



Administrasjonsguide for Cisco IP-konferansetelefon 7832 for Cisco Unified Communications Manager

Utgitt første gang: 2017-08-30

Sist endret: 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

SPESIFIKASJONENE OG INFORMASJONEN MED HENSYN TIL PRODUKTENE I DENNE HÅNDBOKEN KAN ENDRES UTEN VARSEL. ALLE ERKLÆRINGER, ANBEFALINGER OG ALL INFORMASJON SKAL VÆRE NØYAKTIG, MEN FREMLEGGES UTEN NOEN FORM FOR GARANTI, HVERKEN DIREKTE ELLER INDIREKTE. BRUKERNE MÅ TA DET FULLE ANSVARET FOR BRUK AV PRODUKTENE.

PROGRAMVARELISENSEN OG DEN BEGRENSEDE GARANTIE SOM FØLGER MED PRODUKTET, ER ANGITT I INFORMASJONSPAKKEN SOM LEVERES MED PRODUKTET, OG ER EN DEL AV DENNE REFERANSEN. HVIS DU IKKE FINNER PROGRAMVARELISENSEN ELLER DEN BEGRENSEDE GARANTIE, KAN DU KONTAKTE CISCO-REPRESENTANTEN FOR Å FÅ EN KOPI.

Følgende informasjon er for FCC-samsvar for klasse A-enheter: Dette utstyret er testet og funnet å overholde retningslinjene for en digital enhet i klasse A, i henhold til kapittel 15 i FCC-reglene. Disse grensene er utformet for å gi rimelig beskyttelse mot skadelig interferens når utstyret driftes i et kommersielt miljø. Dette utstyret genererer, bruker og kan utstråle radiofrekvensenergi, og dersom det ikke installeres og brukes i henhold til bruksanvisningen, kan det forårsake skadelig interferens på radiokommunikasjon. Bruk av dette utstyret i et boligområde kan forårsake skadelig interferens, noe som fører til at brukere må korrigere interferensen på egen bekostning.

Følgende informasjon er for FCC-samsvar for klasse B-enheter: Dette utstyret er testet og funnet å overholde retningslinjene for en digital enhet i klasse B, i henhold til kapittel 15 i FCC-reglene. Disse grensene er utformet for å gi rimelig beskyttelse mot skadelig interferens i en boliginstallasjon. Dette utstyret genererer, bruker og kan utstråle radiofrekvensenergi, og dersom det ikke installeres og brukes i henhold til instruksjonene, kan det forårsake skadelig interferens på radiokommunikasjon. Det finnes imidlertid ingen garantier for at ikke interferens kan forekomme i en bestemt installasjon. Hvis utstyret fører til interferens på radio- eller TV-mottak, noe som kan fastslås ved å slå utstyret av og på, oppfordres brukere til å prøve å korrigere interferensen ved hjelp av ett eller flere av følgende tiltak:

- Rett inn mottakerantennen på nytt eller omplasser den.
- Øk avstanden mellom utstyret og mottakeren.
- Koble utstyret til et uttak på en annen krets enn den mottakeren er koblet til.
- Rådfør deg med en forhandler eller en erfaren radio/TV-tekniker for å få hjelp.

Endringer av produktet som ikke er godkjent av Cisco, kan oppheve gyldigheten av FCC-godkjenningen og frata deg retten til å bruke produktet.

Ciscos implementering av TCP-hodekomprimering er en tilpasning av et program som University of California, Berkeley (UCB) har utviklet som en del av UCBS fritt tilgjengelige domeneversjon av operativsystemet UNIX. Med enerett. Copyright © 1981, Regents of the University of California.

TIL TROSS FOR EVENTUELLE GARANTIER I DETTE DOKUMENTET, ER ALLE DOKUMENTFILER OG ALL PROGRAMVARE FRA DISSE LEVERANDØRENE LEVERT "SOM DE ER" MED EVENTUELLE FEIL. CISCO OG OVENNEVNTE LEVERANDØRER FRASKRIVER SEG ALLE GARANTIER, DIREKTE ELLER INDIREKTE, INKLUDERT, UTEN BEGRENSNINGER, GARANTIENE OM SALGBARHET OG EGNETHET FOR SÆRSKILTE FORMÅL. FRASKRIVELSE GJELDER OGSÅ ENHVER FORM FOR ANSVAR SOM FØLGE AV EVENTUELL KRENKELSE AV TREDJEPARTS RETTIGHETER OG GARANTIER I FORBINDELSE MED HANDEL, BRUK ELLER HANDELSKUTYME.

IKKE I NOE TILFELLE SKAL CISCO ELLER RESPEKTIVE LEVERANDØRER VÆRE ANSVARLIGE FOR INDIREKTE SKADER, SPESIELLE SKADER, ELLER FØLGESKADER, INKLUDERT, UTEN BEGRENSNING, TAP AV FORTJENESTE ELLER TAP AV ELLER SKADE PÅ DATA SOM OPPSTÅR SOM FØLGE AV BRUK ELLER MANGEL PÅ BRUK AV DENNE HÅNDBOKEN, SELV OM CISCO ELLER RESPEKTIVE LEVERANDØRER ER BLITT GJORT OPPMERKSOM PÅ MULIGHETENE FOR SLIKE SKADER.

Eventuelle IP-adresser og telefonnumre som brukes i dette dokumentet, er ikke ment å skulle være faktiske adresser og telefonnumre. Eventuelle eksempler, kommandoutdata, diagrammer over nettverkstopologi og andre tall som er inkludert i dokumentet, er bare for illustrasjonsformål. Eventuell bruk av faktiske IP-adresser eller telefonnumre i illustrasjoner, er utilsiktet og tilfeldig.

Alle utskrevne kopier og dupliserte, myke kopier av dette dokumentet regnes som ikke kontrollert. Se den gjeldende elektroniske versjonen for den nyeste versjonen.

Cisco har mer enn 200 kontorer verden over. Adresser, telefonnumre og faksnr finner du på Ciscos nettsted: www.cisco.com/go/offices.

Cisco og Cisco-logoen er varemerker eller registrerte varemerker for Cisco og/eller tilknyttede selskaper i USA og andre land. Hvis du vil vise en liste over Cisco-varemerkene, går du til denne URL-adressen: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Tredjeparts varemerker som nevnes her, tilhører sine respektive eiere. Bruken av ordet partner antyder ikke et partnerskapsforhold mellom Cisco og noe annet selskap. (1721R)

© 2017–2023 Cisco Systems, Inc. Med enerett.



INNHold

KAPITTEL 1

Ny og endret informasjon 1

Ny og endret informasjon om fastvareversjon 14.2(1)	1
Ny og endret informasjon om fastvareversjon 14.1(1)	1
Ny og endret informasjon om fastvareversjon 14.0(1)	2
Ny og endret informasjon om fastvareversjon 12.8(1)	2
Ny og endret informasjon om fastvareversjon 12.7(1)	2
Ny og endret informasjon om fastvareversjon 12.6(1)	2
Ny og endret informasjon om fastvareversjon 12.5(1)SR3	2
Ny og endret informasjon om fastvareversjon 12.5(1)SR2	3
Ny og endret informasjon om fastvareversjon 12.5(1)SR1	3
Ny og endret informasjon om fastvareversjon 12.5(1)	3
Ny og endret informasjon om fastvareversjon 12.1(1)	4

DEL I:

Om Cisco IP-konferansetelefonen 5

KAPITTEL 2

Maskinvare for Cisco IP-konferansetelefoner 7

Den Cisco IP Conference Phone 7832	7
Knapper og maskinvare på Cisco IP-telefon 7832	9
Funksjonsknapper på konferansetelefoner	10
Beslektet dokumentasjon	10
Dokumentasjon for Cisco IP-konferansetelefon 7832	10
Dokumentasjon Cisco Unified Communications Manager	10
Dokumentasjon Cisco Business Edition 6000	10
Dokumentasjon, støtte og retningslinjer for sikkerhet	10
Sikkerhetsoversikt for Cisco-produktet	11
Terminologiforskjeller	11

KAPITTEL 3	Tekniske detaljer	13
	Spesifikasjoner for fysisk miljø og operativmiljø	13
	Kabelspesifikasjoner	14
	Krav til telefonstrøm	14
	Strømstans	15
	Strømreduksjon	15
	Støttede nettverksprotokoller	15
	Samhandling med Cisco Unified Communications Manager	19
	Samhandling med Cisco Unified Communications Manager Express	19
	Samhandling med talemeldingssystem	20
	Telefonkonfigurasjonsfiler	20
	Telefonens oppførsel under stor trafikk på nettverket	21
	Approgrammeringsgrensesnitt	21

DEL II:	Installasjon av telefoner	23
----------------	----------------------------------	-----------

KAPITTEL 4	Installasjon av Cisco IP-konferansetelefoner	25
	Bekreftede nettverksoppsettet	25
	Aktiveringskode for registrering av lokale telefoner	26
	Aktiveringskode for registrering og Mobile and Remote Access	27
	Aktivere automatisk registrering av telefoner	27
	Installere konferansetelefonen	29
	Måter du kan forsyne konferansetelefonen med strøm	30
	Konfigurere telefonen fra oppsettsmenyene	30
	Ta i bruk et telefonpassord	31
	Tekst- og menyinntasting fra telefonen	32
	Konfigurere nettverksinnstillingene	32
	Felter i Nettverksoppsett	33
	Bekreftede telefonoppstarten	37
	Endre telefonmodell for en bruker	37

KAPITTEL 5	Installasjon av telefoner i Cisco Unified Communications Manager	39
	Konfigurere en Cisco IP-konferansetelefon	39

	Fastslå telefonens MAC-adresse	43
	Metoder for å legge til telefoner	44
	Legge til telefoner enkeltvis	44
	Legge til telefoner ved hjelp av BAT-telefonmalen	45
	Legge til brukere i Cisco Unified Communications Manager	45
	Legge til en bruker fra en ekstern LDAP-katalog	46
	Legge en bruker direkte til i Cisco Unified Communications Manager	46
	Legge til bruker i sluttbrukergruppe	47
	Knytte telefoner til brukere	48
	Survivable Remote Site Telephony	48
<hr/>		
KAPITTEL 6	Administrasjon av selvhjelpsportal	51
	Oversikt over selvhjelpsportalen	51
	Konfigurere brukertilgang til selvhjelpsportalen	51
	Tilpasse visningen av selvhjelpsportalen	52
<hr/>		
DEL III:	Administrasjon av telefon	53
<hr/>		
KAPITTEL 7	Sikkerhet på Cisco IP-konferansetelefoner	55
	Oversikt over sikkerhet for Cisco IP-telefon	55
	Utvidet sikkerhet i telefonnettverket	56
	Støttede sikkerhetsfunksjoner	57
	Sikkerhet for telefonsamtaler	59
	Identifikasjon av sikker telefonkonferanse	60
	Identifikasjon av sikker telefonsamtale	61
	802.1x-godkjenning	62
	Se gjeldende sikkerhetsfunksjoner på telefonen	62
	Vise sikkerhetsprofiler	63
	Konfigurere sikkerhetsinnstillingene	63
	Felt i Sikkerhetsoppsett	63
	Konfigurere et lokalt signifikant sertifikat	64
	Aktivere FIPS-modus	66
<hr/>		
KAPITTEL 8	Tilpassing av Cisco IP-konferansetelefoner	67

Egendefinerte telefonringetoner	67
Konfigurere en tilpasset ringetone	67
Filformater for tilpassede ringetoner	68
Tilpasse ringetonen	69
<hr/>	
KAPITTEL 9	Funksjoner og oppsett for Cisco IP-konferansetelefoner 71
Brukerstøtte for Cisco IP-telefon	71
Migrering av telefonen til en telefon med flere plattformer direkte	71
Konfigurere en ny funksjonstastmal	72
Konfigurere telefontjenester for brukere	73
Konfigurasjon av telefonfunksjoner	73
Konfigurere telefonfunksjoner for alle telefoner	74
Konfigurere telefonfunksjoner for en gruppe telefoner	74
Konfigurere telefonfunksjoner for én telefon	75
Produktspesifikk konfigurasjon	75
Deaktivere TLS-chifre	87
Planlegge strømsparing for Cisco IP-telefoner	87
Planlegge EnergyWise på Cisco IP-telefoner	89
Konfigurere Ikke forstyrr	92
Aktivere agenthilsen	93
Konfigurere Varsel for viderekobling av anrop	93
Aktivere Enhetsaktivert innspilling	94
UCR 2008-oppsett	95
Konfigurere UCR 2008 i Konfigurasjon av vanlig enhet	95
Konfigurere UCR 2008 i Vanlig telefonprofil	96
Konfigurere UCR 2008 i Konfigurasjon av bedriftstelefon	96
Konfigurere UCR 2008 i telefon	97
Mobil og ekstern tilgang gjennom Expressway	97
Distribusjonsscenarier	98
Mediebaner og interaktiv etablering av tilkoblinger	99
Konfigurere lagring av brukerlegitimasjon for Expressway-pålogging	99
Problemrapporteringsverktøy	100
Konfigurere en URL for opplasting av kundestøtte	100
Angi etiketten for en linje	101

KAPITTEL 10	Konfigurere bedriftskatalogen og den personlige katalogen	103
	Konfigurere bedriftskatalogen	103
	Konfigurere den personlige katalogen	103
DEL IV:	Feilsøking av telefoner	105
KAPITTEL 11	Overvåking av telefonsystemer	107
	Oversikt over overvåking av telefonsystemer	107
	Status for Cisco IP-telefoner	107
	Vise vinduet Telefoninformasjon	108
	Vise Status-menyen	108
	Vise vinduet Statusmeldinger	108
	Vise vinduet Nettverksstatistikk	113
	Vise vinduet Anropsstatistikk	116
	Nettside for Cisco IP-telefoner	118
	Få tilgang til telefonens nettside	118
	Nettsiden for enhetsinformasjon	118
	Nettsiden for nettverksoppsett	120
	Nettside med Ethernet-informasjon	125
	Nettsider for nettverk	125
	Nettsidene Konsollogger, Kjernedumper, Statusmeldinger og Vis feilsøking	126
	Nettsiden Strømmestatistikk	127
	Be om informasjon fra telefonen i XML	129
	Utdata for kommandoen CallInfo	130
	Utdata for kommandoen LineInfo	130
	Utdata for kommandoen ModeInfo	131
KAPITTEL 12	Vedlikehold	133
	Starte på nytt eller tilbake stille konferansetelefonen	133
	Starte konferansetelefonen på nytt	133
	Tilbake stille konferansetelefoninnstillingene fra Telefon-menyen	133
	Tilbake stille konferansetelefonen til standard fabrikkinnstillinger fra tastaturet	134
	Overvåking av talekvalitet	134

Tips for feilsøking av talekvalitet	135
Rengjøring av Cisco IP-telefon	136
<hr/>	
KAPITTEL 13	Feilsøking 137
Generell feilsøkinginformasjon	137
Oppstartsproblemer	138
Cisco IP-telefon bruker ikke den vanlige oppstartsprosessen	138
Cisco IP-telefon registreres ikke i Cisco Unified Communications Manager	139
Telefonen viser feilmeldinger	140
Telefonen kan ikke koble til TFTP-serveren eller til Cisco Unified Communications Manager	140
Telefonen kan ikke koble til TFTP-serveren	140
Telefonen kan ikke koble til serveren	140
Telefonen kan ikke koble til med DNS	141
Cisco Unified Communications Manager og TFTP-tjenester kjører ikke	141
Skadet konfigurasjonsfil	141
Registrering av telefoner i Cisco Unified Communications Manager	141
Cisco IP-telefon kan ikke hente IP-adresse	142
Problemer med tilbakestilling av telefonen	142
Telefonen tilbakestilles på grunn av vedvarende nettverksbrudd	142
Telefonen tilbakestilles på grunn av feil med DHCP-innstillingene	143
Telefonen tilbakestilles på grunn av en ugyldig statisk IP-adresse	143
Telefonen tilbakestilles ved høy nettverksbelastning	143
Telefonen tilbakestilles på grunn av tilsiktet tilbakestilling	143
Telefonen tilbakestilles på grunn av problemer med DNS eller andre tilkoblingsproblemer	144
Telefonen blir ikke slått på	144
Telefonen kan ikke koble til LAN	144
Problemer med sikkerhet på Cisco IP-telefoner	144
Problemer med CTL-filen	145
Godkjenningsfeil: Telefonen kan ikke godkjenne CTL-filen	145
Telefonen kan ikke godkjenne CTL-filen	145
CTL-filen godkjennes, men andre konfigurasjonsfiler blir ikke godkjent	145
ITL-filen godkjennes, men andre konfigurasjonsfiler blir ikke godkjent	145
TFTP-godkjenning mislykkes	146
Telefonen blir ikke registrert	146

Signerte konfigurasjonsfiler er ikke obligatoriske	146
Lydproblemer	147
Ingen talebane	147
Hakkete tale	147
Generelle problemer med telefonsamtaler	147
Telefonsamtale kan ikke opprettes	147
Telefonen gjenkjenner ikke DTMP-sifrene, eller sifrene er forsinket	148
Feilsøkningsprosedyrer	148
Opprette en telefonproblemrapport fra Cisco Unified Communications Manager	148
Kontrollere TFTP-innstillinger	149
Finne problemer med DNS eller tilkobling	149
Kontrollere DHCP-innstillinger	150
Opprette en ny telefonkonfigurasjonsfil	150
Kontrollere DNS-innstillinger	151
Starte tjeneste	151
Kontrollere feilsøkningsinformasjon fra Cisco Unified Communications Manager	152
Ekstra feilsøkningsinformasjon	153

KAPITTEL 14**Internasjonal brukerstøtte 155**

Installasjonsprogram for språk for endepunkter for Unified Communications Manager	155
Støtte for logging av utenlandssamtaler	155
Språkbegrensning	156



KAPITTEL 1

Ny og endret informasjon

- [Ny og endret informasjon om fastvareversjon 14.2\(1\), på side 1](#)
- [Ny og endret informasjon om fastvareversjon 14.1\(1\), på side 1](#)
- [Ny og endret informasjon om fastvareversjon 14.0\(1\), på side 2](#)
- [Ny og endret informasjon om fastvareversjon 12.8\(1\), på side 2](#)
- [Ny og endret informasjon om fastvareversjon 12.7\(1\), på side 2](#)
- [Ny og endret informasjon om fastvareversjon 12.6\(1\), på side 2](#)
- [Ny og endret informasjon om fastvareversjon 12.5\(1\)SR3, på side 2](#)
- [Ny og endret informasjon om fastvareversjon 12.5\(1\)SR2, på side 3](#)
- [Ny og endret informasjon om fastvareversjon 12.5\(1\)SR1, på side 3](#)
- [Ny og endret informasjon om fastvareversjon 12.5\(1\), på side 3](#)
- [Ny og endret informasjon om fastvareversjon 12.1\(1\), på side 4](#)

Ny og endret informasjon om fastvareversjon 14.2(1)

Følgende informasjon er ny eller endret for fastvareversjon 14.2(1).

Funksjon	Ny eller endret
Støtte for SIP OAuth på SRST	Utvidet sikkerhet i telefonnettverket, på side 56

Ny og endret informasjon om fastvareversjon 14.1(1)

Følgende informasjon er ny eller endret for fastvareversjon 14.1(1).

Funksjon	Ny eller endret
SIP OAuth for proxy TFTP-støtte	Utvidet sikkerhet i telefonnettverket, på side 56
Telefonoverføring uten overgangsbelastning	Migrering av telefonen til en telefon med flere plattformer direkte, på side 71

Ny og endret informasjon om fastvareversjon 14.0(1)

Tabell 1: Ny og endret informasjon

Funksjon	Nye eller endrede deler
SIP OAuth-forbedringer	Utvidet sikkerhet i telefonnettverket, på side 56
Forbedringer i brukergrensesnittet	Survivable Remote Site Telephony, på side 48
OAuth-forbedringer for MRA	Mobil og ekstern tilgang gjennom Expressway, på side 97

Som med fastvareversjon 14,0, støtter telefonene DTLS 1,2. DTLS 1,2 krever Cisco Adaptive Security-aktivering (ASA) versjon 9,10 eller nyere. Du konfigurerer den minste DTLS-versjonen for en VPN-tilkobling i ASA. For mer informasjon, se *ASDM Bok 3: Cisco ASA-serien VPN ASDM-konfigurasjonsveiledning* på <https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html>

Ny og endret informasjon om fastvareversjon 12.8(1)

Følgende informasjon er ny eller endret i fastvareversjon 12.8 (1).

Funksjon	Nytt eller endret innhold
Overføring av telefondata	Endre telefonmodell for en bruker, på side 37
Legg til mer informasjon om webtilgangsfeltet	Produktspesifikk konfigurasjon, på side 75

Ny og endret informasjon om fastvareversjon 12.7(1)

Ingen oppdateringer av administrasjonsveiledning var nødvendige for fastvareversjon 12.7(1).

Ny og endret informasjon om fastvareversjon 12.6(1)

Ingen oppdateringer av administrasjonsveiledning var nødvendige for fastvareversjon 12.6(1).

Ny og endret informasjon om fastvareversjon 12.5(1)SR3

Alle referanser til dokumentasjonen for Cisco Unified Communications Manager har blitt oppdatert til å støtte alle versjoner av Cisco Unified Communications Manager.

Følgende tabell viser endringer i *administrasjonsguiden for Cisco Unified Communications Manager for Cisco IP-konferansetelefon 7832* slik at den støtter fastvareversjon 12.5(1)SR3.

Tabell 2: Revisjoner til administrasjonsguiden for Cisco IP Phone 7832 for fastvareversjon 12.5(1)SR3

Endring	Nytt eller oppdatert område
Støtte for registrering av aktiveringskode og Mobil and Remote Access	Aktiveringskode for registrering og Mobile and Remote Access, på side 27
Støtte for bruk av problemrapportverktøyet fra Cisco Unified Communications Manager.	Opprette en telefonproblemrappport fra Cisco Unified Communications Manager, på side 148

Ny og endret informasjon om fastvareversjon 12.5(1)SR2

Ingen oppdateringer av administrasjonsveiledning var nødvendige for fastvareversjon 12.5(1)SR2.

Fastvareversjon 12.5(1)SR2 erstatter fastvareversjon 12.5(1) og fastvare 12.5(1)SR1. Fastvareversjon 12.5(1) og fastvareversjon 12.5(1)SR1 er utsatt til fordel for fastvareversjon 12.5(1)SR2.

Ny og endret informasjon om fastvareversjon 12.5(1)SR1

Følgende tabell viser endringer i *administrasjonsguiden for Cisco Unified Communications Manager for Cisco IP-konferansetelefon 7832* slik at den støtter fastvareversjon 12.5(1)SR1.

Tabell 3: Endringer i administrasjonsguiden for Cisco IP-konferansetelefon 7832 for fastvareversjon 12.5(1)SR1

Endring	Nytt eller oppdatert område
Støtte for elliptisk kurve	Støttede sikkerhetsfunksjoner, på side 57
Støtte for mediebaner og interaktiv etablering av tilkoblinger	Mediebaner og interaktiv etablering av tilkoblinger, på side 99
Støtte for registrering med aktiveringskode	Aktiveringskode for registrering av lokale telefoner, på side 26

Ny og endret informasjon om fastvareversjon 12.5(1)

Følgende tabell viser endringer i *administrasjonsguiden for Cisco Unified Communications Manager for Cisco IP-konferansetelefon 7832* slik at den støtter fastvareversjon 12.5(1).

Tabell 4: Endringer i administrasjonsguiden for Cisco IP-konferansetelefon 7832 for fastvareversjon 12.5(1)

Endring	Nytt eller oppdatert område
Støtte for dempet internkommunikasjon på Cisco Unified Communications Manager Express	Samhandling med Cisco Unified Communications Manager Express, på side 19
Støtte for deaktivering av TLS-chifre	Produktspesifikk konfigurasjon, på side 75

Endring	Nytt eller oppdatert område
Støtte for Enbloc-oppringing for tastepausetidaker T.302-utvidelsen.	Produktspesifikk konfigurasjon, på side 75

Ny og endret informasjon om fastvareversjon 12.1(1)

Følgende tabell viser endringer som er gjort i *administrasjonsguiden for Cisco Unified Communications Manager for Cisco IP-konferansetelefon 7832* slik at den støtter fastvareversjon 12.1(1).

Endring	Nytt eller oppdatert område
Støtte for Mobile and Remote Access gjennom Expressway	<ul style="list-style-type: none"> • Mobil og ekstern tilgang gjennom Expressway, på side 97 • Distribusjonsscenarioer, på side 98 • Konfigurere lagring av brukerlegitimasjon for Expressway-pålogging, på side 99
Støtte for aktivering eller deaktivering av TLS 1.2 for webservertilgang	Produktspesifikk konfigurasjon, på side 75
Støtte for G722.2 AMR-WB lydkodek	<ul style="list-style-type: none"> • Den Cisco IP Conference Phone 7832, på side 7 • Felt i Anropsstatistikk, på side 116



DEL **I**

Om Cisco IP-konferansetelefonen

- [Maskinvare for Cisco IP-konferansetelefoner, på side 7](#)
- [Tekniske detaljer, på side 13](#)



KAPITTEL 2

Maskinvare for Cisco IP-konferansetelefoner

- [Den Cisco IP Conference Phone 7832, på side 7](#)
- [Knapper og maskinvare på Cisco IP-telefon 7832, på side 9](#)
- [Beslektet dokumentasjon, på side 10](#)
- [Dokumentasjon, støtte og retningslinjer for sikkerhet, på side 10](#)
- [Terminologiforskjeller, på side 11](#)

Den Cisco IP Conference Phone 7832

Cisco IP Conference Phone 7832 styrker kommunikasjon med mennesker i sentrum og kombinerer overlegen høydefinisjon (HD) lydprestasjon og 360 graders dekning for konferanserom og lederkontorer i alle størrelser. Høytaleren har full dupleks, håndfrifunksjonalitet og toveis bredbåndslid (G.722) som gir en fantastisk lydopplevelse. Cisco IP Conference Phone 7832 er en enkel løsning som imøtekommer utfordringene til de fleste romtyper.



Telefonen har sensitive mikrofoner med 360-graders dekning. Denne dekningen gjør det mulig for brukerne å prate med normal stemme og likevel bli tydelig hørt opptil 2,10 meter unna. Telefonen har også teknologi

som motvirker interferens fra mobiltelefoner og andre trådløse enheter, og dermed sørger for at kommunikasjonen er klar og tydelig uten forstyrrelser.

Som andre enheter må en Cisco IP-telefon konfigureres og administreres. Disse telefonene koder og dekoder følgende kodeker:

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



Forsiktig Bruk av en mobiltelefon eller GSM-telefon eller toveis radio i nærheten av en Cisco IP-telefon, kan føre til forstyrrelser. Hvis du vil ha mer informasjon, kan du se produsentdokumentasjonen for enheten som forårsaker forstyrrelsen.

Cisco IP-telefoner formidler tradisjonell telefonifunksjonalitet, for eksempel viderekobling av samtaler og overføring, ny oppringing, kortnumre, telefonkonferanse og tilgang til et talemeldingssystem. Cisco IP-telefoner formidler også en rekke andre funksjoner.

På samme måte som med andre nettverksenheter må du konfigurere Cisco IP-telefoner slik at de blir klargjort for tilgang til Cisco Unified Communications Manager og resten av IP-nettverket. Ved hjelp av DHCP har du færre innstillinger å konfigurere på en telefon. Hvis nettverket krever det, kan du imidlertid konfigurere informasjon manuelt, for eksempel IP-adresse, TFTP-server og subnettsinformasjon.

Cisco IP-telefon kan samhandle med andre tjenester og enheter i IP-nettverket for å formidle utvidet funksjonalitet. Du kan for eksempel integrere Cisco Unified Communications Manager med LDAP3-protokollen (Lightweight Directory Access Protocol 3) for standard bedriftskatalog for å gi brukere muligheten til å søke etter kontaktinformasjon om kollegaer direkte fra sin IP-telefon. Du kan også bruke XML til å gi brukere muligheten til å få tilgang til informasjon om for eksempel vær, aksjer, dagens sitat og annen nettbasert informasjon.

Cisco IP-telefon er en nettverksenhet, og derfor kan du også hente detaljert statusinformasjon direkte fra den. Ved hjelp av denne informasjonen kan du få hjelp med feilsøking av problemer som brukere kanskje opplever ved bruk av IP-telefonen. Du kan også vise statistikk om en aktiv samtale eller fastvareversjoner på telefonen.

For at Cisco IP-telefon skal fungere i IP-telefonnettverket, må den kobles til en nettverksenhet, for eksempel en Cisco Catalyst-svitsj. Du må også registrere Cisco IP-telefon med et Cisco Unified Communications Manager-system før du sender og mottar samtaler.




Knapper og maskinvare på Cisco IP-telefon 7832


Følgende figur viser Cisco IP-konferansetelefon 7832.

Figur 1: Knapper og funksjoner på Cisco IP-konferansetelefon 7832



Tabellen nedenfor beskriver knappene på Cisco IP-konferansetelefon 7832.

1	Demp-feltet	 Slå mikrofonen på eller av. Når mikrofonen er dempet, lyser LED-stripen rødt.
2	LED-stripe	Indikerer anropsstatuser: <ul style="list-style-type: none"> • Grønn, lysende – aktiv samtale • Grønn, blinkende – innkommende anrop • Grønn, pulserende – samtale på vent • Rød, lysende – dempet samtale
3	Funksjonsknapper	 Få tilgang til funksjoner og tjenester.
4	Navigasjonsfeltet og Velg -tasten	 Bla gjennom menyer, uthev elementer, og velg det uthevede elementet. Når telefonen er ledig, trykker du på Opp for å få tilgang til listen over sist brukte samtaler, og Ned for å få tilgang til listen over favoritter.

5	Volumknapp	 <p>Juster volumet på den høytalende telefonen (telefonrøret er av) og ringevolumet (telefonrøret er på).</p> <p>Når du endrer volumet, lyser LED-stripelyset hvitt for å vise at volumet endres.</p>
---	------------	--

Funksjonsknapper på konferansetelefoner

Du får tilgang til funksjonene på telefonen ved hjelp av funksjonstastene. Funksjonstaster, som du finner under skjermen, gir deg tilgang til funksjonen som vises på skjermen over funksjonstasten. De programmerbare funksjonstastene endres avhengig av hva du gjør for øyeblikket.

Funksjonstastene ●●-funksjonstasten angir at flere funksjonstastfunksjoner er tilgjengelige.

Beslektet dokumentasjon

Bruk de følgende avsnittene til å få relevant informasjon.

Dokumentasjon for Cisco IP-konferansetelefon 7832

Finn dokumentasjon som er spesifikk for ditt språk, telefonmodell og anropskontrollsystem på siden [produktstøtte](#) for Cisco IP-telefon 7800-serien.

Dokumentasjon Cisco Unified Communications Manager

Se *Cisco Unified Communications Manager-dokumentasjonsveiledningen* og andre publikasjoner som er spesifikke for din versjon av Cisco Unified Communications Manager. Naviger fra følgende dokumentasjons-URL:

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

Dokumentasjon Cisco Business Edition 6000

Se *Cisco Business Edition 6000-dokumentasjonsveiledningen* og andre publikasjoner som er spesifikke for din versjon av Cisco Business Edition 6000. Naviger fra følgende URL:

<https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html>

Dokumentasjon, støtte og retningslinjer for sikkerhet

Hvis du vil ha informasjon om hvordan du henter dokumentasjon, får kundestøtte, formidler tilbakemelding om dokumentasjon, går gjennom retningslinjene for sikkerhet samt får tilgang til anbefalte aliaser og generelle

Cisco-dokumenter, kan du se den månedlige nyhetsartikkelen *What's New in Cisco Product Documentation*, som også viser en oversikt over all ny og revidert teknisk Cisco-dokumentasjon, på følgende adresse:

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

Abonner på *Nyheter innen produktdokumentasjon fra Cisco* som en RSS-feed (Really Simple Syndication) og angi at innholdet skal leveres direkte til skrivebordet ved hjelp av et leserprogram. RSS-feedene er en gratistjeneste, og Cisco støtter for øyeblikket RSS versjon 2.0.

Sikkerhetsoversikt for Cisco-produktet

Dette produktet inneholder kryptografiske funksjoner og er underlagt amerikansk lovgivning og lokal lovgivning om import, eksport, overføring og bruk. Levering av kryptografiske Cisco-produkter gir ikke tredjeparter rett til å importere, eksportere, distribuere eller bruke kryptering. Importører, eksportører, distributører og brukere er ansvarlige for å overholde lovgivningen i USA og lokal lovgivning for det enkelte land. Ved å bruke dette produktet, samtykker du til å følge gjeldende lover og regler. Hvis du ikke kan overholde amerikansk og lokal lovgivning, må du returnere dette produktet umiddelbart.

Mer informasjon om amerikanske eksportbestemmelser finner du på <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>.

Terminologiforskjeller

I dette dokumentet inkluderer termen *Cisco IP-telefon* Cisco IP-konferansetelefon 7832.

Tabellen nedenfor inneholder noen av terminologiforskjellene i *brukerveiledningen for Cisco IP-konferansetelefon 7832*, *administrasjonsguiden for Cisco IP-konferansetelefon 7832 for Cisco Unified Communications Manager* og dokumentasjonen for Cisco Unified Communications Manager.

Tabell 5: Terminologiforskjeller

Brukerveiledning	Administrasjonsveiledning
Meldingsindikatorer	Melding venter-indikator (MWI)
Talepostsystem	Talemeldingssystem



KAPITTEL 3

Tekniske detaljer

- Spesifikasjoner for fysisk miljø og operativmiljø, på side 13
- Kabelspesifikasjoner, på side 14
- Krav til telefonstrøm, på side 14
- Støttede nettverksprotokoller, på side 15
- Samhandling med Cisco Unified Communications Manager, på side 19
- Samhandling med Cisco Unified Communications Manager Express, på side 19
- Samhandling med talemeldingssystem, på side 20
- Telefonkonfigurasjonsfiler, på side 20
- Telefonens oppførsel under stor trafikk på nettverket, på side 21
- Programmeringsgrensesnitt, på side 21

Spesifikasjoner for fysisk miljø og operativmiljø

Tabellen nedenfor viser spesifikasjoner for fysisk miljø og operativmiljø for konferansetelefonen.

Tabell 6: Spesifikasjoner for fysisk miljø og operativmiljø

Spesifikasjon	Verdi eller skala
Driftstemperatur	32° til 104°F (0 til 40 °C)
Relativ luftfuktighet under bruk	10 % til 90 % (ikke-kondenserende)
Oppbevaringstemperatur	14° til 140°F (-10 til 60 °C)
Høyde	8,9 tommer (226 mm)
Bredde	8,9 tommer (226 mm)
Dybde	2,14 tommer (54,4 mm)
Vekt	2,0 lb (0,907 kg)

Spesifikasjon	Verdi eller skala
Strøm	<ul style="list-style-type: none"> IEEE PoE klasse 2. Telefonen er kompatibel med både IEEE 802.3af og IEEE 802.3at LLDP-protokoll (Link Layer Discovery Protocol) – Power over Ethernet Hvis de tilkoblede LAN-svitsjene ikke støtter PoE, kreves en ekstern PoE
Kabler	Kategori 3/5/5e/6 for 10-Mbps-kabler med 4 par Kategori 5/5e/6 for 100-Mbps-kabler med 4 par Merk Kabler har 4 par med ledninger med totalt 8 ledere.
Distansekrav	I henhold til Ethernet-spesifikasjonen er maksimum kabellengde mellom

Hvis du vil ha mer informasjon, kan du se *databladet for Cisco IP-konferansetelefon 7832*:
<http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7800-series/datasheet-listing.html>

Kabelfesifikasjoner

- RJ-45-kontakt for LAN 10/100BaseT-tilkoblingen.

Krav til telefonstrøm

Cisco IP-konferansetelefon kan bruke disse strømkildene:

- Power over Ethernet (PoE)
- Cisco IP-konferansetelefon 7832 PoE midspankabel og Cisco Power Cube 3
- Cisco IP-telefon strøminjektor



Merk Midspankabelen er ikke tilgjengelig for øyeblikket.

Tabell 7: Retningslinjer for Cisco IP-konferansetelefon-strøm

Strømtype	Retningslinjer
PoE-strøm: Formidles av en svitsj via Ethernet-kabelen som er knyttet til telefonen.	Hvis du vil sikre uforstyrret bruk av telefonen, må du sørge for at svitsjen har en reservestrømforsyning. Kontroller at CatOS- eller IOS-versjonen som kjører på svitsjen, støtter din tiltenkte telefon. Se dokumentasjonen for svitsjen for informasjon om operativsystemversjonen.

Strømtype	Retningslinjer
Ekstern strøm – leveres via Cisco IP-konferansetelefon 7832 PoE midspankabel og Cisco Power Cube 3	Midspankabelen og strømadapteren gir strøm til Ethernet-kabelen. Når du installerer en telefon som bruker strøm fra midspanadapteren, kobler du a strømforsyningen før du kobler Ethernet-kabelen til telefonen. Når du fjerner en t bruker midspanadapteren, må du koble Ethernet-kabelen fra telefonen før du fjern strømforsyningen fra adapteren.
Ekstern strøm – leveres via Cisco IP-telefon-strøminjektoren	Strøminjektoren gir strøm til Ethernet-kabelen. Når du installerer en telefon som bruker strøm fra strøminjektoren, kobler du inje strømforsyningen før du kobler Ethernet-kabelen til telefonen. Når du fjerner en t bruker injektoren, må du koble Ethernet-kabelen fra telefonen før du fjerner strøm fra injektoren.

