtal visar en ikon som visar samtalsprioriteten. Autentiserade användare kan gå före samtal antingen till riktade stationer eller via fullständigt prenumererade TDM-trunkar.

Den här funktionen säkerställer kommunikationen för personer i ledande ställning gentemot viktiga organisationer och personal.

MLPP används ofta med AS-SIP (Assured Services SIP). Mer information om hur du konfigurerar MLPP finns i kapitlet ”Configure Multilevel Precedence and Preemption” i *Systemkonfigurationshandbok för Cisco Unified Communications Manager*.

Konfigurera mall för programstyrda knappar

Med Cisco Unified Communications Manager Administration kan du associera upp till 18 programstyrda knappar med program som stöds av telefonen. Cisco Unified Communications Manager har stöd för funktionsknappmallar för standardanvändare och för standardfunktioner.

Ett program som stöder programstyrda knappar har en eller flera mallar för programstyrda knappar som ingår. Du kan ändra standardmallen för programstyrda knappar genom att kopiera den, byta namn på den och sedan uppdatera den nya mallen. Du kan även ändra en knappmall för funktioner som inte är standard.

Kontrollparametern för programstyrda knappar visar om programstyrda knappar på en telefon styrs av funktionen Mall för programstyrda knappar. Kontrollparametern för programstyrda knappar är ett obligatoriskt fält.

Mer information om hur du konfigurerar den här funktionen finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

Cisco IP-telefon har inte stöd för alla programstyrda knappar som kan konfigureras i Konfiguration av mall för programstyrda knappar i Cisco Unified Communications Manager Administration. I Cisco Unified Communications Manager kan du aktivera eller inaktivera vissa programstyrda knappar i konfigurationsinställningarna för policykontroll. I följande tabell visas de funktioner och programstyrda knappar som kan konfigureras i en mall för programstyrda knappar och anger om detta stöds i Cisco IP-telefon.



OBS! Med Cisco Unified Communications Manager kan du konfigurera alla funktionsknappar i en funktionsknappmall, men funktionsknappar som inte stöds visas inte i telefonen.

Tabell 38. Konfigurerbara programstyrda knappar

Funktion	Konfigurerbara programstyrda knappar i konfigurationen för mall för programstyrda knappar	Stöds som programstyrd knapp
Svara	Svara (Answer)	Stöds
Ring igen	Återuppringning (CallBack)	Stöds
Vidarebefordra alla samtal	Vidarekoppla alla (cfwdAll)	Stöds
Parkera samtal	Parkera samtal (Park)	Stöds
Hämta samtal	Samtal besvaras (Pickup)	Stöds
Bryt in	Bryt in	Stöds

Funktion	Konfigurerbara programstyrda knappar i konfigurationen för mall för programstyrda knappar	Stöds som programstyrd knapp
BrytInKf	Conference Barge	Stöds
Konferens	Konferens (Confrn)	Stöds
Konferenslista	Konferenslista (ConfList)	Stöds
vidarekoppla	Omedelbar röstmeddel.(OmRstmedd)	Stöds
Stör ej	Växla Stör ej (DND)	Stöds
Avsluta samtal	Avsluta samtal (EndCall)	Stöds
Hämta gruppsamtal	Grupphämtning (GPickUp)	Stöds
Parkera	Parkera (Hold)	Stöds
Svarsgrupp	HLogg (HLog)	Stöds
Delta	Koppling (Join)	Stöds inte
Spårning	Växla identifiering av störande samtal (MCID)	Stöds
Meet me	Möte (MeetMe)	Stöds
Mobile Connect	Mobilitet (Mobility)	Stöds
Nytt samtal	Nytt samtal (NewCall)	Stöds
Hämta annan	Nästa samtal (oPickup)	Stöds
PLK-stöd för köstatistik	Köstatus	Stöds inte
Kvalitetsrapporteringsverktyg (QRT)	Kvalitetsrapporterings- verktyg (QRT)	Stöds
Ring igen	Återuppringning (Redial)	Stöds
Ta bort senaste konferensdeltagare	Ta bort senaste konferensdeltagare (Remove)	Stöds inte
Återuppta	Åter (Resume)	Stöds
Markera	Välj (Select)	Stöds inte
Snabbval	Kortnummer (AbbrDial)	Stöds
Överföra	Överför (Trfr)	Stöds
Video Mode Command	Videolägeskommando (VidMode)	Stöds inte

Arbetsordning

- Steg 1** Gå till Cisco Unified Communications Manager Administration och välj ett av följande fönster:
- Om du vill konfigurera mallar för programstyrda knappar väljer du **Enhet > Enhetsinställningar > Mall för programstyrda knappar**.
 - Om du vill tilldela en mall för programstyrda knappar till en telefon väljer du **Enhet > Telefon** och konfigurerar fältet Mall för programstyrda knappar.
- Steg 2** Spara ändringarna.

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Mallar för telefonknappar

Med telefonknappsmallar kan du tilldela kortnummer och samtalshanteringsfunktioner till programmerbara knappar. Samtalshanteringsfunktioner som kan tilldelas till knappar är Svar, Mobilitet och Alla samtal.

Ändra helst mallarna innan du registrera telefoner i nätverket. På detta sätt kan du få tillgång till anpassade telefonknappsmallalternativ från Cisco Unified Communications Manager vid registreringen.

Ändra mall för telefonknappar

Mer information om IP-telefontjänster och konfiguration av linjeknappar finns i dokumentationen om din utgåva av Cisco Unified Communications Manager.

Arbetsordning

- Steg 1** Använd Cisco Unified Communications Manager Administration och välj **Enhet > Enhetsinställningar > Telefonknappsmall**.
- Steg 2** Klicka på **Sök**.
- Steg 3** Välj telefonmodell.
- Steg 4** Välj **Kopiera**, ange ett namn på den nya mallen och välj sedan **Spara**.
Fönstret Konfiguration av telefonknappsmall öppnas.
- Steg 5** Identifiera den knapp som du vill tilldela och välj **Tjänst-URL** i listrutan Funktioner för tillhörande linje.
- Steg 6** Välj **Spara** så skapas en ny telefonknappsmall för tjänst-URL:n.
- Steg 7** Välj **Enhet > Telefon** och öppna fönstret Telefonkonfiguration för telefonen.
- Steg 8** Välj den nya telefonknappsmallen i listrutan Telefonknappsmall.
- Steg 9** Välj **Spara** så lagras ändringen och välj sedan **Använd konfig** så införs ändringen.

Telefonanvändaren kan nu få tillgång till självbetjäningssportalen och kan associera tjänsten med en knapp på telefonen.

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Tilldela telefonknappmallen för alla samtal

Tilldela en knapp för alla samtal i telefonmallen för användare med flera delade linjer.

När du konfigurerar en knapp för alla samtal på telefonen kan användare använda knappen Alla samtal till följande:

- Visa en konsoliderad lista över aktuella samtal från alla linjer på telefonen.
- Visa en lista över alla missade samtal från alla linjer på telefonen (under samtalshistorik).
- Ringa ett samtal på användarens primära linje när användaren lyfter luren. Som standard placeras Alla samtal till användarens primära linjen vid utgående samtal.

Arbetsordning

Steg 1 Ändra telefonknappmallen om du vill använda knappen Alla samtal.

Steg 2 Tilldela mallen till telefonen.

Konfigurera adressboken eller kortnummer som IP-telefontjänst

Du kan ändra en telefonknappmall för att associera en tjänst webbadress med en programmerbar knapp. Om du gör det ger användarna en enda knapp tillgång till adressboken och kortnummer. Innan du ändrar telefonknappmallen måste du konfigurera adressboken eller kortnummer som en IP-telefon. Mer information finns i dokumentationen till din utgåva av Cisco Unified Communications Manager.

För att konfigurera adressboken eller kortnummer som en IP-telefon tjänst (om den inte redan är en tjänst), så här:

Arbetsordning

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

Find och lista IP-telefontjänster skyltfönster.

Steg 2 Klicka på **Lägg till nytt**.

IP Phone Services konfigurations skyltfönster.

Steg 3 Ange följande inställningar:

- Tjänstenamn: Ange **Personlig adressbok**.
- Tjänstebeskrivning: Ange en beskrivning av tjänsten.
- Tjänst-URL
För PAB, ange följande URL:
http://<Unified CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab
För kortnummer, ange följande URL:
http://<Unified-CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd
- Säker tjänst-URL
För PAB, ange följande URL:
https://<Unified CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab
För kortnummer, ange följande URL:
https://<Unified-CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd
- Tjänstekategori: Välj **XML-tjänst**.
- Tjänstetyp: Välj **Kataloger**.
- Aktivera: Markera kryssrutan.
http://<IP_address> or https://<IP_address> (beror på protokollet som Cisco IP-telefon stöder.)

Steg 4 Välj **Spara**.

OBS! Om du ändrar tjänstens URL, tar bort en IP-telefons tjänstparameter eller ändrar namnet på en telefontjänstparameter för en telefontjänst som användarna prenumererar på måste du klicka på **Uppdatera prenumerationer** för att uppdatera alla närvarande tecknade användare med ändringarna. Annars måste användarna börja om sin prenumeration på tjänsten för att skapa en rätt webbadress.

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Ändra telefonknappmallen för adressboken eller kortnummer

Du kan ändra en telefonknappmall för att associera en tjänst webbadress med en programmerbar knapp. Om du gör det ger användarna en enda knapp tillgång till adressboken och kortnummer. Innan du ändrar telefonknappmallen måste du konfigurera adressboken eller kortnummer som en IP-telefon.

Mer information om IP-telefontjänster och konfiguration av linjeknappar finns i dokumentationen om din utgåva av Cisco Unified Communications Manager.

Arbetsordning

- Steg 1** Använd Cisco Unified Communications Manager Administration och välj **Enhet > Enhetsinställningar > Telefonknappsmall**.
- Steg 2** Klicka på **Sök**.
- Steg 3** Välj telefonmodell.
- Steg 4** Välj **Kopiera**, ange ett namn på den nya mallen och välj sedan **Spara**.
Fönstret Konfiguration av telefonknappsmall öppnas.
- Steg 5** Identifiera den knapp som du vill tilldela och välj **Tjänst-URL** i listrutan Funktioner för tillhörande linje.
- Steg 6** Välj **Spara** så skapas en ny telefonknappsmall för tjänst-URL:n.
- Steg 7** Välj **Enhet > Telefon** och öppna fönstret Telefonkonfiguration för telefonen.
- Steg 8** Välj den nya telefonknappsmallen i listrutan Telefonknappsmall.
- Steg 9** Välj **Spara** så lagras ändringen och välj sedan **Använd konfig** så införs ändringen.
Telefonanvändaren kan nu få tillgång till självbetjäningsportalen och kan associera tjänsten med en knapp på telefonen.

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

VPN-konfiguration

Funktionen Cisco VPN hjälper dig att bibehålla nätverkets säkerhet och ge användare en säker och tillförlitlig metod för att ansluta till företagets nätverk. Använd den här funktionen när:

- En telefon finns utanför ett betrott nätverk
- Nätverkstrafiken mellan telefon och Cisco Unified Communications Manager löper över ett nätverk som inte är betrott

Det finns tre vanliga metoder för att autentisera klienter via en VPN-anslutning:

- Digitala certifikat
- Lösenord
- Användarnamn och lösenord

Varje metod har fördelar. Men om företagets säkerhetspolicy tillåter rekommenderar vi en certifikatbaserad metod eftersom certifikat ger en smidig inloggning utan några åtgärder från användaren. Både LSC- och MIC-certifikat stöds.

Om du vill konfigurera en VPN-funktion måste du först etablera enheten lokalt och sedan kan du distribuera enheten utanför kontoret.

Mer information om certifieringsautentisering och VPN-nätverk finns under det tekniska meddelandet *AnyConnect VPN Phone with Certificate Authentication on an ASA Configuration Example*. Webbadressen

till det här dokumentet är

<http://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html>

Med en lösenords- eller användarnamn och lösenordsbaserad metod uppmanas användaren att ange inloggningsuppgifter. Ange inloggningsuppgifterna enligt företagets säkerhetspolicy. Du kan även konfigurera inställningen för att aktivera beständigt lösenord så att användarens lösenord sparas på telefonen. Användarens lösenord sparas tills antingen ett misslyckat inloggningsförsök inträffar, användaren rensar lösenordet manuellt eller telefonen återställs eller blir utan ström.

En annan användbart verktyg är inställningen Aktivera automatisk nätverksidentifiering. När du markerar den här kryssrutan kan VPN-klienten bara köras när programmet känner av att det är utanför företagets nätverk. Den här inställningen är inaktiverad som standard.

Telefonen stöder Cisco SVC IP Phone klientversion 1.0 som klienttyp.

Ytterligare information om underhåll, konfigurering och användning av ett virtuellt privat nätverk med VPN finns i *Säkerhetshandboken till Cisco Unified Communications Manager* under kapitlet Konfigurera VPN-nätverk. Webbadressen till det här dokumentet är

<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

Cisco VPN-funktionen använder SSL (Secure Sockets Layer) för att bibehålla nätverkssäkerhet.



OBS! Ange inställningen för alternativ TFTP-server när du konfigurerar en telefon för distansarbete för SSL VPN till ASA med inbyggd klient.

Ställa in ytterligare linjeknappar

Aktivera Förbättrat linjeläge för att använda knapparna på båda sidorna om telefonskärmen som linjeknappar. Aviseringar om prognostiserad uppringning och inkommande samtal med åtgärder aktiveras som standard i förbättrat linjeläge.

Innan du börjar

Du måste skapa en ny, anpassad telefonknappsmall.

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 **Linjeläge** till **Förbättrat linjeläge**.
 - Steg 4** Gå till området Enhetsinformation och ställ in fältet **Telefonknappsmall** till en anpassad mall.
 - Steg 5** Välj **Använd konfig**.
 - Steg 6** Välj **Spara**.
 - Steg 7** Starta om telefonen.

Relaterade ämnen

[Miljö för sessionslinjeläge](#), på sidan 158

Funktioner som är tillgängliga i förbättrat linjeläge

Förbättrat linjeläge (ELM) kan användas med Mobil åtkomst och fjärråtkomst genom Expressway.

ELM kan också användas med en övergångslinje, en samtalsroutningskonfigurationen där samtal vidarebefordras till en annan delad linje om den första delade linjen är upptagen. Om ELM används tillsammans med en övergångslinje konsolideras senaste samtal på delade linjer under ett enda katalognummer. Mer information om övergångslinjer finns i *Konfigurationshandbok för funktioner i Cisco Unified Communications Manager* för Cisco Unified Communications Manager version 12.0 (1) eller senare.

ELM har stöd för de flesta men inte alla funktioner. Aktivering av en funktion innebär inte att den används. Läs följande tabell för att bekräfta att en funktion stöds.

Tabell 39. Funktioner som stöds och Förbättrat linjeläge

Funktion	Stöds	Version av den fasta programvaran
Svara	Ja	11.5 (1) och senare
Svara på samtal automatiskt	Ja	11.5 (1) och senare
Bryt in/BrytInKf	Ja	11.5 (1) och senare
Parkering av dirigerat samtal med BLF	Ja	12.0 (1) och senare
Bluetooth Smartphone-integrering	Nej	-
Bluetooth-USB-headset	Ja	11.5 (1) och senare
Ring igen	Ja	11.5 (1) och senare
Övervakare	Nej	-
Vidarebefordra alla samtal	Ja	11.5 (1) och senare
Parkera samtal	Ja	12.0 (1) och senare
Samtalsparkering linjestatus	Ja	12.0 (1) och senare
Hämta samtal	Ja	11.5 (1) och senare
Hämta samtal linjestatus	Ja	11.5 (1) och senare
Vidarebefordra alla samtal på flera linjer	Ja	11.5 (1) och senare
Cisco Extension Mobility-tvärkluster	Ja	12.0 (1) och senare har stöd för den här funktionen.
Cisco IP Manager Assistant (IPMA)	Nej	-
Cisco Unified Communications Manager Express	Nej	-

Funktion	Stöds	Version av den fasta programvaran
Konferens	Ja	11.5 (1) och senare
CTI (Computer Telephony Integration)-program	Ja	11.5 (1) och senare
Neka	Ja	11.5 (1) och senare
Enhetsanropad inspelning	Ja	11.5 (1) SR1 och senare
Stör ej	Ja	11.5 (1) och senare
Förbättrad SRST	Nej	-
Anknytningsmobilitet	Ja	11.5 (1) och senare
Hämta gruppsamtal	Ja	12.0 (1) och senare har stöd för den här funktionen.
Parkera	Ja	11.5 (1) och senare
Svarsgrupper	Ja.	12.0 (1) och senare
Varning vid inkommande samtal med konfigurerbar timer	Nej	-
Snabbtelefon	Ja	11.5 (1) och senare
Knappexpansionsmodul	Expansionsmodulen för Cisco IP-telefon 8851/8861 och expansionsmodulen för Cisco IP-telefon 8865 stöder förbättrat linjeläge	12.0 (1) och senare
SpårID	Ja	11.5 (1) och senare
Meet me	Ja	11.5 (1) och senare
Mobile Connect	Ja	11.5 (1) och senare
Prioritet och förtur på flera nivåer (MLPP)	Nej	-
Ljud av	Ja	11.5 (1) och senare
Hämta annan	Ja	12.0 (1) och senare
Support för köstatus med programmerbar linjeknapp	Ja	11.5 (1) och senare
Funktionen Privat	Ja	11.5 (1) och senare
Köstatus	Ja	11.5 (1) och senare

Funktion	Stöds	Version av den fasta programvaran
Kvalitetsrapporterings- verktyg (QRT)	Ja	11.5 (1) och senare
Stöd för språk som läses från höger till vänster	Nej	-
Ring igen	Ja	11.5 (1) och senare
Tyst övervakning och inspelning	Ja	11.5 (1) SR1 och senare
Snabbval	Ja	11.5 (1) och senare
SRST (Survivable Remote Site Telephony)	Ja	11.5 (1) och senare
Överföra	Ja	11.5 (1) och senare
Samtal med URI (Uniform Resource Identifier)	Ja	11.5 (1) och senare
Videosamtal	Ja	11.5 (1) och senare
Visuell röstbrevlåda	Ja	11.5 (1) och senare
Röstbrevlåda	Ja	11.5 (1) och senare

Relaterade ämnen

[Miljö för sessionslinjeläge](#), på sidan 158

Ställa in timer för TLS-återupptagande

Genom återupptagning av TLS-session kan en TLS-session återupptas utan att behöva upprepa hela TLS-autentiseringsprocessen. Det kan avsevärt minska den tid det tar för TLS-anslutningen att utbyta data.

Även om telefonerna har stöd för TLS-sessioner, har inte alla TLS-sessioner stöd för TLS-återupptagande. I följande lista beskrivs de olika sessionerna med stöd för TLS-återupptagande:

- TLS-session för SIP-signalering: stöder återupptagning
- HTTPs-klienten: stöder återupptagning
- CAPF: stöder återupptagning
- TVS: stöder återupptagning
- EAP-TLS: stöder inte återupptagning
- EAP-FAST: stöder inte återupptagning
- VPN-klient: stöder inte återupptagning

Mer information finns 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** Ställ in parametern Timer för TLS-återupptagande.
Intervall för timern är 0 till 3 600 sek. Standardvärdet är 3 600. Om fältet anges som 0 är återupptagning av TLS-sessionen inaktiverad.
-

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Aktivera intelligenta närhetstjänster



OBS! Den här proceduren gäller endast för Bluetooth-aktiverade telefoner. Cisco IP-telefon 8811, 8841, 8851NR och 8865NR stöder inte Bluetooth.

Med intelligenta närhetstjänster kan du dra nytta av telefonens akustiska egenskaper med mobilenheten eller surfplattan. Användaren parkopplar den mobila enheten eller surfplattan till telefonen via Bluetooth.

När den mobila enheten är parkopplad kan användaren ringa och ta emot mobilsamtal på telefonen. Med hjälp av en surfplatta kan användaren dirigera ljudet från surfplattan till telefonen.

Användare kan parkoppla flera mobila enheter, surfplattor och ett Bluetooth-headset till telefonen. Men bara en enhet och ett headset kan anslutas samtidigt.

Arbetsordning

- Steg 1** Utgå från Cisco Unified Communications Manager Administration och välj **Telefon > Enhet**
- Steg 2** Gå till telefonen som du vill ändra.
- Steg 3** Leta reda på fältet Bluetooth och ställ in fältet på **Aktiverad**.
- Steg 4** Leta reda på fältet Tillåta Bluetooth-mobila Handsfree-läge och ställ in fältet på **Aktiverad**.
- Steg 5** Spara ändringarna och använd dem på telefonen.
-

Ställa in upplösning för videosändning

Cisco IP-telefon 8845, 8865 och 8865NR stöder videosamtal följande format:

- 720p (1280 x 720)
- WVGA(800x480)
- 360p (640 x 360)

- 240p (432 x 240)
- VGA (640 x 480)
- CIF (352 x 288)
- SIF (352 x 240)
- QCIF (176 x 144)

Cisco IP-telefon med videokapacitet balanserar bästa upplösning för bandbredd baserat på telefonkonfiguration eller begränsad upplösning. Exempel: Vid ett direkt 88 x 5- till 88 x 5-samtal sänder inte telefonerna 720p, de sänder 800 x 480. Denna begränsning beror enbart på 5-tums WVGA-skärmutlösningen på 88 x 5 som blir 800 x 480.

Typ av video	Videoupplösning	Bilddrutor per sekund (fps)	Bitshastighetsintervall för video
720p	1280 x 720	30	1360 – 2500 kbps
720p	1280 x 720	15	790 – 1359 kbps
WVGA	800 x 480	30	660 – 789 kbps
WVGA	800 x 480	15	350 – 399 kbps
360p	640 x 360	30	400 – 659 kbps
360p	640 x 360	15	210 – 349 kbps
240p	432 x 240	30	180 – 209 kbps
240p	432 x 240	15	64 – 179 kbps
VGA	640 x 480	30	520 – 1500 kbps
VGA	640 x 480	15	280 – 519 kbps
CIF	352 x 288	30	200 – 279 kbps
CIF	352 x 288	15	120 – 199 kbps
SIF	352 x 240	30	200 – 279 kbps
SIF	352 x 240	15	120 – 199 kbps
QCIF	176 x 144	30	94 – 119 kbps
QCIF	176 x 144	15	64 – 93 kbps

Headsethantering på äldre versioner av Cisco Unified Communications Manager

Om du har en version av Cisco Unified Communications Manager äldre än 12.5 (1) SU1 kan du fjärrkonfigurera Ciscos inställningar för headset för användning med lokala telefoner.

Konfigurationen av fjärrheadset på Cisco Unified Communications Manager version 10.5 (2), 11.0 (1), 11.5 (1), 12.0 (1) och 12.5 (1) kräver att du hämtar en fil från webbplatsen med [Ciscos programvaruhämtningar](#), redigerar filen och sedan överför filen på Cisco Unified Communications Manager TFTP-server. Filen är en JSON-fil (JavaScript Object Notification). Den uppdaterade headsetkonfigurationen tillämpas för företagsheadset under ett tidsintervall om 10 till 30 minuter för att förhindra kvarvarande uppgifter i TFTP-servern.



OBS! Du kan hantera och konfigurera headset med hjälp av Cisco Unified Communications Manager Administration version 11.5 (1) SU7.

Observera följande när du arbetar med JSON-filen:

- Inställningarna tillämpas inte om en eller flera hakparenteser saknas i koden. Kontrollera formatet med hjälp av ett onlineverktyg som JSON Formatter.
- Ange inställningen för **updatedTime** till den aktuella epoch-tiden, annars tillämpas inte konfigurationen. Alternativt kan du öka värdet för **updatedTime** med +1 så att det är större än i den tidigare versionen.
- Ändra inte namnet på parametern, då tillämpas inte inställningen.

Mer information om TFTP-tjänsten finns i kapitlet ”Manage Device Firmware” (Hantera fast programvara för enheter) i *administrationsguiden för Cisco Unified Communications Manager IM och Presence Service*.

Uppgradera telefonerna till den senaste versionen av den fasta programvaran innan du installerar filen `defaultheadsetconfig.json`. I följande tabell beskrivs de standardinställningar som du kan justera med JSON-filen.

Ladda ned standardkonfigurationsfilen för headset

Innan du fjärrkonfigurerar parametrarna för headset måste du ladda ned den senaste exempel-JSON-filen (JavaScript Object Notation).

Arbetsordning

- Steg 1** Gå till följande URL: <https://software.cisco.com/download/home/286320550>.
- Steg 2** Välj **Headset i 500-serien**.
- Steg 3** Välj headset-serie.
- Steg 4** Välj en mapp att ladda ner till och välj zip-filen.
- Steg 5** Klicka på **Hämta** eller **Lägg till i varukorg** och följ instruktionerna.

Steg 6 Zippa upp filen till en katalog på datorn.

Och sedan då?

[Ändra standardkonfigurationsfilen för headset, på sidan 200](#)

Ändra standardkonfigurationsfilen för headset

Observera följande när du arbetar med JSON-filen (JavaScript Object Notation):

- Inställningarna tillämpas inte om en eller flera hakparenteser saknas i koden. Kontrollera formatet med hjälp av ett onlineverktyg som JSON Formatter.
- Ange inställningen ”**updatedAtTime**” till den aktuella epoch-tiden, annars tillämpas inte konfigurationen.
- Bekräfta att **firmwareName** är det senaste, annars tillämpas inte konfigurationen.
- Ändra inte namnet på någon parameter, då tillämpas inte inställningarna.

Arbetsordning

Steg 1 Öppna filen `defaultheadsetconfig.json` med en textredigerare.

Steg 2 Redigera **updatedAtTime** och de värden för headsetparametrar som du vill ändra.