Strømstans

Tilgangen til nødtefontjenester via telefonen krever at telefonen får strøm. Hvis et avbrudd i strømforsyningen oppstår, fungerer ikke nødtefontjenesten før strømmen er tilbake igjen. Hvis strømstans eller andre forstyrrelser oppstår, må du kanskje tilbake stille eller rekonfigurere utstyret på nytt før du kan bruke nødtefontjenesten.

Strømreduksjon

Du kan redusere mengden energi som Cisco IP-telefon bruker, ved hjelp av modusen Strømsparing eller EnergyWise (Power Save Plus).

Strømsparing

I modusen Strømsparing er ikke bakgrunnsbelysningen på skjermen slått på når telefonen ikke er i bruk. Telefonen forblir i strømsparingsmodus i angitt tid eller til brukeren trykker på en tast.

Power Save Plus (EnergyWise)

Cisco IP-telefon støtter modusen Cisco EnergyWise (Power Save Plus). Når nettverket inneholder en EW-kontroller (EnergyWise), for eksempel en Cisco-svitsj med funksjonen EnergyWise aktivert, kan du konfigurere disse telefonene til å gå til hvilemodus (avslått) og aktiveringsmodus (påslått) etter en definert plan for å redusere strømforbruket ytterligere.

Konfigurer hver telefon til å aktivere eller deaktivere innstillinger for EnergyWise. Hvis EnergyWise er aktivert, konfigurer du et tidspunkt for hvilemodus og aktiveringsmodus samt andre parametere. Disse parametere sendes til telefonen som en del av XML-filen for telefonkonfigurasjonen.

Beslektede emner

[Planlegge strømsparing for Cisco IP-telefoner](#), på side 87

[Planlegge EnergyWise på Cisco IP-telefoner](#), på side 89

Støttede nettverksprotokoller

Cisco IP-konferansetelefoner støtter flere bransjestandardprotokoller og Cisco-nettverksprotokoller som kreves for talekommunikasjon. Tabellen nedenfor viser en oversikt over nettverksprotokollene som telefonene støtter.

Tabell 8: Støttede nettverksprotokoller på Cisco IP-konferansetelefon

Nettverksprotokoll	Formål	Bruksmerknader
BootP-protokoll (Bootstrap Protocol)	BootP aktiverer en nettverksenhet, for eksempel telefonen, for å oppdage bestemt oppstartsinformasjon, for eksempel IP-adressen.	–
CDP-protokoll (Cisco Discovery Protocol)	CDP er en enhetsregistreringsprotokoll som fungerer på alt Cisco-produsert utstyr. En enhet kan bruke CDP til å flagge til eksistens for andre enheter og motta informasjon om andre enheter i nettverket.	Telefonen bruker CDP til å formidle informasjon, for eksempel ekstra VLAN-ID, strømstyringsdetaljer per port og informasjon om QoS-konfigurasjon (Quality of Service) med Ciscos Catalyst-svitsjen.
DHCP-protokoll (Dynamic Host Configuration Protocol)	DHCP tildeler og tilordner en IP-adresse dynamisk til nettverksenheter. Ved hjelp av DHCP kan du koble til en IP-telefon i nettverket slik at telefonen kan brukes uten at du trenger å tilordnet en IP-adresse manuelt eller konfigurere ekstra nettverksparametere.	DHCP er aktivert som standard. Hvis DHCP er deaktivert, må du konfigurere IP-adressen, nettverksmasken, gatewayen og en TFTP-server manuelt på hver telefon lokalt. Det anbefales at du bruker det tilpassede DHCP-alternativet 150. Ved hjelp av denne metoden kan du konfigurere TFTP-serverens IP-adresse som alternativverdi. Hvis du vil ha flere støttede DHCP-konfigurasjoner, kan du se dokumentasjon for din versjon av Cisco Unified Communications Manager. Merk Hvis du ikke kan bruke alternativ 150, bruker du DHCP-alternativ 66.
HTTP-protokoll (Hypertext Transfer Protocol)	HTTP er standardprotokollen for overføring av informasjon og flytting av dokumenter på tvers av Internett.	Telefoner bruker HTTP til XML-tjenester, klargjøring, oppgraderinger og feilsøkinger.
HTTPS-protokoll (Hypertext Transfer Protocol Secure)	HTTPS er en kombinasjon av HTTP med SSL/TLS-protokollen, som gir kryptering og sikker identifikasjon av servere.	Nettapplikasjoner med både HTTP- og HTTPS-støtte har to URL-er konfigurert. Telefoner som støtter HTTPS, velger HTTPS-URL-en. Et låseikon vises hvis tilkoblingen til tjenesten skjer via HTTPS.

Nettverksprotokoll	Formål	Bruksmerknader
IEEE 802.1X	IEEE 802.1X-standarden definerer en klientserverbasert tilgangskontroll og godkjenningsprotokoll som hindrer at uautoriserte klienter kan koble til et lokalt nettverk via offentlig tilgjengelige porter. Før klienten er godkjent, tillater 802.1X-tilgangskontrollen bare EAPOL-trafikk (Extensible Authentication Protocol over LAN) via porten som klienten er koblet til. Etter at godkjenningen er bekreftet, kan normal trafikk gå via porten.	Telefonen implementerer IEEE 802.1X-standarden via støtte for følgende godkjenningsmetoder: EAP-FAST og EAP-TLS. Når 802.1X-godkjenning er aktivert på telefonen, må du deaktivere tale-VLAN.
IP-protokoll (Internet Protocol)	IP er en meldingsprotokoll som adresserer og sender pakker på tvers av nettverket.	Hvis nettverksenheter vil kommunisere med IP, må de ha en tilordnet IP-adresse, nettverk og gateway. ID-er for IP-adresser, subnett og gatewayer blir tilordnet automatisk hvis du bruker telefonen med DHCP-protokollen (Dynamic Host Configuration Protocol). Hvis du ikke bruker DHCP, må du tilordne disse egenskapene manuelt til hver telefon lokalt. Telefonene støtter IPv6-adresse. Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.
LLDP-protokoll (Link Layer Discovery Protocol)	LLDP er en standardisert nettverksregistreringsprotokoll (minner om CDP) som støttes på noen Cisco- og tredjepartsenheter.	Telefonen støtter LLDP på PC-porten.
LLDP-MED-protokoll (Link Layer Discovery Protocol-Media Endpoint Devices)	LLDP-MED er en utvidelse av LLDP-standarden som er utviklet for taleprodukter.	Telefonen støtter LLDP-MED på svitsjporten for formidling av informasjon, for eksempel: <ul style="list-style-type: none"> • Konfigurasjon av Tale-VLAN • Enhetsregistrering • Strømstyring • Lagerstyring Hvis du ønsker mer informasjon om støtte for LLDP-MED, kan du se dokumentet <i>LLDP-MED and Cisco Discovery Protocol</i> på denne koblingen: http://www.cisco.com/US/tech/telecom/cisco_wlc_ppa000a00466.html
RTP-protokoll (Real-Time Transport Protocol)	RTP er en standardprotokoll for transport av sanntidsdata, for eksempel interaktiv tale og video, via datanettverk.	Telefoner bruker RTP-protokollen til å sende og motta taletrafikk i sanntid fra andre telefoner og gatewayer.

Nettverksprotokoll	Formål	Bruksmerknader
RTCP-protokoll (Real-Time Control Protocol)	RTCP fungerer sammen med RTP for å formidle QoS-data (for eksempel jitter, ventetid og rundturforsinkelse) i RTP-strømmer.	RTCP er aktivert som standard.
SIP-protokoll (Session Initiation Protocol)	SIP er IETF-standarden (Internet Engineering Task Force) for multimediekonferanser via IP. SIP er en ASCII-basert programlagsprotokoll (definert i RFC 3261) som kan brukes til å opprette, vedlikeholde og avslutte samtaler mellom to eller flere endepunkter.	På samme måte som andre VoIP-protokoller, er SIP utformet til å adressere funksjonene for signaliserings- og øktbehandling i et pakketelefonnettverk. Signalisering tillater at samtaleinformasjon kan overføres på tvers av nettverk. Øktbehandling gi muligheten til å kontrollere attributtene til en ende-til-ende-samtale. Cisco IP-telefon støtter SIP-protokollen når telefonene opererer i Kun IPv6, Kun IPv4 og både i Kun IPv4 og Kun IPv6.
SRTP-protokoll (Secure Real-Time Transfer protocol)	SRTP er en utvidelse av lyd-/videoprofilen for RTP-protokollen, og den sørger for integriteten til RTP- og RTCP-pakkene ved å formidle godkjenning, integritet og kryptering av mediepakker mellom to endepunkter.	Telefoner bruker SRTP til kryptering av medier.
TCP-protokoll (Transmission Control Protocol)	TCP er en tilkoblingsorientert transportkontroll.	Telefoner bruker TCP til å koble til Cisco Unified Communications Manager og til å få tilgang til XML-tjenester.
TLS-protokoll (Transport Layer Security)	TLS er en standardprotokoll for sikring og godkjenning av kommunikasjon.	Når sikkerhet er implementert, bruker telefoner TLS-protokollen for sikker registrering med Cisco Unified Communications Manager. Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.
TFTP-protokoll (Trivial File Transfer Protocol)	Ved hjelp av TFTP kan du overføre filer via nettverket. På telefonen kan du ved hjelp av TFTP hente en konfigurasjonsfil som er spesifikk for telefontypen.	TFTP krever en TFTP-server i nettverket, og denne kan identifiseres automatisk fra DHCP-serveren. Hvis du vil at en telefon skal bruke en annen TFTP-server enn den som er angitt av DHCP-serveren, må du tilordne IP-adressen for TFTP-serveren manuelt ved hjelp av menyen Nettverksoppsett på telefonen. Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.
UDP-protokoll (User Datagram Protocol)	UDP er en forbindelsesløs meldingsprotokoll for levering av datapakker.	Telefoner sender og mottar RTP-strømmer, som bruker UDP.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Samhandling med Cisco Unified Communications Manager

Cisco Unified Communications Manager er et åpent samtalebehandlingssystem i bransjestandarden. Programvaren for Cisco Unified Communications Manager starter og avslutter samtaler mellom telefoner, og integrerer tradisjonell PBX-funksjonalitet med IP-bedriftsnettverket. Cisco Unified Communications Manager håndterer komponentene i telefonisystemet, som for eksempel telefoner, tilgangsgatewayer og ressurser som er nødvendige for funksjoner som telefonkonferanser og rutingplanlegging. Cisco Unified Communications Manager formidler også:

- Fastvare for telefoner
- CTL-filer (Certificate Trust List) og ITL-filer (Identity Trust List) som bruker TFTP og HTTP tjenester
- Telefonregistrering
- Samtalebevaring, slik at en medieøkt fortsetter hvis signalisering blir avbrutt mellom den primære kommunikasjonsbehandleren og en telefon

Du finner informasjon om hvordan du konfigurerer Cisco Unified Communications Manager til å fungere med telefonene som er beskrevet i dette kapitlet, i dokumentasjonen for din spesifikke versjon av Cisco Unified Communications Manager.



Merk Hvis telefonmodellen du vil konfigurere, ikke vises i rullegardinlisten Telefontype i Cisco Unified Communications Manager Administration, installerer du den siste enhetspakken for din versjon av Cisco Unified Communications Manager fra Cisco.com.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Samhandling med Cisco Unified Communications Manager Express

Når telefonen fungerer med Cisco Unified Communications Manager Express (Unified CME), må den gå i CME-modus.

Når en bruker starter konferansesfunksjonen, tillater koden at telefonen bruker lokal eller nettverksbasert maskinvare for konferansebroen.

Telefonene støtter ikke følgende handlinger:

- Overføring – støttes bare i et scenario med overføring av oppkoblet samtale.
- Konferanse – støttes bare i et scenario med overføring av oppkoblet samtale.
- Delta – støttes ved bruk av Konferanse-knappen eller tilbakeringingstilgang.
- Vent – støttes ved hjelp av Vent-knappen.
- Bryte inn og slå sammen – støttes ikke.

- Direkte overføring – støttes ikke.
- Velg – støttes ikke.

Brukere kan ikke opprette konferanser og overføre samtaler på tvers av forskjellige linjer.

Unified CME støtter intercom-samtaler, her også kalt dempet internkommunikasjon. Men siden avvises av telefonen under samtaler.

Samhandling med talemeldingssystem

Cisco Unified Communications Manager lar deg integrere med forskjellige talemeldingssystemer, inkludert Cisco Unity Connection-talemeldingssystemet. Fordi du kan integrere med ulike systemer, må du gi brukere informasjon om hvordan de bruker ditt bestemte system.

Hvis du vil gjøre det mulig for en bruker å overføre til talepost, kan du sette opp et * xxxxx-ringemønster og konfigurere det som Viderekoble alle anrop til talepost. Hvis du vil ha mer informasjon, kan du se dokumentasjonen for Cisco Unified Communications Manager.

Gi følgende informasjon til hver bruker:

- Hvordan de får tilgang til talemeldingssystem-kontoen.
 - Pass på at du har brukt Cisco Unified Communications Manager til å konfigurere Meldinger-knappen på Cisco IP-telefon.
- Startpassordet som gir tilgang til talemeldingssystemet.
 - Konfigurer et standard passord for talemeldingssystemet for alle brukere.
- Hvordan telefonen angir at det er talemeldinger som venter.
 - Bruk Cisco Unified Communications Manager til å sette opp en melding venter-indikator-metode (MWI).

Telefonkonfigurasjonsfiler

Konfigurasjonsfiler for en telefon blir lagret på TFTP-serveren og angir parametre for tilkobling til Cisco Unified Communications Manager. Når du gjør endringer i Cisco Unified Communications Manager som krever at telefonen blir tilbakestilt, endres vanligvis telefonkonfigurasjonsfilen automatisk.

Konfigurasjonsfiler inneholder også informasjon om hvilken bildeinnlasting telefonen skal kjøre. Hvis denne bildeinnlastingen er forskjellig fra den som er lastet på telefonen, kontakter telefonen TFTP-serveren for å be om de nødvendige innlastingsfilene.

Hvis du konfigurerer sikkerhetsrelaterte innstillinger i Cisco Unified Communications Manager Administration, inneholder telefonkonfigurasjonsfilen sensitive opplysninger. Du kan beskytte opplysningene i en konfigurasjonsfil ved å konfigurere den for kryptering. Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager. En telefon ber om en konfigurasjonsfil når den blir tilbakestilt og registreres hos Cisco Unified Communications Manager.

En telefon har tilgang til en standard konfigurasjonsfil kalt XmlDefault.cnf.xml på TFTP-serveren når følgende betingelser er oppfylt:

- Du har aktivert automatisk registrering i Cisco Unified Communications Manager

- Telefonen har ikke blitt lagt til i Cisco Unified Communications Manager-databasen
- Telefonen registreres for første gang

Telefonens oppførsel under stor trafikk på nettverket

Alt som svekker nettverksytelsen, kan påvirke lyd kvaliteten på telefonen, og i noen tilfeller kan det avbryte en samtale. Kilder til ytelsesreduksjon kan innbefatte, men er ikke begrenset til, følgende aktiviteter:

- Administrative oppgaver, som en intern portskanning eller en sikkerhetsskanning.
- Angrep på nettverket, som et tjenestenektangrep.

Approgrammeringsgrensesnitt

Cisco støtter bruk av telefonens API fra tredjepartsprogrammer som er testet og sertifisert gjennom Cisco av programutvikleren fra tredjepart. Eventuelle telefonproblemer som er knyttet til ikke-sertifisert programsamhandling, må være behandlet av tredjeparten, og vil ikke bli behandlet av Cisco.

Hvis du vil ha støttemodell for Cisco sertifiserte tredjepartsprogrammer/løsninger, kan du se nettsiden [Cisco Solution Partner-program](#) for å få mer informasjon.



DEL II

Installasjon av telefoner

- [Installasjon av Cisco IP-konferansetelefoner, på side 25](#)
- [Installasjon av telefoner i Cisco Unified Communications Manager, på side 39](#)
- [Administrasjon av selvhjelpsportal, på side 51](#)



KAPITTEL 4

Installasjon av Cisco IP-konferansetelefoner

- Bekrefte nettverksoppsettet, på side 25
- Aktiveringskode for registrering av lokale telefoner, på side 26
- Aktiveringskode for registrering og Mobile and Remote Access, på side 27
- Aktivere automatisk registrering av telefoner, på side 27
- Installere konferansetelefonen, på side 29
- Konfigurere telefonen fra oppsettsmenyene, på side 30
- Konfigurere nettverksinnstillingene, på side 32
- Bekrefte telefonoppstarten, på side 37
- Endre telefonmodell for en bruker, på side 37

Bekreft nettsoppsettet

Ved distribusjon av et nytt IP-telefonisystem må systemansvarlige og nettverksadministratorer gjennomføre flere innledende konfigurasjonsoppgaver for å klargjøre nettverket for IP-telefonitjenesten. Hvis du vil ha informasjon og en kontrolliste for oppsett og konfigurasjon av et Cisco IP-telefoninettverk, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Hvis telefonen skal fungere optimalt som et endepunkt i nettverket, må nettverket oppfylle bestemte krav. Ett krav er riktig båndbredde. Telefonene krever mer båndbredde enn de anbefalte 32 kbps når de registreres i Cisco Unified Communications Manager. Vurder dette høyere båndbreddekravet når du konfigurerer din QoS-båndbredde. For mer informasjon kan du se *Cisco Collaboration System 12.x Solution Reference Network Designs (SRND)* eller nyere (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html).



Merk Telefonen viser dato og klokkeslett fra Cisco Unified Communications Manager. Klokkeslettet som vises på telefonen, kan avvike fra klokkeslettet i Cisco Unified Communications Manager med inntil 10 sekunder.

Prosedyre

Trinn 1 Konfigurer et VoIP-nettverk til å oppfylle følgende krav:

- VoIP konfigureres på rutere og gatewayer.

- Cisco Unified Communications Manager installeres på nettverket og konfigureres til å håndtere samtalebehandling.

Trinn 2 Konfigurer nettverket til å støtte ett av følgende:

- DHCP-støtte
- Manuell tilordning av IP-adresse, gateway og nettverksmaske

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Aktiveringskode for registrering av lokale telefoner

Du kan bruke registrering med aktiveringskode til å sette opp nye telefoner på en rask måte uten å bruke automatisk registrering. Med denne fremgangsmåten styrer du registreringsprosessen med ett av følgende verktøy:

- Cisco Unified Communications verktøy for mengdeadministrasjon (BAT)
- Cisco Unified Communications Manager Administration-grensesnittet
- Administrative XML Web Service (AXL)

Aktiver denne funksjonen fra **enhetsinformasjon**-delen på telefonens konfigurasjonsside. Velg **Krev registrering med aktiveringskode** hvis du vil at denne funksjonen skal gjelde én enkelt lokal telefon.

Brukere må angi en aktiveringskode før telefonene kan registreres. Registrering med aktiveringskode kan brukes på enkelttelefoner, en gruppe med telefoner eller for et helt nettverk.

Det er en enkel måte for brukere å registrere telefonene sine på, fordi de bare oppgir en 16-sifret aktiveringskode. Koder oppgis manuelt eller med en QR-kode dersom telefonen har et videokamera. Vi anbefaler at du bruker en sikker metode for å gi brukere denne informasjonen. Når en bruker er tilordnet en telefon, er denne informasjonen tilgjengelig i selvhjelpsportalen. Når en bruker oppretter tilgang til koden gjennom portalen, føres dette i revisjonsloggen.

Aktiveringskoder kan bare brukes én gang, og de utløper som standard etter én uke. Hvis en kode utløper, må du gi brukeren en ny.

Du vil se at dette er en enkel måte å sikre nettverket på, da en telefon ikke kan bli registrert før MIC-sertifikatet (Manufacturing Installed Certificate) og aktiveringskoden har blitt bekreftet. Metoden gjør det også enkelt å registrere flere telefoner om gangen, da den ikke bruker verktøyet for automatisk registrert telefonstøtte (TAPS) eller automatisk registrering. Registreringshastigheten er én telefon per sekund, eller omtrent 3600 telefoner per time. Du kan legge til telefoner med Cisco Unified Communications Manager Administrative, med Administrative XML Web Service (AXL) eller med BAT.

Eksisterende telefoner tilbakestilles når de har blitt konfigurert for registrering med aktiveringskode. De registreres ikke før aktiveringskoden har blitt oppgitt og telefonens MIC har blitt bekreftet. Informer gjeldende brukere om at du vil gå over til registrering med aktiveringskode før du gjennomfører det.

Du finner mer informasjon i *Administrasjonsveiledning for Cisco Unified Communications Manager og IM og Presence Service, versjon 12.0(1)* eller nyere.

Aktiveringskode for registrering og Mobile and Remote Access

Du kan bruke registrering av aktiveringskode med Mobile and Remote Access ved distribusjon av Cisco IP-telefoner for eksterne brukere. Denne funksjonen er en sikker måte å distribuere lokale telefoner på når automatisk registrering ikke er nødvendig. Men du kan konfigurere en telefon for automatisk registrering når lokalt, og aktiveringskoder når lokalt. Denne funksjonen ligner på registrering av aktiveringskode for lokale telefoner, men den gjør også aktiveringskoden tilgjengelig for lokale telefoner.

Registrering av aktiveringskode for Mobile and Remote Access krever Cisco Unified Communications Manager 12.5 (1)SU1 eller nyere, og Cisco Expressway X 12.5 eller nyere. Smart lisensiering bør også være aktivert.

Du aktiverer denne funksjonen fra Cisco Unified Communications Manager Administration, men vær oppmerksom på følgende:

- Aktiver denne funksjonen fra **enhetsinformasjon**-delen på telefonens konfigurasjonsside.
- Velg **Krev registrering med aktiveringskode** hvis du vil at denne funksjonen bare skal gjelde én enkelt lokal telefon.
- Velg **Tillat aktiveringskode via MRA** og **Krev registrering med aktiveringskode** hvis du vil bruke registrering med aktiveringskode for en enkelt lokal telefon. Hvis telefonen er lokal, endres den til modus for Mobile and Remote Access og bruker Expressway. Hvis telefonen ikke kan nå Expressway, registreres den ikke før den ikke er lokal.

Hvis du vil ha mer informasjon, kan du se følgende dokumenter:

- *Administrasjonsveiledning for Cisco Unified Communications Manager og IM og Presence Service, versjon 12.0(1)*
- *Mobile and Remote Access via Cisco Expressway* for Cisco Expressway X12.5 eller senere

Aktivere automatisk registrering av telefoner

Cisco IP-telefon krever at Cisco Unified Communications Manager håndterer samtalebehandling. Se dokumentasjonen for din versjon av Cisco Unified Communications Manager eller den kontekstavhengige hjelpen i Cisco Unified Communications Manager Administration for å kontrollere at Cisco Unified Communications Manager er konfigurert riktig til å behandle telefonen og rute og behandle samtaler på riktig måte.

Før du installerer Cisco IP-telefon, må du velge en metode for å legge til telefoner i Cisco Unified Communications Manager-databasen.

Ved å aktivere automatisk registrering før du installerer telefonene, kan du:

- Legge til telefoner uten først å samle inn MAC-adresser fra telefonene.
- Legge til en Cisco IP-telefon automatisk i Cisco Unified Communications Manager-databasen når du kobler telefonen til IP-telefonnettverket. Under den automatiske registreringen tilordner Cisco Unified Communications Manager det neste sekvensielle katalognummeret til telefonen.
- Registrere telefoner raskt i Cisco Unified Communications Manager-databasen og endre innstillinger, for eksempel katalognumrene, fra Cisco Unified Communications Manager.

- Flytte automatisk registrerte telefoner til nye plasseringer og tilordne dem til andre enhetsutvalg uten at det påvirker telefonenes katalognumre.

Automatisk registrering er som standard deaktivert. I noen tilfeller vil du kanskje ikke bruke automatisk registrering, for eksempel hvis du vil tilordne et bestemt katalognummer til telefonen, eller hvis du vil bruke en sikker tilkobling med Cisco Unified Communications Manager. Hvis du vil ha informasjon om hvordan du aktiverer automatisk registrering, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager. Når du konfigurerer gruppen for kombinert modus via CTL-klienten for Cisco, blir automatisk registrering automatisk deaktivert, men det er mulig å aktivere denne funksjonen. Når du konfigurerer gruppen for usikret modus via CTL-klienten for Cisco, blir ikke automatisk registrering automatisk aktivert.

Du kan legge til telefoner med automatisk registrering og TAPS, som er verktøyet for automatisk registrert telefonstøtte (Tool for AutoRegistered Phones Support), uten først å samle inn MAC-adressene fra telefoner.

TAPS fungerer med masseadministrasjonsverktøyet (BAT) for å oppdatere en gruppe telefoner som allerede var lagt til i Cisco Unified Communications Manager-databasen med falske MAC-adresser. Bruk TAPS til å oppdatere MAC-adresser og laste ned forhåndsdefinerte konfigurasjoner for telefoner.

Cisco anbefaler at du bruker automatisk registrering og TAPS til å legge til færre enn 100 telefoner i nettverket. Hvis du vil legge til mer enn 100 telefoner i nettverket, bruker du masseadministrasjonsverktøyet (BAT).

Hvis du vil implementere TAPS, ringer du eller sluttbrukeren til et TAPS-katalognummer og følger taleinstruksjonene. Etter at prosessen er fullført, inneholder telefonen katalognummeret og andre innstillinger, og telefonen blir oppdatert i Cisco Unified Communications Manager Administration med den riktige MAC-adressen.

Bekreft at automatisk registrering er aktivert og er riktig konfigurert i Cisco Unified Communications Manager Administration før du kobler Cisco IP-telefon til nettverket. Hvis du vil ha informasjon om hvordan du aktiverer og konfigurerer automatisk registrering, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Automatisk registrering må aktiveres i Cisco Unified Communications Manager Administration for at TAPS skal fungere.

Prosedyre

-
- Trinn 1** I Cisco Unified Communications Manager Administration klikker du på **System > Telefon**.
- Trinn 2** Klikk på **Søk**, og velg den påkrevde serveren.
- Trinn 3** Konfigurer disse feltene i **Autoregistreringsinformasjon**.
- **Universell enhetsmal**
 - **Universell linjemal**
 - **Innledende katalognummer**
 - **Avsluttende katalognummer**
- Trinn 4** Fjern merket i avmerkingsboksen **Autoregistrering deaktivert på denne Cisco Unified Communications Manager**.
- Trinn 5** Klikk på **Lagre**.

Trinn 6 Klikk på **Bruk konfigurasjon**.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Installere konferansetelefonen

Etter at telefonen har koblet til nettverket, begynner telefonoppstartsprosessen og telefonen registreres i Cisco Unified Communications Manager. Du må konfigurere nettverksinnstillingene på telefonen hvis du deaktiverer DHCP-tjenesten.

Hvis du brukte automatisk registrering, må du oppdatere den spesifikke konfigurasjonsinformasjonen for telefonen, for eksempel knytte telefonen til en bruker, endre knappetabellen eller katalognummeret.

Når telefonen er koblet til, fastsetter den om en ny fastvareopplasting bør installeres på telefonen.

Før du begynner

Kontroller at du har den nyeste fastvareversjonen installert på din Cisco Unified Communications Manager. Se etter oppdaterte enhetspakker her:

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

Prosedyre

Trinn 1 Velg strømforsyningskilde for telefonen:

- Power over Ethernet (PoE)
- Cisco Unified IP-telefon-strøminjektor

Hvis du vil ha mer informasjon, kan du se [Måter du kan forsyne konferansetelefonen med strøm](#), på side 30.

Trinn 2 Koble telefonen til svitsjen.

- Hvis du bruker PoE, kobler du Ethernet-kabelen til LAN-porten og kobler den andre enden inn i telefonen.
- Hvis du bruker Cisco Unified IP-telefon-strøminjektoren, kobler du injektoren til LAN-porten med én Ethernet-kabel. Koble strømledningen til injektoren, og koble ledningen til det elektriske uttaket. Bruk en annen Ethernet-kabel til å koble injektoren til konferansetelefonen.

Hver telefon leveres med én Ethernet-kabel i boksen.

Trinn 3 Følg med på telefonoppstartsprosessen. Dette trinnet bekrefter at telefonen blir konfigurert riktig.

Trinn 4 Hvis du ikke bruker automatisk registrering, må du konfigurere sikkerhetsinnstillingene manuelt på telefonen.

Se [Konfigurere sikkerhetsinnstillingene](#), på side 63.

Trinn 5 La telefonen oppgradere til den gjeldende fastvareavbildningen som er lagret på din Cisco Unified Communications Manager.

Trinn 6 Foreta et anrop med telefonen for å bekrefte at den og funksjonene virker som de skal.

Trinn 7 Formidle informasjon til sluttbrukere om hvordan de bruker telefonen og konfigurerer telefonalternativene. Dette trinnet sørger for at brukere har tilstrekkelig informasjon, slik at de kan bruke Cisco-telefonene optimalt.

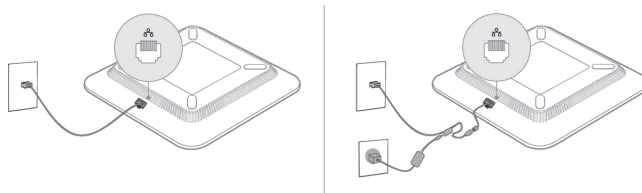
Måter du kan forsyne konferansetelefonen med strøm

Konferansetelefonen må ha strøm fra én av disse kildene:

- Power over Ethernet (PoE), som leveres av nettverket.
- Cisco IP-telefon-strøminjektor.
- En PoE-strømkabel og Power Cube 3.

Figuren nedenfor viser strømalternativene for PoE og PoE-strømkabel.

Figur 2: Strømalternativer for konferansetelefoner



Konfigurere telefonen fra oppsettsmenyene

Telefonen har mange konfigurerbare nettverksinnstillinger du kanskje må endre før telefonen fungerer slik den skal for brukerne. Du har tilgang til disse innstillingene fra menyer på telefonen, og du kan endre noen av dem.

Telefonen har følgende oppsettsmenyer:

- Nettverksoppsett: Inneholder alternativer for å vise og konfigurere en rekke nettverksinnstillinger.
 - IPv4-oppsett: Denne undermenyen inneholder ekstra nettverksalternativer.
 - IPv6-oppsett: Denne undermenyen inneholder ekstra nettverksalternativer.
- Sikkerhetsoppsett: Inneholder alternativer for å vise og konfigurere en rekke sikkerhetsinnstillinger.





Merk Du kan kontrollere om en telefon har tilgang til menyen Innstillinger eller til alternativer på denne menyen. Bruk feltet **Tilgang til innstillinger** i vinduet Cisco Unified Communications Manager Administration Telefonkonfigurasjon for å kontrollere tilgangen. Følgende verdier godtas i feltet **Tilgang til innstillinger**:

- Aktivert: Gir tilgang til menyen Innstillinger.
- Deaktivert: Forhindrer tilgang til de fleste oppføringer i Innstillingsmenyen Brukeren kan fortsatt få tilgang til **Innstillinger > Status**.
- Begrenset: Gir tilgang til menyelementene Brukerpreferanser og Status meny elementer, og tillater at volumendringer kan lagres. Hindrer tilgang til andre alternativer på menyen Innstillinger.

Hvis du ikke har tilgang til en mulighet i Admin Settings menyen, sjekk **Innstillinger Access** felt.

Du konfigurerer innstillinger som kun er tilgjengelig for visning på telefonen i Cisco Unified Communications Manager Administration.

Prosedyre

- Trinn 1** Trykk på **Programmer** .
- Trinn 2** Trykk på **Innstillinger**.
- Trinn 3** Velg **Administratorinnstillinger**.
- Trinn 4** Angi om nødvendig passordet, og klikk deretter **Logg på**.
- Trinn 5** Velg **Nettverksoppsett** eller **Sikkerhetsoppsett**.
- Trinn 6** Gjør ett av følgende for å vise den ønskede menyen:
 - Bruk navigasjonspilene for å velge ønsket meny, og trykk deretter på **Velg**.
 - Bruk tastaturet på telefonen til å angi nummeret som samsvarer med menyen.
- Trinn 7** Hvis du vil vise en undermeny, gjentar du trinn 5.
- Trinn 8** Hvis du vil avslutte en meny, trykker du på **Tilbake** .

Beslektede emner

- [Starte på nytt eller tilbakestille konferansetelefonen](#), på side 133
- [Konfigurere nettverksinnstillingene](#), på side 32
- [Konfigurere sikkerhetsinnstillingene](#), på side 63

Ta i bruk et telefonpassord


Du kan bruke et passord på telefonen. Hvis du bruker et passord, kan det ikke gjøres noen endringer i de administrative alternativene på telefonen uten å oppgi passord på telefonskjermen Administratorinnstillinger.

Prosedyre

- Trinn 1** I Cisco Unified Communications Manager Administration navigerer du til konfigurasjonsvinduet Felles telefonprofil (**Enhet > Enhetsinnstillinger > Felles telefonprofil**).
- Trinn 2** Angi et passord i alternativet Local Phone Unlock Password (Lås opp passord for lokal telefon).
- Trinn 3** Bruk passordet for den vanlige telefonprofilen som telefonen bruker.
-

Tekst- og menyinntasting fra telefonen

Når du redigerer verdien for en alternativinnstilling, gjør du følgende:

- Bruk pilene på navigasjonsplaten til å merke feltet du vil redigere. Trykk på **Velg** på navigasjonsplaten for å aktivere feltet. Etter at feltet er aktivert, kan du angi verdier.
- Bruk tastene på tastaturet til å angi tall og bokstaver.
- Hvis du vil angi bokstaver med tastaturet, bruker du en tilsvarende talltast. Trykk på tasten én eller flere ganger for å vise en bestemt bokstav. For eksempel, trykk **2** tasten én gang for “a,” to ganger raskt for “b,” og tre ganger raskt for “c.” Etter en kort pause vil markøren automatisk flytte seg slik at du kan skrive inn neste bokstav.
- Trykk på funksjonstasten  hvis du gjør en feil. Denne funksjonstasten sletter tegnet til venstre for markøren.
- Trykk på **Gjenopprett** før du trykker på **Bruk** for å forkaste endringer du har gjort.
- Hvis du vil angi et punktum (for eksempel i en IP-adresse), trykker du på * på tastaturet.
- Hvis du vil angi et kolon for en IPv6-adresse, trykker du på * på tastaturet.



Merk Cisco IP-telefon har flere metoder for å tilbake stille eller gjenopprette alternativinnstillinger hvis det blir nødvendig.

Beslektede emner

[Starte på nytt eller tilbake stille konferansetelefonen](#), på side 133

[Ta i bruk et telefonpassord](#), på side 31

Konfigurere nettverksinnstillingene

Prosedyre

- Trinn 1** Trykk på **Innstillinger**.
- Trinn 2** Velg **Administratorinnstillinger > Nettverksoppsett**.
- Trinn 3** Angi feltene som beskrevet i [Felter i Nettverksoppsett](#), på side 33.

Når du har angitt feltene, må du kanskje starte telefonen på nytt.

Felter i Nettverksoppsett

Menyen Nettverksoppsett inneholder felter og undermenyer for IPv4 og IPv6.

Hvis du vil endre noen av feltene, må du slå av DHCP.

Tabell 9: Menyen Nettverksoppsett

Oppføring	Type	Standard	Beskrivelse
IPv4-oppsett	Meny		Se tabellen “Undermenyen IPv4-oppsett”. Dette alternativet vises bare når telefonen er konfigurert i Kun IPv4-modus eller i dobbeltstakkmodus.
IPv6-oppsett	Meny		Se tabellen “Undermenyen IPv6-oppsett”.
Vertsnavn	Streng		Vertsnavnet på telefonen. Ved bruk av DHCP tildeles dette navnet automatisk.
Domenenavn	Streng		Navnet på DNS-domenet (Domain Name System) som telefonen befinner seg i. Hvis du vil endre dette feltet, må du slå av DHCP.
Operativ VLAN-ID			Operativ VLAN (Virtual Local Area Network) som er konfigurert på en Cisco Catalyst-svitsj som telefonen er medlem av.
VLAN-ID for admin			Ekstra VLAN som telefonen er medlem av.
Svitsjeportoppsett	Automatisk forhandling 10 halv 10 full 100 halv 100 full	Automatisk forhandling	Hastighet og dupleks for svitsjeporten, der: <ul style="list-style-type: none"> • 10 halv = 10-BaseT/halv dupleks • 10 full = 10-BaseT/full dupleks • 100 halv = 100-BaseT/halv dupleks • 100 full = 100-BaseT/full dupleks
LLDP-MED: Svitsjeport	Deaktivert Aktivert	Aktivert	Angir om LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) er aktivert på svitsjeporten.