En exempelskript visas nedan. Detta skript tillhandahålls endast som referens. Använd det som vägledning när du konfigurerar dina headsetparametrar. Använd den JSON-fil som följde med din fasta programvara.

```
{
  "headsetConfig": {
    "templateConfiguration": {
      "configTemplateVersion": "1",
      "updatedAtTime": 1537299896,
      "reportId": 3,
      "modelSpecificSettings": [
        {
          "modelSeries": "530",
          "models": [
            "520",
            "521",
            "522",
            "530",
            "531",
            "532"
          ],
          "modelFirmware": [
            {
              "firmwareName": "LATEST",
              "latest": true,
              "firmwareParams": [
                {
                  "name": "Speaker Volume",
                  "access": "Both",
                  "usageId": 32,
                  "value": 7
                },
                {

```



```

        "name": "Microphone Gain",
        "access": "Both",
        "usageId": 33,
        "value": 2
    },
    {
        "name": "Sidetone",
        "access": "Both",
        "usageId": 34,
        "value": 1
    },
    {
        "name": "Equalizer",
        "access": "Both",
        "usageId": 35,
        "value": 3
    }
]
}
},
{
    "modelSeries": "560",
    "models": [
        "560",
        "561",
        "562"
    ],
    "modelFirmware": [
        {
            "firmwareName": "LATEST",
            "latest": true,
            "firmwareParams": [
                {
                    "name": "Speaker Volume",
                    "access": "Both",
                    "usageId": 32,
                    "value": 7
                },
                {
                    "name": "Microphone Gain",
                    "access": "Both",
                    "usageId": 33,
                    "value": 2
                },
                {
                    "name": "Sidetone",
                    "access": "Both",
                    "usageId": 34,
                    "value": 1
                },
                {
                    "name": "Equalizer",
                    "access": "Both",
                    "usageId": 35,
                    "value": 3
                },
                {
                    "name": "Audio Bandwidth",
                    "access": "Admin",
                    "usageId": 36,
                    "value": 0
                }
            ]
        }
    ]
}
}

```

```

        "name": "Bluetooth",
        "access": "Admin",
        "usageId": 39,
        "value": 0
    },
    {
        "name": "DECT Radio Range",
        "access": "Admin",
        "usageId": 37,
        "value": 0
    }
    {
        "name": "Conference",
        "access": "Admin",
        "usageId": 41,
        "value": 0
    }
    ]
    }
    ]
    }
    }
}

```

Steg 3 Spara defaultheadsetconfig.json.

Och sedan då?

Installera standardkonfigurationsfilen.

Installera standardkonfigurationsfilen på Cisco Unified Communications Manager

När du har redigerat filen defaultheadsetconfig.json installerar du den i Cisco Unified Communications Manager med TFTP filhanteringsverktyg.

Arbetsordning

- Steg 1** Från Cisco Unified OS Administration väljer du **Programvaruuppggraderingar > TFTP filhantering**.
 - Steg 2** Välj **Överför fil**.
 - Steg 3** Välj **Välj fil** och navigera till filen defaultheadsetconfig.json.
 - Steg 4** Välj **Överför fil**.
 - Steg 5** Klicka på **Stäng**.
-

Starta om Cisco TFTP-server

När du har överfört filen `defaultheadsetconfig.json` till TFTP-katalogen startar du om Cisco TFTP-server och återställer telefonerna. Efter cirka 10–15 minuter börjar hämtningsprocessen och de nya konfigurationerna tillämpas på headseten. Det tar ytterligare 10–30 minuter innan inställningarna verkställs.

Arbetsordning

- Steg 1** Logga in till Cisco Unified Serviceability och välj **Verktyg > Kontrollcenter – Funktionstjänster**.
 - Steg 2** I listrutan **Server** väljer du den server som Cisco TFTP-tjänst körs på.
 - Steg 3** Klicka på radioknappen som motsvarar tjänsten **Cisco TFTP**.
 - Steg 4** Klicka på **Starta om**.
-



KAPITEL 10

Företagskatalog och den personliga katalogen

- [Inställning av företagskatalog, på sidan 205](#)
- [Inställning av personlig katalog, på sidan 205](#)
- [Inställning av användarens personliga telefonkatalog, på sidan 206](#)

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.

Cisco IP-telefon använder dynamisk fördelning för SecureApp på både klient och servrar. Detta säkerställer att din telefon kan läsa certifikat som är större än 4 kB och ger färre antal värden hittades inte-felmeddelanden när en användare försöker öppna sin katalog.

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 xv

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
- Verktyg för adressbokssynkronisering (TABSynch)

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 självbetjäningssportalen i Cisco Unified Communications.
- Från Cisco IP-telefonen – välj **Kontakter** för att söka i företagskatalogen eller användarens personliga katalog.
- Från ett Microsoft Windows-program – användare kan använda TABSynch-verktyget för att synkronisera sina PAB:ar med adressboken i Microsoft Windows (WAB). Kunder som vill använda adressboken i Microsoft Outlook (OAB) bör börja med att importera data från OAB till WAB. TabSync kan sedan användas för att synkronisera WAB med den personliga katalogen. Instruktioner om TABSync finns i [Hämta Cisco IP-telefon synkroniserade adressbok, på sidan 206](#) och [Ställ in synkronisering, på sidan 207](#).

Cisco IP-telefon använder dynamisk fördelning för SecureApp på både klient och servrar. Detta säkerställer att din telefon kan läsa certifikat som är större än 4 kB och ger färre antal värden hittades inte-felmeddelanden när en användare försöker öppna sin katalog.

För att säkerställa att användarna av Cisco IP-telefon adressbokssynkronisering endast får åtkomst till sina slutanvändardata kan du aktivera Cisco UXL Web Service i Cisco Unified Serviceability.

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

Inställning av användarens personliga telefonkatalog

Användare kan konfigurera personliga katalogposter i Cisco IP-telefon. För att konfigurera en personlig katalog måste användaren ha åtkomst till följande:

- Självbetjäningssportalen: Se till att användarna vet hur de får åtkomst till sin självbetjäningssportal. Mer information finns i [Konfigurera användaråtkomst till självbetjäningssportalen, på sidan 79](#).
- Adressbokssynkronisering i Cisco IP-telefon: Se till att distribuera installationsprogrammet till användarna. Se [Hämta Cisco IP-telefon synkroniserade adressbok, på sidan 206](#).



OBS! Synkronisering av Cisco IP-telefon adressbok stöds enbart för Windows-versioner som inte stöds (exempelvis Windows XP och tidigare). Verktöget stöds inte i nyare versioner av Windows. Framgent kommer den att tas bort från plugin-listan i Cisco Unified Communications Manager.

Hämta Cisco IP-telefon synkroniserade adressbok

Om du vill hämta en kopia av synkroniseringsprogrammet och skicka till dina användare gör du så här:

Arbetsordning

- Steg 1** Om du vill hämta installationsprogrammet väljer du **Program > Plugin-program** från Cisco Unified Communications Manager Administration.

- Steg 2** Välj **Hämta** intill plugin-programmet i Cisco IP-telefon synkroniserade adressbok.
- Steg 3** När dialogrutan Filhämtning visas väljer du **Spara**.
- Steg 4** Skicka TabSyncInstall.exe-filen och instruktionerna i [Användning av Cisco IP-telefon synkroniserade adressbok, på sidan 207](#) för alla användare som behöver detta program.
-

Användning av Cisco IP-telefon synkroniserade adressbok

Cisco IP-telefon adressbokssynkroniseringsverktyg synkroniserar data som lagras i din adressbok i Microsoft Windows med Cisco Unified Communications Manager-katalogen och den personliga adressboken i självbetjäningssportalen.



- Tips** För att lyckas synkronisera Windows-adressboken med den personliga adressboken bör alla Windows-adressboksanvändare matas in i Windows-adressboken innan du utför följande procedurer.
-

Installera synkroniseringsprogrammet

För att installera Cisco IP-telefon adressbokssynkronisering gör du så här:

Arbetsordning

- Steg 1** Be att få installationsfilen för Cisco IP-telefon adressbokssynkronisering från systemadministratören.
- Steg 2** Dubbelklicka på TabSyncInstall.exe fil som administratören tillhandahåller.
- Steg 3** Välj **Kör**.
- Steg 4** Välj **Nästa**.
- Steg 5** Läs licensavtalet information och välj **Jag accepterar**. Välj **Nästa**.
- Steg 6** Välj i vilken katalog du vill installera programmet och klicka på **Nästa**.
- Steg 7** Välj **Installera**.
- Steg 8** Välj **Slutför**.
- Steg 9** Slutför processen genom att följa stegen i [Ställ in synkronisering, på sidan 207](#).
-

Ställ in synkronisering

Om du vill konfigurera Cisco IP-telefon synkroniseringsverktyg för adressboken gör du så här:

Arbetsordning

- Steg 1** Öppna Cisco IP-telefon synkroniseringsverktyg för adressboken.
- Om du accepterade standardinstallationskatalogen kan du öppna programmet genom att välja **Start > Alla program > Cisco Systems > TabSync**.
- Steg 2** Om du vill konfigurera användarinformation väljer du **Användare**.

- Steg 3** Ange Cisco IP-telefon användarnamn och lösenord och välj **OK**.
- Steg 4** Om du vill konfigurera Cisco Unified Communications Manager serverinformation väljer du **Server**.
- Steg 5** Ange IP-adress eller värddomän och portnummer för Cisco Unified Communications Manager-servern och välj **OK**.
- Om du inte har denna information kontaktar du systemadministratören.
- Steg 6** Om du vill starta katalogsynkroniseringsprocessen väljer du **Synkronisera**.
- Synkroniseringsstatusfönstret visar status på adressbokssynkroniseringen. Om du valde regeln ”user intervention for duplicate entries” och du har dubblade adressboksposter, visas fönstret Duplicate Selection.
- Steg 7** Välj den post som du vill inkludera i din personliga adressbok och välj **OK**.
- Steg 8** När synkroniseringen är klar väljer du **Avsluta** för att stänga Cisco Unified Callmanagers synkronisering av adressboken.
- Steg 9** Om du vill kontrollera om synkroniseringen fungerade loggar du in i självbetjäningssportalen och väljer **Personlig adressbok**. Användarna från Windows adressbok ska listas.
-



DEL **IV**

Felsökning för Cisco IP-telefon

- [Övervakning av telefonsystem, på sidan 211](#)
- [Felsökning, på sidan 245](#)
- [Underhåll, på sidan 263](#)
- [Internationell användarsupport, på sidan 269](#)



KAPITEL 11

Övervakning av telefonsystem

- [Status på Cisco IP-telefonen, på sidan 211](#)
- [Webbsidan för Cisco IP-telefon, på sidan 226](#)
- [Begära information från telefonen i XML, på sidan 241](#)

Status på Cisco IP-telefonen

I det här avsnittet beskrivs hur du visar modellinformation, statusmeddelanden och nätverksstatistik på Cisco IP-telefon i 8800-serien.

- **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.

Mer information om felsökning finns i [Felsökning, på sidan 245](#).

Visa telefoninformationsfönstret

Om du vill visa skärmen Modellinformation gör du så här:

Arbetsordning

- Steg 1** Tryck på **Program** .
- Steg 2** Välj **Telefoninformation**.

Om användaren är ansluten till en säker eller autentiserad server visas en motsvarande ikon (lås eller certifikat) på telefoninformationsskärmen till höger om serveralternativet. Om användaren inte är ansluten till en säker eller autentiserad server visas ingen ikon.

Steg 3 Om du vill avsluta skärmen Modellinformation trycker du på **Avsluta**.

Fälten för telefoninformation

I följande tabell beskrivs inställningarna för telefoninformation.

Tabell 40. Inställningar för telefoninformation

Alternativ	Beskrivning
Modellnummer	Modellnummer på telefonen.
IPv4-adress	Telefonens IP-adress.
Värddamn	Telefonens värddamn.
Aktiv laddning	Version av den fasta programvaran installerad på telefonen. Användaren kan trycka på Detaljer för mer information.
Inaktiv laddning	Inaktiv belastning visas bara när en hämtning pågår. En hämtningsikon och statusen ”Uppgradering pågår” eller ”Uppgradering misslyckades” visas också. Om en användare trycker på Detaljer under en uppdatering visas filnamnet och komponenterna som hämtas. En ny avbildning för inbyggd programvara kan anges att hämtas i förväg i ett fönster för underhåll. I stället för att vänta på att alla telefoner ska hämta den inbyggda programvaran växlar systemet snabbare mellan återställningen av befintlig programvara till inaktiv status och installation av ny programvara. När hämtningen är klar ändras ikonen för att ange slutförd status. En bock visas vid en lyckad hämtning och ett ”X” visas vid en misslyckad hämtning. Om det är möjligt fortsätter resten av programvaran att laddas ned.
Senaste uppdatering	Datum för senaste uppdatering av den fasta programvaran.
Aktiv server	Domännamnet för den server där telefonen är registrerad.
Standby-server	Domännamnet för standby-servern.

Visa statusmenyn


Menyn Status innehåller följande alternativ, som ger information om telefonen och telefonåtgärder:

- Statusmeddelanden: Visar skärmen Statusmeddelanden som visar en logg över viktiga systemmeddelanden.
- Ethernet-statistik: Visar skärmen Ethernet-statistik som visar statistik över Ethernet-trafik.
- Trådlös statistik: Visar skärmen Trådlös statistik om det behövs.
- Samtalsstatistik: Visar räknare och statistik för det aktuella samtalet.

- Aktuell åtkomstpunkt: Visar skärmen Aktuell åtkomstpunkt, om tillämpligt.

Så här visar du menyn Status:


Arbetsordning

-
- Steg 1** Om du vill visa statusmenyn trycker du på **Program** .
- Steg 2** Välj **Admin.inställningar > Status**.
- Steg 3** Om du vill avsluta menyn Status trycker du på **Avsluta**.
-

Visa fönstret Statusmeddelanden

I fönstret Statusmeddelanden visas de 30 senaste statusmeddelanden som telefonen har genererat. Du kan öppna den här skärmen när som helst, även om telefonen inte är klar med startprocessen.