Tabell 10: Undermenyen IPv4-oppsett

Oppføring	Type	Standard	Beskrivelse
DHCP	Deaktivert Aktivert	Aktivert	Aktiverer eller deaktiverer bruk av DHCP.
IP-adresse			IPv4-adressen (Internet Protocol versjon 4) til telefonen. Hvis du vil endre dette feltet, må du slå av DHCP.
Nettverksmaske			Nettverksmasken som telefonen bruker. Hvis du vil endre dette feltet, må du slå av DHCP.
Standardruter 1			Standardruter som telefonen bruker. Hvis du vil endre dette feltet, må du slå av DHCP.
DNS-server 1			Den primære DNS-serveren (Domain Name System) (DNS-server 1) som telefonen bruker. Hvis du vil endre dette feltet, må du slå av DHCP.
Alternativ TFTP	Nei Ja	Nei	Angir om telefonen bruker en alternativ TFTP-server.
TFTP-server 1			Primær TFTP-server (Trivial File Transfer Protocol) som telefonen bruker. Hvis du setter alternativet Alternativ TFTP til På, må du angi en annen verdi enn null for alternativet TFTP-Server 1. Hvis verken den primære TFTP-serveren eller reserve-TFTP-serveren er oppført i CTL- eller ITL-filen på telefonen, må du låse opp filen før du kan lagre endringene for alternativet TFTP-Server 1. I så fall sletter telefonen filen når du lagrer endringer for alternativet TFTP-Server 1. En ny CTL- eller ITL-fil lastes ned fra den nye TFTP-Server 1-adressen. Se TFTP-merknadene etter den siste tabellen.

Oppføring	Type	Standard	Beskrivelse
TFTP-server 2			<p>Sekundær TFTP-server som brukes av telefonen.</p> <p>Hvis verken den primære TFTP-serveren eller reserve-TFTP-serveren er oppført i CTL- eller ITL-filen på telefonen, må du låse opp filen før du kan lagre endringene for alternativet TFTP-Server 2. I så fall sletter telefonen filen når du lagrer endringer for alternativet TFTP-Server 2. En ny CTL- eller ITL-fil lastes ned fra den nye TFTP-Server 2-adressen.</p> <p>Se delen om TFTP-merknader etter den siste tabellen.</p>
DHCP-adresse frigitt	Nei Ja	Nei	

Tabell 11: Undermenyen IPv6-oppsett

Oppføring	Type	Standard	Beskrivelse
DHCPv6 aktivert	Deaktivert Aktivert	Aktivert	Aktiverer eller deaktiverer bruk av IPv6 DHCP.
IPv6-adresse			<p>Telefonens IPv6-adresse.</p> <p>Hvis du vil endre dette feltet, må du slå av DHCP.</p>
IPv6-prefikslengde			<p>Lengde på IPv6-adresse.</p> <p>Hvis du vil endre dette feltet, må du slå av DHCP.</p>
Standard IPv6-ruter 1			<p>Standard IPv6-ruter.</p> <p>Hvis du vil endre dette feltet, må du slå av DHCP.</p>
IPv6 DNS-server 1			<p>Primær IPv6 DNS-server</p> <p>Hvis du vil endre dette feltet, må du slå av DHCP.</p>
Alternativ TFTP for IPv6	Nei Ja	Nei	Angir om telefonen bruker en alternativ IPv6 TFTP-server.

Oppføring	Type	Standard	Beskrivelse
IPv6 TFTP-server 1			Primær IPv6 TFTP-server som brukes av telefonen. Se delen om TFTP-merknader etter denne tabellen.
IPv6 TFTP-server 2			Sekundær IPv6 TFTP-server som brukes av telefonen. Se delen om TFTP-merknader etter denne tabellen.
IPv6-adresse frigitt	Nei Ja	Nei	

Før du kan konfigurere alternativer for IPv6-oppsett på enheten, må IPv6 være aktivert og konfigurert i Cisco Unified Communication Administration. Følgende enhetskonfigurasjonfelt gjelder for IPv6-konfigurasjon:

- IP-adressemodus
- Innstilling for signalisering for IP-adressemodus

Hvis IPv6 er aktivert i Unified-gruppen, er standardinnstillingen for IP-adressemodus IPv4 og IPv6. I denne adressemodusen vil telefonen hente og bruke én IPv4-adresse og én IPv6-adresse. Den kan bruke IPv4- og IPv6-adressen til medier etter behov. Telefonen bruker enten IPv4- eller IPv6-adressen til samtalestyringssignalisering.

Hvis du vil ha mer informasjon om IPv6, kan du se:

- “Felles enhetskonfigurasjon” i *Funksjons- og tjenesteveiledning for Cisco Unified Communications Manager*, kapitlet “IPv6-støtte i Cisco Unified Communications-enheter”.
- *IPv6-distribusjonsveiledning for Cisco Collaboration Systems versjon 12.0*, som du finner her: <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html>

TFTP-merknader

Når telefonen leter etter TFTP-serveren, prioriterer telefonen manuelt tilordnede TFTP-servere, uavhengig av protokoll. Hvis konfigurasjon din inneholder både IPv6- og IPv4-TFTP-servere, prioriterer telefonen rekkefølgen som den ser etter TFTP-server i, ved å prioritere manuelt tilordnede IPv6-TFTP-servere og IPv4-TFTP-servere. Telefonen ser etter TFTP-serveren i denne rekkefølgen:

1. Eventuelle manuelt tilordnede IPv4-TFTP-servere
2. Eventuelle manuelt tilordnede IPv6-servere
3. DHCP-tilordnede TFTP-servere
4. DHCPv6-tilordnede TFTP-servere

For informasjon om CTL- og ITL-filer, se *Sikkerhetsveiledning for Cisco Unified Communications Manager*.

Bekreftede telefonoppstarten

Etter at telefonen er koblet til en strømkilde, går den automatisk gjennom en oppstartsdiagnoseprosess.

Prosedyre

Slå på telefonen.

Når hovedskjermbildet vises, har telefonen startet opp riktig.

Endre telefonmodell for en bruker

Du eller brukeren kan endre telefonmodell for en bruker. Endringen kan være nødvendig av en rekke årsaker, for eksempel:

- Du har oppdatert Cisco Unified Communications Manager (Unified CM) til en programvareversjon som ikke støtter telefonmodellen.
- Brukeren vil ha en annen telefonmodell enn den de har.
- Telefonen må repareres eller erstattes.

Unified CM identifiserer den gamle telefonen og bruker den gamle telefonens MAC-adresse til å identifisere den gamle telefonens konfigurasjon. Unified CM kopierer den gamle telefonens konfigurasjon til oppføringen for den nye telefonen. Den nye telefonen har deretter samme konfigurasjon som den gamle telefonen.

Begrensning: Hvis den gamle telefonen har flere linjer eller linjeknapper enn den nye telefonen, blir ikke de ekstra linjene eller linjeknappene konfigurert på den nye telefonen.

Telefonen starter på nytt når konfigurasjonen er fullført.

Før du begynner

Konfigurer Cisco Unified Communications Manager i samsvar med instruksjonene i *Funksjonskonfigurasjonsveiledning for Cisco Unified Communications Manager*.

Du trenger en ny, ubrukt telefon med forhåndsinstallert fastvareversjon 12.8 (1) eller senere.

Prosedyre

- Trinn 1** Slå av den gamle telefonen.
- Trinn 2** Slå på den nye telefonen.
- Trinn 3** Velg **Erstatt en eksisterende telefon** på den nye telefonen.
- Trinn 4** Skriv inn det primære internnummeret til den gamle telefonen.
- Trinn 5** Hvis den gamle telefonen hadde en tilordnet PIN-kode, skriver du inn PIN-koden.
- Trinn 6** Trykk på **Send**

Trinn 7 Hvis brukeren har mer enn én enhet, velger du enheten som skal erstattes, og trykker på **Fortsett**.



KAPITTEL 5

Installasjon av telefoner i Cisco Unified Communications Manager

- [Konfigurere en Cisco IP-konferansetelefon, på side 39](#)
- [Fastslå telefonens MAC-adresse, på side 43](#)
- [Metoder for å legge til telefoner, på side 44](#)
- [Legge til brukere i Cisco Unified Communications Manager, på side 45](#)
- [Legge til bruker i sluttbrukergruppe, på side 47](#)
- [Knytte telefoner til brukere, på side 48](#)
- [Survivable Remote Site Telephony, på side 48](#)

Konfigurere en Cisco IP-konferansetelefon

Hvis automatisk registrering ikke er aktivert, og telefonen ikke finnes i Cisco Unified Communications Manager Database, må du konfigurere Cisco IP-telefon i Cisco Unified Communications Manager Administration manuelt. Noen oppgaver i denne prosedyren er valgfrie, avhengig av systemet og brukerbehovene.

Hvis du vil ha mer informasjon om trinnene, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Gjennomfør konfigurasjonstrinnene i følgende prosedyre ved hjelp av Cisco Unified Communications Manager Administration.

Prosedyre

Trinn 1

Samle inn følgende informasjon om telefonen:

- Telefonmodell
- MAC-adresse: se [Fastslå telefonens MAC-adresse, på side 43](#)
- Fysisk plassering av telefonen
- Navnet på eller bruker-ID-en for telefonbrukeren
- Enhetsutvalg

- Informasjon om partisjon, anropssøkeområde og plassering
- Katalognummer (DN) som skal tilordnes til telefonen
- Cisco Unified Communications Manager-bruker som skal knyttes til telefonen
- Informasjon om telefonbruk som påvirker funksjonstastmalen, telefonfunksjoner, IP-telefon tjenester eller telefonprogrammer

Hvis du vil ha mer informasjon, kan du se i dokumentasjonen for din versjon av Cisco Unified Communications Manager og se de relaterte koblingene.

Trinn 2 Kontroller at du har tilstrekkelige enhetslisenser for telefonen.

Hvis du vil ha mer informasjon, kan du se lisensieringsdokumentet for din versjon av Cisco Unified Communications Manager.

Trinn 3 Definer enhetsutvalgene. Velg **System > Enhetsutvalg**.

Enhetsgrupper definerer vanlige egenskaper for enheter, for eksempel region, dato-/klokkeslettgruppe og funksjonstastmal.

Trinn 4 Definer profilen for vanlig telefon. Velg **Enhet > Enhetsinnstillinger > Vanlig telefonprofil**.

Vanlige telefonprofiler formidler data som Cisco TFTP-serveren krever, og i tillegg vanlige telefoninnstillinger, for eksempel Ikke forstyrr og alternativer for funksjonskontroll.

Trinn 5 Definer et anropssøkeområde. I Cisco Unified Communications Manager Administration klikker du **Ruting av samtale > Kontrollklasse > Anropssøkeområde**.

Et anropssøkeområde er en samling med partisjoner som det søkes i for å finne ut hvordan et oppringt nummer blir rutet. Anropssøkeområdet for enheten og anropssøkeområdet for katalognummeret brukes sammen. Katalognummerets CSS har forrang over enhetens CSS.

Trinn 6 Konfigurer en sikker profil for enhetstypen og protokollen. Velg **System > Sikkerhet > Profil for telefonsikkerhet**.

Trinn 7 Konfigurer telefonen. Velg **Enhet > Telefon**.

- Finn telefonen du vil endre, eller legg til en ny telefon.
- Konfigurer telefonen ved å fylle ut de obligatoriske feltene i ruten Enhetsinformasjon i vinduet Telefonkonfigurasjon.
 - MAC-adresse (obligatorisk): Kontroller at verdien består av 12 heksadesimale tegn.
 - Beskrivelse: Angi en nyttig beskrivelse som er til hjelp hvis du må søke etter informasjon om denne brukeren.
 - Enhetsutvalg (obligatorisk)
 - Vanlig telefonprofil
 - Anropssøkeområde
 - Plassering
 - Eier (Bruker eller Anonym), og Eiers bruker-ID hvis Bruker velges

Enheten med dets standardinnstillinger legges til i Cisco Unified Communications Manager-databasen.

Hvis du vil ha informasjon om feltene i Produktspesifikk konfigurasjon, kan du se “?” Hjelp-tasten i vinduet Telefonkonfigurasjon og den relaterte koblingen.

Merk Hvis du vil legge til både telefonen og brukeren i Cisco Unified Communications Manager-databasen samtidig, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

- c) I området Protokollspesifikk informasjon i dette vinduet velger du en profil for enhetsikkerhet og angir sikkerhetsmodusen.

Merk Velg en sikkerhetsprofil basert på den totale sikkerhetsstrategien til firmaet. Hvis telefonen ikke støtter sikkerhet, velger du en usikret profil.

- d) I området Informasjon om internnummer merker du av for Aktiver mobilt internnummer hvis denne telefonen støtter Cisco Mobilt internnummer.

- e) Klikk på **Lagre**.

Trinn 8

Velg **Enhet > Enhetsinnstillinger > SIP-profil** for å konfigurere SIP-parametrene.

Trinn 9

Velg **Enhet > Telefon** for å konfigurere katalognumre (linjer) på telefonen ved å fylle ut de obligatoriske feltene i vinduet Konfigurasjon av katalognummer.

- a) Finn telefonen.

- b) I vinduet Telefonkonfigurasjon klikker du Linje 1 i venstre rute i vinduet.

Konferansetelefoner har bare én linje.

- c) I feltet Katalognummer angir du et gyldig nummer som kan ringes.

Merk Dette feltet må inneholde de samme nummeret som vises i feltet Telefonnummer i vinduet Konfigurasjon av sluttbruker.

- d) I rullegardinlisten Rut partisjon velger du partisjonen som katalognummeret tilhører. Hvis du ikke vil begrense tilgangen til katalognummeret, velger du <None> for delingen.

- e) Fra rullegardinlisten Anropssøkeområde velger du det riktige anropssøkeområdet. Verdien du velger, gjelder for alle enheter som bruker dette katalognummeret.

- f) I området Innstillinger for henting av anrop og viderekobling av anrop velger du elementene (for eksempel Viderekoble alle, Viderekoble opptatt internnummer) og de tilsvarende numrene som anrop skal sendes til.

Eksempel:

Hvis du vil at innkommende interne og eksterne anrop som mottar et opptattsignal, skal viderekobles til taleposten for denne linjen, merker du av for Talepost ved siden av elementene Viderekoble opptatt internnummer og Viderekoble opptatt eksterntnummer i kolonnen til venstre i området Innstillinger for henting av anrop og viderekobling av anrop.

- g) Under Linje 1 i ruten Enhet konfigurerer du følgende felt:

- Vis feltet ID for intern anroper: Du kan angi fornavnet og etternavnet til brukeren av denne enheten slik at navnet vises for alle interne anrop. La feltet være tomt for at systemet skal vises internnummeret.
- Maske for eksternt telefonnummer: Angi telefonnummeret (eller masken) som brukes til å sende informasjon om anroperens ID når et anrop foretas fra denne linjen. Du kan angi maksimalt 24 numeriske tegn og “X”-tegn. X representerer katalognummeret og må vises på slutten av mønstret.

Eksempel:

Hvis du angir masken 408902XXXX, viser et eksternt anrop fra internummer 6640 nummeret 4089026640 for en anroperes ID.

Denne innstillingen gjelder bare for den gjeldende enheten såfremt du ikke merker av i avmerkingsboksen til høyre (Oppdater innstillinger for delt enhet) og klikker **Overfør valgt**. Avmerkingsboksen til høyre vises bare hvis andre enheter deler dette katalognummeret.

h) Velg **Lagre**.

Hvis du vil ha mer informasjon om katalognumre, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager og de relaterte koblingene.

Trinn 10

(Valgfritt) Knytt brukeren til en telefon. Klikk **Tilknytt sluttbrukere** nederst i vinduet Telefonkonfigurasjon for å knytte en bruker til en linje som blir konfigurert.

- Bruk **Søk** sammen med søkefeltene til å finne brukeren.
- Merk av i avmerkingsboksen ved siden av brukernavnet, og klikk **Legg til valgt**.

Brukernavnet og bruker-IDen vises i ruten Brukere knyttet til linje i vinduet Konfigurasjon av katalognummer.

c) Velg **Lagre**.

Brukeren er nå knyttet til Linje 1 på telefonen.

Trinn 11

(Valgfritt) Knytt brukeren til enheten:

- Velg **Brukerbehandling > Sluttbruker**.
- Bruk søkeboksene og **Søk** til å finne brukeren du har lagt til.
- Klikk brukerens ID.
- I området Tilknytninger til katalognummer på skjermen velger du Primært internummer i rullegardinlisten.
- (Valgfritt) I området Informasjon om mobilitet merker du av for Aktiver mobilitet.
- I området Informasjon om tillatelser bruker du knappen **Legg til i tilgangskontrollgruppe** for å legge til denne brukeren i en brukergruppe.

Du vil for eksempel kanskje legge til brukeren i en gruppe som er definert som en standard CCM-sluttbrukergruppe.

- Hvis du vil vise detaljene for en gruppe, merker du gruppen og klikker **Vis detaljer**.
- I området Mobilt internummer merker du av for Aktiver mobilt internummer på tvers av grupper) hvis brukeren kan bruke tjenesten Mobilt internummer på tvers av grupper).
- I området Enhetsinformasjon klikker du **Enhetsilknytninger**.
- Bruk søkefeltene og **Søk** til å finne enheten du vil knytte til brukeren.
- Merk enheten og klikk **Lagre valgte/endringer**.
- Klikk **Søk** ved siden av den aktuelle koblingen "Tilbake til bruker" i høyre hjørne øverst på skjermen.
- Velg **Lagre**.

Trinn 12

Tilpass funksjonstastmalene. Velg **Enhetsinnstillinger > Funksjonstastmal**.

Bruk siden til å legge til, slette eller endre rekkefølgen på funksjonstastfunksjonene som vises på brukerens telefon for å oppfylle krav til funksjonsbruk.

Konferansetelefonen har spesielle funksjonstastkrav. Se de relaterte koblingene for mer informasjon.

Trinn 13

Konfigurere Cisco IPP-telefontjenester og tilordne tjenester. Velg **Enhetsinnstillinger > Telefontjenester**.

Formidler IP-telefon tjenester til telefonen.

Merk Brukere kan legge til eller endre tjenester på telefonen fra selvhjelpsportalen i Cisco Unified Communications.

Trinn 14

(Valgfritt) Legg til brukerinformasjon i den globale katalogen for Cisco Unified Communications Manager. Velg **Brukerbehandling > Sluttbruker**, og klikk deretter **Legg til ny** og konfigurere de obligatoriske feltene. Obligatoriske felt er angitt med en stjerne (*).

Merk Hvis firmaet ditt bruker en LDAP-katalog (Lightweight Directory Access Protocol) til å lagre informasjon om brukere, kan du installere og konfigurere Cisco Unified Communications til å bruke din eksisterende LDAP-katalog. Se [Konfigurere bedriftskatalogen](#), på side 103. Etter at feltet Aktiver synkronisering fra LDAP-serveren er aktivert, kan du ikke legge til flere brukere fra Cisco Unified Communications Manager Administration.

- Angi en verdi for feltene bruker-ID og Etternavn.
- Tilordne et passord (for selvhjelpsportalen).
- Tilordne en PIN-kode (for Cisco Mobilt internummer og Personlig katalog).
- Knytt brukeren til en telefon.

Gir brukere kontroll over telefonen ved at de for eksempel kan viderekoble samtaler eller legge til kortnumre eller tjenester.

Merk Noen telefoner, for eksempel telefoner i konferanserom, har ikke en tilknyttet bruker.

Trinn 15

(Valgfritt) Knytt en bruker til en brukergruppe. Velg **Brukerbehandling > Brukerinnstillinger > Tilgangskontrollgruppe**.

Tilordne brukere til en vanlig liste med roller og tillatelser som gjelder for alle brukere i en brukergruppe. Administratorer kan administrere brukergreper, roller og tillatelser for å kontrollere tilgangsnivået (og dermed sikkerhetsnivået) for systembrukere.

Hvis sluttbrukere skal får tilgang til selvhjelpsportalen i Cisco Unified Communications, må du legge til brukere i standard sluttbrukergruppe i Cisco Unified Communications Manager.

Beslektede emner

[Funksjoner og oppsett for Cisco IP-konferansetelefoner](#), på side 71

[Produktspesifikk konfigurasjon](#), på side 75

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

[Konfigurere en ny funksjonstastmal](#), på side 72

Fastslå telefonens MAC-adresse

Hvis du vil legge til telefoner i Cisco Unified Communications Manager, må du fastslå MAC-adressen til en telefon.

Prosedyre

Gjør ett av følgende:

- På telefonen velger du **Innstillinger** > **Telefoninformasjon** og går til feltet MAC-adresse.
- Se på MAC-etiketten på baksiden av telefonen.
- Vis websiden for telefonen og klikk **Enhetsinformasjon**.

Metoder for å legge til telefoner

Etter at du har installert Cisco IP-telefon, kan du velge ett av følgende alternativer for å legge til telefoner i Cisco Unified Communications Manager-databasen.

- Legge til telefoner enkeltvis ved hjelp av Cisco Unified Communications Manager Administration
- Legge til flere telefoner ved hjelp av verktøyet for mengdeadministrasjon (BAT – Bulk Administration Tool)
- Automatisk registrering
- BAT og TAPS (Tool for Auto-Registered Phones Support)

Før du legger til telefoner enkeltvis eller med BAT, må du ha MAC-adressen til telefonen. Hvis du vil ha mer informasjon, kan du se [Fastslå telefonens MAC-adresse, på side 43](#)

Hvis du vil ha mer informasjon om masseadministrasjonsverktøyet, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Legge til telefoner enkeltvis

Samle inn MAC-adressen og telefoninformasjonen for telefonen du vil legge til i Cisco Unified Communications Manager.

Prosedyre

Trinn 1 I Cisco Unified Communications Manager Administration velger du **Enhet** > **Telefon**.

Trinn 2 Klikk på **Legg til ny**.

Trinn 3 Velg telefontypen.

Trinn 4 Velg **Neste**.

Trinn 5 Fyll ut informasjonen om telefonen, inkludert MAC-adressen.

Hvis du vil ha fullstendige instruksjoner og begrepsinformasjon Cisco Unified Communications Manager, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Trinn 6 Velg **Lagre**.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Legge til telefoner ved hjelp av BAT-telefonmalen

Ved hjelp av masseadministrasjonsverktøyet (BAT) for Cisco Unified Communications kan du utføre satsvise operasjoner, inkludert registrering av flere telefoner.

Hvis du vil legge til telefoner som bare bruker masseadministrasjonsverktøyet (ikke sammen med TAPS), må du hente den riktige MAC-adressen for hver telefon.

Hvis du vil ha mer informasjon om hvordan du bruker masseadministrasjonsverktøyet, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Prosedyre

-
- Trinn 1** Fra Cisco Unified Communications Administration velger du **Masseadministrasjon > Telefoner > Telefonmal**.
- Trinn 2** Klikk på **Legg til ny**.
- Trinn 3** Velg telefontype og klikk **Neste**.
- Trinn 4** Angi detaljene for telefonspesifikk parametere, for eksempel Enhetsutvalg, Telefonknappmal og Profil for enhetssikkerhet.
- Trinn 5** Klikk på **Lagre**.
- Trinn 6** Velg **Enhet > Telefon > Legg til ny** for å legge til en telefon ved hjelp av telefonmalen for masseadministrasjonsverktøyet.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Legge til brukere i Cisco Unified Communications Manager

Du kan vise og vedlikeholde informasjon om brukerne som er registrert i Cisco Unified Communications Manager. Cisco Unified Communications Manager tillater også at hver bruker utfører disse oppgavene:

- Gå til bedriftskatalogen og andre tilpassede kataloger fra en Cisco IP-telefon.
- Opprett en personlig katalog.
- Konfigurer kortnumre og numre for viderekobling av anrop.
- Abonner på tjenester som er tilgjengelig fra en Cisco IP-telefon.

Prosedyre

-
- Trinn 1** Hvis du vil legge til én bruker om gangen, kan du se [Legge en bruker direkte til i Cisco Unified Communications Manager](#), på side 46.

- Trinn 2** Hvis du vil legge til grupper med brukere, bruker du masseadministrasjonsverktøyet. Med denne metoden kan du også bruke det samme passordet for alle brukere.
- Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Legge til en bruker fra en ekstern LDAP-katalog

Hvis du la til en bruker i en LDAP-katalog (en annen katalogen enn på en Cisco Unified Communications-server), kan du umiddelbart synkronisere LDAP-katalogen til Cisco Unified Communications Manager som du legger til brukeren og brukertelefonen på.



-
- Merk** Hvis du ikke synkroniserer LDAP-katalogen til Cisco Unified Communications Manager umiddelbart, avgjør tidsplanen for synkronisering av LDAP-katalogen i vinduet LDAP-katalog når neste automatiske synkronisering er planlagt. Synkronisering må utføres før du kan knytte en ny bruker til en enhet.
-

Prosedyre

-
- Trinn 1** Logg på Cisco Unified Communications Manager Administration.
- Trinn 2** Velg **System > LDAP > LDAP-katalog**.
- Trinn 3** Bruk **Søk** til å finne LDAP-katalogen.
- Trinn 4** Klikk navnet på LDAP-katalogen.
- Trinn 5** Klikk **Perform Full Sync Now (Utfør fullstendig synkronisering nå)**.
-

Legge en bruker direkte til i Cisco Unified Communications Manager

Hvis du ikke bruker en LDAP-katalog (Lightweight Directory Access Protocol), kan du legge til en bruker direkte med Cisco Unified Communications Manager Administration ved å gjøre følgende:



-
- Merk** Hvis LDAP er synkronisert, kan du ikke legge til en bruker med Cisco Unified Communications Manager Administration.
-

Prosedyre

-
- Trinn 1** I Cisco Unified Communications Manager Administration velger du **Brukerbehandling > Sluttbruker**.
- Trinn 2** Klikk på **Legg til ny**.

- Trinn 3** I ruten Brukerinformasjon angir du følgende:
- Bruker-ID: Skriv inn sluttbrukeridentifikasjonsnavnet. Cisco Unified Communications Manager tillater ikke endring av bruker-ID etter at den er opprettet. Du kan bruke følgende spesialtegn: =, +, <, >, #, ;, \, “”, og mellomrom. **Eksempel:** olanordmann
 - Passord og Bekreft passord: Angi fem eller flere alfanumeriske tegn eller spesialtegn for sluttbrukerpassordet. Du kan bruke følgende spesialtegn: =, +, <, >, #, ;, \, “”, og mellomrom.
 - Etternavn: Skriv inn sluttbrukerens etternavn. Du kan bruke følgende spesialtegn: =, +, <, >, #, ;, \, “”, og mellomrom. **Eksempel:** nordmann
 - Telefonnummer: Angi hovedkatalognummeret for sluttbrukeren. Sluttbrukere kan ha flere linjer på telefonen. **Eksempel:** 26640 (Ola Nordmanns internnummer)
- Trinn 4** Klikk på **Lagre**.
-

Legge til bruker i sluttbrukergruppe

Hvis du vil legge til en bruker i standard sluttbrukergruppe for Cisco Unified Communications Manager, gjør du følgende:

Prosedyre

- Trinn 1** Fra Cisco Unified Communications Manager Administration velger du **Brukerbehandling > Brukerinnstillinger > Tilgangskontrollgruppe**.
- Vinduet Søk etter og vis brukere vises.
- Trinn 2** Angi de riktige søkekriteriene og klikk **Søk**.
- Trinn 3** Velg koblingen **Standard CCM-sluttbrukere**. Vinduet Konfigurasjon av brukergroupe for standard CCM-sluttbrukere vises.
- Trinn 4** Velg **Legg til sluttbrukere i gruppe**. Vinduet Søk etter og vis brukere vises.
- Trinn 5** Bruk boksene i rullegardinlisten Finn bruker til å finne brukere du vil legge til, og klikk **Finn**.
- Det vises en liste over brukere som samsvarer med søkekriteriene.
- Trinn 6** I listen over oppføringer som vises, klikker du i avmerkingsboksen ved siden av brukerne du vil legge til i denne brukerguppen. Hvis listen er lang, bruker du koblingene nederst til å vise flere resultater.
- Merk** Listen over søkeresultater viser ikke brukere som allerede tilhører brukerguppen.
- Trinn 7** Velg **Legg til valgt**.
-

Knytte telefoner til brukere

Du knytter telefoner til brukere i vinduet Sluttbruker i Cisco Unified Communications Manager.

Prosedyre

-
- Trinn 1** I Cisco Unified Communications Manager Administration velger du **Brukerbehandling > Sluttbruker**. Vinduet Søk etter og vis brukere vises.
- Trinn 2** Angi de riktige søkekriteriene og klikk **Søk**.
- Trinn 3** I listen over oppføringer som vises, velger du koblingen for brukeren.
- Trinn 4** Velg **Enhetstilknytning**.
Vinduet Enhetstilknytning for bruker vises.
- Trinn 5** Angi de riktige søkekriteriene og klikk **Søk**.
- Trinn 6** Velg enheten du vil knytte til brukeren, ved å merke av i boksen til venstre for enheten.
- Trinn 7** Velg **Lagre valgte/endringer** for å knytte enheten til brukeren.
- Trinn 8** Fra rullegardinlisten Relaterte koblinger i hjørnet øverst til høyre i vinduet velger du **Tilbake til bruker** og klikker **Søk**.
Vinduet Konfigurasjon av sluttbruker vises, og de tilknyttede enhetene du valgte, vises i ruten Kontrollerte enheter.
- Trinn 9** Velg **Lagre valgte/endringer**.
-

Survivable Remote Site Telephony

Survivable Remote Site Telephony (SRST) sørger for at de grunnleggende telefonfunksjonene forblir tilgjengelige når kontakten med Cisco Unified Communications Manager blir brutt. I dette scenariet kan telefonen beholde en pågående samtale aktiv, og brukeren har tilgang til et delsett med tilgjengelige funksjoner. Når failover forekommer, mottar brukeren en varselmelding på telefonen.

Hvis du vil ha mer informasjon om SRST, kan du se <http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html>

Tabellen nedenfor beskriver tilgjengeligheten av funksjoner under failover.

Tabell 12: Støtte for SRST-funksjon

Funksjon	Støttet	Merknader
Nytt anrop	Ja	
Avslutt samtale	Ja	
Ring på nytt	Ja	

Funksjon	Støttet	Merknader
Svare	Ja	
Sette på vent	Ja	
Gjenoppta	Ja	
Konferanse	Ja	Bare treveis og lokale kombinasjoner.
Konferanseliste	Nei	
Overføre samtaler	Ja	Bare konsultasjon.
Overføre til aktive samtaler (direkte overføring)	Nei	
Automatisk svar	Ja	
Samtale venter	Ja	
Oppringer-ID	Ja	
Unified-øktspresentasjon	Ja	Konferanse er den eneste funksjonen som støttes på grunn av andre funksjonsbegrensninger.
Talepost	Ja	Talepost blir ikke synkronisert med andre brukere i denne Cisco Unified Communications Manager-gruppen.
Viderekoble alle anrop	Ja	Viderekoblingsfunksjonen er bare tilgjengelig på telefonen som angir viderekoblingen, fordi det ikke finnes noen delte linjer i SRST-modus. Innstillingene for viderekobling av alle anrop blir ikke beholdt ved failover til SRST fra Cisco Unified Communications Manager, eller fra SRST-failback til Communications Manager. Alle opprinnelige aktive forekomster av anrop som skulle viderekobles i Communications Manager, må angis når enheten kobler til Communications Manager på nytt etter failover.
Kortnummer	Ja	
Ingen talepost (iDivert)	Nei	Funksjonstasten iDivert vises ikke.
Linjefiltre	Delvis	Linjer støttes men kan ikke deles.
Parkeringsovervåking	Nei	Funksjonstasten Parkering vises ikke.

Funksjon	Støttet	Merknader
Utvidet indikasjon for Melding venter	Nei	Meldingsantallmerker vises ikke på telefonskjermen. Kun ikonet Melding venter vises.
Rettet samtaleparkering	Nei	Funksjonstasten vises ikke.
Tilbakestilling av vent	Nei	Samtaler forblir på vent på ubestemt tid.
Ekstern på vent	Nei	Samtaler vises som lokale samtaler på vent.
Møterom	Nei	Funksjonstasten Møterom vises ikke.
GrAnrop	Nei	Funksjonstasten vises ikke.
Gruppeanropshenting	Nei	Funksjonstasten vises ikke.
Annen anropshenting	Nei	Funksjonstasten vises ikke.
ID for useriøse anrop	Nei	Funksjonstasten vises ikke.
QRT	Nei	Funksjonstasten vises ikke.
Arbeidsgruppe	Nei	Funksjonstasten vises ikke.
Mobilitet	Nei	Funksjonstasten vises ikke.
Privat-funksjon	Nei	Funksjonstasten vises ikke.
Ring tilbake	Nei	Funksjonstasten Ring tilbake vises ikke.
Tjeneste-URL	Ja	Den programmerbare linjenøkkelen med en tjeneste-nettadresse som er tilordnet, vises.



KAPITTEL 6

Administrasjon av selvhjelpsportal

- [Oversikt over selvhjelpsportalen, på side 51](#)
- [Konfigurere brukertilgang til selvhjelpsportalen, på side 51](#)
- [Tilpasse visningen av selvhjelpsportalen, på side 52](#)

Oversikt over selvhjelpsportalen

Fra selvhjelpsportalen i Cisco Unified Communications kan brukere tilpasse og kontrollere telefonfunksjoner og -innstillinger.

Som administrator kontrollerer du tilgang til selvhjelpsportalen. Du må også formidle informasjon til brukerne slik at de får tilgang til selvhjelpsportalen.

Før en bruker kan få tilgang til Cisco Unified Communications Self Care Portal, må du bruke Cisco Unified Communications Manager Administrasjon for å legge til brukeren i en standard Cisco Unified Communications Manager Sluttbrukergruppe.

Du må formidle følgende informasjon til sluttbrukere om selvhjelpsportalen:

- URL-en som gir tilgang til programmet. Dette er URL-en:
`https://<server_name:portnumber>/ucmuser/`, der `server_name` er vertsnavnet der webserveren er installert, og `portnumber` er portnummeret på den vertsdatamaskinen.
- En bruker-ID og et standardpassord for å få tilgang til programmet.
- En oversikt over oppgavene som brukere kan utføre med portalen.

Disse innstillingene tilsvare verdiene du la inn da du la til brukeren i Cisco Unified Communications Manager.

Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din spesifikke Cisco Unified Communications Manager versjon.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Konfigurere brukertilgang til selvhjelpsportalen

Før en bruker får tilgang til selvhjelpsportalen, må du godkjenne tilgangen.

Prosedyre

- Trinn 1** In Cisco Unified Communications Manager Administrasjon, velg **Brukerbehandling > Sluttbruker**.
 - Trinn 2** Søk etter brukeren.
 - Trinn 3** Klikk koblingen for brukerens ID.
 - Trinn 4** Kontroller at brukeren har et passord og en PIN-kode konfigurert.
 - Trinn 5** I delen Tillatelsesinformasjon kontrollerer du at listen over grupper inkluderer **Standard CCM-sluttbrukere**.
 - Trinn 6** Velg **Lagre**.
-

Tilpasse visningen av selvhjelpsportalen

De fleste alternativer vises på selvhjelpsportalen. Du må imidlertid angi følgende alternativer ved hjelp av innstillingene for Konfigurasjon av bedriftsparametere i Cisco Unified Communications Manager Administration:

- Vis innstillinger for ringetone
- Vis innstillinger for linjeetikett



Merk Innstillingene gjelder for alle sider på selvhjelpsportalen på nettstedet.

Prosedyre

- Trinn 1** I Cisco Unified Communications Manager Administration velger du **System > Bedriftsparametere**.
 - Trinn 2** I området Selvhjelpsportal angir du en verdi for feltet **Standardserver for selvhjelpsportal**.
 - Trinn 3** Aktiver eller deaktiver parameterne som brukere har tilgang til i portalen.
 - Trinn 4** Velg **Lagre**.
-



DEL III

Administrasjon av telefon

- [Sikkerhet på Cisco IP-konferansetelefoner, på side 55](#)
- [Tilpassing av Cisco IP-konferansetelefoner, på side 67](#)
- [Funksjoner og oppsett for Cisco IP-konferansetelefoner, på side 71](#)
- [Konfigurere bedriftskatalogen og den personlige katalogen, på side 103](#)



KAPITTEL 7

Sikkerhet på Cisco IP-konferansetelefoner

- [Oversikt over sikkerhet for Cisco IP-telefon, på side 55](#)
- [Utvidet sikkerhet i telefonnettverket, på side 56](#)
- [Støttede sikkerhetsfunksjoner, på side 57](#)
- [Se gjeldende sikkerhetsfunksjoner på telefonen, på side 62](#)
- [Vise sikkerhetsprofiler, på side 63](#)
- [Konfigurere sikkerhetsinnstillingene, på side 63](#)

Oversikt over sikkerhet for Cisco IP-telefon

Sikkerhetsfunksjonene beskytter mot alvorlige trusler, inkludert trusler mot identiteten til telefonen og dataene. Disse funksjonene etablerer og opprettholder godkjente kommunikasjonsstrømmer mellom telefonen og Cisco Unified Communications Manager-serveren, og sørger for at telefonen bruker bare digitalt signerte filer.

Cisco Unified Communications Manager Release 8.5(1) og nyere inkluderer Sikkerhet som standard, som inneholder følgende sikkerhetsfunksjoner for Cisco IP-telefon uten å kjøre CTL-klienten:

- Signering av telefonkonfigurasjonsfiler
- Kryptering av telefonkonfigurasjonsfil
- HTTPS med Tomcat og andre webtjenester



Merk Sikker signalisering og mediefunksjoner krever likevel at du kjører CTL-klienten og bruker eToken-enheter.