Arbetsordning

-
- Steg 1** Tryck på **Program** .
- Steg 2** Välj **Admin.inställningar > Status > Statusmeddelanden**.
- Steg 3** Du kan ta bort aktuella statusmeddelanden genom att trycka på **Rensa**.
- Steg 4** Om du vill avsluta skärmen Statusmeddelanden trycker du på **Avsluta**.
-

Statusmeddelandefält

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

Tabell 41. Statusmeddelanden på Cisco Unified IP-telefon

Meddelande	Beskrivning	Möjlig förklaring och åtgärd
Fel: TFTP CFG storlek	Konfigurationsfilen är för stor för filsystemet på telefonen.	Slå av telefonen.
CRC-fel	Den hämtade programfilen är skadad.	Skaffa en ny kopia av telefonen placera den i TFTPPath-katalog i den här katalogen när TFTP-s avstängd. Annars kan filerna sl
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 IP-adress är tillgänglig för tele
CTL och ITL installerade	CTL- och ITL-filerna har installerats på telefonen.	Ingen. Detta meddelande är en CTL-filen eller ITL-filen har in
CTL installerad	En CTL-fil med listan över betrodda adresser för certifikat har installerats på telefonen.	Ingen. Detta meddelande är en CTL-filen har inte installerats t

Meddelande	Beskrivning	Möjlig förklaring och åtgärd
CTL-uppdateringen misslyckades	Telefonen kunde inte uppdatera CTL-filen med betrodda adresser för certifikat.	Problem med CTL-filen på TFTP-
DHCP-timeout	DHCP-servern svarade inte.	Nätverket är upptaget: Felen bör lösa sig när nätet minskar. Ingen nätverksanslutning mellan DHCP-servern och telefonen: Kontrollera nätverksanslutningen. DHCP-servern är nere: Kontrollera DHCP-servern. Fel kvarstår: Överväg att tilldela en
DNS-timeout	DNS-servern svarade inte.	Nätverket är upptaget: Felen bör lösa sig när nätet minskar. Ingen nätverksanslutning mellan DHCP-servern och telefonen: Kontrollera nätverksanslutningen. DNS-servern är nere: Kontrollera DNS-servern.
DNS: Okänd värd	DNS kunde inte lösa namnet på TFTP-servern eller Cisco Unified Communications Manager.	Kontrollera att värdnamn för TFTP-servern eller Cisco Unified Communications Manager finns i DNS. Överväg att använda IP-adresser i
Duplicerad IP	En annan enhet använder den IP-adress som är tilldelad till telefonen.	Om telefonen har en statisk IP-adress och inte har tilldelat en dubblätt av IP-adresser. Om du använder DHCP ska du kontrollera DHCP-serverkonfigurationen.
Raderar CTL- och ITL-filer	Raderar CTL- och ITL-filer	Ingen. Detta meddelande är endast
Fel vid uppdatering av språk	En eller flera lokaliseringsfiler kunde inte hittas i TFTP-sökvägs katalogen eller är inte giltiga. Språket har inte ändrats.	Gå till Cisco Unified Operating System Administration och kontrollera att följande filer ligger i språk Management: <ul style="list-style-type: none"> • De finns i katalogen med sammanlagt för nätverket: <ul style="list-style-type: none"> • tones.xml • De finns i katalogen med sammanlagt för användaren: <ul style="list-style-type: none"> • glyphs.xml • dictionary.xml • kate.xml

Meddelande	Beskrivning	Möjlig förklaring och åtgärd
Hittar inte filen <Cfg File>	Den namnbaserade filen och standardkonfigurationsfilen fanns inte på TFTP-servern.	<p>Konfigurationsfilen för en telefon finns inte tillgänglig i Cisco Unified Communications Manager-databasen genererar TFTP-servern ett felmeddelande om att CFG-filen saknas.</p> <ul style="list-style-type: none"> • Telefonen är inte registrerad i Cisco Unified Communications Manager. Du måste manuellt lägga till telefonen i Cisco Unified Communications Manager för att möjliggöra automatisk registrering av telefonen. För mer information finns i Telefontilläggsmetoder. • Om du använder DHCP som konfigurationsmetod, DHCP-servern pekar på rätt server för att hämta konfigurationen av TFTP-servern. • Om du använder statiska konfigurationer, kontrollera att konfigurationen av TFTP-servern är korrekt.
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 fortfarande registreras i Cisco Unified Communications Manager.
IP-adress släppt	Telefonen är konfigurerad för att släppa IP-adressen.	Telefonen fortsätter vara inaktiva tills du återställer DHCP-adressen.
ITL installerad	ITL-filen är installerad i telefonen.	Ingen. Detta meddelande är endast synligt om ITL-filen har inte installerats tidigare.
Ladda förkastad HC	Programmet som hämtades är inte kompatibelt med telefonens maskinvara.	<p>Detta inträffar om du försöker ladda programvaran på den här telefonen med maskinvaruförändringar.</p> <p>Kontrollera det last-ID som tilldelats till telefonen (Cisco Unified Communications Manager Telefon). Registrera om lasten om det är nödvändigt.</p>
Ingen standardrouter	DHCP eller den statiska konfigurationen anger inte en standardrouter.	<p>Om telefonen har en statisk IP-konfiguration, standardroutern är konfigurerad i konfigurationen.</p> <p>Om du använder DHCP, har DHCP-servern konfigurerat en standardrouter. Kontrollera DHCP-servern.</p>
Ingen IP för DNS-server	Ett namn angavs men DHCP eller den statiska IP-konfigurationen anger inte en DNS-serveradress.	<p>Om telefonen har en statisk IP-konfiguration, DNS-servern är konfigurerad i konfigurationen.</p> <p>Om du använder DHCP, har DHCP-servern konfigurerat en DNS-server. Kontrollera DHCP-servern.</p>
Ingen lista med pålitliga adresser installerad	CTL-filen eller ITL-filen är inte installerade på telefonen.	Listan över betrodda är inte konfigurerad i Cisco Unified Communications Manager, som är standard.
Telefonen gick inte att registrera. Certnyckelstorleken är inte FIPS-kompatibel.	FIPS kräver att servercertifikat RSA är 2048 bitar eller mer.	Uppdatera certifikatet.

Meddelande	Beskrivning	Möjlig förklaring och åtgärd
Omstart begärd av Cisco Unified Communications Manager	Telefonen startar om på grund av en begäran från Cisco Unified Communications Manager.	Konfigurationsändringar har troligen gjorts i Cisco Unified Communications Manager. Kontrollera att ändringarna är valda så att ändringarna införs.
TFTP-åtkomstfel	TFTP-servern pekar på en katalog som inte finns.	Om du använder DHCP ska du kontrollera att servern pekar på rätt TFTP-server. Om du använder statiska IP-adresser ska du kontrollera konfigurationen av TFTP-servern.
TFTP-fel	Telefonen känner inte igen en felkod som TFTP-servern har angett.	Kontakta Cisco TAC.
TFTP: Timeout	TFTP-servern svarade inte.	Nätverket är upptaget: Felen bör lösa sig när nätet minskar. Ingen nätverksanslutning mellan telefon och TFTP-servern: Kontrollera nätverksanslutningen. TFTP-servern är nere: Kontrollera statusen för TFTP-servern.
Tidsgränsen överskreds	Försök med supplikant för 802.1X-transaktionen men tidsgränsen nåddes eftersom en autentisering saknades.	Autentiseringens tidsgräns nås typiskt om 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 gick att uppdatera nya CTL- och ITL-filer. Möjliga orsaker till underkännandet: <ul style="list-style-type: none"> • Ett nätverksfel inträffade. • TFTP-servern var nere. • Den nya säkerhetstoken som definierades i CTL-filen och TFTP-certifikatet som signerar ITL-filen har införts, men de aktuella CTL- och ITL-filer i telefonen är fortfarande giltiga. • Internt telefonfel inträffade. Möjliga lösningar: <ul style="list-style-type: none"> • Kontrollera nätverksanslutningen. • Kontrollera om TFTP-servern svarar normalt. • Om TVS-servern stöds i Cisco Unified Communications Manager kontrollera om TVS-servern är aktiv och fungerar normalt. • Kontrollera om säkerhetstoken är giltiga. Ta bort CTL- och ITL-filer manuellt om lösningarna misslyckas och återställ telefonen.
Lista med pålitliga adresser uppdaterad	CTL- eller ITL-filen eller båda filerna uppdateras.	Ingen. Detta meddelande är endast ett varningsskript.

Meddelande	Beskrivning	Möjlig förklaring och åtgärd
Versionsfel	Namnet på telefonens inläsningsfil är fel.	Se till att telefonens lastfil har
XmlDefault.cnf.xml eller .cnf.xml som motsvarar telefonens enhetsnamn	Namn på konfigurationsfilen.	Ingen. Detta meddelande anger konfigurationsfilen för telefon

Relaterade ämnen


[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Visa skärmen Nätverksinformation

Använd informationen som visas på nätverksinfoskärmen för att lösa anslutningsproblem på en telefon.

Ett meddelande visas på telefonen om en användare har problem med att ansluta till ett telefonnätverk.

Arbetsordning


-
- Steg 1** Om du vill visa statusmenyn trycker du på **Program** .
 - Steg 2** Välj **Admin.inställningar > Status > Statusmeddelanden**.
 - Steg 3** Välj **Nätverksinfo**.
 - Steg 4** Om du vill avsluta Nätverksinfo trycker du på **Avsluta**.
-

Visa skärmen Nätverksstatistik

Skärmen Nätverksstatistik visar information om telefon- och nätverksprestanda.

Om du vill visa skärmen Nätverksstatistik gör du så här:

Arbetsordning

-
- Steg 1** Tryck på **programknappen** .
 - Steg 2** Välj **Admin.inställningar>Status>Nätverksstatistik**.
 - Steg 3** Om du vill återställa statistiken för Rx-ramar, Tx-ramar och Rx Broadcasts till 0 trycker du på **Rensa**.
 - Steg 4** Avsluta skärmen Ethernet-statistik genom att trycka på **Avsluta**.
-

Ethernet-information om samtalsstatistik

Följande tabell beskriver informationen på skärmen med Ethernet-statistik.

Tabell 42. Ethernet-information om samtalsstatistik

Objekt	Beskrivning
Rx Frames	Antal paket som telefonen har mottagit.

Objekt	Beskrivning
Tx Frames	Antalet paket som telefonen har skickat.
Rx Broadcasts	Antal sändningspaket som telefonen har tagit emot.
Orsak till omstart	Orsak till senaste återställningen av telefonen. Anger ett av följande värden: <ul style="list-style-type: none"> • Initialized • TCP-timeout • CCM-avsl-TCP-anst • TCP-Bad-ACK • CM-reset-TCP • CM-aborted-TCP • CM-NAKed • KeepaliveTO • Failback • Phone-Keypad • Återställ telefon-IP • Reset-Reset • Reset-Restart • Phone-Reg-Rej • Programvara förkastad HC • CM-ICMP-Onåbar • Telefon-Avbryt
Förfluten tid	Mängden tid som förflutit sedan telefonen senast startades om.
Port 1	Länktillstånd och anslutning av nätverksport. Till exempel Auto 100 Mb Full-Duplex innebär att nätverksporten är i ett länkat tillstånd och har autobalanserat en anslutning med full duplex och 100 Mbps.
Port 2	Länktillstånd och anslutning av PC-port.
DHCP-status (IPv4/IPv6)	<ul style="list-style-type: none"> • Visar endast DHCPv4-status, till exempel DHCP BOUND, i endast IPv4-läge. • Visar endast DHCPv6-status, till exempel ROUTER ADVERTISE, i IPv6-läge. • Information om DHCPv6-läge visas.

Följande tabeller beskrivs de meddelanden som visas för DHCPv4- och DHCPv6-status.

Tabell 43. Ethernet-meddelanden om DHCPv4-statistik

DHCPv4-status	Beskrivning
CDP INIT	CDP är inte bundet eller WLAN är inte i tjänst
DHCP BOUND	DHCPv4 är bundet

DHCPv4-status	Beskrivning
DHCP DISABLED	DHCPv4 är inaktiverat
DHCP INIT	DHCPv4 är initierat
DHCP INVALID	DHCPv4 är ogiltigt. Det här är första status
DHCP RENEWING	DHCPv4 förnyas
DHCP REBINDING	DHCPv4 binds om
DHCP REBOOT	DHCPv4 är initierat vid omstart
DHCP REQUESTING	DHCPv4 skickar begäran
DHCP RESYNC	DHCPv4 är omsynkroniserat
DHCP WAITING COLDBOOT TIMEOUT	DHCPv4 startar
DHCP UNRECOGNIZED	Okänd DHCPv4-status
DISABLED DUPLICATE IP	Duplicerad IPv4-adress
DHCP TIMEOUT	DHCPv4-timeout
IPV4 STACK TURNED OFF	Telefonen är i endast IPv6-läget med IPv4-stacken avstängd
ILLEGAL IPV4 STATE	Ogiltig IPv4-status och bör inte inträffa

Tabell 44. Ethernet-meddelanden om DHCPv6-statistik

DHCPv6-status	Beskrivning
CDP INIT	CDP initieras
DHCP6 BOUND	DHCPv6 är bundet
DHCP6 DISABLED	DHCPv6 är inaktiverat
DHCP6 RENEW	DHCPv6 förnyas
DHCP6 REBIND	DHCPv6 binds om
DHCP6-INIT	DHCPv6 initieras
DHCP6 SOLICIT	DHCPv6 ber
DHCP6 REQUEST	DHCPv6 skickar begäran
DHCP6 RELEASING	DHCPv6 frisläpper
DHCP6 RELEASED	DHCPv6 är frisläppt
DHCP6 DISABLING	DHCPv6 inaktiverar


DHCPv6-status	Beskrivning
DHCP6 DECLINING	DHCPv6 avvisar
DHCP6 DECLINED	DHCPv6 är avvisad
DHCP6 INFOREQ	DHCPv6 är INFOREQ
DHCP6 INFOREQ DONE	DHCPv6 är INFOREQ DONE
DHCP6 INVALID	DHCPv6 är ogiltigt. Det här är första status
DISABLED DUPLICATE IPV6	DHCP6 är inaktiverat, men duplicerad IPv6 har upptäckts
DHCP6 DECLINED DUPLICATE IP	DHCP6 is DECLINED -- DUPLICATE IPV6 DETECTED
ROUTER ADVERTISE., (DUPLICATE IP)	Duplicerad automatiskt konfigurerad IPv6-adress
DHCP6 WAITING COLDBOOT TIMEOUT	DHCPv6 startar
DHCP6 TIMEOUT USING RESTORED VAL	DHCPv6-timeout, med hjälp av sparat värdet i flashminne
DHCP6 TIMEOUT CANNOT RESTORE	DHCP6-timeout och det finns ingen säkerhetskopiering i flashminne
IPV6 STACK TURNED OFF	Telefonen är i endast IPv4-läget med IPv6-stacken avstängd
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY	IPv6-adress är inte från router eller DHCPv6-server
ILLEGAL IPV6 STATE	Ogiltig IPv6-status och bör inte inträffa

Visa skärmen Trådlös statistik

Den här proceduren avser endast trådlös Cisco IP-telefon 8861.