Hvis du vil ha mer informasjon om sikkerhetsfunksjoner, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Et viktig lokalt sertifikat (LSC-sertifikat) installeres på telefoner etter at du utfører de nødvendige oppgavene som er forbundet med CAPF (Certificate Authority Proxy Function). Du kan bruke Cisco Unified Communications Manager Administration til å konfigurere et LSC-sertifikat. Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Et LSC-sertifikat kan ikke brukes som brukersertifikatet for EAP-TLS med WLAN-godkjenning.

Alternativt kan du starte installasjonen av et LSC-sertifikat fra menyen Sikkerhetsoppsett på telefonen. På denne menyen kan du også oppdatere eller fjerne et LSC-sertifikat.

Cisco IP-konferansetelefon 7832 er i overensstemmelse med FIPS (Federal Information Processing Standard). FIPS-modus krever en RSA-nøkkelstørrelse på 2048 biter eller mer for å fungere riktig. Hvis RSA-serversertifikatet ikke er 2048 biter eller større, registreres ikke telefonen i Cisco Unified Communications Manager, og meldingen Telefonen kunne ikke registreres. Sertifikatnøkkelstørrelsen er ikke kompatibel med FIPS (Phone failed to register. Cert key size is not FIPS compliant) vises på telefonen.

Du kan ikke bruke private nøkler (LSC eller MIC) i FIPS-modus.

Hvis telefonen har et eksisterende LSC-sertifikat som er mindre enn 2048 biter, må du oppdatere LSC-nøkkelstørrelsen til 2048 biter eller mer før du aktiverer FIPS.

Beslektede emner

[Konfigurere et lokalt signifikant sertifikat](#), på side 64

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Utvidet sikkerhet i telefonnettverket

Du kan aktivere Cisco Unified Communications Manager 11.5(1) og 12.0(1), slik at du kan arbeide i et utvidet sikkerhetsmiljø. Ved hjelp av disse forbedringene fungerer telefonnettverket basert på et sett med strenge sikkerhets- og risikostyringskontroller for å beskytte deg og brukerne.

Cisco Unified Communications Manager 12.5 (1) støtter ikke et utvidet sikkerhetsmiljø. Deaktiver FIPS før du oppgraderer til Cisco Unified Communications Manager 12.5(1), ellers fungerer ikke TFTP og andre tjenester som de skal.

Det utvidede sikkerhetsmiljøet inkluderer følgende funksjoner:

- Godkjenning av søk etter kontakter.
- TCP som standardprotokoll for ekstern revisjonslogging.
- FIPS-modus.
- En forbedret policy for legitimasjon.
- Støtte for SHA-2-serien med hash-koder for digitale signaturer.
- Støtte for en RSA-nøkkelstørrelse på 3072 og 4096 biter.

Ved hjelp av Cisco Unified Communications Manager versjon 14,0 og FAS Tvare versjon 14,0 og nyere for Cisco IP-telefon, støtter telefonene SIP OAuth-autentifisering.

OAuth støttes for Proxy Trivial File Transfer Protocol (TFTP) med Cisco Unified Communications Manager versjon 14.0 (1) SU1 eller nyere, og fastvareversjon for Cisco IP-telefon 14.1 (1). Proxy TFTP og OAuth for Proxy TFTP støttes ikke på Mobile Remote Access (MRA).

Hvis du vil ha mer informasjon om sikkerhet, kan du se følgende:

- *Systemkonfigurasjonsveiledning for Cisco Unified Communications Manager*, versjon 14.0(1) eller nyere (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>).
- *Sikkerhetsveiledning for Cisco Unified Communications Manager* (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>)



Merk Cisco IP-telefon kan bare lagre et begrenset antall ITL-filer (Identity Trust List). Antallet ITL-filer må ikke overstige grensen på 64 000, så du må begrense antallet ITL-filer som Cisco Unified Communications Manager sender til telefonen.

Støttede sikkerhetsfunksjoner

Sikkerhetsfunksjonene beskytter mot alvorlige trusler, inkludert trusler mot identiteten til telefonen og dataene. Disse funksjonene etablerer og opprettholder godkjente kommunikasjonsstrømmer mellom telefonen og Cisco Unified Communications Manager-serveren, og sørger for at telefonen bruker bare digitalt signerte filer.

Cisco Unified Communications Manager Release 8.5(1) og nyere inkluderer Sikkerhet som standard, som inneholder følgende sikkerhetsfunksjoner for Cisco IP-telefon uten å kjøre CTL-klienten:

- Signering av telefonkonfigurasjonsfiler
- Kryptering av telefonkonfigurasjonsfil
- HTTPS med Tomcat og andre webtjenester



Merk Sikker signalisering og mediefunksjoner krever likevel at du kjører CTL-klienten og bruker eToken-enheter.

Implementering av sikkerhet i Cisco Unified Communications Manager-systemet hindrer identitetstyveri av telefonen og Cisco Unified Communications Manager-serveren, hindrer datamanipulering og hindrer manipulering av samtalsignalisering og mediestrømmer.

For unngå disse truslene etablerer og opprettholder Cisco IP-telefonnettverket sikrede (krypterte) kommunikasjonsstrømmer mellom en telefon og serveren, signerer filer digitalt før de overføres til en telefon og krypterer mediestrømmer og samtalsignalisering mellom Cisco IP-telefoner.

Et viktig lokalt sertifikat (LSC-sertifikat) installeres på telefoner etter at du utfører de nødvendige oppgavene som er forbundet med CAPF (Certificate Authority Proxy Function). Du kan bruke Cisco Unified Communications Manager Administration til å konfigurere et LSC-sertifikat, som beskrevet i sikkerhetsveiledningen for Cisco Unified Communications Manager. Alternativt kan du starte installasjonen av et LSC-sertifikat fra menyen Sikkerhetsoppsett på telefonen. På denne menyen kan du også oppdatere eller fjerne et LSC-sertifikat.

Et LSC-sertifikat kan ikke brukes som brukersertifikatet for EAP-TLS med WLAN-godkjenning.

Telefonene bruker telefonens sikkerhetsprofil, som angir om enheten er usikret eller sikret. Hvis du vil ha informasjon om hvordan du bruker sikkerhetsprofilen på telefonen, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Når du konfigurerer sikkerhetsrelaterte innstillinger i Cisco Unified Communications Manager Administration, inneholder telefonkonfigurasjonsfilen sensitive opplysninger. Du kan beskytte opplysningene i en konfigurasjonsfil ved å konfigurere den for kryptering. Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Implementering av sikkerhet i Cisco Unified Communications Manager-systemet hindrer identitetstyveri av telefonen og Cisco Unified Communications Manager-serveren, hindrer datamanipulering og hindrer manipulering av samtalsignalisering og mediestrømmer.

Tabellen nedenfor viser en oversikt over sikkerhetsfunksjonene som Cisco IP-konferansetelefon 7832 støtter. Hvis du vil ha mer informasjon om disse funksjonene, Cisco Unified Communications Manager og Cisco IP-telefon-sikkerhet, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Tabell 13: Oversikt over sikkerhetsfunksjoner

Funksjon	Beskrivelse
Bildegodkjenning	Signerte binære filer (med filtypen .sbn) hindrer redigering av bilder og fører til at en telefon ikke kan fullføre godkjenningsprosessen.
Installasjon av sertifikat på kundeområde	Hver telefon krever et unikt sertifikat for enhetsgodkjenning. Telefonen krever et sertifikat, men for ekstra sikkerhet kan du gå til Cisco Unified Communications Manager ved hjelp av CAPF-funksjonen (Certificate Authority Proxy Function) for å generere et sertifikat (Certificate) fra menyen Sikkerhetskonfigurasjon på telefonen.
Enhetsgodkjenning	Foregår mellom Cisco Unified Communications Manager-serveren og telefonen. Fastslår om en sikker tilkobling mellom telefonen og Cisco Unified Communications Manager er åpen for sikker signalisering mellom enhetene ved hjelp av TLS. Hvis de ikke kan godkjennes av Cisco Unified Communications Manager, blir forbindelsen avsluttet.
Filgodkjenning	Validerer digitalt signerte filer som telefonen laster ned. Telefonen laster ned filer som ble opprettet. Filer som ikke blir godkjent, blir ikke skrevet til disk.
Signaliseringsgodkjenning	Bruker TLS-protokollen til å validere at ingen redigering har blitt gjort på meldinger.
Produsentinstallert sertifikat	Hver telefon inneholder et unikt MIC-sertifikat (Manufacturing Identification Code) som et permanent og unikt bevis på telefonens identitet, og det tillater tilkobling til Cisco Unified Communications Manager.
Sikker SRST-referanse	Etter at du har konfigurert en SRST-referanse for sikkerhet og tilgjengelighet i Cisco Unified Communications Manager Administration, legger TFTP-serveren til SRST-sertifikatet og deretter en TLS-tilkobling til samhandle med den SRST-aktive serveren.
Mediekryptering	Bruker SRTP til å sørge for at mediestrømmene mellom støttede enheter er kryptert. Inkluderer oppretting av et mediehoovednøkkelpar for enhetene og de tilhørende nøklene blir transportert.
CAPF-funksjon (Certificate Authority Proxy Function)	Implementerer deler av sertifikatgenereringsprosedyren som er relatert til sertifikatgenerering og sertifikatinstallasjon. CAPF-funksjonen kan brukes til å generere sertifikater på vegne av telefonen, eller den kan konfigureres til å generere sertifikater for andre enheter.
Sikkerhetsprofiler	Angir om telefonen er usikret, godkjent eller kryptert.
Krypterte konfigurasjonsfiler	Lar deg sikre personvernet til konfigurasjonsfilene på telefonen.
Valgfri deaktivering av webserverfunksjonaliteten for en telefon	Du kan hindre tilgang til en webside på en telefon som viser informasjon om sikkerhet.

Funksjon	Beskrivelse
Telefonforsterking	<p>Ekstra sikkerhetsalternativer som du kontrollerer fra Cisco</p> <ul style="list-style-type: none"> • Disable access to web pages for a phone (Deaktiver tilgang til nettsider) <p>Merk Du kan se gjeldende innstillinger for alternativet i telefonen.</p>
802.1X-godkjenning	Telefonen kan bruke 802.1X-godkjenning til å be om og få tilgang til nettverket.
AES 256-kryptering	<p>Når telefonene er koblet til Cisco Unified Communications Manager for signaliserings- og mediekryptering. Dermed kan telefonene bruke kryptering som samsvarer med SHA-2-standardene (Secure Hash Algorithm 2). De nye chifrene er:</p> <ul style="list-style-type: none"> • For TLS-tilkoblinger: <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • For sRTP: <ul style="list-style-type: none"> • AEAD_AES_256_GCM • AEAD_AES_128_GCM <p>Hvis du vil ha mer informasjon, kan du se dokumentasjonen til Cisco Unified Communications Manager.</p>
ECDSA-sertifikater (Elliptic Curve Digital Signature Algorithm)	Som del av en common criteria-sertifisering (CC) har Cisco implementert ECDSA-sertifikater som påvirker alle Voice Operating System (VOS)-produkter fra Cisco Unified Communications Manager.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Sikkerhet for telefonsamtaler

Når sikkerhet er implementert for en telefon, kan du identifisere sikre telefonsamtaler med ikoner på telefonskjermen. Du kan også fastslå om den tilkoblede telefonen er sikker og beskyttet dersom du hører en sikkerhetstone på begynnelsen av samtalen.

I en sikker samtale blir samtalsignalisering og mediestrømmer kryptert. En sikker samtale har et høyt nivå av sikkerhet, noe som gir samtalen både integritet og beskytter personvernet. Når en pågående samtale krypteres, endres ikonet for pågående samtale til høyre for tidtakeren for samtalevarighet på telefonskjermen til følgende

ikon:  .



Merk Hvis samtalen rutes via samtalefaser utenom IP, for eksempel PSTN, er samtalen ikke sikker selv om den krypteres innenfor IP-nettverket og har et tilknyttet låseikon.

I en sikker samtale spilles det av en sikkerhetstone på begynnelsen av en samtale for å angi at den andre tilkoblede telefonen også mottar og overfører sikker lyd. Hvis samtalen din kobles til en usikret telefon, spilles ikke sikkerhetstonen av.




Merk Sikre samtaler støttes mellom to telefoner. Sikker konferanse, Cisco Extension Mobility og delte linjer kan konfigureres av en sikker konferansebro.

Når en telefon konfigureres som sikker (kryptert og klarert) i Cisco Unified Communications Manager, kan den bli gitt statusen "Beskyttet". Deretter kan den beskyttede telefonen om ønskelig konfigureres til å spille av en tone på begynnelsen av en samtale:

- Beskyttet enhet: Hvis du vil endre statusen for en sikker telefon til Beskyttet, merker du av for Beskyttet enhet i vinduet Telefonkonfigurasjon i Cisco Unified Communications Manager Administration (**Enh** > **Telefon**).
- Spill av tone for sikker samtale: Hvis du vil aktivere den beskyttede telefonen slik at den spiller av en tone for å angi en sikker eller usikret samtale, setter du innstillingen Spill av tone for sikker samtale til Sann. Som standard er Spill av tone for sikker samtale satt til Usann. Du angir dette alternativet i Cisco Unified Communications Manager Administration (**System** > **Tjenesteparametere**). Velg serveren og deretter Unified Communications Manager-tjenesten. I vinduet Konfigurasjon av tjenesteparameter velger du alternativet i området Funksjon - sikker tone. Standardverdien er Usann.

Identifikasjon av sikker telefonkonferanse

Du kan starte en sikker telefonkonferanse og overvåke sikkerhetsnivået for deltakerne. En sikker telefonkonferanse etableres ved å gjøre følgende:

1. En bruker starter konferansen fra en sikker telefon.
2. Cisco Unified Communications Manager tilordner en sikker konferansebro til samtalen.
3. Etter hvert som deltakere legges til, bekrefter Cisco Unified Communications Manager sikkerhetsmodusen for hver telefon og opprettholder sikkerhetsnivået for konferansen.
4. Telefonen viser sikkerhetsnivået for telefonkonferansen En sikker konferanse viser sikkerhetsikonet  til høyre for **Konferanse** på telefonskjermen.



Merk Sikre samtaler støttes mellom to telefoner. For beskyttede telefoner er noen funksjoner, for eksempel telefonkonferanser, delte linjer og mobilt internummer, ikke tilgjengelige når en sikker samtale konfigureres.

Tabellen nedenfor inneholder informasjon om endringer i sikkerhetsnivåene for konferansen avhengig av sikkerhetsnivået for initiativtakertelefonen, sikkerhetsnivåene for deltakerne og tilgjengeligheten av sikre konferansebroer.


Tabell 14: Sikkerhetsbegrensninger i forbindelse med telefonkonferanser

Sikkerhetsnivå for initiativtakertelefon	Funksjon som brukes	Sikkerhetsnivå for deltakere	Resultater av handling
Usikret	Konferanse	Sikre	Usikret konferansebro Usikret konferanse
Sikre	Konferanse	Minst ett medlem er usikret.	Sikker konferansebro Usikret konferanse
Sikre	Konferanse	Sikre	Sikker konferansebro Sikker konferanse på krypteringsnivå
Usikret	Møterom	Minste sikkerhetsnivå er kryptert.	Initiativtakeren mottar meldingen Does n Security Level, call rejecte (Oppfyller ikke sikkerhetsni avvist.).
Sikre	Møterom	Minste sikkerhetsnivå er usikret.	Sikker konferansebro Konferanse godtar alle anrop.

Identifikasjon av sikker telefonsamtale

En sikker samtale etableres når din telefon og telefonen i den andre enden konfigureres for sikker samtale. Den andre telefonen kan befinne seg i samme Cisco IP-nettverk eller i et nettverk utenfor IP-nettverket. Sikre samtaler kan bare gjennomføres mellom to telefoner. Telefonkonferanser må støtte sikker samtale etter at en sikker konferansebro er konfigurert.

En sikker samtale etableres ved å gjøre følgende:

1. En bruker starter samtalen fra en sikker telefon (sikret sikkerhetsmodus).
2. Telefonen viser sikkerhetsikonet  på telefonskjermen. Dette ikonet angir at telefonen er konfigurert for sikre samtaler, men det betyr ikke at den andre tilkoblede telefonen også er det samme.
3. Brukeren hører en sikkerhetstone hvis samtalen kobles til en annen sikker telefon, noe som angir at begge ender av samtalen er kryptert og sikker. Hvis samtalen kobles til en usikret telefon, hører ikke brukeren sikkerhetstonen.



Merk Sikre samtaler støttes mellom to telefoner. For beskyttede telefoner er noen funksjoner, for eksempel telefonkonferanser, delte linjer og mobilt internummer, ikke tilgjengelige når en sikker samtale konfigureres.

Bare beskyttede telefoner spiller av disse tonene for sikre og usikrede samtaler. Ubeskyttede telefoner spiller aldri av toner. Hvis den totale samtalestatusen endres i løpet av samtalen, endres tonen, og den beskyttede telefonen spiller av den riktige tonen.

En beskyttet telefon spiller av en tone eller ikke i følgende tilfeller:

- Når alternativet Spill av tone for sikker samtale er aktivert:

- Når sikre ende-til-ende-medier etableres og samtalestatusen er sikker, spiller telefonen av tonen for sikker samtale (tre lange pip med pause mellom hvert pip).
- Når usikrede ende-til-ende-medier etableres og samtalestatusen er usikret, spiller telefonen av tonen for usikret samtale (seks lange pip med kort pause mellom hvert pip).

Hvis alternativet Spill av tone for sikker samtale er deaktivert, spilles det ikke av noen tone.

802.1x-godkjenning

Cisco IP-telefon støtter 802.1X-godkjenning.

Cisco IP-telefon og Cisco Catalyst-svitsjer bruker tradisjonelt CDP-protokollen (Cisco Discovery Protocol) til å identifisere hverandre og definere parametere, for eksempel VLAN-tildeling og innebygde strømkrav.

Støtte for 802.1X-godkjenning krever flere komponenter:

- Cisco IP-telefon: Telefonen sender forespørselen om tilgang til nettverket. Telefoner inneholder en 802.1X-anmoder. Denne anmoderen tillater at nettverksadministratorer kontrollerer tilkoblingen for IP-telefon til LAN-svitsjeportene. Den gjeldende versjonen av telefonens 802.1X-anmoder bruker alternativene EAP-FAST og EAP-TLS for nettverksgodkjenning.
- Cisco Catalyst-bryter (eller en annen tredjepartsbryter): Svitsjen må støtte 802.1X, slik at den kan fungere som godkjenner og sende meldingene mellom telefonen og godkjenningsserveren. Etter at utvekslingen er fullført, gir eller avslår svitsjen tilgang til nettverket for telefonen.

Du må utføre følgende handlinger for å konfigurere 802.1X.

- Konfigurer de andre komponentene før du aktiverer 802.1X-godkjenning på telefonen.
- Konfigurer Tale-VLAN – 802.1X-standarden omfatter ikke VLAN-er, og derfor må du konfigurere denne innstillingen basert på svitsjstøtten.
 - Aktivert – Hvis du bruker en svitsj som støtter godkjenning på flere domener, kan du fortsette å bruke tale-VLAN.
 - Deaktivert – Hvis svitsjen ikke støtter godkjenning på flere domener, deaktiverer du tale-VLAN og vurderer å tilordne porten til opprinnelig VLAN.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Se gjeldende sikkerhetsfunksjoner på telefonen

Hvis du vil ha mer informasjon om sikkerhetsfunksjonene og om Cisco Unified Communications Manager og Cisco IP-telefon-sikkerhet, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Prosedyre

Trinn 1

Velg **Innstillinger**.

Trinn 2 Velg **Administrasjonsinnstillinger > Sikkerhetsoppsett**.

De fleste sikkerhetsfunksjonene er tilgjengelige bare hvis en sertifikatklaringsliste (CTL) er installert på telefonen.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Vise sikkerhetsprofiler

Alle Cisco IP-telefon-telefoner som støtter Cisco Unified Communications Manager, bruker en sikkerhetsprofil, som definerer om telefonen er usikret, godkjent eller kryptert. Hvis du vil ha informasjon om hvordan du konfigurerer sikkerhetsprofilen og bruker profilen på telefonen, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Prosedyre

Trinn 1 I Cisco Unified Communications Manager Administration velger du **System > Sikkerhet > Phone Security Profile (Profil for telefonsikkerhet)**.

Trinn 2 Gå til innstillingen Sikkerhetsmodus.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Konfigurere sikkerhetsinnstillingene

Prosedyre

Trinn 1 Trykk på **Innstillinger**.

Trinn 2 Velg **Administrasjonsinnstillinger > Sikkerhetsoppsett**.

Trinn 3 Konfigurer feltene.
Når du har angitt feltene, må du kanskje starte telefonen på nytt.

Felt i Sikkerhetsoppsett

Menyen Sikkerhetsoppsett inneholder felt og undermenyer for klareringslister og 802.1x-godkjenning.

Tabell 15: Menyene Sikkerhetsoppsett

Oppføring	Type	Standard	Beskrivelse
Sikkerhetsmodus			Skrivebeskyttet

Oppføring	Type	Standard	Beskrivelse
LSC			Se Konfigurere et lokalt signifikant sertifikat , på side 64.
Klareringsliste	Meny		Se tabellen “Undermenyen Klareringsliste”.
802.1x-godkjenning	Meny		Se tabellen “Undermenyen 802.1x-godkjenning”.

Tabell 16: Undermenyen Klareringsliste

Oppføring	Type	Standard	Beskrivelse
CTL-fil	Meny		Viser en liste over CTL-filer
ITL-fil	Meny		Viser en liste over ITL-filer
Konfigurasjon (signert)	Meny		Se tabellen “Undermenyen Konfigurasjon”.

Tabell 17: Undermenyen Konfigurasjon

Oppføring	Type	Standard	Beskrivelse
SRST-ruter			Viser IP-adressen til SRST.

Tabell 18: Undermenyen 802.1x-godkjenning

Oppføring	Type	Standard	Beskrivelse
Enhetsgodkjenning	Deaktivert Aktivert	Deaktivert	
Transaksjonsstatus	Undermeny		Se tabellen “Undermenyen Transaksjonsstatus”.

Tabell 19: Undermenyen Transaksjonsstatus

Oppføring	Type	Standard	Beskrivelse
Transaksjonsstatus	Frakoblet Tilkoblet		
Protokoller			Liste over protokoller.

Konfigurere et lokalt signifikant sertifikat

Denne fremgangsmåten gjelder for konfigurasjon av LSC med godkjenningsstrengmetoden.

Før du begynner

Sørg for at konfigurasjonene av sikkerhet for Cisco Unified Communications Manager og CAPF-funksjonen (Certificate Authority Proxy Function) er fullført:

- CTL- eller ITL-filen har et CAPF-sertifikat.
- I Cisco Unified Communications Operating System Administration bekrefter du at CAPF-sertifikatet er installert.
- CAPF-sertifikatet kjører og er konfigurert.

Hvis du vil ha mer informasjon om disse innstillingene, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Prosedyre

Trinn 1 Hent CAPF-godkjenningsskoden som ble angitt da CAPF-sertifikatet ble konfigurert.

Trinn 2 Trykk på **Programmer**  på telefonen.

Trinn 3 Velg **Innstillinger** på telefonen.

Trinn 4 Velg **Administratorinnstillinger > Sikkerhetsoppsett**.

Merk Du kan kontrollere tilgang til menyen Innstillinger ved hjelp av feltet Settings Access (Tilgang til innstillinger) i vinduet Telefonkonfigurasjon i Cisco Unified Communications Manager Administration.

Trinn 5 Velg **LSC** og trykk på **Velg** eller **Oppdater**.

Telefonen ber om en godkjenningstreng.

Trinn 6 Angi godkjenningsskoden og trykk på **Send**.

Telefonen begynner å installere, oppdatere eller fjerne LSC-sertifikatet, avhengig av hvordan CAPF-sertifikatet er konfigurert. I løpet av prosedyren vises det en rekke meldinger i feltet for LSC-alternativet på menyen Sikkerhetskonnfigurasjon, slik at du kan følge med på fremdriften. Når prosedyren er fullført, vises Installert eller Ikke installert på telefonen.

Installasjon, oppdatering eller fjerning av LSC-sertifikatet kan ta en stund.

Når installasjonen av telefonen er fullført, vises meldingen *Installert*. Hvis telefonen viser *Ikke installert*, kan det hende godkjenningstrengen er ugyldig eller telefonoppgraderingen ikke er aktivert. Hvis CAPF-sertifikatet sletter LSC-sertifikatet, viser telefonen *Ikke installert* for å angi at operasjonen var vellykket. CAPF-serveren logger feilmeldingene. Se dokumentasjonen for CAPF-serveren for å finne loggene og forstå betydningen av feilmeldingene.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Aktivere FIPS-modus

Prosedyre

- Trinn 1** I Cisco Unified Communications Manager Administration velger du **Enhet > Telefon** og finner telefonen.
 - Trinn 2** Gå til området Produktspesifikk konfigurasjon.
 - Trinn 3** Sett feltet **FIPS-modus** til Aktivert.
 - Trinn 4** Velg **Bruk konfigurasjon**.
 - Trinn 5** Velg **Lagre**.
 - Trinn 6** Start telefonen på nytt.
-



KAPITTEL 8

Tilpassing av Cisco IP-konferansetelefoner

- [Egendefinerte telefonringetoner, på side 67](#)
- [Tilpasse ringetonen, på side 69](#)

Egendefinerte telefonringetoner

Cisco IP-telefon leveres med to standard ringetoner som er implementert i maskinvaren: Chirp1 og Chirp2. Cisco Unified Communications Manager inneholder også et standardsett med ekstra ringetoner som er implementert i programvaren som PCM-filer (Pulse Code Modulation). Sammen med en XML-fil, som beskriver ringetonealternativene som er tilgjengelige på nettstedet, finnes PCM-filene i TFTP-katalogen på hver Cisco Unified Communications Manager Server.



Obs Alle filnavnene skiller mellom små og store bokstaver. Endringene tas ikke i bruk på telefonen hvis du bruker feil store og små bokstaver i filnavnet.

Hvis du vil ha mer informasjon, kan du se kapitlet "Egendefinerte ringetoner og bakgrunner", [Funksjonskonfigureringsveiledning for Cisco Unified Communications Manager](#).

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Konfigurere en tilpasset ringetone

Prosedyre

- Trinn 1** Opprett en PCM-fil for hver tilpassede ringetone (én ringetone per fil).
Sørg for at PCM-filene overholder formatretningslinjene som er oppført i delen Filformater for tilpasset ringetone.
- Trinn 2** Last opp de nye PCM-filene du opprettet, til Cisco TFTP-serveren for hver forekomst av Cisco Unified Communications Manager i gruppen.
Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

- Trinn 3** Bruk et tekstredigeringsprogram til å redigere filen Ringlist-wb.
- Se delen “Filformater for tilpasset ringetone” hvis du vil ha informasjon om hvordan du formaterer denne filen, og se en eksempelversjon av filen Ringlist-wb.xml.
- Trinn 4** Lagre endringene og lukk filen Ringlist-wb.
- Trinn 5** Slik bufrer du den nye filen Ringlist-wb.xml:
- Stopp og start TFTP-tjenesten ved hjelp av Cisco Unified Serviceability
 - Deaktiver og aktiver parameteren for TFTP-tjenesten “Aktiver bufring av konstante og binære filer ved oppstart” på nytt. Du finner denne parameteren i området Avanserte tjenesteparametere.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Filformater for tilpassede ringetoner

Filen Ringlist-wb.xml definerer et XML-objekt som inneholder en liste med ringetoner. Denne filen inneholder opptil 50 ringetoner. Hver ringetone inneholder en peker til PCM-filen som brukes for den ringetonen, og i tillegg tekst som vises på menyen Ringtone på en Cisco IP-telefon for den ringetonen. Cisco TFTP-serveren for hver forekomst av Cisco Unified Communications Manager inneholder denne filen.

XML-objektet CiscoIPPhoneRinglist bruker følgende enkle kodesett til å beskrive informasjonen:

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

Følgende egenskaper gjelder for definisjonsnavnene. Du må inkludere det obligatoriske feltet Visningsnavn og Filnavn for hver ringetone.

- DisplayName angir navnet på den tilpassede ringetonen for den tilknyttede PCM-filen som vises på menyen Ringtone på Cisco IP-telefon.
- FileName angir navnet på PCM-filen for den tilpassede ringetonen som skal knyttes til DisplayName.



Merk Feltene DisplayName og FileName må ikke bestå av mer enn 25 tegn.

Dette eksemplet viser filen Ringlist-wb.xml som definerer to ringetoner:

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

PCM-filene for ringetonene må oppfylle følgende krav for riktig avspilling på Cisco IP-telefoner:

- Raw PCM (ingen toppstekst)
- 8000 lydsnutter per sekund
- 8 biter per lydsnutt
- Mu-law-komprimering
- Maksimal ringetonestørrelse = 16080 lydsnutter
- Minimal ringetonestørrelse = 240 lydsnutter
- Antallet lydsnutter i ringetonen = mer enn 240.
- Ringetonestart og -slutt ved nullkryssing.

Hvis du vil opprette PCM-filer for tilpassede ringetoner, bruker du en standard lydredigeringspakke som støtter disse kravene til filformater.

Tilpasse ringetonen

Du kan konfigurere telefoner slik at brukere hører ulike ringetoner for interne og eksterne anrop. Avhengig av hva du foretrekker, kan du velge blant tre ulike ringetoner:

- Standard: Forskjellig ringetone for interne og eksterne anrop.
- Intern: Ringetonen for interne anrop brukes for alle anrop.
- Ekstern: Ringetonen for eksterne anrop brukes for alle anrop.

Always Use Dial Tone (Bruk alltid ringetone) er et obligatorisk felt i Cisco Unified Communications Manager.

Prosedyre

- Trinn 1** I Cisco Unified Communications Manager Administration velger du **System > Tjenesteparametere**.
- Trinn 2** Velg den riktige serveren.
- Trinn 3** Velg **Cisco CallManager** som tjeneste.
- Trinn 4** Gå til ruten Parametere på tvers av grupper.
- Trinn 5** Sett **Bruk alltid ringetone** til ett av følgende:
- Ekstern
 - Intern
 - Standard
- Trinn 6** Velg **Lagre**.
- Trinn 7** Start telefonene på nytt.
-



KAPITTEL 9

Funksjoner og oppsett for Cisco IP-konferansetelefoner

- [Brukerstøtte for Cisco IP-telefon, på side 71](#)
- [Migrering av telefonen til en telefon med flere plattformer direkte, på side 71](#)
- [Konfigurere en ny funksjonstastmal, på side 72](#)
- [Konfigurere telefontjenester for brukere, på side 73](#)
- [Konfigurasjon av telefonfunksjoner, på side 73](#)

Brukerstøtte for Cisco IP-telefon

Hvis du er systemansvarlig, er du mest sannsynlig hovedkilden til informasjon for brukere av Cisco IP-telefon i nettverket eller firmaet. Det er viktig å formidle oppdatert og grundig informasjon til sluttbrukere.

For at brukerne skal kunne bruke enkelte av funksjonene på Cisco IP-telefon optimalt (inkludert Tjenester og alternativer for talemeldingssystem), må du eller nettverksteamet ditt sende informasjon, eller de må kunne kontakte deg for å få hjelp. Sørg for at du formidler navnet på kontaktpersoner til brukerne, og i tillegg hvordan de kan kontakte disse personene.

Det anbefales at du oppretter en webside på den interne kundestøttesiden, som formidler viktig informasjon til sluttbrukere om Cisco IP-telefon de bruker.

Vurder å inkludere følgende typer informasjon på denne siden:

- Brukerveiledninger for alle Cisco IP-telefon-modeller du støtter
- Informasjon om hvordan du får tilgang til Cisco Unified Communications Self Care Portal
- Liste med støttede funksjoner
- Brukerveiledning eller hurtigreferanse for talepostsystemet

Migrering av telefonen til en telefon med flere plattformer direkte

Du kan raskt overføre bedriftstelefonen til en telefon med flere plattformer i ett trinn uten å bruke overgangsfastvarebelastning. Alt du trenger, er å skaffe og godkjenne migreringslisensen fra serveren.

Hvis du vil ha mer informasjon, kan du se https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-iphone.html

Konfigurere en ny funksjonstastmal

Du må legge til funksjonstaster i en funksjonstastmal for å gi brukere tilgang til enkelte funksjoner. Hvis du for eksempel vil at brukerne skal kunne bruke Ikke forstyr, må du aktivere funksjonstasten. Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Du vil kanskje opprette flere maler. Du kan for eksempel opprette en mal for telefonen i et konferanserom, og en annen mal for en telefon på et lederkontor.

Denne prosedyren tar deg gjennom trinnene for å opprette en ny funksjonstastmal, og tilordne den til en bestemt telefon. I likhet med andre telefonfunksjoner kan du bruke malen for alle konferansetelefonene eller en gruppe med telefoner.

Prosedyre

-
- Trinn 1** Logge på Cisco Unified Communications Manager Administration som administrator.
- Trinn 2** Velg **Enhet > Enhetsinnstillinger > Funksjonstastmal**.
- Trinn 3** Klikk **Søk**.
- Trinn 4** Velg ett av følgende alternativer:
- Cisco Unified Communications Manager 11.5 og tidligere versjoner –**standardbruker**
 - Cisco Unified Communications Manager 12.0 og nyere versjoner –**personlig konferansebruker** eller **offentlig konferansebruker**.
- Trinn 5** Klikk på **Kopi**.
- Trinn 6** Endre navnet på malen.
For eksempel 7832 konferanserommal.
- Trinn 7** Klikk på **Lagre**.
- Trinn 8** Gå til siden **Konfigurer funksjonstastoppsett** på menyen øverst til høyre.
- Trinn 9** For hver anropsstatus kan du angi funksjoner som skal vises.
- Trinn 10** Klikk på **Lagre**.
- Trinn 11** Gå tilbake til **Søk/vis-skjermen** fra menyen øverst til høyre.
Du ser den nye malen i mallisten.
- Trinn 12** Velg **Enhet > Telefon**.
- Trinn 13** Finn telefonen som skal ha den nye malen, og velg den.
- Trinn 14** I feltet **Funksjonstastmal** velger du den nye funksjonstastmalen.
- Trinn 15** Klikk på **Lagre** og **Bruk konfigurasjon**.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Konfigurere telefontjenester for brukere

Du kan gi brukere tilgang til telefontjenester på Cisco IP-telefon. Du kan også tilordne en knapp til forskjellige telefontjenester. IP-telefonen behandler hver tjeneste som et eget program.

Før en bruker får tilgang til en tjeneste:

- Bruk Cisco Unified Communications Manager Administration til å konfigurere tjenester som ikke er til stede som standard.
- Brukeren må abonnere på tjenester ved hjelp av Selvhjelpsportal for Cisco Unified Communications. Dette nettbasert programmet formidler et grafisk brukergrensesnitt (GUI) for begrenset sluttbrukerkonfigurasjon for programmer på IP-telefonen. En bruker kan imidlertid ikke abonnere på tjenester du konfigurerer som et bedriftsabonnement.

Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Før du konfigurerer tjenester, må du samle inn URL-ene for nettstedene du vil konfigurere, og bekrefte at brukere har tilgang til de nettstedene fra bedriftens IP-telefonnettverk. Aktiviteten er ikke tilgjengelig for standardtjenestene som Cisco formidler.

Prosedyre

-
- Trinn 1** I Cisco Unified Communications Manager Administration velger du **Enhet (Device) > Enhetsinnstillinger (Device Settings) > Telefontjenester (Phone Services)**.
- Trinn 2** Bekreft at brukerne har tilgang til Selvhjelpsportal for Cisco Unified Communications. Derfra kan de velge og abonnere på konfigurerte tjenester.
- Se [Oversikt over selvhjelpsportalen, på side 51](#) for et sammendrag av informasjonen du må formidle til sluttbrukere.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Konfigurasjon av telefonfunksjoner

Du kan konfigurere telefoner til å ha en rekke funksjoner basert på behovet til brukerne. Du kan bruke funksjoner på alle telefoner, en gruppe telefoner eller enkeltstående telefoner.

Når du konfigurerer funksjoner, viser Cisco Unified Communications Manager Administration vinduet informasjon som gjelder for alle telefoner samt informasjon om gjelder for telefonmodellen. Informasjonen som er spesifikk for telefonmodellen, vises i området Produktspesifikt konfigurasjonsoppsett i vinduet.

Hvis du vil ha informasjon om feltene som gjelder for alle telefonmodeller, kan du se Cisco Unified Communications Manager dokumentasjonen.

Når du angir en verdi for et felt, er vinduet du angir feltet for, viktig fordi vinduer har ulik prioritet. Prioritetsrekkefølgen er:

1. Enkeltstående telefoner (høyest prioritet)
2. Gruppe med telefoner
3. Alle telefoner (lavest prioritet)

Hvis du for eksempel ikke vil at en bestemt gruppe brukere skal ha tilgang til telefonens websider, men resten av brukerne skal ha det, kan du:

1. Aktivere tilgang til telefonens webside for alle brukere.
2. Deaktivere tilgang til telefonens websider for hver individuelle bruker, eller konfigurere en brukergruppe og deaktivere tilgang til telefonens websider for gruppen med brukere.
3. Hvis en bestemt bruker i brukergruppen trenger tilgang til telefonens websider, kan du gi tilgang til den bestemte brukeren.