Om du vill visa skärmen Trådlös statistik gör du så här:

Arbetsordning

-
- Steg 1** Tryck på **Program** .
 - Steg 2** Välj **Admin.inställningar>Status > Trådlös statistik**.
 - Steg 3** Om du vill nollställa statistiken för trådlöst trycker du på **Rensa**.
 - Steg 4** Avsluta skärmen Trådlös statistik genom att trycka på **Avsluta**.
-

WLAN-statistik

I följande tabell beskrivs WLAN-statistik på telefonen.

Tabell 45. WLAN-statistik på Cisco Unified IP-telefon

Objekt	Beskrivning
tx-byte	Antal byte som telefonen har överfört.
rx-byte	Antal byte som telefonen har mottagit.
tx-paket	Antal paket som telefonen har överfört.
rx-paket	Antal paket som telefonen har mottagit.
tx-paket tappade	Antalet paket som tagits bort under överföringen.
rx-paket tappade	Antalet paket som tagits bort under mottagningen.
Fel i tx-paket	Antalet felaktiga paket som telefonen överfört.
Fel i rx-paket	Antalet felaktiga paket som telefonen mottagit.
Tx-ramar	Antal överförda MSDU.
tx multicast-ramar	Antalet överförda multicast-MSDU.
tx-omförsök	Antalet MSDU som har överförts efter en eller flera återöverföringar.
tx flera omförsök	Antalet multicast-MSDU som har överförts efter en eller flera återöverföringar.
tx-fel	Antalet MSDU som inte har överförts på grund av att antalet överföringsförsök överskrider gränsen för omförsök.
rts lyckades	Räknaren skall ökas när en CTS tas emot som svar på en RTS.
rts-fel	Räknaren skall ökas när en CTS inte tas emot som svar på en RTS.
ack-fel	Räknaren skall ökar när en ACK inte tas emot som förväntat.
rx-dubblade ramar	Antalet mottagna ramar som sekvenskontrollfältet identifierar som en dubblett.
rx-fragmenterade paket	Antalet mottagna MPDU av typen Data eller Management.
roaming-beräkning	Antal utförda roaming.

Visa fönstret Samtalsstatistik


Du kan visa skärmen Samtalsstatistik på telefonen om du vill se räknare, statistik och röstkvalitetsmått på det senaste samtalet.



OBS! Du kan också fjärrvisa information om samtalsstatistik genom att använda en webbläsare för att få tillgång till webbsidan med strömmande statistik. Den här webbsidan innehåller ytterligare RTCP-statistik som inte är tillgänglig i telefonen.

Ett enda samtal kan använda flera röstströmmar, men data samlas endast in för den sista röstströmmen. En röstström är en paketström mellan två ändpunkter. Om en ändpunkt parkeras, stannar röstströmmen även om samtalet fortfarande är anslutet. När samtalet återupptas startar en ny röstpaketström och nya samtalsdata skriver över tidigare samtalsdata.

Arbetsordning

- Steg 1** Tryck på **programknappen** .
- Steg 2** Välj **Admin.inställningar > Status > Samtalsstatistik**.
- Steg 3** Avsluta skärmen Samtalsstatistik genom att trycka på **Avsluta**.

Samtalsstatistikfält

I följande tabell beskrivs alternativen på Samtalsstatistikskärmen.

Tabell 46. Objekt i samtalsstatistiken för Cisco Unified Phone

Objekt	Beskrivning
Mottagarcodec	Typ av mottagen röstström (RTP-strömmande ljud från codec): <ul style="list-style-type: none"> • G.729 • G.722 • G722.2 AMR-WB • G.711 mu-law • G.711 A-law • iLBC • Opus • iSAC

Objekt	Beskrivning
Avsändarcodec	Typ av överförd röstström (RTP-strömmande ljud från codec): <ul style="list-style-type: none"> • G.729 • G.722 • G722.2 AMR-WB • G.711 mu-law • G.711 A-law • iLBC. • Opus • iSAC
Mottagarstorlek	Storlek på röstpaket, i millisekunder, i den mottagande röstströmmen (RTP strömmande ljud).
Avsändarstorlek	Storlek på röstpaket, i millisekunder, i den sändande röstströmmen.
Mottagarpaket	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.
Mottagarens förlorade paket	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.

Objekt	Beskrivning
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.
Dolda sekunder	Antal sekunder som har dolda händelser (förlorade ramar) från början av röstströmmen (med allvarligt dolda sekunder).
Strikt dolda sekunder	Antal sekunder som har mer än 5 procent dolda händelser (förlorade ramar) från början av röstströmmen.
Fördröjning	Uppskattning av nätverkssatens, uttryckt i millisekunder. Representerar ett löpande medelvärde av rundtursfördröjningen som mätts upp när RTCP-mottagarrapportblocken togs emot.

Visa fönstret Aktuell åtkomstpunkt

Skärmen Aktuell åtkomstpunkt visar statistik om åtkomstpunkten som en Cisco IP-telefon 8861 använder för trådlös kommunikation.

Arbetsordning

-
- Steg 1** Tryck på **programknappen** .
 - Steg 2** Välj **Admin.inställningar > Status > Aktuell åtkomstpunkt**.
 - Steg 3** Om du vill lämna skärmen Aktuell åtkomstpunkt trycker du på **Avsluta**.
-

Aktuella fält för åtkomstpunkter

I följande tabell beskrivs fälten på skärmen Aktuell åtkomstpunkt.

Tabell 47. Objekt för aktuell åtkomstpunkt

Objekt	Beskrivning
Namn på åtkomstpunkt	Namn på åtkomstpunkten, om den är CCX-kompatibel; i annat fall visas MAC-adress här.
MAC-adress	Åtkomstpunktens MAC-adress.
Frequency (Frekvens)	Senaste frekvens där den här åtkomstpunkten observerats.
Aktuell kanal	Senaste kanal där den här åtkomstpunkten observerats.
Senaste RSSI	Den senaste RSSI som den här åtkomstpunkten observerats.
Signalintervall	Antal tidsenheter mellan signalerna. En tidsenhet är 1,024 millisekunder.

Objekt	Beskrivning
Möjlighet	Det här fältet innehåller ett antal delfält som används för att ange begärda eller annonserade valfria funktioner.
Grundläggande hastigheter	Datahastigheter som krävs av åtkomstpunkten och åtkomstpunkten där stationen måste kunna fungera.
Tillägghastigheter	Datahastigheter som stöds av åtkomstpunkten och åtkomstpunkten som är tillgänglig som tillval för den relevanta stationen.
VHT(rx)-hastigheter som stöds	RX MCS-set som stöds av VHT och mottogs från åtkomstpunkten.
VHT(tx)-hastigheter som stöds	TX MCS-set som stöds av VHT och mottogs från åtkomstpunkten.
HT MCS som stöds	MCS-set som stöds av HT och mottogs från åtkomstpunkten.
DTIM-period	Var x:e signal är en dtim-period. Efter varje DTIM-signal skickar åtkomstpunkten alla broadcast- eller multicast-paket som ligger i kö i enheter i energisparläge.
Landsnummer	En tvåställig landskod. Landsinformationen kanske inte visas om landets informationsdel inte finns i signalen.
Kanaler	En lista över kompatibla kanaler (från landets informationsdelar).
Strömbegränsning	Mängden energi som maximal sändningsström bör minskas från gränsvärdet för regleringsdomän.
Strömgräns	Maximal sändningsström i dBm som tillåts för den kanalen.
Kanalanvändning	Procentandel tid, som normalt är 255, där åtkomstpunkten har upptäckt att mediet var upptaget, vilket indikeras av den fysiska eller virtuella operatörens avkänningsmekanism.
Antal stationer	Det totala antalet STA:er som för närvarande är associerade med den här åtkomstpunkten.
Åtkomstkapacitet	Ett ej tilldelat heltal som anger återstående mängd medietid tillgänglig genom explicit åtkomstkontroll i enheter om 32 mikrosekunder per sekund. Om värdet är 0 saknar åtkomstpunkten stöd för informationselementet och kapaciteten är okänd.
WMM stöds	Stöd för Wi-Fi-multimedieanknytningar.
UAPSD stöds	Åtkomstpunkten har stöd för Unscheduled Automatic Power Save Delivery. Kanske endast finns tillgängligt om WMM stöds. Den här funktionen är nödvändig för samtalstid och maximal samtalsdensitet på den trådlösa IP-telefonen.
Proxy-ARP	CCX-kompatibel åtkomstpunkt stöder IP ARP-förfrågningar åt den associerade stationen. Den här funktionen är nödvändig för standby-tid på den trådlösa IP-telefonen.

Objekt	Beskrivning
CCX-version	Om åtkomstpunkten är CCX-kompatibel visar det här fältet CCX-version.
Värde för pengarna	Innehåller information om kön Bästa försök.
Bakgrund	Innehåller information om kön Bakgrund.
Video	Innehåller information om kön Video.
Röst	Innehåller information om kön Röst.

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 som ger en mängd olika strömningsstatistik.
- System: Visar en hyperlänk som startar om telefonen.

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

För åtkomst av webbsidan för en telefon gör du så här:



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:
- 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**.
 - På Cisco IP-telefon trycker du på **Program** , väljer **Admin.inställningar > Nätverksinställning > Ethernet-inställning > IPv4-inställning** och bläddrar sedan till fältet IP-adress.
- Steg 2** Öppna en webbläsare och ange följande URL, där *IP_address* är IP-adressen till Cisco IP-telefon:

`http://IP_address`

Enhetsinfo

Området Enhetsinformation på en telefonwebbsida visar enhetsinställningar och relaterad information om telefonen. Följande tabell beskriver dessa poster.



OBS! Några av punkterna i nedanstående tabell gäller inte för alla telefonmodeller.

Om du vill visa området **Enhetsinformation** öppnar du webbsidan för telefonen enligt [Åtkomst till webbsidan för telefonen, på sidan 226](#) och klickar sedan på hyperlänken **Enhetsinformation**.

Tabell 48. Alternativ i området Enhetsinformation

Objekt	Beskrivning
Tjänsteläge	Telefonens tjänsteläge.
Service namn	Domän för tjänsten.
Tjänstetillstånd	Aktuell status på tjänsten.
MAC-adress	MAC-adress till telefonen.
Värddamn	Unikt, fast namn som tilldelas automatiskt till telefonen baserat på MAC-adressen.
Telefonnummer	Katalognummer som tilldelats till telefonen.
Programvaru-ID	Programmets firmware-version som körs i telefonen.
Bootladdnings-ID	Starta firmware-version.
Version	ID på den fasta programvaran som körs i telefonen.
Knappexpansionsmodul 1	ID för den första expansionsmodulen, om tillämpligt. Detta gäller Cisco IP-telefon 8851, 8851NR, 8861, 8865 och 8865NR.
Knappexpansionsmodul 2	ID för den andra expansionsmodulen, om tillämpligt. Detta gäller Cisco IP-telefon 8851, 8851NR, 8861, 8865 och 8865NR.
Knappexpansionsmodul 3	ID för den tredje expansionsmodulen, om tillämpligt. Detta gäller Cisco IP-telefon 8851, 8851NR, 8861, 8865 och 8865NR.
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.

Objekt	Beskrivning
UDI	<p>Visar följande UDI-information (Cisco Unique Device Identifier) om telefonen:</p> <ul style="list-style-type: none"> • Enhetstyp: Anger typen av maskinvara. Till exempel telefonskärmar för alla telefonmodeller. • Enhetsbeskrivning: Visar namn på den telefon som associeras med den angivna modelltypen. • Produkt-ID: Anger telefonmodellen. • Versions-ID (VID) – Anger det större versionsnumret för maskinvaran. • Serienummer: Visar det unika serienumret på telefonen.
Knappexpansionsmodul UDI	<p>Cisco UDI (Uniquw Device Identifier) för expansionsmodulen. Detta gäller Cisco IP-telefon 8851, 8851NR, 8861, 8865 och 8865NR.</p>
Headsetets namn	<p>Visar namnet på anslutet Cisco-headset i den vänstra kolumnen. Den högra kolumnen innehåller följande information:</p> <ul style="list-style-type: none"> • Port – visar hur headsetet ansluter till telefonen. <ul style="list-style-type: none"> • USB • AUX • Version – visar version av fast programvara på headset. • Radioområde – visar styrkan som konfigurerats för DECT-radion. Gäller enbart Cisco-headset i 560-serien. • Bandbredd – visar om headsetet använder bredband eller smalband. Gäller enbart Cisco-headset i 560-serien. • Bluetooth – visar om Bluetooth är aktiverat eller inaktiverat. Gäller enbart Cisco-headset i 560-serien. • Konferens – visar om konferensfunktionen är aktiverad eller inaktiverad. Gäller enbart Cisco-headset i 560-serien. • Källa för fast programvara – Visar tillåten uppgraderingsmetod för fast programvara: <ul style="list-style-type: none"> • Begränsa till enbart UCM • Tillåt från UCM eller Cisco-molnet <p>Gäller enbart Cisco-headset i 560-serien.</p>
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.

Objekt	Beskrivning
Datum	Datum i datum/tid-gruppen som telefonen tillhör. Denna information kommer från Cisco Unified Communications Manager.
Ledigt systemminne	Mängden ledigt minne på telefonen
Ledigt Java-heapminne	Mängden ledigt internminne för Java-heapen
Ledigt Java-poolminne	Mängden ledigt internminne för Java-poolen
FIPS-läge aktiverat	Anger om FIPS-läge (Federal Information Processing Standard) har aktiverats.

Ställa in nätverk

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.



OBS! Några av punkterna i nedanstående tabell gäller inte för alla telefonmodeller.

Om du vill visa området **Nätverksinställning** öppnar du webbsidan för telefonen som beskrivs i [Åtkomst till webbsidan för telefonen, på sidan 226](#) och klickar sedan på hyperlänken **Nätverksinställning**.

Tabell 49. Alternativ i området Nätverksinställning

Objekt	Beskrivning
MAC-adress	MAC-adress till telefonen.
Värddnamn	Värddnamn 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	IPv4-adress till telefonen.
Nätmask	Nätmask som telefonen använder.
Standardrouter	Standardrouter som telefonen använder.
DNS-server 1-3	Primär DNS-server (DNS-server 1) och valfria DNS-reservservrar (DNS-server 2 och 3) som används.
Alt. TFTP	Anger om telefonen använder en alternativ TFTP-server.

Objekt	Beskrivning
TFTP-server 1	Primär TFTP-server som telefonen använder.
TFTP-server 2	TFTP-reservserver som telefonen använder.
DHCP-adressen släppt	Anger inställningen för alternativet rReleased i DHCP-adressen på telefonmenyn Nätverkskonfiguration.
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.
CUCM server1–5	<p>Värdsnamn eller IP-adresser, i prioriterad ordning, för Cisco Unified Communications Manager som telefonen kan registrera. Ett alternativ kan också visa IP-adressen för en SRST-router som begränsad Cisco Unified Communications Manager-funktion, om en sådan router är tillgänglig.</p> <p>För en tillgänglig server visar ett alternativ Cisco Unified Communications Manager-servrens namn och ett av följande tillstånd:</p> <ul style="list-style-type: none"> • Aktivt: Cisco Unified Communications Manager-server där telefonen för närvarande använder samtalsbehandlingsfunktioner • Standby: Cisco Unified Communications Manager-server som telefonen växlar över till när den aktuella servern blir otillgänglig • Tomt: Ingen aktuell anslutning till denna Cisco Unified Communications Manager-server <p>Ett alternativ kan även omfatta en SRST-beteckning som identifierar en SRST-router för Cisco Unified Communications Manager med en begränsad uppsättning funktioner. Denna router förutsätter att samtalsbehandlingen om alla andra Cisco Unified Communications Manager-servrar blir otillgängliga. SRST Cisco Unified Communications Manager visas alltid sist i listan över servrar, även om den är aktiv. Du kan konfigurera SRST-routeradressen i avsnittet Enhetsgrupp i fönstret Cisco Unified Communications Manager Configuration.</p>
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 tjänster för Cisco Unified IP-telefon.
Passiv URL	URL som visas på telefonen när telefonen är i viloläge under den tid som anges i fältet Inaktiv URL. Ingen meny är öppen.
Passiv URL-timer	Antal sekunder som telefonen är i viloläge och ingen meny är öppen innan XML-tjänsten som anges i URL för inaktivitet aktiveras.
Proxyserver-URL	URL till proxyservern som gör HTTP-begäranden till icke-lokala värddresser på uppdrag av telefonens 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 webbservrar.

Objekt	Beskrivning
Ställa in SW-port	Hastighet och duplex i växelporten, där: <ul style="list-style-type: none"> • 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
Ställa in PC-port	Hastighet och duplex i PC-porten, där: <ul style="list-style-type: none"> • 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 PC-porten
Inaktiv PC-port	Anger om PC-porten på telefonen är aktiverad eller inaktiverad.
Användarplats	Användarspråk som associeras med telefonanvändaren. Identifierar en uppsättning detaljer för att stödja användare, inklusive språk, teckensnitt, datum- och tidsformat och textinformat på alfanumeriskt tangentbord.
Nätverksplats	Nätverksspråk som associeras med telefonanvändaren. Identifierar en uppsättning detaljer till stöd för telefonen i ett visst läge, inklusive definitioner av toner och kadenser som telefonen använder.
Användarspråkversion	Version av användarens språk som laddas på telefonen.
Systemtonerversión	Version av nätverksspråk som laddas på telefonen.
Högtalare aktiverad	Anger om högtalartelefonen är aktiverad på telefonen.
GARP aktiverat	Anger om telefonen lär in MAC-adresser från svar på opå kallad ARP.
Vidarebefordra till PC-port	Anger om telefonen vidarebefordrar paket som sänds och tas emot på nätverksporten till åtkomst till PC-porten.
Videofunktion aktiverad	Anger om telefonen kan delta i videosamtal när den ansluter till en lämpligt utrustad kamera.
Röst-VLAN aktiverat	Anger om telefonen tillåter en enhet som är ansluten till PC-porten att få åtkomst till röst-VLAN.
PC VLAN aktiverat	VLAN som identifierar och tar bort 802.1p/Q-taggar från paket som skickas till datorn.
Automatiskt linjeval aktiverat	Anger om telefonen automatiskt väljer en linje när telefonluren lyfts.
Samtalskontroll för DSCP-protokollet	DSCP IP-klassificering för samtalsstyrning.

Objekt	Beskrivning
DSCP för konfiguration	DSCP IP-klass för alla telefonkonfigurationsöverföringar.
DSCP för tjänster	DSCP IP-klass för telefonbaserade tjänster.
Säkerhetsläge (osäkert)	Säkerhetsläge som är inställt för telefonen.
Webbåtkomst aktiverad	Anger om webbåtkomst är aktiverad (Ja) eller inaktiverad (Nej) för telefonen.
SSH-åtkomst aktiverad	Anger om SSH-porten är aktiverad eller inaktiverad.
CDP: SW-port	Anger om CDP-stöd finns i väljarporten (aktiverat som standard). Aktivera CDP-växelporten för VLAN-tilldelning till telefonen, strömbalansering, QoS-hantering och 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 indikerar att CDP endast ska inaktiveras i väljarporten om telefonen är ansluten till en annan växel än Cisco. CDP-värden för nuvarande PC- och växelport visas på inställningsmenyn.
CDP: PC-port	Anger om CDP stöds i PC-porten (aktiverat som standard). När CDP är inaktiverat i Cisco Unified Communications Manager visas en varning som indikerar att inaktivering av CDP i PC-porten hindrar CVTA från att fungera. CDP-värden för nuvarande PC- och växelport visas på inställningsmenyn.
LLDP-MED:SW-port	Anger om LLDP-MED har aktiverats i väljarporten.
LLDP-MED:PC-port	Anger om LLDP-MED har aktiverats i PC-porten.
LLDP-kraftsprioritet	Telefonströmprioritet till växeln så att växeln kan ge rätt ström till telefonerna. Inställningar <ul style="list-style-type: none"> • Okänt: Detta är standardvärdet. • Låg • hög • Kritiskt
LLDP tillgångs-ID	Resurs-ID som tilldelas till telefonen för lagerhantering.
CTL-fil	MD5-hash för CTL-filen.
ITL-fil	ITL-filen innehåller den initiala listan över betrodda anslutningar.
ITL-signatur	MD5-hash för ITL-filen
CAPF-server	CPF servern används
TVS	Den viktigaste komponenten i Säkerhet som standard. Med TVS kan Cisco Unified IP-telefon autentisera programserverar som EM-tjänster, katalogen och MIDlet:ar under HTTPS-etableringen.
TFTP-server	Namnet på den TFTP-server som används av telefonen.
TFTP-server	Namnet på den TFTP-server som används av telefonen.

Objekt	Beskrivning
Automatisk portsynkronisering	Anger om telefonen automatiskt synkroniserar porthastigheten för att eliminera paketförlust.
Fjärrkonfiguration för växelport	Anger om SW-porten styrs från en fjärrplats.
Fjärrkonfiguration för PC-port	Anger om PC-porten styrs från en fjärrplats.
IP-adresseringsläge	Identifierar adresseringsläget: <ul style="list-style-type: none"> • Endast IPv4 • IPv4 och IPv6 • Endast IPv6
IP-inställningslägeskontroll	Anger IP-adressversion som telefonen använder under signalering med Cisco Unified Communications Manager när både IPv4 och IPv6 är tillgängliga på telefonen.
IP-inställningsläge för media	
Automatisk IPv6-konfiguration	Anger att enheten använder en IPv4-adress vid anslutning till Cisco Unified Communications Manager.
Skydd mot dubblett av IPv6-adress	
IPv6-godkänd omdirigering av meddelanden	Anger om telefonen accepterar omdirigeringsmeddelanden från samma router som används för destinationsnummer.
IPv6-svar på begäran om multicast-eko	Anger att telefonen skickar ett Echo Reply-meddelande som svar på ett Echo Request-meddelande som skickats till en endast IPv6-adress.
IPv6-laddningsserver	Används för att optimera installationstiden för uppgradering av telefonens fasta programvara över WAN genom att lagra bilder lokalt för att eliminera behovet att korsa WAN-länken för varje uppgradering.
IPv6-loggserver	
IPv6-CAPF-server	Anger IP-adress och port till fjärrloggningsservern som telefonen skickar loggmeddelanden till.
DHCPv6	Anger den metod som telefonen använder för att få endast IPv6-adressen. När DHCPv6 aktiveras hämtar telefonen IPv6-adressen från DHCPv6-servern eller via Stateless Address Autoconfiguration (SLAAC) som skickats från den IPv6-aktiverade routern. Och om DHCPv6 inaktiveras har telefonen tillståndskänslig (från DHCPv6-servern) eller tillståndslös (från SLAAC) IPv6-adress. OBS! Till skillnad från DHCPv4 inaktiveras även DHCPv6 och telefonen kan generera en SLAAC-adress om den har aktiverad automatisk konfiguration.

Objekt	Beskrivning
IPv6-adress	Visar telefonens aktuella endast IPv6-adress. Två adressformat stöds: <ul style="list-style-type: none"> • Åtta grupper med hexadecimala siffror åtskiljda med kolon X:X:X:X:X:X:X:X • Komprimerat format som döljer flera grupper med efterföljande nollor och visar i stället med två kolon.
IPv6-prefixlängd	Visar aktuell endast IPv6-prefixlängd för undernätet.
IPv6-standardrouter	Visar IPv6-standardrouter som används av telefonen.
IPv6 DNS-server 1–2	Visar den primära och sekundära DNSv6-server som används av telefonen
Alternativ IPv6 TFTP	Visar om en alternativ IPv6 TFTP-server används.
IPv6 TFTP-server 1–2	Visar den primära och sekundära IPv6 TFTP-server som används av telefonen.
IPv6-adressen släppt	Visar om användaren har publicerat den IPv6-relaterade informationen.
Energywise-strömnivå	Strömnivån som ska användas när telefonen är i viloläge.
EnergyWise-domän	EnergyWise-domänen som telefonen finns i.
DF_BIT	Anger DF-bitinställningen för paket.

Nätverksstatistik

Följande hyperlänkar för nätverksstatistik på en telefonwebbsida ger information om nätverkstrafik på telefonen:

- Ethernet-information: Visar information om Ethernet-trafik.
- Åtkomst: Visar information om nätverkstrafiken till och från PC-porten på telefonen.
- Nätverk: Visar information om nätverkstrafiken till och från nätverksport på telefonen.

Om du vill visa ett område med nätverksstatistik öppnar du telefonwebbsidan och klickar sedan på **Ethernet-information** och hyperlänken **Åtkomst** eller **Nätverk**.

Webbsida med Ethernet-information

Följande tabell beskriver innehållet på webbsidan med Ethernet-Information.

Tabell 50. 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.

Objekt	Beskrivning
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 åtkomst och nätverk

I följande tabell beskrivs informationen på webbsidor för åtkomst och nätverk.