Beslektede emner

[Konfigurere lagring av brukerlegitimasjon for Expressway-pålogging](#), på side 99

Konfigurere telefonfunksjoner for alle telefoner

Prosedyre

- Trinn 1** Sign in to Cisco Unified Communications Manager Administrasjon som administrator.
- Trinn 2** Velg **System** > **Konfigurasjon av bedriftstelefon**.
- Trinn 3** Angi feltene du vil endre.
- Trinn 4** Merk av i avmerkingsboksen **Overstyr bedriftsinnstillinger** for alle endrede felt.
- Trinn 5** Klikk på **Lagre**.
- Trinn 6** Klikk på **Bruk konfigurasjon**.
- Trinn 7** Start telefonene på nytt.

Merk Dette vil påvirke alle telefonene i din organisasjon.

Beslektede emner

[Produktspesifikk konfigurasjon](#), på side 75

Konfigurere telefonfunksjoner for en gruppe telefoner

Prosedyre

- Trinn 1** Sign in to Cisco Unified Communications Manager Administrasjon som en administrator.
- Trinn 2** Velg **Enhet** > **Enhetsinnstillinger** > **Vanlig telefonprofil**.
- Trinn 3** Finn profilen.
- Trinn 4** Gå til ruten Produktspesifikt konfigurasjonsoppsett og angi feltene.

- Trinn 5** Merk av i avmerkingsboksen **Overstyr bedriftsinstillinger** for alle endrede felt.
- Trinn 6** Klikk på **Lagre**.
- Trinn 7** Klikk på **Bruk konfigurasjon**.
- Trinn 8** Start telefonene på nytt.

Beslektede emner

[Produktspesifikk konfigurasjon](#), på side 75

Konfigurere telefonfunksjoner for én telefon

Prosedyre

- Trinn 1** Logg inn på Cisco Unified Communications Manager Administrasjon som en administrator.
- Trinn 2** Velg **Enhet > Telefon**
- Trinn 3** Finn telefonen som er knyttet til brukeren.
- Trinn 4** Gå til ruten Produktspesifikk konfigurasjonsoppsett og angi feltene.
- Trinn 5** Merk av for **Override Common Settings (Overstyr vanlige innstillinger)** for alle endrede felt.
- Trinn 6** Klikk på **Lagre**.
- Trinn 7** Klikk på **Bruk konfigurasjon**.
- Trinn 8** Start telefonen på nytt.

Beslektede emner

[Produktspesifikk konfigurasjon](#), på side 75

Produktspesifikk konfigurasjon

Tabellen nedenfor beskriver feltene i ruten Oppsett for produktspesifikk konfigurasjon. Noen felt i denne tabellen vises kun på siden **Enhet > Telefon**.

Tabell 20: Felt i Produktspesifikk konfigurasjon

Feltnavn	Felttype eller valg	Standard	Beskrivelse
Tilgang til innstillinger	Deaktivert Aktivert Begrenset	Aktivert	Aktiverer, deaktiverer eller begrenser tilgang til lokale konfigurasjonsinnstillinger på menyen Innstillinger. Med begrenset tilgang kan du få tilgang til menyene Innstillinger og Status. Med deaktivert tilgang kan du få tilgang til Status-menyen.

Feltnavn	Felttype eller valg	Standard	Beskrivelse
GARP (Gratuitous ARP)	Deaktivert Aktivert	Deaktivert	Aktiverer eller deaktiverer muligheten for telefonen til å memorere MAC-adresser fra GARP. Denne funksjonen kreves for å overvåke eller spille inn talestrømmer.
Nettilgang	Deaktivert Aktivert	Deaktivert	Aktiverer eller deaktiverer tilgang til telefonens websider via en webleser. Forsiktig Hvis du aktiverer dette feltet, kan du vise sensitiv informasjon om telefonen.
Deaktiver TLS 1.0 og TLS 1.1 for webtilgang	Deaktivert Aktivert	Deaktivert	Kontrollerer bruken av TLS 1.2 for en webserver-tilkobling. <ul style="list-style-type: none"> • Deaktivert – en telefon som er konfigurert for TLS 1.0, TLS 1.1 eller TLS 1.2, kan fungere som en HTTPS-server. • Aktivert – bare en telefon som er konfigurert for TLS 1.2, kan fungere som en HTTPS-server.
Enbloc-oppringing	Deaktivert Aktivert	Deaktivert	Styrer oppringingsmetoden. <ul style="list-style-type: none"> • Deaktivert – Cisco Unified Communications Manager venter på at tastepausetidtakeren skal utløpe når det finnes overlappende oppringingsplaner eller rutemønstre. • Aktivert – hele oppringingsstrengen sendes til Cisco Unified Communications Manager når inntastingen er fullført. For å unngå T.302-tidtakertidsavbruddet anbefaler vi at du aktiverer Enbloc-oppringing når det finnes overlappende oppringingsplaner eller rutemønstre. <p>Tvungne godkjenningkoder(FAC) eller klientkoder (CMC) støtter ikke enbloc-oppringing. Hvis du bruker FAC eller CMC til å behandle anropstilgang og rapportering, kan du ikke bruke denne funksjonen.</p>
Dager med inaktiv bakgrunnsbelysning	Dager i uken		Definerer dagene som bakgrunnsbelysningen ikke aktiveres automatisk på tidspunktet som er angitt i feltet Tid for bakgrunnsbelysning på. Velg dagen eller dagene fra rullegardinlisten. Hvis du vil velge mer enn én dag, Ctrl+klikker du hver dag. Se Planlegge strømsparing for Cisco IP-telefoner, på side 87.

Feltnavn	Felttype eller valg	Standard	Beskrivelse
Tid for bakgrunnsbelysning på	tt:mm	07:30	<p>Definerer tidspunktet for hver dag da bakgrunnsbelysningen aktiveres automatisk (bortsett fra dagene som er angitt i feltet Bakgrunnsbelysning inaktiv).</p> <p>Angi tidspunktet i dette feltet i 24-timers klokkeformat, der 0:00 er midnatt.</p> <p>For eksempel, for å automatisk slå på bakgrunnsbelysningen kl. 07:00 om morgenen. (0700), skriv inn 07:00. For å slå på bakgrunnsbelysningen kl. 02:00 på ettermiddagen, angir du 14:00.</p> <p>Hvis dette feltet er tomt, aktiveres bakgrunnsbelysningen automatisk klokken 0:00.</p> <p>Se Planlegge strømsparing for Cisco IP-telefoner, på side 87.</p>
Varighet for bakgrunnsbelysning på	tt:mm	10:30	<p>Definerer hvor lenge bakgrunnsbelysningen forblir aktivert etter tidspunktet som er angitt i feltet Tid for bakgrunnsbelysning på.</p> <p>Hvis du for eksempel vil beholde bakgrunnsbelysningen aktivert i 4 timer og 30 minutter etter at den aktiveres automatisk, angir du 04:30.</p> <p>Hvis dette feltet er tomt, deaktiveres belysningen på slutten av dagen (0:00).</p> <p>Hvis Tid for bakgrunnsbelysning på er satt til 0:00 og verdien for Varighet for bakgrunnsbelysning på er tom (eller 24:00), deaktiveres ikke bakgrunnsbelysningen.</p> <p>Se Planlegge strømsparing for Cisco IP-telefoner, på side 87.</p>
Tidsavbrudd for inaktiv bakgrunnsbelysning	tt:mm	1:00	<p>Definerer hvor lenge telefonen er inaktiv før bakgrunnsbelysningen deaktiveres. Gjelder bare når bakgrunnsbelysningen var deaktivert som planlagt, og ble aktivert av en bruker (ved å trykke på en knapp på telefonen eller løfte av røret).</p> <p>Hvis du for eksempel vil deaktivere bakgrunnsbelysningen når telefonen har vært inaktiv i 1 time og 30 minutter etter at en bruker aktiverte bakgrunnsbelysningen, angir du 01:30.</p> <p>Se Planlegge strømsparing for Cisco IP-telefoner, på side 87.</p>
Bakgrunnsbelysning på ved innkommende anrop	Deaktivert Aktivert	Aktivert	Aktiverer bakgrunnsbelysningen ved innkommende anrop.

Felt navn	Felttype eller valg	Standard	Beskrivelse
Aktiver Power Save Plus	Dager i uken		<p>Definerer hvilke dager telefonen skal deaktiveres på. Velg dagen eller dagene fra rullegardinlisten. Hvis du vil velge mer enn én dag, Ctrl+klikker du hver dag.</p> <p>Når Aktiver Power Save Plus er aktivert, mottar du en melding om nødsituasjoner (e911).</p> <p>Forsiktig Når modusen Power Save Plus ("modusen") er aktivert, blir endepunkter som er konfigurert for modusen, deaktivert for nødansrop, og de kan heller ikke motta innkommende anrop. Når du velger denne modusen, godtar du samtidig følgende: (i) Du tar det hele og fulle ansvar for å formidle alternative metoder for nødansrop og mottak av anrop mens modusen er aktivert; (ii) Cisco er ikke ansvarlig i forbindelse med ditt valg av denne modusen, og alt erstatningsansvar i forbindelse med aktivering av modusen ligger hos deg; og (iii) Du informerer brukerne om hvilke følger modusen får for samtaler, anrop og annet.</p> <p>Hvis du vil deaktivere Power Save Plus, må du fjerne merket for Tillat EnergyWise-overstyringer. Hvis det fortsatt er merket av for alternativet Tillat EnergyWise-overstyringer i feltet Aktiver Power Save Plus, blir ikke Power Save Plus deaktivert.</p> <p>Se Planlegge EnergyWise på Cisco IP-telefoner, på side 89.</p>

Felt navn	Felttype eller valg	Standard	Beskrivelse
Tid for telefon på	tt:mm	00:00	<p>Fastslår når telefonen slås automatisk på for dagene som er angitt i feltet Aktiver Power Save Plus.</p> <p>Angi tidspunktet i dette feltet i 24-timers klokkeformat, der 00:00 er midnatt.</p> <p>For eksempel, for å automatisk slå på telefonen kl. 07:00 om morgenen. (0700), skriv inn 07:00. For å slå på telefonen kl. 14:00 på ettermiddagen. angir du 14:00.</p> <p>Standardverdien er tom, som vil si 00:00.</p> <p>Verdien i feltet Tid for telefon på må være minst 20 minutter senere enn verdien i feltet Tid for telefon av. Hvis tiden i Tid for telefon av for eksempel er 07:00, kan ikke tiden i Tid for telefon på være tidligere enn 07:20.</p> <p>Se Planlegge EnergyWise på Cisco IP-telefoner, på side 89.</p>
Tid for telefon av	tt:mm	24:00	<p>Definerer tiden på dagen da telefonen slås av for dagene som er valgt i feltet Aktiver Power Save Plus. Hvis feltene Tid for telefon på og Tid for telefon av inneholder den samme verdien, slås ikke telefonen av.</p> <p>Angi tidspunktet i dette feltet i 24-timers klokkeformat, der 00:00 er midnatt.</p> <p>For eksempel, for å automatisk slå av telefonen kl. 07:00 om morgenen. (0700), skriv inn 07:00. For å slå av telefonen kl. 14:00 på ettermiddagen. angir du 14:00.</p> <p>Standardverdien er tom, som vil si 00:00.</p> <p>Verdien i feltet Tid for telefon på må være minst 20 minutter senere enn verdien i feltet Tid for telefon av. Hvis tiden i Tid for telefon av for eksempel er 7:00, kan ikke tiden i Tid for telefon på være tidligere enn 7:20.</p> <p>Se Planlegge EnergyWise på Cisco IP-telefoner, på side 89.</p>

Feltnavn	Felttype eller valg	Standard	Beskrivelse
Tidsavbrudd for telefon av ved inaktivitet	mm	60	<p>Angir hvor lenge telefonen må være inaktiv før den slås av.</p> <p>Tidsavbruddet oppstår i følgende situasjoner:</p> <ul style="list-style-type: none"> • Når telefonen har vært i modusen Power Save Plus som planlagt og modusen ble avsluttet fordi telefonbrukeren trykket på Valg-tasten. • Når telefonen slås på igjen med den tilknyttede svitsjen. • Når verdien i feltet Tid for telefon av er nådd, men telefonen er i bruk. <p>Se Planlegge EnergyWise på Cisco IP-telefoner, på side 89.</p>
Aktiver lydvarsel	Avmerkingsboks	Ikke avmerket	<p>Når dette alternativet er aktivert, spiller telefonen av et lydvarsel 10 minutter før tiden som er angitt i feltet Tid for telefon av.</p> <p>Denne avmerkingsboksen gjelder bare hvis det er valgt én eller flere dager i listen Aktiver Power Save Plus.</p> <p>Se Planlegge EnergyWise på Cisco IP-telefoner, på side 89.</p>
EnergyWise-domene	Opptil 127 tegn		<p>Identifiserer EnergyWise-domenet som telefonen befinner seg i.</p> <p>Se Planlegge EnergyWise på Cisco IP-telefoner, på side 89.</p>
EnergyWise Secret (EnergyWise-hemmelighet)	Opptil 127 tegn		<p>Identifiserer det hemmelige sikkerhetspassordet som brukes til å kommunisere med endepunktene i EnergyWise-domenet.</p> <p>Se Planlegge EnergyWise på Cisco IP-telefoner, på side 89.</p>

Felt navn	Felttype eller valg	Standard	Beskrivelse
Tillat EnergyWise-overstyringer	Avmerkingsboks	Ikke avmerket	<p>Fastslår om du tillater at policyen for EnergyWise-domenekontrolleren sender oppdateringer om strømnivå til telefonene. Følgende betingelser gjelder:</p> <ul style="list-style-type: none"> • Én eller flere dager må velges i feltet Aktiver Power Save Plus. • Innstillingene i Cisco Unified Communications Manager Administration trer i kraft etter planen selv om EnergyWise sender en overstyring. <p>Hvis verdien i feltet Tid for telefon av for eksempel er satt til 22:00, verdien i feltet Tid for telefon på er 06:00 og det er valgt én eller flere dager i feltet Aktiver Power Save Plus.</p> <ul style="list-style-type: none"> • Hvis EnergyWise angir at telefonen skal slås av klokken 20:00, gjelder den innstillingen (såfremt telefonen ikke brukes) til det konfigurerte tidspunktet 06:00 for Tid for telefon på. • Klokken 06:00 slås telefonen på og gjenopptar mottak av strømnivåendringer fra innstillingene i Cisco Unified Communications Manager Administration. • Hvis du vil endre strømnivået for telefonen igjen, må EnergyWise sende en ny kommando for endring av strømnivå. <p>Hvis du vil deaktivere Power Save Plus, må du fjerne merket for Tillat EnergyWise-overstyringer. Hvis det fortsatt er merket av for alternativet Tillat EnergyWise-overstyringer i feltet Aktiver Power Save Plus, blir ikke Power Save Plus deaktivert.</p> <p>Se Planlegge EnergyWise på Cisco IP-telefoner, på side 89.</p>
Policy for deltagelse og direkteoverføring	Samme linje, aktivert Samme linje, deaktivert	Samme linje, aktivert	<p>Styrer om en bruker kan delta i og overføre samtaler.</p> <ul style="list-style-type: none"> • Samme linje, aktivert – Brukere kan direkteoverføre eller bli med i en samtale på den gjeldende linjen til en annen samtale på samme linje. • Samme linje, deaktivert – Brukere kan ikke bli med i eller overføre samtaler på samme linje. Funksjonen for å delta i og overføre samtaler er deaktivert, og brukeren kan ikke bruke dem.

Feltnavn	Felttype eller valg	Standard	Beskrivelse
Innspillingstone	Deaktivert Aktivert	Deaktivert	Kontrollerer avspillingen av tonen når en bruker spiller inn en samtale
Lokalt volum for innspillingstone	Heltall 0-100	100	Kontrollerer volumet på innspillingstone for den lokale brukeren.
Volum for ekstern innspillingstone	Heltall 0-100	50	Kontrollerer volumet for innspillingstone for den eksterne brukeren.
Varighet for innspillingstone	Heltall 1-3000 millisekunder		Kontrollerer varigheten av innspillingstone.
Tidsmåler for funksjonstasten "flere"	Heltall 0, 5-30 sekunder	5	Kontrollerer hvor lenge en rad med sekundære funksjonstaster vises før telefonen viser det opprinnelige settet med funksjonstaster. 0 deaktiverer tidtakeren.
Loggserver	Streng med opptil 256 tegn		Identifiserer IPv4-syslog-serveren for feilsøking av telefonen. Formatet for adressen er: adresse: <port>@@base=<0-7>;pfs=<0-1> Se Kontrollere feilsøkinginformasjon fra Cisco Unified Communications Manager , på side 152.
Ekstern logg	Deaktivert Aktivert	Deaktivert	Kontrollerer muligheten til å sende logger til syslog-serveren. Se Kontrollere feilsøkinginformasjon fra Cisco Unified Communications Manager , på side 152.

Feltnavn	Felttype eller valg	Standard	Beskrivelse
Loggprofil	Standard Forhåndsinnstilt Telefoni SIP Brukergrensesnitt Nettverk Media Oppgradering Tilbehør Sikkerhet Energywise MobileRemoteAccess	Forhåndsinnstilt	Angir den forhåndsdefinerte loggingsprofilen. <ul style="list-style-type: none"> • Standard – Standard loggingsnivå for feilsøking • Forhåndsinnstilt – Overskriver ikke telefonens innstilling for logging av lokal feilsøking • Telefoni – Logger informasjon om telefoni- eller samtalefunksjoner • SIP – Logger informasjon om SIP-signalisering • Brukergrensesnitt – Logger informasjon om telefonens brukergrensesnitt • Nettverk – Logger nettverksinformasjon • Media – Logger medieinformasjon • Oppgradering – Logger oppgraderingsinformasjon • Tilbehør – Logger tilbehørsinformasjon • Sikkerhet – Logger sikkerhetsinformasjon • Energywise – Logger energisparingsinformasjon • MobileRemoteAccess – Logger MRA via Expressway-informasjon. <p>Se Kontrollere feilsøkingsinformasjon fra Cisco Unified Communications Manager, på side 152.</p>
IPv6-loggserver	Streng med opptil 256 tegn		Identifiserer IPv6-syslog-serveren for feilsøking av telefonen. <p>Se Kontrollere feilsøkingsinformasjon fra Cisco Unified Communications Manager, på side 152.</p>
Cisco Discovery Protocol (CDP): Svitsjeport	Deaktivert Aktivert	Aktivert	Kontrollerer Cisco Discovery Protocol på telefonen.
Link Layer Discovery Protocol – Media Endpoint Discover (LLDP-MED): Svitsjeport	Deaktivert Aktivert	Aktivert	Aktiverer LLDP-MED på svitsjeporten.
LLDP Asset ID (ID for LLDP-ressurs)	Streng, opptil 32 tegn		Identifiserer ressurs-ID-en som er tilordnet til telefonen for lagerstyring.

Feltnavn	Felttype eller valg	Standard	Beskrivelse
Energy Efficient Ethernet (EEE): svitsjeport	Deaktivert Aktivert	Deaktivert	Styrer EEE på svitsjeporten.
LLDP-strømprioritet	Ukjent Lav Høy Kritisk	Ukjent	Tilordner en telefonstrømprioritet til svitsjen, slik at den formidler strøm på riktig måte til telefonene.
802.1x-godkjenning	Brukerkontrollert Deaktivert Aktivert	Brukerkontrollert	Angir statusen for 802.1x-godkjenningsfunksjonen. <ul style="list-style-type: none"> • Brukerkontrollert – Brukeren kan konfigurere 802.1x på telefonen. • Deaktivert – 802.1x-godkjenning brukes ikke. • Aktivert – 802.1x-godkjenning brukes, og du kan konfigurere godkjenningen for telefonene.
Ekstern konfigurasjon av svitsjeport	Deaktivert Automatisk forhandling 10 halv 10 full 100 halv 100 full	Deaktivert	Tillater at du konfigurerer hastighets- og dupleksinformasjonen for telefonens svitsjeport eksternt. Dette forbedrer ytelsen for store distribusjoner med bestemte portinnstillinger. Hvis svitsjeportene er konfigurert for ekstern portkonfigurasjon i Cisco Unified Communications Manager, kan ikke dataene endres på telefonen.
SSH-tilgang	Deaktivert Aktivert	Deaktivert	Kontrollerer tilgangen til SSH-daemon gjennom port 22. Ved å la port 22 være åpen, vil telefonen være sårbar for Denial og Service-angrep (DoS).
Ringetonespråk	Standard Japan	Standard	Kontrollerer ringemønsteret.
TLS Resumption Timer (Tidaker for TLS-gjenopptakelse)	Heltall 0-3600 sekunder	3600	Kontrollerer muligheten til å gjenoppta en TLS-økt uten å gjenta hele TLS-godkjenningsprosessen. Hvis feltet er satt til 0, blir gjenopptakelsen av TLS-økten deaktivert.
FIPS-modus	Deaktivert Aktivert	Deaktivert	Aktiverer eller deaktiverer FIPS-modus (Federal Information Processing Standards) på telefonen.
Registrer samtalelogg fra delt linje	Deaktivert Aktivert	Deaktivert	Angir om en anropslogg skal registreres fra en delt linje.

Feltnavn	Felttype eller valg	Standard	Beskrivelse
Minste ringevolum	0 – Lydløs 1–15	0 – Lydløs	Kontrollerer minste ringevolum for telefonen.
Peer-fastvaredeling	Deaktivert Aktivert	Aktivert	<p>Tillater at telefonen finner andre telefoner av samme modell på subnett og deler oppdaterte fastvarefiler. Hvis telefonen har en ny fastvareopplasting, kan den deles med de andre telefonene. Hvis én av telefonene har en ny fastvareopplasting, kan telefonen laste ned fastvaren fra den andre telefonen i stedet for fra TFTP-serveren.</p> <p>Peer-fastvaredeling:</p> <ul style="list-style-type: none"> • Begrenser opphoping av TFTP-overføringer til sentraliserte eksterne TFTP-servere. • Fjerner behovet for å kontrollere fastvareoppgraderinger manuelt. • Reduserer telefonens nedetid under oppgraderinger når et stort antall telefoner tilbakestilles samtidig. • Hjelper med fastvareoppgraderinger på bransjekontorer eller ved eksterne kontorer som kjører via WAN-koblinger med begrenset båndbredde.
Lasteserver	Streng med opptil 256 tegn		Identifiserer den alternative IPv4-serveren som telefonen bruker til å hente fastvareinnlastinger og -oppgraderinger.
IPv6-lasteserver	Streng med opptil 256 tegn		Identifiserer den alternative IPv6-serveren som telefonen bruker til å hente fastvareinnlastinger og -oppgraderinger.

Feltnavn	Felttype eller valg	Standard	Beskrivelse
Registrer feil ved tilkobling til Unified CM	Normal Forsinket	Normal	<p>Fastslår følsomheten som telefonen har for å registrere en feil med tilkoblingen til Cisco Unified Communications Manager (Unified CM), som er det første trinnet før enheten tar i bruk en sikkerhetskopi av Unified CM/SRST.</p> <p>Gyldige verdier angir Normal (registrering av en feil i tilkoblingen til Unified CM skjer ved standard systemhastighet) eller Forsinket (registrering av en failover i tilkoblingen til Unified CM skjer omtrent fire ganger langsommere enn for Normal).</p> <p>Velg Normal for raskere registrering av en feil i tilkoblingen til Unified CM. Velg Forsinket hvis du foretrekker at failover skal være litt forsinket, slik at du gir tilkoblingen mulighet til å gjenopprettes.</p> <p>Den nøyaktige tidsforskjellen mellom Normal og Forsinket avhenger av mange variabler som endres kontinuerlig.</p>
ID for spesialkrav	Streng		Kontrollerer tilpassede funksjoner fra ES-innlastinger (Engineering Special).
HTTPS-server	http og https aktivert bare https	http og https aktivert	Kontrollerer typen kommunikasjon til telefonen. Hvis du velger Bare HTTPS, er telefonkommunikasjonen sikrere.
Lagring av brukerlegitimasjon for Expressway-pålogging	Deaktivert Aktivert	Deaktivert	<p>Kontrollerer om telefonen lagrer brukerens påloggingsinformasjon. Når dette alternativet er deaktivert, får alltid brukeren en melding om å logge på Expressway-serveren for MRA (Mobile and Remote Access).</p> <p>Hvis du vil gjøre det enklere for brukere å logge inn, aktiverer du dette feltet slik at Expressway-innloggingsopplysningene beholdes. Dermed trenger brukeren bare å angi påloggingsinformasjon første gang. Hver gang deretter (når telefonen slås på utenfor kontoret) er påloggingsinformasjonen ferdigutfylt på påloggings skjermen.</p> <p>Hvis du vil ha mer informasjon, kan du se Konfigurere lagring av brukerlegitimasjon for Expressway-pålogging, på side 99</p>

Feltnavn	Felttype eller valg	Standard	Beskrivelse
Customer support upload URL (URL for opplasting av kundestøtte)	Streng, opptil 256 tegn		Formidler URL-en for problemrapporteringsverktøyet (PRT). Hvis du tar i bruk enheter med MRA via Expressway, må du også legge til adressen til PRT-serveren i listen over tillatte HTTP-servere på Expressway-serveren. Hvis du vil ha mer informasjon, kan du se Konfigurere lagring av brukerlegitimasjon for Expressway-pålogging, på side 99
Deaktiver TLS-chifre	Se Deaktivere TLS-chifre, på side 87 .	Ingen	Deaktiverer det valgte TLS-chifferet. Deaktiver mer enn én chifferserie ved å velge og holde inne Ctrl -tasten på tastaturet til datamaskinen.

Deaktivere TLS-chifre

Du kan deaktivere TLS-chifre (Transport Layer Security) med parameteren **Deaktivere TLS-chifre**. Dermed kan du skreddersy sikkerheten for kjente sikkerhetsproblemer, og du kan tilpasse nettverket ditt til firmaets retningslinjer for chifre.

Standardinnstillingen er Ingen (None).

Deaktiver mer enn én chifferserie ved å velge og holde inne **Ctrl**-tasten på tastaturet til datamaskinen. Hvis du velger alle telefonchifrene, påvirkes telefonens TLS-tjeneste. Alternativene er:

- 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

Du finner mer informasjon om telefonsikkerhet i *Sikkerhetsoversikt for Cisco IP-telefon 7800 og 8800-serien* (<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html>).

Planlegge strømparing for Cisco IP-telefoner

Hvis du vil spare strøm og sørge for at telefonskjermvisningen varer så lenge som mulig, kan du konfigurere skjermen til å slås av når den ikke må være aktiv.

Du kan konfigurere innstillinger i Cisco Unified Communications Manager Administration for å slå av skjermen på et bestemt tidspunkt noen dager og hele dagen andre dager. Du kan for eksempel velge å slå av skjermen etter arbeidstid på ukedager og hele dagen på lørdager og søndager.

Du kan utføre noen av disse handlingene til å slå på skjermen når den er avslått:

- Trykk på en knapp på telefonen.
Telefonen utfører handlingen angitt av knappen i tillegg til å slå på skjermen.
- Løft opp håndsettet.

Når du slår på skjermen, forblir den på helt til telefonen har vært inaktiv i et bestemt tidsrom, og deretter slår den seg av automatisk.

Prosedyre

Trinn 1 I Cisco Unified Communications Manager Administration velger du **Enhet > Telefon**.

Trinn 2 Finn telefonen du må konfigurere.

Trinn 3 Gå til området Produktspesifikk konfigurasjon, og angi følgende felt:

- Viste dager er ikke aktive
- Vis etter tid
- Vis etter varighet
- Vis tidsavbrudd ved inaktivitet

Tabell 21: Konfigurasjonsfelter for strømsparing

Felt	Beskrivelse
Viste dager er ikke aktive	Dagene da skjermen ikke slås på automatisk på tidspunktet som er angitt i feltet Vis etter tid. Velg dagen eller dagene fra rullegardinlisten. Hvis du vil velge mer enn én dag, Ctrl+klikker du hver dag.
Vis etter tid	Tidspunktet hver dag da skjermen slås på automatisk (bortsett fra dagene som er angitt i feltet Viste dager er ikke aktive). Angi tidspunktet i dette feltet i 24-timers klokkeformat, der 00:00 er midnatt. Hvis du for eksempel vil slå på skjermen automatisk klokken 07:00, angir du 07:00 . For å slå på skjermen kl. 14.00 angir du 14:00 . Hvis dette feltet er tomt, slås skjermen automatisk på klokken 0:00.

Felt	Beskrivelse
Vis etter varighet	<p>Hvor lenge skjermen forblir på etter tidspunktet som er angitt i feltet Vis etter tid.</p> <p>Skriv inn verdien i dette feltet i formatet <i>timer:minutter</i>.</p> <p>Hvis du for eksempel vil beholde skjermen på i 4 timer og 30 minutter etter at den slås på automatisk, angir du 04:30.</p> <p>Hvis dette feltet er tomt, slås telefonen av ved slutten av dagen (0:00).</p> <p>Merk Hvis Vis etter tid er 0:00 og Vis etter varighet er tom (eller 24:00), vil skjermen stå på kontinuerlig.</p>
Vis tidsavbrudd ved inaktivitet	<p>Hvor lenge telefonen er inaktiv før skjermen slås av. Gjelder bare når skjermen var avslått som planlagt og ble slått på av en bruker (ved å trykke på en knapp på telefonen eller løfte av håndsettet).</p> <p>Skriv inn verdien i dette feltet i formatet <i>timer:minutter</i>.</p> <p>Hvis du for eksempel vil slå av skjermen når telefonen har vært inaktiv i 1 time og 30 minutter etter at en bruker har slått på skjermen, angir du 01:30.</p> <p>Standardverdien er 01:00.</p>

- Trinn 4** Velg **Lagre**.
- Trinn 5** Velg **Bruk konfigurasjon**.
- Trinn 6** Start telefonen på nytt.

Planlegge EnergyWise på Cisco IP-telefoner

Hvis du vil redusere strømforbruket, konfigurerer du telefonen til å gå til hvilemodus (slås av) og aktiveringsmodus (slås på) hvis systemet inkluderer en EnergyWise-kontroller.

Du konfigurerer innstillingene i Cisco Unified Communications Manager Administration for å aktivere EnergyWise og konfigurerer tidspunktet for hvile- og aktiveringsmodus. Disse parameterne er nært knyttet til parameterne for konfigurering av telefonvisning.

Når EnergyWise er aktivert og hvilemodus er angitt, sender telefonen en forespørsel til svitsjen om å aktivere den på det konfigurerte tidspunktet. Svitsjen returnerer en melding om godkjenning eller avslag på forespørselen. Hvis svitsjen avslår forespørselen eller hvis svitsjen ikke svarer, blir ikke telefonen slått av. Hvis svitsjen godtar forespørselen, går den inaktive telefonen til hvilemodus. Dermed reduseres strømforbruket til et forhåndsinnstilt nivå. En telefon som ikke er inaktiv, konfigurerer en tidtaker for inaktivitet og går til hvilemodus etter at tidtakeren utløper.

Du aktiverer telefonen ved å trykke på Velg. På det planlagte aktiveringstidspunktet gjenoppretter systemet strøm til telefonen, aktiverer den.

Prosedyre

- Trinn 1** Fra Cisco Unified Communications Manager Administration velger du **Enhet > Telefon**.
- Trinn 2** Finn telefonen du må konfigurere.

Trinn 3 Gå til området Produktspesifikk konfigurasjon og angi følgende felt.

- Aktiver Power Save Plus
- Tid for telefon på
- Tid for telefon av
- Tidsavbrudd for telefon av ved inaktivitet
- Aktiver lydvarsel
- EnergyWise-domene
- EnergyWise Secret (EnergyWise-hemmelighet)
- Tillat EnergyWise-overstyringer

Tabell 22: Konfigurasjonsfelter for EnergyWise

Felt	Beskrivelse
Aktiver Power Save Plus	<p>Velger hvilke dager telefonen skal deaktiveres på. Velg flere dager ved å trykke på og holde inne Ctrl-tasten mens du klikker på dagene til tidsplanen.</p> <p>Som standard er ingen dager valgt.</p> <p>Når Aktiver Power Save Plus er merket av, mottar du en melding om nødsituasjoner (e911).</p> <p>Forsiktig Når modusen Power Save Plus (“modusen”) er aktivert, blir endepunkter som er konfigurert for modusen, deaktivert for nødanrop, og de kan heller ikke motta innkommende anrop. Når du velger denne modusen, godtar du samtidig følgende: (i) Du tar det hele og fulle ansvar for å formidle alternative metoder for nødanrop og mottak av anrop mens modusen er aktivert; (ii) Cisco er ikke ansvarlig i forbindelse med ditt valg av denne modusen, og alt erstatningsansvar i forbindelse med aktivering av modusen ligger hos deg; og (iii) Du informerer brukerne om hvilke følger modusen får for samtaler, anrop og annet.</p> <p>Merk Hvis du vil deaktivere Power Save Plus, må du fjerne merket for Tillat EnergyWise-overstyringer. Hvis det fortsatt er merket av for alternativet Tillat EnergyWise-overstyringer i feltet Aktiver Power Save Plus, blir ikke Power Save Plus deaktivert.</p>
Tid for telefon på	<p>Fastslår når telefonen slås automatisk på for dagene som er angitt i feltet Aktiver Power Save Plus.</p> <p>Angi tidspunktet i dette feltet i 24-timers klokkeformat, der 00:00 er midnatt.</p> <p>For eksempel, for å automatisk slå på telefonen kl. 07:00 om morgenen. (0700), skriv inn 07:00. For å slå på telefonen kl. 14:00 på ettermiddagen. angir du 14:00.</p> <p>Standardverdien er tom, som vil si 00:00.</p> <p>Merk Verdien i feltet Tid for telefon på må være minst 20 minutter senere enn verdien i feltet Tid for telefon av. Hvis tiden i Tid for telefon av for eksempel er 07:00, kan ikke tiden i Tid for telefon på være tidligere enn 07:20.</p>

Felt	Beskrivelse
Tid for telefon av	<p>Tiden på dagen da telefonen slås av for dagene som er valgt i feltet Aktiver Power Save Plus. Hvis feltene Tid for telefon på og Tid for telefon av inneholder den samme verdien, slås ikke telefonen av.</p> <p>Angi tidspunktet i dette feltet i 24-timers klokkeformat, der 00:00 er midnatt.</p> <p>For eksempel, for å automatisk slå av telefonen kl. 07:00 om morgenen. (0700), skriv inn 07:00. For å slå av telefonen kl. 14:00 på ettermiddagen. angir du 14:00.</p> <p>Standardverdien er tom, som vil si 00:00.</p> <p>Merk Verdien i feltet Tid for telefon på må være minst 20 minutter senere enn verdien i feltet Tid for telefon av. Hvis tiden i Tid for telefon av for eksempel er 7:00, kan ikke tiden i Tid for telefon på være tidligere enn 7:20.</p>
Tidsavbrudd for telefon av ved inaktivitet	<p>Hvor lenge telefonen må være inaktiv før den slås av.</p> <p>Tidsavbruddet oppstår i følgende situasjoner:</p> <ul style="list-style-type: none"> • Når telefonen har vært i modusen Power Save Plus som planlagt og modusen ble avsluttet fordi telefonbrukeren trykket på Valg-tasten. • Når telefonen slås på igjen med den tilknyttede svitsjen. • Når verdien i feltet Tid for telefon av er nådd, men telefonen er i bruk. <p>Området for feltet er 20 til 1440 minutter.</p> <p>Standardverdien er 60 minutter.</p>
Aktiver lydvarsel	<p>Når dette alternativet er aktivert, spiller telefonen av et lydvarsel 10 minutter før tiden som er angitt i feltet Tid for telefon av.</p> <p>Lydvarselet bruker telefonens ringetone, som kort spilles av til bestemte tider i varselsperioden på 10-minutter. Den varslende ringetonen spilles av med det brukerangitte volumnivået.</p> <p>Lydvarselets tidsplan er:</p> <ul style="list-style-type: none"> • 10 minutter før strømmen slår seg av, spilles ringetonen av fire ganger. • 7 minutter før strømmen slår seg av, spilles ringetonen av fire ganger. • 4 minutter før strømmen slår seg av, spilles ringetonen av fire ganger. • 30 sekunder før strømmen slår seg av, spilles ringetonen av 15 ganger eller til telefonen slår seg av. <p>Denne avmerkingsboksen gjelder bare hvis det er valgt én eller flere dager i listen Aktiver Power Save Plus.</p>
EnergyWise-domene	<p>EnergyWise-domenet som telefonen befinner seg i.</p> <p>Den maksimale lengden i dette feltet er 127 tegn.</p>
EnergyWise Secret (EnergyWise-hemmelighet)	<p>Det hemmelige sikkerhetspassordet som brukes til å kommunisere med endepunktene i EnergyWise-domenet.</p> <p>Den maksimale lengden i dette feltet er 127 tegn.</p>

Felt	Beskrivelse
Tillat EnergyWise-overstyringer	<p>Denne avmerkingsboksen avgjør om du skal tillate at policyen for EnergyWise-domenekontrolleren sender oppdateringer om strømnivå til telefonene. Følgende betingelser gjelder:</p> <ul style="list-style-type: none"> • Én eller flere dager må velges i feltet Aktiver Power Save Plus. • Innstillingene i Cisco Unified Communications Manager Administration trer i kraft etter planen selv om EnergyWise sender en overstyring. <p>Hvis verdien i feltet Tid for telefon av for eksempel er satt til 22:00, verdien i feltet Tid for telefon på er 06:00 og det er valgt én eller flere dager i feltet Aktiver Power Save Plus.</p> <ul style="list-style-type: none"> • Hvis EnergyWise angir at telefonen skal slås av klokken 20:00, gjelder den innstillingen (såfremt telefonen ikke brukes) til det konfigurerte tidspunktet 06:00 for Tid for telefon på. • Klokken 06:00 slås telefonen på og gjenopptar mottak av strømnivåendringer fra innstillingene i Unified Communications Manager Administration. • Hvis du vil endre strømnivået for telefonen igjen, må EnergyWise sende en ny kommando for endring av strømnivå. <p>Merk Hvis du vil deaktivere Power Save Plus, må du fjerne merket for Tillat EnergyWise-overstyringer. Hvis det fortsatt er merket av for alternativet Tillat EnergyWise-overstyringer i feltet Aktiver Power Save Plus, blir ikke Power Save Plus deaktivert.</p>

Trinn 4 Velg **Lagre**.