Tabell 51. Åtkomst- och nätverksfält

Objekt	Beskrivning
Rx totalPkt	Totalt antal paket som telefonen tagit emot.
Rx crcErr	Totalt antal paket som tagits emot med CRC och misslyckats.
Rx alignErr	Totalt antal paket mellan 64 och 1522 byte i längd som tagits emot och som hade dålig FCS (Frame Check Sequence).
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 shortErr	Totalt antal mottagna FCS-felpaket eller justeringsfelpaket som är mindre än 64 byte i storlek.
Rx shortGood	Totalt antal mottagna godtagna paket som är mindre än 64 byte i storlek.
Rx longGood	Totalt antal mottagna godtagna paket som är större än 1522 byte i storlek.
Rx longErr	Totalt antal mottagna FCS-felpaket eller justeringsfelpaket som är större än 1522 byte i storlek.
Rx size64	Totalt antal mottagna paket, inklusive felaktiga paket, som är mellan 0 och 64 byte i storlek.
Rx size65to127	Totalt antal mottagna paket, inklusive felaktiga paket, som är mellan 65 och 127 byte i storlek.
Rx size128to255	Totalt antal mottagna paket, inklusive felaktiga paket, som är mellan 128 och 255 byte i storlek.

Objekt	Beskrivning
Rx size256to511	Totalt antal mottagna paket, inklusive felaktiga paket, som är mellan 256 och 511 byte i storlek.
Rx size512to1023	Totalt antal mottagna paket, inklusive felaktiga paket, som är mellan 512 och 1023 byte i storlek.
Rx size1024to1518	Totalt antal mottagna paket, inklusive felaktiga paket, som är mellan 1024 och 1518 byte i storlek.
Rx tokenDrop	Totalt antal paket som tagits bort på grund av resursbrist (till exempel FIFO Overflow).
Tx excessDefer	Totalt antal paket som försenats från att sändas på grund av upptagen enhet.
Tx lateCollision	Antal gånger som kollisioner inträffat senare än 512 bittider efter start av paketsändningen.
Tx totalGoodPkt	Totalt antal godtagna paket (multicast, broadcast och unicast) som telefonen tagit emot.
Tx Collisions	Totalt antal kollisioner som inträffat medan ett paket sändes.
Tx excessLength	Totalt antal paket som inte överförts på grund av paketet gjorde 16 sändningsförsök.
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.
IPv6-adress för CDP-granne	IP-adress till närliggande enhet har identifierats under CDP-protokollidentifieringen.
Port för CDP-granne	Port till närliggande enhet som telefonen är ansluten till har identifierats av CDP-protokollet.

Objekt	Beskrivning
Enhets-ID för LLDP-granne	Ett ID på en enhet som är ansluten till denna port har identifierats under LLDP-identifieringen.
IPv6-adress för LLDP-granne	IP-adress till närliggande enhet har identifierats av LLDP-protokollet.
Port för LLDP-granne	Port till närliggande enhet som telefonen är ansluten till har identifierats av LLDP-protokollet.
Portinformation	Hastighet och duplexinformation.

Enhetsloggar

Följande enhetslogghyperlänkar på en telefonwebbsida ger information som hjälper till att övervaka och felsöka 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 10 senaste statusmeddelanden som telefonen har genererat sedan den senast startades. Statusmeddelandeskärmen på telefonen visar även den här informationen.
- **Visa felsökning:** Visar felsökningsmeddelanden som kan vara till nytta för Cisco TAC om du behöver hjälp med felsökning.

Direktspelningsstatistik

En Cisco Unified IP-telefon kan strömma information till och från upp till tre 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.

Följande tabell beskriver postern i strömningsstatistikområdena.

Tabell 52. Poster i strömningsstatistikområdet

Objekt	Beskrivning
Fjärradress	IP-adress och UDP-port för strömningsdestinationen.
Lokal adress	IP-adress och UDP-port på telefonen.
Starttid	En intern tidsstämpel visar när Cisco Unified Communications Manager begärde att skulle börja sända paket.
Strömstatus	Indikering om strömning är aktiverat eller inte.
Värddamn	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 anslutning, är 0 om anslutningen är inställd på endast mottagning (skyddat läge).

Objekt	Beskrivning
Sänd. oktetter	Totalt antal lastoktetter av standardnyttolast som telefonen överfört i RTP-datapakets start av denna anslutning. Värdet är 0 om anslutningen är inställd på endast mottagning (skyddat läge).
Avsändarcodec	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 paket	Totalt antal RTP datapaket som har gått förlorade sedan datamottagning startade detta sammanhang. Definieras som antalet förväntade paket mindre antalet paket faktiskt fått. Antalet mottagna paket omfattar alla som är sent eller är dubletter. Värdet visas som 0 om anslutningen var inställd på skicka skyddat läge.
Genomsn. jitter	Uppskattning av medelavvikelse för RTP-datapakets interarrival tid, mätt i millisekunder. Värdet visas som 0 om anslutningen var inställd på skicka skyddat läge.
Mottagarcodec	Typ av ljudkodning som används för den mottagna strömmen.
Mottagarrapporter skickade (se not)	Antal gånger RTCP mottagare Rapporten har skickats.
Tid för mottagarrapport skickad (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 detta sammanhang. Inkluderar paket som mottogs från olika källor om det här samtalet är en mottagning. 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 på anslutningen. Inkluderar paket som mottogs från olika källor om det här samtalet är en mottagning. Värdet visas som 0 om anslutningen var inställd på skicka skyddat läge.
MOS LQK	Poäng som är en objektiv uppskattning av MOS-poängen på lyssnarkvalitet (LQK) som ges från 5 (utmärkt) till 1 (dålig). Denna värdering baseras på hörbara dolda händelser vid random i föregående åttasekundersintervall av röstströmmen. Mer information finns i Röstkvalitetsövervakning, på sidan 266 . OBS! MOS LQK-poängen kan variera beroende på vilken typ av kodek Cisco Unified Communications Manager IP-telefon använder.
Med MOS LQK	Genomsnittlig MOS LQK-poäng som observerats under hela röstströmmen.
Min MOS LQK	Lägst MOS LQK-poäng som observerats från början av röstströmmen.

Objekt	Beskrivning
Max MOS LQK	Lägsta MOS LQK-poäng som observerats från början av röstströmmen. Dessa kodekar ger följande maximal MOS LQK-poäng under normala förhållanden utan ramförlust: <ul style="list-style-type: none"> • G.711 ger 4,5. • G.729 A /AB ger 3,7
MOS LQK-version	Version av Cisco-algoritm som används för att beräkna MOS LQK-poäng.
Dolt förhållande kumulativt	Totalt antal hemlighållande ramar dividerat med totala antalet talramar som mottogs från början av röstströmmen.
Dolt förhållande intervall	Förhållandet mellan hemlighållande ramar till talramar i föregående 3-sekundersintervall av aktivt tal. Om röstaktivitetsdetektering (VAD) är i bruk, kan ett längre intervall krävas för att samla tre sekunder aktivt tal.
Dolt förhållande max	Högsta intervall dölja förhållandet från början av röstströmmen.
Dölj sekunder	Antal sekunder som har dolda händelser (förlorade ramar) från början av röstströmmen till slutet av allvarligt dolda sekunder).
Allvarligt dolda sek	Antal sekunder som har mer än fem procent döljande händelser (förlorade ramar) från början av röstströmmen.
Fördröjning (se not)	Uppskattning av nätverkslatensen, uttryckt i millisekunder. Representerar ett löpande medelvärde 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-mottagarrapporter togs emot.
Tid för mottagarrapport mottagen (se not)	Senaste gången en RTCP-mottagarrapport mottogs.
Mottagare krypterad	Anger om mottagaren använder kryptering.

Objekt	Beskrivning
Sändare krypterad	Anger om sändaren använder kryptering.
Sändarramar	Antal ramar som har skickats.
Sändare delvisa ramar	Antal delvisa ramar som har skickats.
Sändar-IFrames	Antal IFrames som har skickats. IFrames används i videosändningen.
Sändar-IDR-ramar	Antal momentant avkodaruppdaterade (IDR-) ramar som har skickats. IDR-ramar används i videosändningen.
Sändarramhastighet	Hastighet som avsändaren skickar ramar i.
Sändarbandbredd	Bandbredd för avsändaren.
Sändarupplösning	Videoupplösning hos avsändaren.
Mottagarramar	Antal ramar som har tagits emot
Mottagare delvisa ramar	Antal delvisa ramar som har tagits emot
Mottagar-IFrames	Antal IFrames som har tagits emot.
Mottagar-IDR-ramar	Antal IDR-ramar som har tagits emot.
Mottagar-IFrames krävs	Antal begärda IDR-ramar som har tagits emot
Mottagarramhastighet	Hastighet som mottagaren tar emot ramar i.
Mottagarramar förlorade	Antal ramar som inte har tagits emot.
Mottagarramfel	Antal ramar som inte har tagits emot.
Mottagarbandbredd	Mottagarens bandbredd.
Mottagarupplösning	Videoupplösning hos mottagaren.
Domän	Domän som telefonen finns i.
Avsändare deltar	Antal gånger som avsändaren deltog.
Mottagare deltar	Antal gånger som mottagaren deltog
Stopp	Antalet "Bye"-ramar
Sändarens starttid	Tid då avsändaren startade.
Mott- starttid	Tid då mottagaren startade.
Radstatus	Om telefonen utför strömning
Avsändarverktyg	Typ av ljudkodning som används för strömning
Avsändarrapporter	RTCP-avsändarrapporter

Objekt	Beskrivning
Tid för avsändarrapport	Senaste gången en RTCP-avsändarrapport skickades.
Mottagarjitter	Maximalt jitter i strömning
Mottagarverktyg	Typ av ljudkodning som används för strömning
Mottagarrapporter	Antal gånger som rapporten över strömningsstatistik har öppnats via webbsidan.
Tid för mottagarrapport	Intern tidsstämpel som anger när rapporten över strömningsstatistik genererades
Är video	Anger om samtalet var ett videosamtal eller enbart ljud.
Samtals-id	Samtalets identifiering
Grupp-ID	Identifiering av gruppen som telefonen ingår i.



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 samtalsessionsinformation 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 ModelInfo

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

- Allmän felsökning, på sidan 245
- Startproblem, på sidan 246
- Problem med telefonåterställning, på sidan 250
- Telefonen kan inte ansluta till LAN, på sidan 252
- Säkerhetsproblem med Cisco IP-telefon, på sidan 253
- Problem vid videosamtal, på sidan 255
- Allmänna problem med samtal i telefonen, på sidan 256
- Felsökningsförfaranden, på sidan 257
- Kontrollera felsökningsinformationen från Cisco Unified Communications Manager, på sidan 261
- Ytterligare felsökningsinformation, på sidan 262

Allmän felsökning

Följande tabell innehåller allmän information om felsökning för Cisco IP-telefon.

Tabell 53. Felsökning av Cisco IP-telefon

Sammanfattning	Förklaring
Anslutning av en Cisco IP-telefon till en annan Cisco IP-telefon	Cisco stöder inte anslutning av en IP-telefon till en annan IP-telefon via en annan IP-telefon. Varje IP-telefon ska anslutas direkt till en växelport. Om telefoner kopplas ihop i en linje med hjälp av PC-porten kommer telefonerna inte att fungera.
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 kan orsaka att IP-telefoner återställas eller ett aktivt samtal bryts, eller så går det inte att ringa eller svara på samtal. Telefonerna kanske inte fungerar igen förrän sändningsstormen slutar.

Sammanfattning	Förklaring
Flytta en nätverksanslutning från telefonen till en arbetsstation	<p>Om du startar din telefon via nätverksanslutningen måste du vara försiktig sedan väljer att koppla från nätverksanslutningen på telefonen och ansluta till en stationär dator.</p> <p>Försiktighet Nätverkskortet i datorn kan inte få ström genom nätverksanslutningen. Om anslutningen är strömförande kan nätverkskortet förstöras. För att skydda nätverkskortet ska du sekunder eller längre efter att du kopplat loss kabeln från telefonen du ansluter den till en dator. Denna fördröjning ger omkopplaren tillräckligt med tid att inse att det inte längre finns en telefon på linjen och sluta ge ström till kabeln.</p>
Ändra telefonkonfigurationen	<p>Som standard är alternativen för nätverkskonfiguration låsta för att hindra användaren från att göra ändringar som kan påverka deras nätverksanslutning. Du måste låsa upp alternativen för nätverkskonfiguration innan du kan konfigurera dem. Mer information finns i Använda ett telefonlösenord, på sidan 50.</p> <p>OBS! Om administratörlösenordet inte är inställt i en allmän telefon kan användaren ändra nätverksinställningarna.</p>
Kodfelmatchning mellan telefonen och en annan enhet	<p>Statistik om RxType och TxType visar koden som används för samtal mellan Cisco IP-telefon och den andra enheten. Värdena i statistiken måste matcha. Om inte gör det ska du kontrollera att den andra enheten kan hantera kodsamtal och att det finns en transkoder för att hantera tjänsten.</p>
Ljudfelmatchning mellan telefonen och en annan enhet	<p>Statistik om RxSize och TxSize visar storleken på röstpaketet som används i samtalet mellan denna Cisco IP-telefon och den andra enheten. Värdena i statistiken måste matcha.</p>
Loopback	<p>En loopback kan inträffa under följande förutsättningar:</p> <ul style="list-style-type: none"> • Alternativet SW-portkonfigurationen på menyn Nätverkskonfiguration i Cisco Unified Communications Manager är inställt på 10 halv (10-BaseT/halv duplex). • Telefonen får ström från en extern strömkälla. • Telefonen är avstängd (strömförsörjningen är fränkopplad). <p>I detta fall kan växelporten på telefonen inaktiveras och följande meddelande visas i växelkonsolloggen:</p> <pre>HALF_DUX_COLLISION_EXCEED_THRESHOLD</pre> <p>För att lösa detta problem måste du återaktivera porten från växeln.</p>

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

[Verifiering vid telefonstart](#), på sidan 64

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

[Verifiering vid telefonstart](#), på sidan 64

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 257](#).