Trinn 5 Velg **Bruk konfigurasjon**.

Trinn 6 Start telefonen på nytt.

Konfigurere Ikke forstyr

Når Ikke forstyr (DND) er aktivert, blir lysstripen på konferansetelefonen rød.

Du finner mer informasjon under Ikke forstyr i dokumentasjonen for din spesifikke versjon av Cisco Unified Communications Manager.

Prosedyre

Trinn 1 I Cisco Unified Communications Manager Administration velger du **Enhet > Telefon**.

Trinn 2 Finn telefonen som skal konfigureres.

Trinn 3 Angi følgende parametere.

- Ikke forstyr: Med dette alternativet kan du aktivere Ikke forstyr på telefonen.
- Alternativet Ikke forstyr: Innstillingene Ringetone av, Anropsavvisning eller Use Common Phone Profile (Bruk vanlig telefonprofil).

- Varsel om innkommende anrop når Ikke forstyrr er aktivert: Velg varselstypen som skal spilles av for innkommende anrop når Ikke forstyrr er aktivert.

Merk Denne parameteren befinner seg i vinduet Vanlig telefonprofil og vinduet Telefonkonfigurasjon. Vinduet Telefonkonfigurasjon har forrang.

Trinn 4 Velg **Lagre**.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Aktivere agenthilsen

Funksjonen Agenthilsen tillater at en agent oppretter og oppdaterer en forhåndsinnspilt hilsen som spilles av på begynnelsen av en samtale, for eksempel en kundesamtale, før agenten starter å snakke med innringeren. Agenten kan forhåndsinnspille en enkeltstående hilsen eller flere hilsener etter behov samt opprette og oppdatere hilsenene.

Når en kunde ringer, hører både agenten og innringeren den forhåndsinnspilte hilsenen. Agenten kan fortsatt ha volumet dempet til hilsenen er avsluttet, eller han/hun kan besvare anropet over hilsenen.

Alle kodeker som støttes for telefonen, støttes også for samtaler med agenthilsen.

Hvis du vil ha mer informasjon, kan du se informasjonen om innbrudd og personvern i dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Prosedyre

Trinn 1 Fra Cisco Unified Communications Manager Administration velger du **Enhet > Telefon**.

Trinn 2 Finn IP-telefonen du vil konfigurere.

Trinn 3 Gå til ruten Oppsett for enhetsinformasjon og sett **Innebygd bro** til På eller Standard.

Trinn 4 Velg **Lagre**.

Trinn 5 Kontroller innstillingene for broen:

- Velg **System > Tjenesteparametere**.
- Velg den aktuelle serveren og tjenesten.
- Gå til ruten Parametere på tvers av grupper (Enhet - telefon) og sett **Aktivering av innebygd bro** til På.
- Velg **Lagre**.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Konfigurer Varsel for viderekobling av anrop

Du kan kontrollere innstillingene for viderekobling av anrop.

Prosedyre

Trinn 1 I Cisco Unified Communications Manager Administration velger du **Enhet > Telefon**.

Trinn 2 Finn telefonen som skal konfigureres.

Trinn 3 Konfigurer feltene for varsel for viderekobling av anrop.

Felt	Beskrivelse
Navn på anroper	Når det er merket av for dette alternativet, vises navnet på anroperen i varselvinduet. Som standard er det merket av for dette alternativet.
Nummer for anroper	Når det er merket av for dette alternativet, vises nummeret for anroperen i varselvinduet. Som standard er det ikke merket av for dette alternativet.
Viderekoblet nummer	Når det er merket av for dette alternativet, vises informasjonen om anroperen som sist viderekoblet anropet, i varselvinduet. Eksempel: Hvis Anroper A ringer til B, men B har viderekoblet alle anrop til C og C har viderekoblet alle anrop til D, inneholder varselvinduet som D ser, telefoninformasjonen for Anroper C. Som standard er det ikke merket av for dette alternativet.
Oppringt nummer	Når det er merket av for dette alternativet, vises informasjonen om den opprinnelig mottakeren av anropet, i varselvinduet. Eksempel: Hvis Anroper A ringer til B, men B har viderekoblet alle anrop til C og C har viderekoblet alle anrop til D, vil varselvinduet som D ser, dermed inneholde telefoninformasjonen for Anroper B. Som standard er det merket av for dette alternativet.

Trinn 4 Velg **Lagre**.

Aktivere Enhetsaktivert innspilling

Konfigurer funksjonen Enhetsaktivert innspilling fra Cisco Unified Communications Manager Administration. Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Prosedyre

Trinn 1 Sett parameteren for Innebygd bro for IP-telefon til **På**.

Trinn 2 På siden Linjekonfigurasjon setter du Innspillingsalternativ til **Innspilling av utvalgte anrop aktivert** og velger den aktuelle innspillingsprofilen.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

UCR 2008-oppsett

Parameterne som støtter UCR 2008, finnes i Cisco Unified Communications Manager Administration. Tabellen nedenfor beskriver parameterne og angir banen for å endre innstillingen.

Tabell 23: Plassering av UCR 2008-parametere

Parameter	Administrasjonsbane
FIPS-modus	Enhet (Device) > Enhetsinnstillinger (Device Settings) > Felles telefonprofil (Common Phone Profile)
	System > Konfigurasjon av bedriftstelefon (Enterprise Phone Configuration)
	Enhet > Telefoner
SSH-tilgang	Enhet (Device) > Telefon (Phone)
	Enhet (Device) > Enhetsinnstillinger (Device Settings) > Felles telefonprofil (Common Phone Profile)
Nettilgang	Enhet (Device) > Telefon (Phone)
	System > Konfigurasjon av bedriftstelefon (Enterprise Phone Configuration)
	Enhet (Device) > Enhetsinnstillinger (Device Settings) > Felles telefonprofil (Common Phone Profile)
System > Konfigurasjon av bedriftstelefon (Enterprise Phone Configuration)	
IP-adressemodus	Enhet (Device) > Enhetsinnstillinger (Device Settings) > Felles enhetskonfigurasjon (Common Device Configuration)
Innstilling for signalisering for IP-adressemodus	Enhet (Device) > Enhetsinnstillinger (Device Settings) > Felles enhetskonfigurasjon (Common Device Configuration)

Konfigurere UCR 2008 i Konfigurasjon av vanlig enhet

Bruk denne fremgangsmåten til å angi følgende UCR 2008-parametere:

- IP-adressemodus
- Innstilling for signalisering for IP-adressemodus

Prosedyre

- Trinn 1** I Cisco Unified Communications Manager Administration velger du **Enhet > Enhetsinnstillinger > Konfigurasjon av vanlig enhet**.
- Trinn 2** Angi en verdi for parameteren IP-adressemodus.
- Trinn 3** Angi en verdi for parameteren Innstilling for signalisering for IP-adressemodus.
- Trinn 4** Velg **Lagre**.
-

Konfigurere UCR 2008 i Vanlig telefonprofil

Bruk denne fremgangsmåten til å angi følgende UCR 2008-parametere:

- FIPS-modus
- SSH-tilgang
- Nettilgang

Prosedyre

- Trinn 1** I Cisco Unified Communications Manager Administration velger du **Enhet > Enhetsinnstillinger > Vanlig telefonprofil**.
- Trinn 2** Sett parameteren FIPS-modus til **Aktivert**.
- Trinn 3** Sett parameteren SSH-tilgang til **Deaktivert**.
- Trinn 4** Sett parameteren Webtilgang til **Deaktivert**.
- Trinn 5** Sett parameteren 80-biters SRTCP til **Aktivert**.
- Trinn 6** Velg **Lagre**.
-

Konfigurere UCR 2008 i Konfigurasjon av bedriftstelefon

Bruk denne fremgangsmåten til å angi følgende UCR 2008-parametere:

- FIPS-modus
- Nettilgang

Prosedyre

- Trinn 1** I Cisco Unified Communications Manager Administration velger du **System > Konfigurasjon av bedriftstelefon**.
- Trinn 2** Sett parameteren FIPS-modus til **Aktivert**.
- Trinn 3** Sett parameteren Webtilgang til **Deaktivert**.

Trinn 4 Velg **Lagre**.

Konfigurere UCR 2008 i telefon

Bruk denne fremgangsmåten til å angi følgende UCR 2008-parametere:

- FIPS-modus
- SSH-tilgang
- Nettilgang

Prosedyre

- Trinn 1** I Cisco Unified Communications Manager Administration velger du **Enhhet > Telefon**.
- Trinn 2** Sett parameteren SSH-tilgang til **Deaktivert**.
- Trinn 3** Sett parameteren FIPS-modus til **Aktivert**.
- Trinn 4** Sett parameteren nettilgang til **Deaktivert**.
- Trinn 5** Velg **Lagre**.
-

Mobil og ekstern tilgang gjennom Expressway

Mobil og ekstern tilgang gjennom Expressway(MRA) lar eksterne arbeidere koble til bedriftsnettverket enkelt og sikkert uten at det kreves en VPN-klienttunnel. Expressway bruker TLS (Transport Layer Security) til å gjøre nettverkstrafikk sikker. For at en telefon skal kunne godkjenne et Expressway-sertifikat og opprette en TLS-økt må en offentlig Certificate Authority som er klarert av telefonens fastvare, signere Expressway-sertifikatet. Det er ikke mulig å installere eller klarere andre CA-sertifikater på telefoner for godkjenning av et Expressway-sertifikat.

Listen over CA-sertifikater som er bygget inn i telefonens fastvare, er tilgjengelig på <http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-technical-reference-list.html>.

Mobil og ekstern tilgang gjennom Expressway (MRA) fungerer sammen med Cisco Expressway. Du må være kjent med Cisco Expressway-dokumentasjonen, deriblant *Administratorveiledning for Cisco Expressway* og *Veiledning for grunnleggende konfigurasjonsdistribuering for Cisco Expressway*. Cisco Expressway-dokumentasjon er tilgjengelig på

<http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html>.

Bare IPv4-protokollen støttes for brukere av Mobil og ekstern tilgang gjennom Expressway.

Hvis du vil ha mer informasjon om hvordan du arbeider med Mobil og ekstern tilgang gjennom Expressway, kan du se:

- *Cisco Preferred Architecture for Enterprise Collaboration, Design Overview*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD*
- *Unified Communications Mobile and Remote Access via Cisco VCS Deployment Guide*
- *Cisco TelePresence Video Communication Server (VCS), Configuration Guides*
- *Distribusjonshåndbok for Mobile and Remote Access gjennom Cisco Expressway*

I løpet av telefonregistreringsprosessen synkroniserer telefonen datoen og klokkeslettet med NTP-serveren (Network Time Protocol). Sammen med MRA brukes koden for DHCP-alternativ 42 til å finne IP-adressene til NTP-serverne som er angitt for synkronisering av dato og klokkeslett. Men hvis koden for DHCP-alternativ 42 ikke finnes i konfigurasjons-informasjonen, leter telefonen etter koden 0.tandberg.pool.ntp.org for å identifisere NTP-serverne.

Etter registrering bruker telefonen informasjon fra SIP-meldingen til å synkronisere dato og klokkeslett med mindre en NTP-server er konfigurert i telefonkonfigurasjonen for Cisco Unified Communications Manager.



Merk Hvis alternativet TFTP Encrypted Config (TFTP-kryptert konfigurasjon) er avmerket for telefonens sikkerhetsprofil på en av telefonene dine, kan du ikke bruke telefonen med Mobile and Remote Access. MRA-løsningen støtter ikke enheter som samhandler med CAPF (Certificate Authority Proxy Function).

SIP OAuth-modus støttes for MRA. Denne modusen lar deg bruke OAuth-tilgangstoken for godkjenning i sikre miljøer.



Merk For SIP OAuth i Mobile og den eksterne tilgangs modusen (MRA), må du bare bruke aktiveringskode som er startet med mobil og ekstern tilgang når du distribuerer telefonen. Aktivering med brukernavn og passord støttes ikke.

SIP OAuth-modus krever Expressway x 14,0 (1) og nyere, eller Cisco Unified Communications Manager 14,0 (1) og nyere.

Hvis du vil ha mer informasjon om SIP OAuth-modus, kan du se *Funksjonskonfigurasjonsveiledning for Cisco Unified Communications Manager*, versjon 14,0(1)SU8 eller nyere.

Distribusjonsscenarioer

Tabellen nedenfor viser forskjellige distribusjonsscenarioer for Mobil og ekstern tilgang gjennom Expressway.

Scenario	Handlinger
Bruker på kontoret logger på bedriftsnettverket etter å ha distribuert Mobil og ekstern tilgang gjennom Expressway.	Bedriftsnettverket er registrert, og telefonen registreres i Cisco Unified Communications Manager som vanlig.

Scenario	Handlinger
Bruker utenfor kontoret logger på bedriftsnettverket med Mobil og ekstern tilgang gjennom Expressway.	<p>Telefonen registrerer at den er i ekstern modus, påloggingsvinduet for Mobil og ekstern tilgang gjennom Expressway vises, og brukeren kobler til bedriftsnettverket.</p> <p>Brukere må ha et gyldig tjenestenaavn, brukernavn og passord for å koble til nettverket.</p> <p>Brukere må dessuten tilbakestille tjenestemodus for å slette innstillingen for Alternativ TFTP før de kan få tilgang til bedriftsnettverket. Dette sletter innstillingen Alternativ TFTP-server, slik at telefonen oppdager det eksterne nettverket.</p> <p>Hvis en telefon tas i bruk umiddelbart, kan brukere hoppe over kravet om tilbakestilling av nettverksinnstillinger.</p> <p>Hvis brukere har DHCP-alternativ 150 eller alternativ 66 aktivert på nettverksruterer, er det ikke sikkert at de kan logge inn på bedriftsnettverket. Brukere må deaktivere disse DHCP-innstillingene eller konfigurere sin statiske IP-adresse direkte.</p>

Mediebaner og interaktiv etablering av tilkoblinger

Du kan distribuere ICE (Interactive Connectivity Establishment) for å forbedre påliteligheten til MRA-amtaler (Mobile and Remote Access) som krysser en brannmur eller NAT (Network Address Translation). ICE er en valgfri distribusjon som bruker seriell tunnelering og TURN (Traversal Using Relays around NAT) til å velge den beste mediebanen for en samtale.

Sekundære TURN-servere og TURN-server-failover støttes ikke.

Du finner mer informasjon om MRA og ICE i *administrasjonsveiledningen for Cisco Unified Communications Manager, versjon 12.0(1)* eller nyere. Du kan også finne ytterligere informasjon i RFC-dokumenter fra IETF (Internet Engineering Task Force):

- *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)

Konfigurere lagring av brukerlegitimasjon for Expressway-pålogging

Når en bruker logger på nettverket med Mobil og ekstern tilgang gjennom Expressway, blir brukeren bedt om et tjenestedomene, brukernavn og passord. Hvis du aktiverer parameteren Lagring av brukerpåloggingsopplysninger for Expressway-pålogging, kan du lagre brukernes påloggingsopplysninger, slik at de ikke trenger å oppgi denne informasjonen på nytt. Denne parameteren er deaktivert som standard.

Du kan konfigurere lagring av legitimasjon for én telefon, en gruppe telefoner eller alle telefoner.

Beslektede emner

[Konfigurasjon av telefonfunksjoner](#), på side 73

[Produktspesifikk konfigurasjon](#), på side 75

Problemrapporteringsverktøy

Brukere sender problemrapporter til deg ved hjelp av problemrapporteringsverktøyet.



Merk Loggene i problemrapporteringsverktøyet kreves av Cisco TAC når problemer feilsøkes. Loggene slettes hvis du starter telefonen på nytt. Samle inn loggene før telefonene startes på nytt.

Hvis brukerne skal utstede en problemrapport, må de åpne problemrapporteringsverktøyet og oppgi datoen og klokkeslettet da problemet oppstod, og i tillegg en beskrivelse av problemet.

Hvis opplasting av PRT mislykket, kan du få tilgang til PRT-filen for telefonen på URL

http://<phone-ip-address>/FS/<prt-file-name>. Denne URL-en vises på telefonen i følgende situasjoner:

- Hvis telefonen er i fabrikkinnstilt status. URL-en er aktiv i 1 time. Etter 1 time må brukeren prøve å sende telefonloggene på nytt.
- Hvis telefonen har lastet ned en konfigurasjonsfil og samtalestyringssystemet tillater webtilgang til telefonen.

Du må legge til en serveradresse i feltet **URL for opplasting av kundestøtte** i Cisco Unified Communications Manager.

Hvis du tar i bruk enheter med Mobile and Remote Access via Expressway, må du også legge til adressen til PRT-serveren i listen over tillatte HTTP-servere på Expressway-serveren.

Konfigurere en URL for opplasting av kundestøtte

Du må bruke en server med et opplastingsskript for å motta PRT-filer. PRT bruker en HTTP POST-mekanisme med følgende parametere inkludert i opplastingen (bruker MIME-koding i flere deler):

- enhetsnavn (eksempel: "SEP001122334455")
- serienummer (eksempel: "FCH12345ABC")
- brukernavn (brukernavnet som er konfigurert i Cisco Unified Communications Manager, enhetseieren)
- PRT-fil (eksempel: "probrep-20141021-162840.tar.gz")

Det vises et eksempelskript nedenfor. Dette skriptet er bare ment som referanse. Cisco formidler ikke støtte for opplastingsskriptet som er installert på serveren til en kunde.

```
<?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.");
}

?>

```



Merk Telefonene støtter bare HTTP-URL-er.

Prosedyre

- Trinn 1** Konfigurer en server som kan kjøre PRT-opplastingsskriptet.
- Trinn 2** Skriv et skript som kan håndtere parameterne ovenfor, eller rediger eksempelskriptet etter behov.
- Trinn 3** Last opp skriptet til serveren.
- Trinn 4** I Cisco Unified Communications Manager går du til området Produktspesifikt konfigurasjonsoppsett i vinduet for konfigurasjon av den enkeltstående enheten, vinduet Vanlig telefonprofil eller vinduet Konfigurasjon av bedriftstelefon.
- Trinn 5** Merk av for **URL for opplasting av kundestøtte** og angi URL-en for opplastingsserveren.

Eksempel:

<http://example.com/prtscript.php>

- Trinn 6** Lagre endringene.

Angi etiketten for en linje

Du kan konfigurere en telefon til å vise en tekstetikett i stedet for katalognummeret. Bruk denne etiketten til å identifisere linjen etter navn eller funksjon. Hvis brukeren for eksempel deler linjer på telefonen, kan du identifisere linjen med navnet på personen som deler linjen.

Når du legger til en etikett i en utvidelsesmodul, vises bare de første 25 tegnene på en linje.

Prosedyre

- Trinn 1** I Cisco Unified Communications Manager Administration velger du **Enhet > Telefon**.
- Trinn 2** Finn telefonen som skal konfigureres.
- Trinn 3** Finn linjeforekomsten og angi en verdi for feltet Line Text Label (Linjetekstetikett).
- Trinn 4** (Valgfritt) Hvis etiketten må brukes for andre enheter som deler linjen, merker du av i avmerkingsboksen Oppdater innstillinger for delt enhet og klikker på **Overfør valgt**.
- Trinn 5** Velg **Lagre**.
-



KAPITTEL 10

Konfigurere bedriftskatalogen og den personlige katalogen

- [Konfigurere bedriftskatalogen, på side 103](#)
- [Konfigurere den personlige katalogen, på side 103](#)

Konfigurere bedriftskatalogen

Ved hjelp av bedriftskatalogen kan en bruker slå opp telefonnumre for kollegaer. Du må konfigurere bedriftskataloger for at denne funksjonen skal fungere.

Cisco Unified Communications Manager bruker en Lightweight Directory Access Protocol (LDAP)-katalog for å lagre autentiserings- og autorisasjonsinformasjon om brukere av Cisco Unified Communications Manager applikasjoner som samhandler med Cisco Unified Communications Manager. Godkjenning fastsetter brukerrettigheter for tilgang til systemet. Autorisasjon identifiserer telefonressursene som en bruker har tillatelse til å bruke, for eksempel et spesifikt internummer.

Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din spesifikke Cisco Unified Communications Manager versjon.

Etter at brukere har fullført konfigureringen av LDAP-katalogen, kan de bruke tjenesten Bedriftskatalog på telefonen til å slå opp brukere i bedriftskatalogen.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Konfigurere den personlige katalogen

Ved hjelp av den personlige katalogen kan en bruker lagre et sett med personlige numre.

Personlig katalog består av følgende funksjoner:

- Adresseliste
- Kortnumre

Brukere kan benytte disse metodene til å få tilgang til funksjoner i Personlig katalog:

- Fra en nettleser – brukere har tilgang til funksjonene personlig adressebok og kortnumre fra selvhjelpsportalen i Cisco Unified Communications.
- Fra Cisco IP-telefon: Velg **Kontakter** for å søke i bedriftskatalogen eller i brukerens personlige adressebok.

For å konfigurere Personlig katalog fra en webleser, må brukere ha tilgang til selvhjelpsportalen. Du må formidle en URL og påloggingsinformasjon til brukere.



DEL **IV**

Feilsøking av telefoner

- [Overvåking av telefonsystemer, på side 107](#)
- [Vedlikehold, på side 133](#)
- [Feilsøking, på side 137](#)
- [Internasjonal brukerstøtte, på side 155](#)



KAPITTEL 11

Overvåking av telefonsystemer

- [Oversikt over overvåking av telefonsystemer, på side 107](#)
- [Status for Cisco IP-telefoner, på side 107](#)
- [Nettside for Cisco IP-telefoner, på side 118](#)
- [Be om informasjon fra telefonen i XML, på side 129](#)

Oversikt over overvåking av telefonsystemer

Du kan vise omfattende informasjon om telefonen ved hjelp av telefonens statusmeny og websidene på telefonen. Denne informasjonen inkluderer:

- Enhetsinformasjon
- Informasjon om nettverksoppsett
- Nettverksstatistikk
- Enhetslogger
- Strømmestatistikk

Dette kapitlet beskriver informasjonen du kan hente fra telefonens webside. Du kan bruke denne informasjonen til å overvåke bruken av telefonen eksternt samt hjelpe med feilsøking.

Beslektede emner

[Feilsøking](#), på side 137

Status for Cisco IP-telefoner

Delene nedenfor beskriver hvordan du viser modellinformasjon, statusmeldinger og nettverksstatistikk på Cisco IP-telefon i 7800-serien.

- Modellinformasjon: Viser maskinvare- og programvareinformasjon om telefonen.
- Statusmeny: Gir tilgang til skjermer som viser statusmeldingene, nettverksstatistikken og statistikken for den gjeldende samtalen.

Du kan bruke informasjonen som vises på disse skjermene, til å overvåke bruken av telefonen eksternt samt hjelpe med feilsøking.

Du kan også hente mye av denne informasjonen, og hente annen relatert informasjon, eksternt via telefonens webside.


Vise vinduet Telefoninformasjon

Prosedyre

-
- Trinn 1** Trykk på **Innstillinger > Telefoninformasjon**.
- Trinn 2** Hvis du vil avslutte menyen, trykker du på **Avslutt**.
-


Vise Status-menyen

Prosedyre

-
- Trinn 1** Trykk på **Innstillinger > Status**.
- Trinn 2** Hvis du vil avslutte menyen, trykker du på **Tilbake** .
-

Vise vinduet Statusmeldinger

Prosedyre

-
- Trinn 1** Trykk på **Innstillinger > Status > Statusmeldinger**.
- Trinn 2** Hvis du vil avslutte menyen, trykker du på **Tilbake** .
-

Felt i Statusmeldinger

Tabellen nedenfor beskriver statusmeldingene som vises på skjermen Statusmeldinger på telefonen.

Tabell 24: Statusmeldinger på Cisco IP-telefon

Melding	Beskrivelse	Mulig forklaring og handling
Kunne ikke skaffe en IP-adresse fra DHCP	Telefonen har ikke tidligere hentet en IP-adresse fra en DHCP-server. Dette kan bare forekomme når du utfører en umiddelbar tilbakestilling eller tilbakestilling til fabrikkstandardene.	Bekreft at DHCP-serveren er tilgjengelig for telefonen.
TFTP-størrelsesfeil	Konfigurasjonsfilen er for stor for filsystemet på telefonen.	Slå telefonen av og på.

Melding	Beskrivelse	Mulig forklaring og handling
ROM-kontrollsumfeil	Den nedlastede programvarefilen er skadet.	Hent en ny versjon av telefonens faste TFTPPath-katalogen. Du må bare koble til katalogen når TFTP-serverens programvare er installert, ellers blir det hente filene blir skadet.
Lik IP	En annen enhet bruker IP-adressen som er tilordnet til telefonen.	Hvis telefonen har en statisk IP-adresse, må den ikke tilordnet en identisk IP-adresse. Hvis du bruker DHCP, kontrollerer du DHCP-serveren.
Sletter CTL- og ITL-filer	Sletter CTL- eller ITL-filen.	Ingen. Denne meldingen er bare informasjon.
Feil under språkoppdatering	Én eller flere lokaliseringsfiler ble ikke funnet i TFTP-katalogen eller var ugyldige. Brukerspråket ble ikke endret.	Fra Cisco Unified Operating System er det mulig at følgende filer finnes i underkatalogen i TFTP-filbehandlingen: <ul style="list-style-type: none"> I underkatalog med samme navn som språket <ul style="list-style-type: none"> tones.xml I underkatalog med samme navn som språket <ul style="list-style-type: none"> glyphs.xml dictionary.xml kate.xml
Filen ble ikke funnet <Cfg File>	Den navnebaserte filen og standard konfigurasjonsfilen ble ikke funnet på TFTP-serveren.	Konfigurasjonsfilen for en telefon opprettes automatisk til i Cisco Unified Communications Manager. Hvis telefonen ikke finnes i Cisco Unified Communications Manager-databasen, genererer TFTP-serveren ikke konfigurasjonsfil . <ul style="list-style-type: none"> Telefonen er ikke registret med Cisco Unified Communications Manager. Du må legge til telefonen i Cisco Unified Communications Manager manuelt hvis du ikke bruker TFTP-serveren automatisk. Hvis du bruker DHCP, kontrollerer du DHCP-serveren og henviser til riktig TFTP-server. Hvis du bruker statiske IP-adresser, kontrollerer du konfigurasjonen for TFTP-serveren.
Filen ble ikke funnet <CTLFile.tlv>	Denne meldingen vises på telefonen når Cisco Unified Communications Manager-gruppen ikke er i sikker modus.	Har ingen innvirkning. Telefonen kan ikke registreres i Cisco Unified Communications Manager.

Melding	Beskrivelse	Mulig forklaring og handling
IP-adresse frigitt	Telefonen er konfigurert til å frigi IP-adressen.	Telefonen forblir inaktiv til den slås av og tilbakestill DHCP-adressen.
Tidsavbrudd for IPv4 DHCP	IPv4 DHCP-serveren svarte ikke.	<p>Nettverket er opptatt: Feilene bør løses og nettverksbelastningen reduseres.</p> <p>Ingen nettverkstilkobling mellom IPv4 og telefonen: Kontroller nettverkstilkoblingen.</p> <p>IPv4 DHCP-serveren er nede: Kontroller statusen til IPv4 DHCP-serveren.</p> <p>Feilene vedvarer: Vurder å tilordne en annen IP-adresse.</p>
Tidsavbrudd for IPv6 DHCP	IPv6 DHCP-serveren svarte ikke.	<p>Nettverket er opptatt: Feilene bør løses og nettverksbelastningen reduseres.</p> <p>Ingen nettverkstilkobling mellom IPv6 og telefonen: Kontroller nettverkstilkoblingen.</p> <p>IPv6 DHCP-serveren er nede: Kontroller statusen til IPv6 DHCP-serveren.</p> <p>Feilene vedvarer: Vurder å tilordne en annen IP-adresse.</p>
Tidsavbrudd for IPv4 DNS	IPv4 DNS-serveren svarte ikke.	<p>Nettverket er opptatt: Feilene bør løses og nettverksbelastningen reduseres.</p> <p>Ingen nettverkstilkobling mellom IPv4 og telefonen: Kontroller nettverkstilkoblingen.</p> <p>IPv4 DNS-serveren er nede: Kontroller statusen til DNS-serveren.</p>
Tidsavbrudd for IPv6 DNS	IPv6 DNS-serveren svarte ikke.	<p>Nettverket er opptatt: Feilene bør løses og nettverksbelastningen reduseres.</p> <p>Ingen nettverkstilkobling mellom IPv6 og telefonen: Kontroller nettverkstilkoblingen.</p> <p>IPv6 DNS-serveren er nede: Kontroller statusen til DNS-serveren.</p>
Ukjent IPv4 DNS-vert	IPv4 DNS kan ikke løse navnet for TFTP-serveren eller Cisco Unified Communications Manager.	<p>Kontroller at vertsnavnene for TFTP-serveren og Cisco Unified Communications Manager er konfigurert riktig.</p> <p>Vurder å bruke IPv4-adresser i stedet for IPv6-adresser.</p>
Ukjent IPv6 DNS-vert	IPv6 DNS kan ikke løse navnet for TFTP-serveren eller Cisco Unified Communications Manager.	<p>Kontroller at vertsnavnene for TFTP-serveren og Cisco Unified Communications Manager er konfigurert riktig.</p> <p>Vurder å bruke IPv6-adresser i stedet for IPv4-adresser.</p>

Melding	Beskrivelse	Mulig forklaring og handling
Innlasting avviste maskinvarekomp	Programmet som ble lastet ned, er ikke kompatibelt med telefonens maskinvare.	Dette skjer hvis du forsøker å installere programvaren på denne telefonen som krever maskinvareendringer på denne telefonen. Kontroller innlastings-ID-en som er angitt i Cisco Unified Communications Manager (Cisco Unified Communications Manager Telefon). Angi innlastingen som vist i dokumentasjonen.
Ingen standardruter	DHCP eller den statiske konfigurasjonen angav ingen standardruter.	Hvis telefonen har en statisk IP-adresse, er standardruterene konfigurert. Hvis du bruker DHCP, har ikke DHCP standardruter. Kontroller konfigurasjonen.
Ingen IPv4 DNS-server	Et navn ble angitt, men DHCP eller konfigurasjonen av statisk IP-adresse angav ingen adresse til IPv4 DNS-serveren.	Hvis telefonen har en statisk IP-adresse, er DNS-serveren konfigurert. Hvis du bruker DHCP, har ikke DHCP IPv4 DNS-server. Kontroller konfigurasjonen.
Ingen IPv6 DNS-server	Et navn ble angitt, men DHCP eller konfigurasjonen av statisk IP-adresse angav ingen adresse til IPv6 DNS-serveren.	Hvis telefonen har en statisk IP-adresse, er DNS-serveren konfigurert. Hvis du bruker DHCP, har ikke DHCP IPv6 DNS-server. Kontroller konfigurasjonen.
Ingen klareringsliste er installert	CTL-filen eller ITL-filen er ikke installert på telefonen.	Klareringslisten er ikke konfigurert i Cisco Unified Communications Manager, som ikke er standard. Klareringslisten er ikke konfigurert i Cisco Unified Communications Manager. Hvis du vil ha mer informasjon om klareringslisten, se dokumentasjonen for din versjon av Cisco Unified Communications Manager.
Telefonen ble ikke registrert. Sertifikatnøkkelstørrelsen er ikke kompatibel med FIPS.	FIPS krever at sertifikatet for RSA-serveren er 2048 biter eller større.	Oppdater sertifikatet.
Omstart forespurt av Cisco Unified Communications Manager	Telefonen starter på nytt på grunn av en forespørsel fra Cisco Unified Communications Manager.	Konfigurasjonsendringer ble mest sannsynlig gjort i Cisco Unified Communications Manager. Trykk på konfigurasjon ble trykket slik at endringene blir aktivert.
Feil ved TFTP-tilgang	TFTP-serveren henviser til en katalog som ikke finnes.	Hvis du bruker DHCP, kontrollerer DHCP serveren henviser til riktig TFTP-server. Hvis du bruker statiske IP-adresser, kontrollerer DHCP serveren henviser til riktig TFTP-server.
TFTP-feil	Telefonen gjenkjenner ikke en feilkode som TFTP-serveren formidlet.	Kontakt Cisco TAC.


Melding	Beskrivelse	Mulig forklaring og handling
TFTP-tidsavbrudd	TFTP-serveren svarte ikke.	<p>Nettverket er opptatt: Feilene bør løses og nettverksbelastningen reduseres.</p> <p>Ingen nettverkstilkobling mellom TFTP-serveren og telefonen. Kontroller nettverkstilkoblingene.</p> <p>TFTP-serveren er nede: Kontroller konfigurasjonsfilen på TFTP-serveren.</p>
Tidsavbrutt	Anmoderen forsøkte en 802.1X-transaksjon, men ble tidsavbrutt på grunn av en manglende godkjenning.	Godkjenning blir vanligvis tidsavbrutt hvis den ikke er konfigurert på svitsjen.
Oppdatering av klareringsliste mislyktes	Oppdateringen av CTL- og ITL-filer mislyktes.	<p>Telefonen har CTL- og ITL-filer installert, men oppdatere de nye CTL- og ITL-filene.</p> <p>Mulige årsaker til feilen:</p> <ul style="list-style-type: none"> • Det oppstod en nettverksfeil. • TFTP-serveren var nede. • Den nye sikkerhetstokenen som ble angitt i CTL-filen, og TFTP-sertifikatet som ble angitt i ITL-filen, er angitt, men er ikke tilgjengelige i CTL- og ITL-filene på telefonen. • Det oppstod en intern telefonfeil. <p>Mulige løsninger:</p> <ul style="list-style-type: none"> • Kontroller nettverkstilkoblingen. • Kontroller om TFTP-serveren er aktiv og fungerer. • Hvis TVS-serveren (Transactional Voice Service) i Cisco Unified Communications Manager er deaktivert, kontroller om TVS-serveren er aktiv og fungerer. • Kontroller om sikkerhetstokenen er gyldig. <p>Slett CTL- og ITL-filer manuelt hvis oppdateringen mislykkes. Tilbakestill telefonen.</p> <p>Hvis du vil ha mer informasjon om klareringsliste, se dokumentasjonen for din versjon av Cisco Unified Communications Manager.</p>
Klareringsliste oppdatert	CTL-filen, ITL-filen eller begge filene ble oppdatert.	<p>Ingen. Denne meldingen er bare ment som informasjon.</p> <p>Hvis du vil ha mer informasjon om klareringsliste, se dokumentasjonen for din versjon av Cisco Unified Communications Manager.</p>
Versjonsfeil	Navnet på telefonens innlastingsfil er ugyldig.	Kontroller at telefonens innlastingsfil har et gyldig navn.
XmlDefault.cnf.xml eller .cnf.xml samsvarer med navnet på telefonenheten	Navnet på konfigurasjonsfilen.	Ingen. Denne meldingen angir navnet på konfigurasjonsfilen.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Vise vinduet Nettverksstatistikk**Prosedyre**

Trinn 1 Trykk på **Innstillinger** > **Status** > **Nettverksstatistikk**.

Trinn 2 Hvis du vil avslutte menyen, trykker du på **Tilbake** .

Felt i Nettverksstatistikk

Tabellen nedenfor beskriver informasjonen på skjermen Nettverksstatistikk.

Tabell 25: Felt i Nettverksstatistikk


Element	Beskrivelse
Tx-rammer	Antall pakker som telefonen har sendt
Tx broadcast	Antall kringkastingspakker som telefonen har sendt
Tx unicast	Totalt antall unikastpakker som telefonen har sendt.
Rx-rammer	Antall pakker som telefonen har mottatt
Rx broadcast	Antall kringkastingspakker som telefonen har mottatt
Rx unicast	Totalt antall unikastpakker som telefonen har mottatt
Enhets-ID for CDP-nabo	Identifikator for en enhet som er koblet til denne porten, som ble oppdaget av CDP-protokollen.
IP-adresse for CDP-nabo	Identifikator for en enhet som er koblet til denne porten, som ble oppdaget av CDP-protokollen ved hjelp av IP.
CDP-naboport	Identifikator for en enhet som er koblet til denne porten, som ble oppdaget av CDP-protokollen.