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.

Relaterade ämnen

[Visa fönstret Statusmeddelanden](#), på sidan 213

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 258

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.

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.

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 261](#).

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.

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 70](#) 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 70](#).

Om telefonen redan finns i Cisco Unified Communications Manager-databasen kan konfigurationsfilen vara skadad. I [Skadad konfigurationsfil, på sidan 249](#) 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.

Telefonen registrerar inte

Problem

Telefonskärmen visar meddelandet "Ange aktiveringskod eller tjänstedomän".

Lösning

Telefonen saknar en TFTP-adress. Kontrollera att alternativet 150 tillhandahålls av DHCP-servern eller att en alternativ TFTP konfigureras manuellt.

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.

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 **Program** på telefonen och välja **Administrationsinställningar > 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 258](#).

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.

Problem vid videosamtal

Ingen video mellan två Cisco IP-videotelefoner

Problem

Video strömmas inte mellan två Cisco IP-videotelefoner.

Lösning

Kontrollera att ingen mediatimeringspunkt, MTP, används i samtalsflödet.

Videon hackar eller hoppar över bilder

Problem

När jag befinner mig i ett videosamtal buffrar videon eller hoppar över bilder.

Lösning

Kvaliteten på bilden beror på samtalets bandbredd. Genom att höja bithastigheten förbättras kvaliteten på din video, men det kräver mer nätverksresurser. Använd alltid den hastighet som passar bäst för din typ av video. Ett videosamtal med 720p och 15 bildrutor per sekund kräver en bithastighet på 790 kbps eller högre. Ett videosamtal med 720p och 30 bildrutor per sekund kräver en bithastighet på 1 360 kbps eller högre.

Mer information om bandbredd finns i avsnittet Ställa in upplösning för videosändning i kapitlet Telefonfunktioner och inställning.

Lösning

Kontrollera att parametern Högsta bithastigheten för videosamtal är konfigurerad för åtminstone lägsta bithastighetintervallet. I Cisco Unified Communications Manager navigerar du till **System > Information om region > Region**.

Jag kan inte överföra videosamtal

Problem

Jag kan inte överföra ett videosamtal från skrivbordstelefonen till min mobila enhet.

Lösning

Cisco Unified Mobility omfattar inte videosamtal. Ett videosamtal som tas emot på skrivbordstelefonen kan inte plockas upp på mobiltelefonen.

Ingen Video under konferenssamtal

Problem

Ett videosamtal övergår till ett ljudsamtal när jag lägger till två eller fler personer i samtalet.

Du måste använda en videokonferensbrygga för tillfälliga och meet-me-videokonferenser.

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 knappatsen 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.
-

Skapa en konsollogg från din telefon

Du genererar en konsollogg när telefonen inte kan ansluta till nätverket och du inte kan komma åt problemrapportverktyget (PRT).

Innan du börjar

Anslut en konsolkabel till AUX-porten på telefonens baksida.

Arbetsordning


- Steg 1** Tryck på **Program**  på telefonen.

Steg 2 Navigera till **Administrationsinställningar > Aux-port**.

Steg 3 Välj **Samla in konsollogg** för att samla in enhetsloggar.

Kontrollera TFTP-inställningar

Arbetsordning

- Steg 1** På Cisco IP-telefon trycker du på **Program**  och väljer **Admin.inställningar > Nätverksinställning > Ethernet-inställning > IPv4-inställning > TFTP-Server 1**.
- Steg 2** Om du har tilldelat en statisk IP-adress till telefonen, måste du manuellt ange en inställning för TFTP-server 1.
- Steg 3** Om du använder DHCP hämtar telefonen adressen för TFTP-servern från DHCP-servern. Kontrollera att IP-adressen har konfigurerats i Alternativ 150.
- Steg 4** 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 5** Om en lokal DHCP inte erbjuder rätt TFTP-adress kan du aktivera användning av en alternativ TFTP-server i telefonen.
- Detta behövs ofta i ett VPN-scenario.
-

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:
- Inaktivera DHCP.
 - Tilldela statiska IP-värden till telefonen. Använd samma standardrouterinställning som andra fungerande telefoner använder.
 - 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

[Grundläggande återställning](#), på sidan 263

[Fastställ telefonens MAC-adress](#), på sidan 70

Kontrollera DHCP-inställningar

Arbetsordning

-
- Steg 1** På telefonen trycker du på **Program** .
- Steg 2** Välj **Wi-Fi > Nätverksinställning > IPv4-inställning** och välj bland följande alternativ:
- 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 ha 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:
http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html
 - IP-adress, nätmask, standardrouter: Om du har tilldelat en statisk IP-adress till telefonen, måste du manuellt ange inställningar för dessa alternativ.
- Steg 3** 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:
http://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

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv
[Telefontilläggsmetoder](#), på sidan 70

Identifiera 802.1X-autentiseringsproblem

Arbetsordning

Steg 1 Kontrollera att de komponenter som krävs är korrekt konfigurerade.


Steg 2 Bekräfta att delad hemlighet är konfigurerad på telefonen.

- Om delad hemlighet har konfigurerats, kontrollerar du att samma delade hemlighet finns på autentiseringsservern.
- Om delad hemlighet inte har konfigurerats på telefonen, anger du den och kontrollerar att den matchar delad hemlighet på autentiseringsservern.

Verifiera DNS-inställningar

Verifiera DNS-inställningar så här:

Arbetsordning

Steg 1 Tryck på **programknappen** .

Steg 2 Välj **Admin.inställningar > Nätverksinställning > IPv4-inställning > DNS-server 1**.

Steg 3 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, Wi-Fi, VPN, Energywise, MobileRemoteAccess

OBS! Om du vill införa stöd för parametrar på flera nivåer och i flera avsnitt markerar du kryssrutan Loggprofil.

- Fjärrlogg – värden: Inaktivera (standard), Aktivera
- IPv6-loggserver eller loggserver – IP-adress (IPv4- eller IPv6-adress)

OBS! När loggservern inte kan nå slutar telefonen att skicka felsökningsmeddelanden.

- Formatet för IPv4-loggserveradressen är **address :<port>@@base=<0-7>;pfs=<0-1>**
 - Formatet för IPv6-loggserveradressen är **[address] :<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




- Grundläggande återställning, på sidan 263
- Utföra återställning av nätverkskonfiguration, på sidan 265
- Utföra återställning av användarnätverkskonfiguration, på sidan 265
- Ta bort CTL-filen, på sidan 265
- Quality Report Tool, på sidan 266
- Röstkvalitetsövervakning, på sidan 266
- Rengöring av Cisco IP-telefon, på sidan 267

Grundläggande återställning

En grundläggande återställning av en Cisco IP-telefon är ett sätt att återskapa funktioner om telefonen får ett fel eller nollställa och återskapa olika konfigurationer och säkerhetsinställningar.

I följande tabell beskrivs de olika sätten att utföra en grundläggande återställning. Du kan återställa en telefon med någon av dessa åtgärder efter att telefonen har startats. Välj den åtgärd som passar för din situation.

Tabell 54. Metoder för grundläggande återställning

Drift	Åtgärd	Förkl
Starta om telefonen	Tryck Program  . Gå till Admin.inställningar > Återställ inställningar > Återställ enhet .	Åters telefo telefo
Återställ inställningar	Om du vill återställa inställningarna trycker du på Program  och väljer Admin.inställningar > Återställ inställningar > Nätverk .	Åters åters
	Om du vill återställa CTL-filen trycker du på Program  och väljer Admin.inställningar > Återställ inställningar > Säkerhet .	Åters

Återställa telefonen till fabriksinställningarna från telefonens knappsats

Du kan återställa telefonen till fabriksinställningarna. Återställningen rensar alla parametrarna för telefonen.


Arbetsordning

- Steg 1** Koppla från strömmen till telefonen på ett av följande sätt:
- Koppla ur strömadaptern.
 - Koppla ur nätverkskabeln.
- Steg 2** Vänta 5 sekunder.
- Steg 3** Tryck på och håll ner # och koppla in telefonen igen. Släpp # när knapparna **Headset** och **Högtalare** lyser.
- OBS!** I vissa maskinvaruversioner tänds även knappen **Tyst** tillsammans med **Headset** och **Högtalare** när du ansluter telefonen igen. I så fall ska du vänta på att alla slocknar och inte släppa # förrän knapparna **Headset** och **Högtalare** lyser igen.
- Steg 4** Ange följande knappsekvens:
- 123456789*0#**
- Lampan för **Headset** släcks när du trycker på **1**. När du har angett knappsekvensen tänds knappen **Ljud av**.
- Försiktighet** Stäng inte av telefonen förrän den är klar med fabriksåterställningen och huvudskärmen visas.
- Då återställs telefonen.
-

Återställ alla inställningar från Telefon-menyn

Utför den här åtgärden om du vill återställa användar- och nätverksinställningarna till standardvärden.

Arbetsordning

- Steg 1** Tryck på **programknappen** .
- Steg 2** Välj **Admin.inställningar > Återställ inställningar > Alla inställningar**.
- Vid behov kan du låsa upp telefonalternativen.
-

Starta om telefonen från säkerhetskopian

Cisco IP-telefon 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** Koppla ur strömförsörjningen.

- Steg 2** Tryck och håll ned stjärnknappen (*).
- Steg 3** Återanslut strömmen. Fortsätt att trycka på *-knappen tills LED-lampan Tyst släcks.
- Steg 4** Släpp *-knappen.
Telefonen startas om från säkerhetskopian.
-

Utföra återställning av nätverkskonfiguration

Återställer konfiguration av nätverksinställningar till standardvärdena och gör att telefonen återställs. Den här metoden gör att DHCP konfigurerar om telefonens IP-adress.

Arbetsordning

- Steg 1** På menyn Admin.inställningar kan du låsa upp telefonalternativen om det behövs.
- Steg 2** Välj **Återställ inställningar > Nätverkskonfiguration**.
-

Utföra återställning av användarnätverkskonfiguration

Återställer alla användar- och nätverksonfigurationsändringar som du har gjort, men som telefonen inte har skrivit till flashminnet, till tidigare sparade inställningar.

Arbetsordning

- Steg 1** På menyn Admin.inställningar kan du låsa upp telefonalternativen om det behövs.
- Steg 2** Välj **Återställ inställningar > Återställ enhet**.
-

Ta bort CTL-filen

Tar bara bort CTL-filen från telefonen.

Arbetsordning

- Steg 1** På menyn Admin.inställningar kan du låsa upp telefonalternativen om det behövs.
- Steg 2** Välj **Återställ inställningar > Säkerhetsinställningar**.
-

Quality Report Tool

QRT är ett röstkvalitets- och allmänt problemrapporteringsverktyg för Cisco IP-telefoner. QRT-funktionen installeras som en del av Cisco Unified Communications Manager.

Du kan konfigurera Cisco IP-användartelefoner med QRT. När du gör det, kan användare rapportera problem med telefonsamtal genom att trycka på Rapportkvalitet. Denna funktionstangent eller knappen är endast tillgänglig när Cisco IP-telefon är i läget Ansluten, Ansluten konferens, Ansluten överföring eller Lur på.

När en användare trycker Rapportkvalitet, visas en lista över problemområden. Användaren väljer en problemkategori och denna återkoppling loggas i en XML-fil. Aktuell information som loggas beror på användarens val och om destinationsenheten är en Cisco IP-telefon.

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

Relaterade ämnen

[Dokumentation för Cisco Unified Communications Manager](#), på sidan xv

Röstkvalitetsövervakning

För att mäta röstkvalitet samtals 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 55. Ändringar i röst kvalitetsmetrik

Metrisk förändring	Villkor
Dolt förhållande och dolda sekunder ökar avsevärt	Försämrad nätverksfunktion från paketförluster eller hög jitter.

Metrisk förändring	Villkor
Dolt förhållande är nära eller på noll, men röstkvaliteten är dålig.	<ul style="list-style-type: none"> • Brus eller distorsion i ljudkanal såsom eko eller ljudnivåer. • Tandemsamtal som genomgår flera kodningar/avkodningar, som samtal till ett mobilnät eller telefonkortsnet. • Akustiska problem som kommer från en högtalartelefon, mobiltelefon med handsfree eller trådlöst headset. <p>Kontrollera räknare för paketsändningen (TxCnt) och paketmottagningen (RxCnt) för att kontrollera att röstpaketet flödar.</p>
MOS LQK-poäng minskar kraftigt	<p>Försämrad nätverksfunktion från paketförluster eller höga jitternivåer:</p> <ul style="list-style-type: none"> • En minskad genomsnittlig MOS LQK kan tyda på en utbredd och jämn försämring. • Enskilda MOS LQK-minskningar kan tyda på tillfällig försämring. <p>Dubbelkontrollera om dolt förhållande och dolda sekunder beror på paketförlust och jitter.</p>
MOS LQK-poäng ökar kraftigt	<ul style="list-style-type: none"> • 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, på sidan 269](#)
- [Stöd för internationell samtalsloggning, på sidan 269](#)
- [Språkbegränsning, på sidan 270](#)

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 xv](#)

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 visa den förkortade lokala versionen av numret, utan internationell symbol eller landsnummer.

Språkbegränsning

Det finns ingen lokaliserad KATE-support (Keyboard Alphanumeric Text Entry) för följande asiatiska språk:

- 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.

Kinesiska indata fungerar på liknande sätt som för datorer och mobiltelefoner på kinesiska. Kinesiska språkinstallationsprogrammet krävs för kinesiska indata ska fungera.