Element	Beskrivelse
<p>Årsak til omstart: Én av disse verdiene:</p> <ul style="list-style-type: none"> • Tilbakestilling av maskinvare (strømpåslåing blir tilbakestilt) • Tilbakestilling av programvare (minnekontroller blir også tilbakestilt) • Tilbakestilling av programvare (minnekontroller blir ikke tilbakestilt) • Overvåking tilbakestilt • Initialisert • Ukjent 	<p>Årsaken til den siste tilbakestillingen for telefonen</p>
<p>Port 1</p>	<p>Koblingsstatus og tilkobling for nettverksporten (eksempelvis betyr 100 full at PC-porten er i oppkoblingsstatus og har forhandlet en tilkobling på 100 Mbps med full dupleks automatisk)</p>
<p>IPv4</p>	<p>Informasjon om DHCP-statusen. Dette inkluderer følgende stater:</p> <ul style="list-style-type: none"> • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • DISABLED DUPLICATE IP • SET DHCP COLDBOOT • SET DHCP DISABLED • SET DHCP FAST

Element	Beskrivelse
IPv6	<p data-bbox="828 289 1520 321">Informasjon om DHCP-statusen. Dette inkluderer følgende stater:</p> <ul style="list-style-type: none"> <li data-bbox="865 338 992 365">• CDP INIT <li data-bbox="865 390 1065 417">• DHCP6 BOUND <li data-bbox="865 443 1102 470">• DHCP6 DISABLED <li data-bbox="865 495 1065 522">• DHCP6 RENEW <li data-bbox="865 548 1070 575">• DHCP6 REBIND <li data-bbox="865 600 1024 627">• DHCP6 INIT <li data-bbox="865 653 1073 680">• DHCP6 SOLICIT <li data-bbox="865 705 1089 732">• DHCP6 REQUEST <li data-bbox="865 758 1118 785">• DHCP6 RELEASING <li data-bbox="865 810 1105 837">• DHCP6 RELEASED <li data-bbox="865 863 1114 890">• DHCP6 DISABLING <li data-bbox="865 915 1117 942">• DHCP6 DECLINING <li data-bbox="865 968 1105 995">• DHCP6 DECLINED <li data-bbox="865 1020 1089 1047">• DHCP6 INFOREQ <li data-bbox="865 1073 1167 1100">• DHCP6 INFOREQ DONE <li data-bbox="865 1125 1078 1152">• DHCP6 INVALID <li data-bbox="865 1178 1227 1205">• DISABLED DUPLICATE IPV6 <li data-bbox="865 1230 1284 1257">• DHCP6 DECLINED DUPLICATE IP <li data-bbox="865 1283 1138 1310">• ROUTER ADVERTISE <li data-bbox="865 1335 1362 1362">• DHCP6 WAITING COLDBOOT TIMEOUT <li data-bbox="865 1388 1365 1415">• DHCP6 TIMEOUT USING RESTORED VAL <li data-bbox="865 1440 1333 1467">• DHCP6 TIMEOUT CANNOT RESTORE <li data-bbox="865 1493 1198 1520">• IPV6 STACK TURNED OFF <li data-bbox="865 1545 1138 1572">• ROUTER ADVERTISE <li data-bbox="865 1598 1138 1625">• ROUTER ADVERTISE <li data-bbox="865 1650 1273 1677">• UNRECOGNIZED MANAGED BY <li data-bbox="865 1703 1138 1730">• ILLEGAL IPV6 STATE

Vise vinduet Anropsstatistikk

Prosedyre

- Trinn 1** Trykk på **Innstillinger > Status > Anropsstatistikk**.
- Trinn 2** Hvis du vil avslutte menyen, trykker du på **Tilbake** .

Felt i Anropsstatistikk

Tabellen nedenfor beskriver elementene på skjermen Anropsstatistikk.

Tabell 26: Anropsstatistikkelementer

Element	Beskrivelse
Mottakerkodek	Type mottatt talestrøm (RTP-strømmelyd fra kodek): <ul style="list-style-type: none"> • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS • iSAC
Avsenderkodek	Type sendt talestrøm (RTP-strømmelyd fra kodek): <ul style="list-style-type: none"> • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS • iSAC
Mottakerstørrelse	Størrelse på talepakker, i millisekunder, i mottakstalestrømmen (bare RTP-strømming).

Element	Beskrivelse
Avsenderstørrelse	Størrelse på talepakker, i millisekunder, i sendetalestrømmen.
Mottatte pakker	Antallet RTP-talepakker som ble mottatt siden talestrømmen startet. Merk Dette antallet er ikke nødvendigvis identisk med antallet RTP-talepakker som ble mottatt siden anropet startet, fordi anropet kanskje var blitt satt på vent.
Avsenderpakker	Antallet RTP-talepakker som ble sendt siden talestrømmen startet. Merk Dette antallet er ikke nødvendigvis identisk med antallet RTP-talepakker som ble sendt siden anropet startet, fordi anropet kanskje var blitt satt på vent.
Gjsn. jitter	Anslått gjennomsnittlig RTP-pakkejitter (dynamisk forsinkelse som oppstår for en pakke når den sendes gjennom nettverket), i millisekunder, som ble registrert siden mottakstalestrømmen startet.
Maks. jitter	Maksimal jitter, i millisekunder, som ble registrert siden mottakstalestrømmen startet.
Mottaker forkastet	Antallet RTP-talepakker i mottakstalestrømmen som ble forkastet (ugyldige pakker, for sene pakker og så videre). Merk Telefonen forkaster støypakker for nyttelestype 19 som Cisco-gatewayer genererer, fordi de øker denne telleren trinnvis.
Tapte pakker	Manglende RTP-pakker (mistet under sending).
Metrikkverdier for talekvalitet	
Akkumulert skjult omfang	Totalt antall skjulte rammer delt på totalt antall talerammer som ble mottatt fra starten på talestrømmen.
Skjult omfang for intervall	Antall skjulte rammer til talerammer i det foregående intervallet med aktiv tale på 3 sekunder. Hvis du bruker talegjenkjenning (VAD), kreves det kanskje et lengre intervall for å akkumulere tre sekunder med aktiv tale.
Maks. skjult omfang	Høyeste skjulte omfang for intervall fra starten av talestrømmen.
Skjulte sekunder	Antallet sekunder som har skjulte hendelser (tapte rammer) fra starten av talestrømmen (inkluderer svært skjulte sekunder).
Sekunder med mange skjulte elementer	Antallet sekunder som har mer enn 5 prosent skjulte hendelser (tapte rammer) fra starten av talestrømmen.
Ventetid	Anslag om nettverksventetid uttrykt i millisekunder. Representerer et aktivt gjennomsnitt av løkkeforsinkelsen, som måles når sperringer for RTCP-mottakerrapporten mottas.

Nettside for Cisco IP-telefoner

Hver Cisco IP-telefon har en webside, der du finner omfattende informasjon om telefonen, inkludert:

- Enhetsinformasjon: Viser enhetsinnstillinger og aktuell informasjon for telefonen.
- Nettverksoppsett: Viser informasjon om nettverksoppsettet og om andre telefoninnstillinger.
- Nettverksstatistikk: Viser hyperkoblinger som formidler informasjon om nettverkstrafikk.
- Enhetslogger: Viser hyperkoblinger som formidler informasjon du kan bruke til feilsøking.
- Strømmestatistikk: Viser hyperkoblinger til omfattende strømmestatistikk.

Denne delen beskriver informasjonen du kan hente fra telefonens webside. Du kan bruke denne informasjonen til å overvåke bruken av telefonen eksternt samt hjelpe med feilsøking.

Du kan også hente mye av denne informasjonen direkte fra en telefon.

Få tilgang til telefonens nettside



Merk Hvis du ikke har tilgang til websiden, kan den være deaktivert som standard.

Prosedyre

Trinn 1

Hent IP-adressen for Cisco IP-telefon ved hjelp av en av disse metodene:

- a) Søk etter telefonen i Cisco Unified Communications Manager Administration ved å velge **Enhets > Telefon**. Telefoner som er registrert i Cisco Unified Communications Manager, viser IP-adressen i vinduet Søk etter og vis liste over telefoner samt øverst i vinduet Telefonkonfigurasjon.
- b) På telefonen trykker du på **Innstillinger > Administratorinnstillinger > Nettverksoppsett > IPv4-oppsett**, og deretter blir du til feltet IP-adresse.

Trinn 2

Åpne en nettleser og angi følgende URL, der *IP_address* er IP-adressen til Cisco IP-telefon:

http://<IP_address>

Nettsiden for enhetsinformasjon

Området Enhetsinformasjon på websiden på en telefon viser enhetsinnstillinger og aktuell informasjon for telefonen. Tabellen nedenfor beskriver disse elementene.

Hvis du vil vise området Enhetsinformasjon, går du til websiden for telefonen og klikker hyperkoblingen **Enhetsinformasjon**.

Tabell 27: Nettsidefelter med enhetsinformasjon

Felt	Beskrivelse
Tjenestemodus	Telefonens tjenestemodus.
Tjenestedomene	Telefonens tjenestedomene.
Tjenestestatus	Tjenestens gjeldende status.
MAC-adresse	Telefonens MAC-adresse (Media Access Control).
Vertsnavn	Unikt, fast navn som tilordnes til telefonen automatisk basert på MAC-adressen.
Telefonens katalognummer	Katalognummeret som er tilordnet til telefonen.
ID for programinnlasting	Identifiserer programinnlastingsversjonen.
ID for oppstartsinnlasting	Angir oppstartsinnlastingsversjonen.
Versjon	ID for fastvaren som kjører på telefonen.
Maskinvarerevisjon	Verdi for mindre endring i telefonens maskinvare.
Serienummer	Telefonens unike serienummer.
Modellnummer	Telefonens unike modellnummer.
Melding venter	Angir om en talemelding venter på hovedlinjen for denne telefonen.
UDI	Viser følgende UDI-informasjon (Unique Device Identifier) om Cisco-telefonen: <ul style="list-style-type: none"> • Maskinvaretypen • Navn på telefonmodell • Produktidentifikator • Versjons-ID (VID) – angir det overordnede versjonsnummeret for maskinvare. • Serienummer
Tidspunkt	Tidspunkt for dato-/klokkeslettgruppen som telefonen tilhører. Denne informasjonen kommer fra Cisco Unified Communications Manager.
Tidssone	Tidssone for dato-/klokkeslettgruppen som telefonen tilhører. Denne informasjonen kommer fra Cisco Unified Communications Manager.
Dato	Dato for dato-/klokkeslettgruppen som telefonen tilhører. Denne informasjonen kommer fra Cisco Unified Communications Manager.
Ledig systemminne	Mengden tilgjengelig systemminne.
Ledig Java Heap-minne	Mengden ledig minne for Java Heap.

Felt	Beskrivelse
Ledig Java Pool-minne	Mengden ledig minne for Java Pool.
FIPS-modus aktivert	Angir om FIPS-modus (Federal Information Processing Standard) er aktivert.

Nettsiden for nettverksoppsett

Området Nettverksoppsett på en telefonwebseite viser informasjon om nettverksoppsettet og om andre telefoninnstillinger. Tabellen nedenfor beskriver disse elementene.

Du kan vise og angi mange av disse elementene fra menyen Nettverksoppsett på Cisco IP-telefon.

Hvis du vil vise området Nettverksoppsett, går du til websiden for telefonen og klikker hyperkoblingen **Nettverksoppsett**.

Tabell 28: Elementer i området Nettverksoppsett

Element	Beskrivelse
MAC-adresse	Telefonens MAC-adresse (Media Access Control).
Vertsnavn	Vertsnavn som DHCP-serveren tilordnet til telefonen.
Domenenavn	Navnet på DNS-domenet (Domain Name System) som telefonen befinner seg i
DHCP-server	IP-adresse for DHCP-serveren (Dynamic Host Configuration Protocol) som telefonen henter IP-adresse fra.
BOOTP-server	Angir om telefonen henter konfigurasjonen fra en BootP-server (Bootstrap Protocol).
DHCP	Angir om telefonen bruker DHCP.
IP-adresse	IP-adressen (Internet Protocol) til telefonen.
Nettverksmaske	Nettverksmasken som telefonen bruker.
Standardruter 1	Standardruter som telefonen bruker.
DNS-server 1-3	Primær DNS-server (Domain Name System) (DNS-server 1) og valgfrie DNS-reserveservere (DNS-server 2 og 3) som telefonen bruker.
Alternativ TFTP	Angir om telefonen bruker en alternativ TFTP-server.
TFTP-server 1	Primær TFTP-server (Trivial File Transfer Protocol) som telefonen bruker.
TFTP-server 2	TFTP-reserveserver (Trivial File Transfer Protocol) som telefonen bruker.
DHCP-adresse frigitt	Angir innstillingen for alternativet DHCP-adresse frigitt.
Operativ VLAN-ID	Operativ VLAN (Virtual Local Area Network) som er konfigurert på en Cisco Catalyst-svitsj; telefonen er medlem av.
VLAN-ID for admin	Ekstra VLAN som telefonen er medlem av.

Element	Beskrivelse
Unified CM 1-5	<p>Vertsnavn eller IP-adresser, i prioritert rekkefølge, for Cisco Unified Communications Manager som telefonen kan registreres med. Et element kan også vise IP-adressen for en SRST-ruter som formidler begrenset Cisco Unified Communications Manager-funksjonalitet, hvis en slik ruter er tilgjengelig.</p> <p>For en tilgjengelig server viser elementet IP-adressen for Cisco Unified Communications Manager-serveren og én av følgende statuser:</p> <ul style="list-style-type: none"> • Aktiv: Cisco Unified Communications Manager-serveren som telefonen for øyeblikkelig formidler samtalebehandlingstjenester fra • Ventemodus: Cisco Unified Communications Manager-serveren som telefonen bytter til, mens gjeldende serveren blir utilgjengelig • Tom: Ingen gjeldende tilkobling til denne Cisco Unified Communications Manager-serveren <p>Et element kan også inkludere SRST-betegnelsen (Survivable Remote Site Telephony), som refererer til en SRST-ruter som kan formidle Cisco Unified Communications Manager-funksjonalitet med begrensede funksjoner. Denne ruteren tar kontroll over samtalebehandlingen hvis alle Unified Communications Manager-servere blir utilgjengelige. SRST-serveren for Cisco Unified Communications Manager vises alltid til slutt i listen over servere, selv om den er aktiv. I tillegg kan du konfigurere SRST-ruteradressen i delen Enhetsutvalg i vinduet Konfigurasjon av Cisco Unified Communications Manager.</p>
Informasjons-URL	URL-en til hjelpeteksten som vises på telefonen.
Katalog-URL	URL-en til serveren som telefonen henter kataloginformasjon fra.
Meldings-URL	URL-en til serveren som telefonen henter meldingstjenester fra.
Tjeneste-URL	URL-en til serveren som telefonen henter Cisco IP-telefon-tjenester fra.
Inaktiv URL	URL-en som telefonen viser når den har vært inaktiv så lenge som verdien i feltet Tid inaktiv URL angir og ingen meny er åpen.
Tid inaktiv URL	Antallet sekunder som telefonen er inaktiv ingen meny er åpen før XML-tjenesten som telefonen angir, blir aktivert.
URL for proxy-server	URL for proxy-server som sender HTTP-forespørsler til ikke-lokale vertsadresser på vegne av telefonens HTTP-klient, og formidler svar fra den ikke-lokale verten til telefonens HTTP-klient.
URL for godkjenning	URL som telefonen bruker til å validere forespørsler som sendes til telefonens webserver.

Element	Beskrivelse
Svitsjeportoppsett	Hastighet og dupleks for svitsjeporten, der: <ul style="list-style-type: none"> • A = Automatisk forhandling • 10H = 10-BaseT/halv dupleks • 10F = 10-BaseT/full dupleks • 100H = 100-BaseT/halv dupleks • 100F = 100-BaseT/full dupleks • 1000F = 1000-BaseT/full dupleks • Ingen kobling = Ingen tilkobling til svitsjeporten
Brukerspråk	Brukerspråk som forbindes med telefonbrukeren. Identifiserer et sett med detaljert informasjon til støtte brukere, inkludert språk, skrift, dato- og klokkeslettformatering og informasjon om alfabetisk tastatur.
Nettverksspråk	Nettverksspråk som forbindes med telefonbrukeren. Identifiserer et sett med detaljert informasjon til støtte telefonen på en bestemt plassering, inkludert definisjoner av tonene og rytmene som telefonen bruker.
Versjon for brukerspråk	Versjonen for brukerspråket som er lastet på telefonen.
Versjon for nettverksspråk	Versjonen for nettverksspråket som er lastet på telefonen.
Høytaleren er aktivert	Angir om høytaleren er aktivert på telefonen.
Gruppelytting	Angir om funksjonen Gruppelytting er aktivert på telefonen. Ved hjelp av Gruppelytting kan du lytte til samtaler ved hjelp av telefonrøret og samtidig lytte til høytaleren.
GARP aktivert	Angir om telefonen memorerer MAC-adressene fra GARP-svar (Gratuitous ARP).
Autovalg av linje er aktivert	Angir om telefonen bytter samtalefokus til innkommende anrop på alle linjer.
DSCP for samtalestyring	DSCP IP-klassifisering for samtalestyringssignalisering.
DSCP for konfigurasjon	DSCP IP-klassifisering for telefonkonfigurasjonsoverføring.
DSCP for tjenester	DSCP IP-klassifisering for telefonbaserte tjenester.
Sikkerhetsmodus	Sikkerhetsmodus som er angitt for telefonen.
nettilgang er aktivert	Angir om nettilgang er aktivert (Ja) eller deaktivert (Nei) for telefonen.
SSH-tilgang aktivert	Angir om telefonen godtar eller blokkerer SSH-tilkoblingene.

Element	Beskrivelse
CDP: Svitsjeport	Angir om CDP-støtte finnes på svitsjeporten (standard er aktivert). Aktiver CDP på svitsjeporten for VLAN-tilordning for telefonen, strømforhandling, QoS-ad og 802.1x-sikkerhet Aktiver CDP på svitsjeporten når telefonen kobler til en Cisco-svitsj. Når CDP er deaktivert i Cisco Unified Communications Manager, vises det en advarsel om deaktiveres på svitsjeporten bare hvis telefonen kobles til en annen svitsj enn en Cisco-sv CDP-verdiene for den gjeldende PC- og svitsjeporten vises på menyen Innstillinger.
LLDP-MED: Svitsjeport	Angir om LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) er ak svitsjeporten.
LLDP-strømprioritet	Formidler telefonens strømprioritet til svitsjen, slik at den formidler strøm på riktig måte ti Innstillinger inkluderer: <ul style="list-style-type: none"> • Ukjent: Dette er standardverdien. • Lav • Høy • Kritisk
LLDP Asset ID (ID for LLDP-ressurs)	Identifiserer ressurs-ID-en som er tilordnet til telefonen for lagerstyring.
CTL-fil	Identifiserer CTL-filen.
ITL-fil	ITL-filen inneholder den opprinnelige klareringslisten.
ITL-signatur	Forbedrer sikkerheten ved hjelp av SHA-1 (Secure Hash Algorithm) I CTL- og ITL-filer.
CAPF-server	Navnet på CAPF-serveren som brukes av telefonen.
TVS	Hovedkomponenten i Sikkerhet som standard. Ved hjelp av TVS (Trust Verification Serv Cisco Unified IP-telefon godkjenne programservere, for eksempel EM-tjenester, kataloger o under HTTPS-opprettingen.
TFTP-server	Navnet på TFTP-serveren som brukes av telefonen.
Automatisk portsynkronisering	Synkroniserer portene til en lavere hastighet som fjerner muligheten for pakketap.
Ekstern konfigurasjon av svitsjeport	Tillater at en administrator kan konfigurere hastigheten og funksjonen for porten til tabellen f med Cisco-skrivebordssamarbeid eksternt ved hjelp av Cisco Unified Communications M Administration.
IP-adressemodus	Viser IP-adresseringsmodusen som er tilgjengelig på telefonen.
Moduskontroll for IP-preferanse	Angir IP-adresseversjonen som telefonen bruker under signalisering med Cisco Unified Com Manager når både IPv4 og IPv6 er tilgjengelig på telefonen.

Element	Beskrivelse
IP-preferansemodus for media	Angir at enheten bruker en IPv4-adresse for medier til å koble til Cisco Unified Communications Manager.
Automatisk IPv6-konfigurasjon	Angir om den automatiske konfigurasjonen er aktivert eller deaktivert på telefonen.
IPv6 DAD	Bekrefter hvis unike de nye unicast-IPv6-adressene er før de tilordnes til grensesnitt.
IPv6 godtar omadresserte meldinger	Angir om telefonen godtar omadresseringsmeldingene fra den samme ruter som brukes for målnummeret.
IPv6-svar på Multicast Echo-forespørsel	Angir at telefonen sender en Echo Reply-melding som svar på en Echo Request-melding som til en IPv6-adresse.
IPv6-lasteserver	Brukes til å optimalisere installasjonstiden for oppgraderinger av telefonens fastvare og lette for WAN ved å lagre bilder lokalt. Dermed fjernes behovet for å traversere WAN-koblingen ved oppgradering av hver telefon.
IPv6-loggserver	Angir IP-adressen og porten for den eksterne loggingsmaskinen som telefonen sender loggm til.
IPv6 CAPF-server	Vanlig navn (fra Cisco Unified Communications Manager-sertifikatet) på CAPF-sertifikatet som av telefonen.
DHCPv6	DHCP (Dynamic Host Configuration Protocol) tilordnet IPv6-adresser automatisk til enheter og kobler dem til nettverket. Cisco Unified IP-telefon aktiverer DHCP som standard.
IPv6-adresse	Viser den gjeldende IPv6-adressen for telefonen, eller tillater at brukeren angir en ny IPv6-adresse.
IPv6-prefikslengde	Viser den gjeldende prefikslengden for subverket, eller tillater at brukeren angir en ny prefiks.
Standard IPv6-ruter 1	Viser standardruter som brukes av telefonen, eller tillater at brukeren angir en ny IPv6-standardruter.
IPv6 DNS-server 1	Viser den primære DNSv6-serveren som brukes av telefonen, eller tillater at brukeren angir en ny DNSv6-server.
IPv6 DNS-server 2	Viser den sekundære DNSv6-serveren som brukes av telefonen, eller tillater at brukeren angir en ny sekundær DNSv6-server.
Alternativ TFTP for IPv6	Tillater at brukeren aktiverer bruk av en alternativ (sekundær) TFTP-server for IPv6.
IPv6 TFTP-server 1	Viser den primære TFTP-serveren for IPv6 som brukes av telefonen, eller tillater at brukeren angir en ny primær TFTP-server.
IPv6 TFTP-server 2	Viser den sekundære TFTP-serveren for IPv6 som brukes hvis den primære TFTP-serveren ikke er tilgjengelig, eller tillater at brukeren angir en ny sekundær TFTP-server.
IPv6-adresse frigitt	Tillater at brukeren frigir IPv6-relatert informasjon.
EnergyWise-strømnivå	En måling av energien som brukes av enheter i et EnergyWise-nettverk.
EnergyWise-domene	En administrativ gruppering av enheter med det formål å overvåke og kontrollere strømtilførsel.

Nettside med Ethernet-informasjon

Tabellen nedenfor beskriver innholdet på websiden Ethernet-informasjon.

Tabell 29: Elementer i Ethernet-informasjon

Element	Beskrivelse
Tx-rammer	Totalt antall pakker som telefonen sender.
Tx broadcast	Totalt antall kringkastingspakker som telefonen sender.
Tx multicast	Totalt antall multikastpakker som telefonen sender.
Tx unicast	Totalt antall unikastpakker som telefonen sender.
Rx-rammer	Totalt antall pakker som telefonen har mottatt.
Rx broadcast	Totalt antall kringkastingspakker som telefonen har mottar.
Rx multicast	Totalt antall multikastpakker som telefonen har mottar.
Rx unicast	Totalt antall unikastpakker som telefonen har mottar.
Rx PacketNoDes	Totalt antall avledede pakker som DMA-beskrivelsen (Direct Memory Access) forårsaker.

Nettsider for nettverk

Tabellen nedenfor beskriver informasjonen på nettsidene for Nettverksområde.



Merk Når du klikker på **Nettverk**-koblingen under Nettverksstatistikk, vises siden “Portinformasjon”.

Tabell 30: Elementer i nettverksområdet

Element	Beskrivelse
Rx totalPkt	Totalt antall pakker som telefonen har mottatt.
Rx multicast	Totalt antall multikastpakker som telefonen har mottatt.
Rx broadcast	Totalt antall kringkastingspakker som telefonen har mottatt.
Rx unicast	Totalt antall unikastpakker som telefonen har mottatt.
Rx tokenDrop	Totalt antall pakker som ble avbrutt på grunn av manglende ressurser (for eksempel FIFO-overflyt).
Tx totalGoodPkt	Totalt antall feilfrie pakker (multikast, kringkasting og unikast) som telefonen mottok.

Element	Beskrivelse
Tx broadcast	Totalt antall kringkastingspakker som telefonen har sendt.
Tx multicast	Totalt antall multikastpakker som telefonen har sendt.
LLDP FramesOutTotal	Totalt antall LLDP-rammer som telefonen har sendt.
LLDP AgeoutsTotal	Totalt antall LLDP-rammer som ble tidsavbrutt i bufferen.
LLDP FramesDiscardedTotal	Totalt antall LLDP-rammer som blir forkastet når en av de obligatoriske TLV-ene mangler, har feil rekkefølge eller inneholder en ugyldig strenglengde.
LLDP FramesInErrorsTotal	Totalt antall LLDP-rammer som ble mottatt med én eller flere identifiserbare feil.
LLDP FramesInTotal	Totalt antall LLDP-rammer som telefonen mottar.
LLDP TLVDiscardedTotal	Totalt antall LLDP TLV-er som er forkastet.
LLDP TLVUnrecognizedTotal	Totalt antall LLDP TLV-er som ikke gjenkjennes på telefonen.
Enhets-ID for CDP-nabo	Identifikator for en enhet som er koblet til denne porten som CDP oppdaget.
IP-adresse for CDP-nabo	IP-adresse for den oppdagede naboenhetsen som CDP oppdaget.
IPv6-adresse for CDP-nabo	IPv6-adresse for den oppdagede naboenhetsen som CDP oppdaget.
CDP-naboport	Naboenhetsport som telefonen er koblet til, som CDP oppdaget.
Enhets-ID for LLDP-nabo	Identifikator for en enhet som er koblet til denne porten, som LLDP oppdaget.
IP-adresse for LLDP-nabo	IP-adresse for naboenhetsen som LLDP oppdaget.
IPv6-adresse for LLDP-nabo	IPv6-adresse for naboenhetsen som CDP oppdaget.
LLDP-naboport	Naboenhetsport som telefonen er koblet til, som LLDP oppdaget.
Portinformasjon	Hastighets- og dupleksinformasjon.

Nettsidene Konsollogger, Kjernedumper, Statusmeldinger og Vis feilsøking

Hyperkoblingene Konsollogger, Kjernedumper, Statusmeldinger og Vis feilsøking under overskriften Enhetslogger gir informasjon som bidrar til å overvåke og feilsøke telefonen.

- Konsollogger – inkluderer hyperkoblinger til enkeltstående loggfiler. Konsolloggfilene inkluderer feilsøkings- og feilmeldinger som telefonen mottok.
- Kjernedumper – inkluderer hyperkoblinger til enkeltstående dumpfiler. Kjernedumpfilene inkluderer data fra et telefonkrasj.
- Statusmeldinger – viser de 10 siste statusmeldingene som telefonen har generert siden den sist ble slått på. Denne informasjonen vises også på skjermen Statusmeldinger på telefonen.

- Vis feilsøking – viser feilsøkingsmeldinger som kan være nyttige for Cisco TAC hvis du trenger hjelp med feilsøking.

Nettsiden Strømmestatistikk

En Cisco IP-telefon kan strømme informasjon til og fra opptil fem enheter samtidig. En telefon strømmer informasjon når den er opptatt i en samtale eller kjører en tjeneste som sender eller mottar lyd eller data.

Områdene for strømmestatistikken på en telefonwebseite inneholder informasjon om strømmene.

Hvis du vil vise et område for strømmestatistikk, går du til nettsiden for telefonen og klikker på en hyperkobling for **strømming**.

Tabellen nedenfor beskriver elementene i området Strømmestatistikk.

Tabell 31: Strømmestatistikk-felter

Element	Beskrivelse
Ekstern adresse	IP-adresse og UDP-port for strømmemålet.
Lokal adresse	IP-adresse og UDP-port for telefonen.
Starttidspunkt	Internt tidsstempel angir når Cisco Unified Communications Manager ba om at telefonen begynne å overføre pakker.
Strømmestatus	Angir om strømming er aktiv eller ikke.
Vertsnavn	Unikt, fast navn som tilordnes til telefonen automatisk basert på MAC-adressen.
Avsenderpakker	Totalt antall RTP-datapakker som telefonen har overført siden den startet denne tilkoblingen. Verdien er 0 hvis tilkoblingen er satt til modusen Receive-only (Bare motta).
Avsenderoktetter	Totalt antall nyttelastoktetter som telefonen har overført i RTP-datapakker siden den startet denne tilkoblingen. Verdien er 0 hvis tilkoblingen er satt til modusen Receive-only (Bare motta).
Avsenderkodek	Typen lydkodek som gjelder for den overførte strømmen.
Sendte avsenderrapporter (se merknad)	Antallet ganger RTCP-avsenderrapporten har blitt sendt.
Tidspunkt for sending av avsenderrapport (se merknad)	Internt tidsstempel som angir når den siste RTCP-avsenderrapporten ble sendt.
Tapte pakker	Totalt antall RTP-datapakker som har gått tapt siden datamottak startet på denne tilkoblingen. Definert som antallet forventede pakker mindre enn antallet pakker som faktisk har blitt mottatt. Der antallet mottatte pakker inkluderer pakker som er forsinket eller som er identiske med tidligere pakker vises som 0 hvis tilkoblingen ble satt til modusen Send-only (Bare send).
Gjsn. jitter	Anslag om betydelig avvik i ankomsttidspunktet til RTP-datapakken målt i millisekunder. Verdien vises som 0 hvis tilkoblingen ble satt til modusen Send-only (Bare send).
Mottakerkodek	Typen lydkodek som brukes for den mottatte strømmen.

Element	Beskrivelse
Sendte mottakerrapporter (se merknad)	Antallet ganger RTCP-mottakerrapportene har blitt sendt.
Tidspunkt for sending av mottakerrapport (se merknad)	Internt tidsstempel som angir når en RTCP-mottakerrapporten ble sendt.
Mottatte pakker	Totalt antall RTP-datapakker som telefonen har mottatt siden datamottak startet på den første tilkoblingen. Inkluderer pakker som ble mottatt fra forskjellige kilder hvis dette anropet er et multikastanrop. Verdien vises som 0 hvis tilkoblingen ble satt til modusen Send-only (Send-only send).
Mottakeroktetter	Totalt antall nyttelastoktetter som enheten mottok i RTP-datapakker siden datamottak startet på den første tilkoblingen. Inkluderer pakker som ble mottatt fra forskjellige kilder hvis dette anropet er et multikastanrop. Verdien vises som 0 hvis tilkoblingen ble satt til modusen Send-only (Send-only send).
Akkumulert skjult omfang	Totalt antall skjulte rammer delt på totalt antall talerammer som ble mottatt fra starten av talestrømmen.
Skjult omfang for intervall	Antall skjulte rammer til talerammer i det foregående intervallet med aktiv tale på 3 sekunder. Hvis talegjennkjennning (VAD) er i bruk, kreves det kanskje et lengre intervall for å akkumulere tre sekunder med aktiv tale.
Maks. skjult omfang	Høyeste skjulte omfang for intervall fra starten av talestrømmen.
Skjulte sekunder	Antallet sekunder som har skjulte hendelser (tapte rammer) fra starten av talestrømmen (inkluderer svært skjulte sekunder).
Sekunder med mange skjulte elementer	Antallet sekunder som har mer enn fem prosent skjulte hendelser (tapte rammer) fra starten av talestrømmen.
Ventetid (se merknad)	Anslag om nettverksventetid uttrykt i millisekunder. Representerer et aktivt gjennomsnitt for løkkeforsinkelsen, som måles når sperringer for RTCP-mottakerrapporten mottas.
Maks. jitter	Maksimal verdi med umiddelbar jitter i millisekunder.
Avsenderstørrelse	RTP-pakkestørrelse, i millisekunder, for den overførte strømmen.
Mottatte avsenderrapporter (se merknad)	Antallet ganger RTCP-avsenderrapporter har blitt mottatt.
Tidspunkt for mottak av avsenderrapport (se merknad)	Tidspunktet for siste mottak av en RTCP-avsenderrapport.
Mottakerstørrelse	RTP-pakkestørrelse, i millisekunder, for den mottatte strømmen.
Mottaker forkastet	RTP-pakker som ble mottatt fra nettverket, men som ble forkastet fra jitterbufferne.

Element	Beskrivelse
Mottatte mottakerrapporter (se merknad)	Antallet ganger RTCP-mottakerrapporter har blitt mottatt.
Tidspunkt for mottak av mottakerrapport (se merknad)	Tidspunktet for siste mottak av en RTCP-mottakerrapport.



Merk Når protokollen for RTP-kontroll er deaktivert, genereres det ingen data for dette feltet, og dermed vises verdien som 0.

Be om informasjon fra telefonen i XML

Når det gjelder feilsøking, kan du be om informasjon fra telefonen. Informasjonen er i XML-format. Følgende informasjon er tilgjengelig:

- Samtaleinformasjon er informasjon om samtaleøkten for en bestemt linje.
- Linjeinformasjon er informasjon om linjekonfigurasjonen for telefonen.
- Modellinformasjon er informasjon om telefonmodellen.

Før du begynner

nettilgang må ha muligheten til å hente informasjonen.

Telefonen må være knyttet til en bruker.

Prosedyre

Trinn 1 For samtaleinformasjon, skriv inn følgende URL i en nettleser: **http://<phone ip address>/CGI/Java/CallInfo<x>**

hvor

- *<phone ip address>* er IP-adressen til telefonen
- *<x>* er linjenummeret du skal bruke for å få informasjon om.

Kommandoen returnerer et XML-dokument.

Trinn 2 For linjeinformasjon, skriv inn følgende URL i en nettleser: **http://<phone ip address>/CGI/Java/LineInfo**

hvor

- *<phone ip address>* er IP-adressen til telefonen

Kommandoen returnerer et XML-dokument.

Trinn 3 For modellinformasjon, skriv inn følgende URL i en nettleser: `http://<phone ip address>/CGI/Java/ModeInfo`

hvor

- `<phone ip address>` er IP-adressen til telefonen

Kommandoen returnerer et XML-dokument.

Utdata for kommandoen CallInfo

Følgende XML-kode er et eksempel på utdata fra kommandoen 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>
```

Utdata for kommandoen LineInfo

Følgende XML-kode er et eksempel på utdata fra kommandoen 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>

```

Utdata for kommandoen ModelInfo

Følgende XML-kode er et eksempel på utdata fra kommandoen ModelInfo.

```

<?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>

```




KAPITTEL 12

Vedlikehold

- [Starte på nytt eller tilbake stille konferansetelefonen, på side 133](#)
- [Overvåking av talekvalitet, på side 134](#)
- [Rengjøring av Cisco IP-telefon, på side 136](#)

Starte på nytt eller tilbake stille konferansetelefonen

Utfør en grunnleggende tilbakestilling av en telefon for å gjenopprette den hvis det oppstår en feil på telefonen. Du kan også gjenopprette konfigurasjons- og sikkerhetsinnstillinger til standard fabrikkinnstillinger.

Starte konferansetelefonen på nytt

Når du starter telefonen på nytt, går alle brukerendringer eller endringer i nettverksoppsettet som ikke er lagret i flash-minnet på telefonen, tapt.

Prosedyre

Trykk på **Innstillinger** > **Administratorinnstillinger** > **Tilbakestill innstillinger** > **Tilbakestill enhet**.

Tilbake stille konferansetelefoninnstillingene fra Telefon-menyen

Prosedyre

Trinn 1 Trykk på **Innstillinger**.

Trinn 2 Velg **Administratorinnstillinger** > **Tilbakestill innstillinger**.

Trinn 3 Velg tilbakestillingstype.

- **Alle** – gjenoppretter fabrikkinnstillingene.
- **Tilbakestill enhet** – tilbake stiller enheten. De eksisterende innstillingene endres ikke.
- **Nettverk** – tilbake stiller nettverkskonfigurasjonen til standardinnstillingene.
- **Tjenestemodus** – fjerner gjeldende tjenestemodus, deaktiverer VPN og starter telefonen på nytt.

- **Sikkerhet** – tilbakestiller sikkerhetskonnfigurasjonen til standardinnstillingene. Dette alternativet sletter CTL-filen.

Trinn 4 Trykk på **Tilbakestill** eller **Avbryt**.

Tilbakestille konferansetelefonen til standard fabrikkinnstillinger fra tastaturet

Når du tilbakestiller telefonen på tastaturet, tilbakestilles telefonen til fabrikkinnstillingene.

Prosedyre

Trinn 1 Koble fra telefonen:

- Hvis du bruker PoE, trekker du ut LAN-kabelen.
- Hvis du bruker strømadapteren, kobler du fra enheten.

Trinn 2 Vent 5 sekunder.

Trinn 3 Trykk på og hold inne #, og koble til telefonen igjen.

Trinn 4 Når telefonen starter, lyser LED-stripen. Når LED-stripen begynner å lyse, trykker du på **123456789*0#** i rekkefølge.

Eter at du har trykket på disse knappene, gjennomføres det en tilbakestilling til fabrikkinnstillingene på telefonen.

Hvis du trykker på knappene utenfor rekkefølgen, slås telefonen på vanlig måte.

Forsiktig Ikke slå av telefonen før tilbakestillingen til fabrikkinnstillingene er fullført og hovedskjermen vises.

Overvåking av talekvalitet

For å måle talekvaliteten for samtaler som ikke er sendt og mottatt i nettverket, bruker Cisco IP-telefonene disse statistiske metrikkverdiene som er basert på tildekkingshendelser. DSP spiller av tildekkingsrammer for å maskere rammetap i talepakkestrømmen.

- Metrikkverdier for tildekkingsomfang – Vis omfanget av tildekkingsrammer i forhold til totalt antall talerammer. Et intervall for tildekkingsomfang beregnes hvert tredje sekund.
- Metrikkverdier for skjulte sekunder – Vis antallet sekunder det tar før DSP spiller av tildekkingsrammer på grunn av tapte rammer. Et svært “skjult sekund” er et sekund der DSP spiller av mer enn fem prosent med tildekkingsrammer.



Merk Tildekkingsomfang og tildekkingssekunder er primære målinger basert på rammetap. Et tildekkingsomfang på null, angir at IP-nettverket leverer rammer og pakker i tide uten tap.

Du har tilgang til metrikkverdier for talekvalitet fra Cisco IP-telefon ved hjelp av skjermen Anropsstatistikk eller eksternt ved hjelp av Strømmestatistikk.

Tips for feilsøking av talekvalitet

Når du finner omfattende og permanente endringer i metrikkverdiene, bruker du tabellen nedenfor for informasjon om generell feilsøking.

Tabell 32: Endringer i metrikkverdier for talekvalitet

Endring i metrikkverdi	Betingelse
Verdiene for Skjult omfang og Skjulte sekunder øker betydelig	Nettverkssvekkelse på grunn av pakketap eller høyt jitternivå.
Verdien for Skjult omfang er nesten ved null eller null, men talekvaliteten er dårlig.	<ul style="list-style-type: none"> • Støy eller forstyrrelse i lydkanalen, for eksempel ekko eller ulike lydnivåer. • Parallele anrop som blir gjenstand for flere kodinger/dekodinger, for eksempel anrop til et mobilnettverk eller kontantkortnettverk. • Akustikkproblemer som kommer fra høyttaleren, håndfritelefonen eller de trådløse hodetelefonene. <p>Kontroller tellerne for pakkesendingen (TxCnt) og pakkemottaket (RxCnt) for å bekrefte at talepakkene har god flyt.</p>
MOS LQK-verdier er kraftig redusert	<p>Nettverkssvekkelse på grunn av pakketap eller høye jitternivåer:</p> <ul style="list-style-type: none"> • Reduksjon i gjennomsnittlige MOS LQK-verdier kan angi omfattende og enhetlig svekkelse. • Reduksjon i enkeltstående MOS LQK-verdi kan angi svekkelse som fører til brudd. <p>Krysskontroller verdiene for Skjult omfang og Skjulte sekunder for mulig pakketap og jitter.</p>
MOS LQK-verdier har økt kraftig	<ul style="list-style-type: none"> • Kontroller om telefonen bruker en annen kodek enn forventet (RxType og TxType). • Kontroller om MOS LQK-versjonen ble endret etter en fastvareoppgradering.



Merk Metrikkverdier for talekvalitet tar ikke høyde for støy eller forstyrrelse, bare rammetap.

Rengjøring av Cisco IP-telefon

Hvis du vil rengjøre Cisco IP-telefon, bruker du kun en tørr klut og tørker av telefonen og skjermen forsiktig. Ikke bruk væsker eller pulver direkte på telefonen. Væsker og pulver kan skade komponentene og føre til feil, som på alle lignende elektronikkprodukter.

Når telefonen er i dvalemodus, er skjermen blank, og Velg-knappen lyser ikke. Når telefonen er i denne tilstanden, kan du rengjøre skjermen, så lenge du er klar over at telefonen vil forbli i dvalemodus til du er ferdig med rengjøringen.



KAPITTEL 13

Feilsøking

- [Generell feilsøkinginformasjon, på side 137](#)
- [Oppstartsproblemer, på side 138](#)
- [Problemer med tilbakestilling av telefonen, på side 142](#)
- [Telefonen kan ikke koble til LAN, på side 144](#)
- [Problemer med sikkerhet på Cisco IP-telefoner, på side 144](#)
- [Lydproblemer, på side 147](#)
- [Generelle problemer med telefonsamtaler, på side 147](#)
- [Feilsøkingprosedyrer, på side 148](#)
- [Kontrollere feilsøkinginformasjon fra Cisco Unified Communications Manager, på side 152](#)
- [Ekstra feilsøkinginformasjon, på side 153](#)

Generell feilsøkinginformasjon

I tabellen nedenfor finner du generell feilsøkinginformasjon for Cisco IP-telefon.

Tabell 33: Feilsøking for Cisco IP-telefon

Sammendrag	Forklaring
For stor nettverkstrafikk over lang tid fører til at IP-telefoner tilbakestilles eller ikke kan besvare et anrop eller ringe	Lag 2-nettverkstrafikk over lang tid (som varer i flere minutter) på det virkelige nettverket kan føre til at IP-telefoner tilbakestilles, samtaler blir brutt og ikke kan ringe eller besvare et anrop. Det er ikke sikkert at telefonen fungerer når nettverkstrafikken er normalisert.
Flytte en nettverkstilkobling fra telefonen til en arbeidsstasjon	Hvis du bruker telefonen via nettverkstilkoblingen, må du tenke deg om å koble fra nettverkstilkoblingen for telefonen og koble ledningen til en datamaskin. Forsiktig Nettverkskortet i datamaskinen kan ikke motta strøm via nettverkstilkoblingen. Hvis strømmen kommer fra tilkoblingen, kan nettverkskortet bli ødelagt. For å beskytte et nettverkskort må du vente i 10 sekunder eller lenger etter at du har tatt ut ledningen fra datamaskinen før du kobler den til en datamaskin. Denne forsinkelsen gir deg nok tid til å registrere at det ikke lenger finnes en telefon på linjen og stoppe forsyningen av strøm til ledningen.

Sammendrag	Forklaring
Endre telefonkonfigurasjonen	<p>Som standard er innstillingene for administratorpassord låst for å hindre at du gjør endringer som kan påvirke nettverkstilkoblingen. Du må låse opp innstillingene for administratorpassord før du kan konfigurere dem.</p> <p>Se Ta i bruk et telefonpassord, på side 31 for detaljer.</p> <p>Merk Hvis administratorpassordet ikke er angitt i en felles telefonprofil, må brukeren endre nettverksinnstillingene.</p>
Manglende kodeksamsvar mellom telefonen og en annen enhet	<p>RxType- og TxType-statistikken nedenfor viser kodeken som brukes for en samtale mellom denne Cisco IP-telefon og den andre enheten. Verdiene for disse statistikken må samsvare. Hvis ikke de gjør det, må du bekrefte at den andre enheten kan bruke kodeksamtalet eller at en transkoder brukes til å behandle tjenesten. Se Vis Anropsstatistikk, på side 116 hvis du vil vite mer.</p>
Manglende samsvar mellom lydsnutt for telefonen og en annen enhet	<p>RxSize- og TxSize-statistikken nedenfor viser størrelsen på talepakkene som brukes i en samtale mellom denne Cisco IP-telefon og den andre enheten. Verdiene for disse statistikken må samsvare. Se Vise vinduet Anropsstatistikk, på side 116 hvis du vil vite mer.</p>
Tilbakekoblingsbetingelse	<p>En tilbakekoblingsbetingelse kan oppstå når følgende betingelser er oppfylt:</p> <ul style="list-style-type: none"> • Alternativet Svitsjeportkonfigurasjon på telefonen er satt til 10 halv (10-BaseT/halv dupleks). • Telefonen får strøm fra en ekstern strømforsyningskilde. • Telefonen er slått av (strømforsyningen er koblet fra). <p>I dette tilfellet kan svitsjeporten på telefonen bli koblet fra og følgende melding vises i svitsjekonsolloggen:</p> <pre>HALF_DUX_COLLISION_EXCEED_THRESHOLD</pre> <p>Aktiver porten fra svitsjen på nytt for å løse dette problemet.</p>

Oppstartsproblemer

Etter at du har installert en telefon i nettverket og lagt den til i Cisco Unified Communications Manager, skal telefonen starte som beskrevet i emnene nedenfor.

Hvis telefonen ikke starter, kan du se følgende deler for feilsøkinginformasjon.

Beslektede emner

[Bekreftede telefonoppstarten](#), på side 37

Cisco IP-telefon bruker ikke den vanlige oppstartsprosessen

Problem

Når du kobler en Cisco IP-telefon til nettverksporten, bruker ikke telefonen den vanlige oppstartsprosessen, som beskrevet i det aktuelle emnet, og telefonskjermen viser ingen informasjon.

Årsak

Hvis telefonen ikke bruker oppstartsprosessen, kan det skyldes skadede ledninger, dårlig tilkobling, nettverksbrudd, manglende strøm eller at telefonen ikke fungerer.

Løsning

Hvis du vil finne ut om telefonen fungerer, bruker du forslagene nedenfor til å eliminere andre potensielle problemer.

- Bekreft at nettverksporten fungerer:
 - Bytt ut Ethernet-kablene med kabler du vet fungerer.
 - Koble en fungerende Cisco IP-telefon fra en annen port og koble den til denne nettverksporten for å bekrefte at porten er aktiv.
 - Koble Cisco IP-telefon som ikke starter, til en annen nettverksport som du vet fungerer.
 - Koble Cisco IP-telefon som ikke starter, direkte til porten på svitsjen. På den måten fjerner du tilkoblingen til korrigeringspanelet på kontoret.
- Kontroller at telefonen mottar strøm:
 - Hvis du bruker en ekstern strømforsyning, må du kontrollere at det elektriske uttaket fungerer.
 - Hvis du bruker innebygd strøm, må du i stedet bruke ekstern strømforsyning.
 - Hvis du bruker den eksterne strømforsyningen, må du bytte til en enhet som du vet fungerer.
- Hvis telefonen fortsatt ikke starter på riktig måte, slår du den på fra sikkerhetskopiavbildningen av programvaren.
- Hvis telefonen fortsatt ikke starter på riktig måte, utfører du tilbakestilling til fabrikkinnstillingene på telefonen.
- Etter at du har forsøkt disse løsningene, kontakter du en kundestøttemedarbeider for å få hjelp hvis telefonskjermen på Cisco IP-telefon ikke viser noen tegn etter fem minutter.

Beslektede emner

[Bekreft telefonoppstarten](#), på side 37

Cisco IP-telefon registreres ikke i Cisco Unified Communications Manager

Hvis telefonen fortsetter forbi det første trinnet i oppstartsprosessen (lamper blinker), men fortsetter å vise meldinger på skjermen, blir ikke telefonen startet riktig. Telefonen kan ikke startes riktig hvis ikke den kobles til Ethernet-nettverket og registreres på en Cisco Unified Communications Manager-server.

I tillegg kan det hende at Problemer med sikkerhet hindrer at den starter riktig. Se [Feilsøkningsprosedyrer](#), på side 148 hvis du vil ha mer informasjon.

Telefonen viser feilmeldinger

Problem

Statusmeldinger viser feil under oppstart.

Løsning

Mens telefonen går gjennom oppstartsprosessen, kan du vise statusmeldingene som kanskje gir mer detaljert informasjon om årsaken til et problem. Se delen “Vise vinduet Statusmeldinger” hvis du vil ha instruksjoner om hvordan du åpner statusmeldinger og får tilgang til en liste med potensielle feil, samt forklaringer på og løsninger for feilene.

Beslektede emner

[Vise vinduet Statusmeldinger](#), på side 108

Telefonen kan ikke koble til TFTP-serveren eller til Cisco Unified Communications Manager

Problem

Hvis nettverksforbindelsen er brutt mellom telefonen og TFTP-serveren eller Cisco Unified Communications Manager, kan ikke telefonen startes riktig.

Løsning

Kontroller at nettverksforbindelsen fungerer.

Telefonen kan ikke koble til TFTP-serveren

Problem

Innstillingene for TFTP-serveren er kanskje ugyldige.

Løsning

Kontroller TFTP-innstillingene.

Beslektede emner

[Kontrollere TFTP-innstillinger](#), på side 149

Telefonen kan ikke koble til serveren

Problem

Feltene for IP-adressering og ruting er kanskje ikke konfigurert riktig.

Løsning

Du må kontrollere innstillingene for IP-adressering og ruting på telefonen. Hvis du bruker DHCP, skal DHCP-serveren formidle disse verdiene. Hvis du har tilordnet en statisk IP-adresse til telefonen, må du angi disse verdiene manuelt.

Beslektede emner

[Kontrollere DHCP-innstillinger](#), på side 150

Telefonen kan ikke koble til med DNS

Problem

DNS-innstillingene er kanskje ugyldige.

Løsning

Hvis du bruker DNS til å få tilgang til TFTP-serveren eller Cisco Unified Communications Manager, må du angi en DNS-server.

Beslektede emner

[Kontrollere DNS-innstillinger](#), på side 151

Cisco Unified Communications Manager og TFTP-tjenester kjører ikke

Problem

Hvis Cisco Unified Communications Manager eller TFTP-tjenester ikke kjører, er det ikke sikkert at telefoner kan startes riktig. I slike situasjoner er det sannsynlig at det har oppstått en systemfeil, og andre telefoner og enheter kan heller ikke startes riktig.

Løsning

Hvis Cisco Unified Communications Manager ikke kjører, blir alle enheter i nettverket som er avhengige av tjenesten for å foreta anrop, påvirket av dette. Hvis TFTP-tjenesten ikke kjører, er det mange enheter som ikke kan startes. Hvis du vil ha mer informasjon, kan du se [Starte tjeneste, på side 151](#)

Skadet konfigurasjonsfil

Problem

Hvis du forsetter å ha problemer med en bestemt telefon som andre forslag i dette kapitlet ikke løser, kan det hende konfigurasjonsfilen er skadet.

Løsning

Opprette en ny telefonkonfigurasjonsfil.

Beslektede emner

[Opprette en ny telefonkonfigurasjonsfil](#), på side 150

Registrering av telefoner i Cisco Unified Communications Manager

Problem

Telefonen er ikke registret med Cisco Unified Communications Manager

Løsning

En Cisco IP-telefon kan registreres på en Cisco Unified Communications Manager-server bare hvis telefonen legges til på serveren eller hvis automatisk registrering er aktivert. Les gjennom informasjonen og fremgangsmåtene i [Metoder for å legge til telefoner, på side 44](#) for å sørge for at telefonen blir lagt til i Cisco Unified Communications Manager-databasen.

Hvis du vil kontrollere at telefonen finnes i Cisco Unified Communications Manager-databasen, velger du **Enhet > Telefon** fra Cisco Unified Communications Manager Administration. Klikk **Søk** for å søke etter telefonen basert på MAC-adressen. Hvis du vil ha informasjon om hvordan du fastslår en MAC-adresse, kan du se [Fastslå telefonens MAC-adresse, på side 43](#).

Hvis telefonen allerede er i Cisco Unified Communications Manager-databasen, kan det hende konfigurasjonsfilen er skadet. Se [Skadet konfigurasjonsfil, på side 141](#) for informasjon.

Cisco IP-telefon kan ikke hente IP-adresse

Problem

Hvis en telefon ikke kan hente en IP-adresse når den startes, er det ikke sikkert telefonen er på samme nettverk eller VLAN som DHCP-serveren, eller svitsjeporten som telefonen er koblet til, kan være deaktivert.

Løsning

Kontroller at nettverket eller VLAN som telefonen er koblet til, har tilgang til DHCP-serveren, og kontroller at svitsjeporten er aktivert.

Problemer med tilbakestilling av telefonen

Hvis brukere rapporterer at telefonen blir tilbakestilt under samtaler eller mens telefonen er inaktiv, bør du finne ut årsaken. Hvis nettverkstilkoblingen og tilkoblingen til Cisco Unified Communications Manager er stabil, skal ikke telefonen bli tilbakestilt.

En telefon tilbakestilles vanligvis hvis den har problemer med å koble til nettverket eller til Cisco Unified Communications Manager.

Telefonen tilbakestilles på grunn av vedvarende nettverksbrudd

Problem

Det er kanskje vedvarende nettverksbrudd.

Løsning

Vedvarende nettverksavbrudd påvirker data- og taletrafikk på forskjellig måte. Det er kanskje vedvarende nettverksbrudd uten at det har blitt oppdaget. I så fall kan datatrafikk sende tapte pakker på nytt, og verifisere at pakker blir mottatt og overført. For taletrafikk kan imidlertid ikke tapte pakker gjenopprettes. I stedet for å oppdatere en brutt nettverkstilkobling, tilbakestilles telefonen og prøver en ny tilkobling til nettverket. Kontakt systemansvarlig for informasjon om kjente problemer i talenettverket.

Telefonen tilbakestilles på grunn av feil med DHCP-innstillingene

Problem

DHCP-innstillingene er kanskje ugyldige.

Løsning

Kontroller at du har konfigurert telefonen riktig for bruk av DHCP. Kontroller at DHCP-serveren er konfigurert riktig. Kontroller varigheten på DHCP-leieperioden. Det anbefales at du setter leieperioden til 8 dager.

Beslektede emner

[Kontrollere DHCP-innstillinger](#), på side 150

Telefonen tilbakestilles på grunn av en ugyldig statisk IP-adresse

Problem

Den statiske IP-adressen som er knyttet til telefonen, kan være ugyldig.

Løsning

Hvis telefonen er knyttet til en statisk IP-adresse, kontrollerer du at du har angitt riktige innstillinger.

Telefonen tilbakestilles ved høy nettverksbelastning

Problem

Hvis telefonen tilbakestilles på grunn av høy nettverksbelastning, skyldes det mest sannsynlig at du ikke har konfigurert Tale-VLAN.

Løsning

Hvis du isolerer telefonene på et eget tilleggs-VLAN, øker kvaliteten på taletrafikken.

Telefonen tilbakestilles på grunn av tilsiktet tilbakestilling

Problem

Hvis det ikke bare er du som er administrator med tilgang til Cisco Unified Communications Manager, må du kontrollere at ingen andre tilfeldigvis har tilbakestilt telefonene.

Løsning

Du kan sjekke om en Cisco IP-telefon mottok en kommando fra Cisco Unified Communications Manager for å nullstille ved å trykke på **Innstillinger** på telefonen og velge **Administratorinnstillinger** > **Status** > **Nettverksstatistikk**.

- Hvis feltet Årsak til omstart viser **Tilbakestill-Tilbakestill**, mottar telefonen kommandoen **Tilbakestill/Tilbakestill** fra Cisco Unified Communications Manager Administration.

- Hvis feltet Årsak til omstart viser `Tilbakestill-Omstart`, ble telefonen slått av fordi den mottok kommandoen `Tilbakestill/Omstart` fra Cisco Unified Communications Manager Administration.

Telefonen tilbakestilles på grunn av problemer med DNS eller andre tilkoblingsproblemer

Problem

Telefonen fortsetter å bli tilbakestilt, og du mistenker DNS eller andre tilkoblingsproblemer.

Løsning

Hvis telefonen fortsetter å bli tilbakestilt, kan du utelukke DNS eller andre tilkoblingsfeil ved å følge fremgangsmåten i [Finne problemer med DNS eller tilkobling, på side 149](#).

Telefonen blir ikke slått på

Problem

Det virker som om telefonen ikke blir slått på.

Løsning

I de fleste tilfeller starter en telefon på nytt hvis den slås på ved hjelp av en ekstern strømkilde, men den tilkoblingen blir brutt og det byttes til PoE. På samme måte kan det hende en telefon starter på nytt hvis den slås på ved hjelp PoE og deretter kobles til en ekstern strømkilde.

Telefonen kan ikke koble til LAN

Problem

Den fysiske tilkoblingen til LAN kan være brutt.

Løsning

Kontroller at Ethernet-tilkoblingen som Cisco IP-telefon er koblet til, fungerer. Kontroller for eksempel om den bestemte porten eller svitsjen som telefonen er koblet til, er nede og at svitsjen ikke er under omstart. Kontroller også at ingen av kablene er skadet.

Problemer med sikkerhet på Cisco IP-telefoner

Nedenfor finner du feilsøkinginformasjon for sikkerhetsfunksjoner på Cisco IP-telefon. Hvis du vil ha informasjon om løsningene på disse problemene, og hvis du vil ha ekstra feilsøkinginformasjon om sikkerhet, kan du se *Sikkerhetsveiledning for Cisco Unified Communications Manager*.

Problemer med CTL-filen

Innholdet nedenfor beskriver feilsøkingproblemer med CTL-filen.

Godkjenningsfeil: Telefonen kan ikke godkjenne CTL-filen

Problem

Det har oppstått en feil under godkjenning av enhet.

Årsak

CTL-filen har ikke et Cisco Unified Communications Manager-sertifikat eller har et ugyldig sertifikat.

Løsning

Installer et gyldig sertifikat.

Telefonen kan ikke godkjenne CTL-filen

Problem

Telefonen kan ikke godkjenne CTL-filen.

Årsak

Sikkerhetstokenen som signerte den oppdaterte CTL-filen, finnes ikke i CTL-filen på telefonen.

Løsning

Endre sikkerhetstokenen i CTL-filen, og installer den nye filen på telefonen.

CTL-filen godkjennes, men andre konfigurasjonsfiler blir ikke godkjent

Problem

Telefonen kan ikke godkjenne andre konfigurasjonsfiler enn CTL-filen.

Årsak

Det finnes en ugyldig TFTP-oppføring, eller konfigurasjonsfilen er kanskje ikke signert av det tilsvarende sertifikatet i telefonens klareringsliste.

Løsning

Kontroller TFTP-oppføringen og sertifikatet i klareringslisten.

ITL-filen godkjennes, men andre konfigurasjonsfiler blir ikke godkjent

Problem

Telefonen kan ikke godkjenne andre konfigurasjonsfiler enn ITL-filen.

Årsak

Konfigurasjonsfilen er kanskje ikke signert av det tilsvarende sertifikatet i telefonens klareringsliste.

Løsning

Signer konfigurasjonsfilen på nytt med det riktige sertifikatet.

TFTP-godkjenning mislykkes

Problem

Telefonen rapporterer en TFTP-godkjenningsfeil.

Årsak

TFTP-adressen for telefonen finnes ikke i CTL-filen.

Hvis du opprettet en ny CTL-fil med en ny TFTP-oppføring, er det ikke sikkert at den eksisterende CTL-filen på telefonen inneholder en oppføring for den nye TFTP-serveren.

Løsning

Kontroller konfigurasjonen av TFTP-adressen i telefonens CTL-fil.

Telefonen blir ikke registrert

Problem

Telefonen blir ikke registrert med Cisco Unified Communications Manager.

Årsak

CTL-filen inneholder ikke den riktige informasjonen for Cisco Unified Communications Manager-serveren.

Løsning

Endre informasjonen for Cisco Unified Communications Manager-serveren i CTL-filen.

Signerte konfigurasjonsfiler er ikke obligatoriske

Problem

Telefonen krever ikke signerte konfigurasjonsfiler.

Årsak

CTL-filen inneholder ingen TFTP-oppføringer med sertifikater.

Løsning

Konfigurer TFTP-oppføringer med sertifikater i CTL-filen.

Lydproblemer

De neste delene beskriver hvordan du løser lydproblemer.

Ingen talebane

Problem

Én eller flere personer i en samtale hører ingen lyd.

Løsning

Når minst én person i en samtale ikke mottar lyd, er det ikke etablert IP-tilkobling mellom telefonene. Kontroller konfigurasjonen av ruterne og svitsjene for å sjekke at IP-tilkoblingen er konfigurert riktig.

Hakkete tale

Problem

En bruker klager på hakkete tale i en samtale.

Årsak

Det kan være manglende samsvar i jitterkonfigurasjonen.

Løsning

Kontroller statistikken for AvgJtr og MaxJtr. Et stort avvik i disse statistikkene kan antyde at det har oppstått et problem med jitter i nettverket, eller at det forekommer høy nettverksaktivitet uregelmessig.

Generelle problemer med telefonsamtaler

Innholdet nedenfor hjelper med å feilsøke generelle problemer med telefonsamtaler.

Telefonsamtale kan ikke opprettes

Problem

En bruker klager på at han/hun ikke kan foreta et anrop.

Årsak

Telefonen har ingen DHCP IP-adresse og kan ikke registreres i Cisco Unified Communications Manager. Telefoner med en LCD-skjerm viser meldingen `IP konfigureres` eller `Registrerer`. Telefoner uten en LCD-skjerm, spiller av innspillingstonen (i stedet for ringetonen) i telefonrøret når brukeren forsøker å foreta et anrop.

Løsning

1. Kontroller ett av følgende:
 1. At Ethernet-kabelen er koblet til.
 2. At Cisco CallManager-tjenesten kjører på Cisco Unified Communications Manager-serveren.
 3. At begge telefoner er registrert i samme forekomst av Cisco Unified Communications Manager.
2. At loggene for lydserverfeilsøking og lagringsloggene er aktivert for begge telefoner. Aktiver om nødvendig Java-feilsøking.

Telefonen gjenkjenner ikke DTMP-sifrene, eller sifrene er forsinket

Problem

Brukeren klager på at numre vises eller vises langsomt når tastaturet brukes.

Årsak

Hvis du trykker på tastene for raskt, kan det føre til at sifre ikke vises eller vises langsomt.

Løsning

Du må ikke trykke for raskt på tastene.

Feilsøkningsprosedyrer

Disse prosedyrene kan brukes til å identifisere og løse problemer.

Opprette en telefonproblemrapport fra Cisco Unified Communications Manager

Du kan generere en problemrapport for telefonene fra Cisco Unified Communications Manager. Denne handlingen gir samme informasjon som funksjonstasten for problemrapportverktøyet (PRT) genererer på telefonen.


Problemrapporten inneholder informasjon om telefonen og hodetelefonene.

Prosedyre

- Trinn 1** I Cisco Unified CM Administration velger du **Enhet > Telefon**.
- Trinn 2** Klikk på **Søk** og velg én eller flere Cisco IP-telefoner.
- Trinn 3** Klikk på **Generer PRT for valgt** for å samle inn PRT-logger for hodetelefonene som brukes på de valgte Cisco IP-telefonene.
-

Kontrollere TFTP-innstillinger

Prosedyre

- Trinn 1** Trykk på **Programmer**  på telefonen.
- Trinn 2** Trykk på **Innstillinger** på telefonen.
- Trinn 3** Velg **Nettverksoppsett > IPv4-oppsett**.
- Trinn 4** Merk av for feltet TFTP-server 1.
- Hvis du har tilordnet en statisk IP-adresse til telefonen, må du angi en innstilling for alternativet TFTP-server 1 manuelt.
- Hvis du bruker DHCP, henter telefonen adressen til TFTP-serveren fra DHCP-serveren. Kontroller at IP-adressen er konfigurert i alternativ 150.
- Trinn 5** Du kan også stille inn telefonen til å bruke en alternativ TFTP-server. En slik innstilling er spesielt nyttig hvis telefonen nylig ble flyttet fra ett sted til et annet.
- Trinn 6** Hvis den lokale DHCP-serveren ikke formidler riktig TFTP-adresse, stiller du inn telefonen til å bruke en alternativ TFTP-server.
- Dette er ofte nødvendig i VPN-scenarier.
-

Finne problemer med DNS eller tilkobling

Prosedyre

- Trinn 1** Bruk menyen Tilbakestill innstillinger til å tilbakestille telefoninnstillingene til standardverdiene.
- Trinn 2** Endre DHCP- og IP-innstillinger:
- Deaktiver DHCP.
 - Tilordne statiske IP-verdier til telefonen. Bruk den samme standardruterinnstillingen som andre fungerende telefoner bruker.
 - Tilordne en TFTP-server. Bruk den samme TFTP-serveren som andre fungerende telefoner bruker.
- Trinn 3** På Cisco Unified Communications Manager-serveren bekrefter du at de lokale vertsfilene har riktig Cisco Unified Communications Manager-servernavn tilordnet til den riktige IP-adressen.
- Trinn 4** Fra Cisco Unified Communications Manager velger du **System > Server** og bekrefter at referansen til serveren kommer fra IP-adressen og ikke fra DNS-navnet.
- Trinn 5** Fra Cisco Unified Communications Manager velger du **Enhet > Telefon**. Klikk **Søk** for å søke etter denne telefonen. Kontroller at du har tilordnet riktig MAC-adresse til denne Cisco IP-telefon.
- Trinn 6** Slå telefonen av og på.
-

Beslektede emner

[Fastslå telefonens MAC-adresse](#), på side 43

[Starte på nytt eller tilbakestille konferansetelefonen](#), på side 133

Kontrollere DHCP-innstillinger

Prosedyre

Trinn 1 Trykk på **Programmer**  på telefonen.

Trinn 2 Trykk på **Innstillinger** på telefonen.

Trinn 3 Velg **Nettverksoppsett > IPv4-oppsett**.

Trinn 4 Merk av for feltet DHCP-server.

Hvis du har tilordnet en statisk IP-adresse til telefonen, trenger du ikke angi en verdi for alternativet DHCP-server. Hvis du imidlertid bruker en DHCP-server, må dette alternativet ha en verdi. Hvis ingen verdi finnes, kontrollerer du IP-rutingen og VLAN-konfigurasjonen. Se dokumentet *Troubleshooting Switch Port and Interface Problems*, som du finner på denne URL-en:

https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

Trinn 5 Merk av for feltene IP-adresse, Subnett-maske og Standard ruter.

Hvis du tilordner en statisk IP-adresse til telefonen, må du angi innstillinger for disse alternativene manuelt.

Trinn 6 Hvis du bruker DHCP, kontrollerer du IP-adressene som DHCP-serveren distribuerer.

Se dokumentet *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*, som du finner på denne URL-en:

https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Opprette en ny telefonkonfigurasjonsfil

Når du fjerner en telefon fra Cisco Unified Communications Manager-databasen, slettes konfigurasjonsfilen fra TFTP-serveren for Cisco Unified Communications Manager. Telefonkatalognummeret eller -numrene blir beholdt i Cisco Unified Communications Manager-databasen. De kalles "utilordnede katalognumre" og kan brukes for andre enheter. Hvis utilordnede katalognumre ikke brukes av andre enheter, kan disse slettes fra Cisco Unified Communications Manager-databasen. Du kan bruke ruteplanrapporten til å vise og slette utilordnede referansenumre. Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din versjon av Cisco Unified Communications Manager.

Endring av knappene i en telefonknappmal, eller tilordning av en annen telefonknappmal til en telefon, kan føre til katalognumre som ikke lenger er tilgjengelige fra telefonen. Katalognumrene er fortsatt tilordnet til telefonen i Cisco Unified Communications Manager-databasen, men telefonen har ingen knapp til å besvare anrop med. Disse katalognumrene må fjernes fra telefonen og om nødvendig slettes permanent.

Prosedyre

Trinn 1 Fra Cisco Unified Communications Manager velger du **Enhet > Telefon** og klikker **Søk** for å finne telefonen som har problemer.

Trinn 2 Velg **Slett** for å fjerne telefonen fra Cisco Unified Communications Manager-databasen.

Merk Når du fjerner en telefon fra Cisco Unified Communications Manager-databasen, slettes konfigurasjonsfilen fra TFTP-serveren for Cisco Unified Communications Manager. Telefonkatalognummeret eller -numrene blir beholdt i Cisco Unified Communications Manager-databasen. De kalles "utilordnede katalognumre" og kan brukes for andre enheter. Hvis utilordnede katalognumre ikke brukes av andre enheter, kan disse slettes fra Cisco Unified Communications Manager-databasen. Du kan bruke ruteplanrapporten til å vise og slette utilordnede referansenumre.

Trinn 3 Legg til telefonen i Cisco Unified Communications Manager-databasen igjen.

Trinn 4 Slå telefonen av og på.

Beslektede emner

[Metoder for å legge til telefoner](#), på side 44

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Kontrollere DNS-innstillinger

Prosedyre

Trinn 1 Trykk på **Programmer**  på telefonen.

Trinn 2 Trykk på **Innstillinger** på telefonen.

Trinn 3 Velg **Nettverksoppsett > IPv4-oppsett**

Trinn 4 Kontroller at feltet DNS-Server 1 er riktig angitt.

Trinn 5 Du må også kontrollere at CNAME-oppføringen ble registrert på DNS-serveren for TFTP-serveren og for Cisco Unified Communications Manager-systemet.

Du må også sørge for at DNS er konfigurert til å utføre omvendte oppslag.

Starte tjeneste

En tjeneste må være aktivert før den kan startes eller stoppes.

Prosedyre

Trinn 1 Fra Cisco Unified Communications Manager Administration velger du **Cisco Unified Serviceability** i rullegardinlisten Navigasjon og klikker **Søk**.

Trinn 2 Velg **Verktøy > Kontrollsenter - funksjonstjenester**.

Trinn 3 Velg den primære Cisco Unified Communications Manager-serveren fra rullegardinlisten Server.

Vinduet viser tjenestene for serveren du valgte, statusen for tjenestene, og et tjenestekontrollpanel for å starte og stoppe en tjeneste.

Trinn 4 Hvis en tjeneste har stoppet, klikke du den tilsvarende alternativknappen og deretter **Start**.

Symbolet Tjenestestatus endres fra en firkant til en pil.

Kontrollere feilsøkingsinformasjon fra Cisco Unified Communications Manager

Hvis du har problemer med telefonen som du ikke kan løse selv, kan du få hjelp av Cisco TAC. Du må aktivere feilsøking for telefonen, gjenskape problemet, deaktivere feilsøking og sende loggene til TAC for analyse.

Feilsøking lagrer detaljert informasjon, og derfor går kommunikasjonstrafikken saktere på telefonen slik at den ikke responderer så raskt. Etter at du har lagret loggene, må du deaktivere feilsøking for at telefonen skal fungere normalt igjen.

Feilsøkingsinformasjonen inneholder kanskje en ensifret tallkode som gjenspeiler alvoret i situasjonen. Situasjoner er gradert på følgende måte:

- 0 - Nødsituasjon
- 1 - Varsel
- 2 - Kritisk
- 3 - Feil
- 4 - Advarsel
- 5 - Varsling
- 6 - Informasjon
- 7 - Feilsøking

Kontakt Cisco TAC for mer informasjon og for å få hjelp.

Prosedyre

Trinn 1

I Cisco Unified Communications Manager Administration velger du ett av følgende vinduer:

- **Enhet (Device) > Enhetsinnstillinger (Device settings) > Felles telefonprofil (Common Phone Profile)**
- **System > Konfigurasjon av bedriftstelefon (Enterprise Phone Configuration)**
- **Enhet (Device) > Telefon (Phone)**

Trinn 2

Angi følgende parametere:

- Loggprofil – verdier: Forhåndsinnstilt (standard), Standard, Telefoni, SIP, Brukergrensesnitt, Nettverk, Media, Oppgradering, Tilbehør, Sikkerhet, Energywise, MobileRemoteAccess
- Ekstern logg - verdier: Deaktiver (standard), Aktiver
- IPv6-loggsrerver eller Loggsrerver – IP-adresse (IPv4- eller IPv6-adresse)

Merk Når du ikke får kontakt med loggsrerveren, stopper telefonen å sende feilsøkingsmeldinger.

- Formatet for IPv4-loggserveradressen er **adresse**: <port>@@base=<0-7>;pfs=<0-1>
 - Formatet for IPv6-loggserveradressen er [**adresse**] :<port>@@base=<0-7>;pfs=<0-1>
 - Der:
 - IPv4-adressen er atskilt med en prikk (.)
 - IPv6-adressen er atskilt med et kolon (:)
-

Ekstra feilsøkingsinformasjon

Hvis du har flere spørsmål om feilsøking av telefonen, går du til følgende Cisco-nettsted og finner den ønskede telefonmodellen:

<https://www.cisco.com/cisco/web/psa/troubleshoot.html>



KAPITTEL 14

Internasjonal brukerstøtte

- [Installasjonsprogram for språk for endepunkter for Unified Communications Manager, på side 155](#)
- [Støtte for logging av utenlandssamtaler, på side 155](#)
- [Språkbegrensning, på side 156](#)

Installasjonsprogram for språk for endepunkter for Unified Communications Manager

Som standard blir Cisco IP-telefon konfigurert med språkinstillingen Engelsk - USA. For å bruke Cisco IP-telefoner fra andre steder, må du installere den spesifikke lokalspesifikke versjonen av endepunkter for Unified Communications Manager språkinstallasjonsprogram for hver Cisco Unified Communications Manager server i gruppen. Installasjonsprogrammet for språk installerer den nyeste oversatte teksten for telefonens brukergrensesnitt og landsspesifikke telefoner i systemet slik at det blir tilgjengelige for Cisco IP-telefon.

Hvis du vil ha tilgang til installasjonsprogrammet for språk som kreves for en versjon, går du til siden [Programvarenedlasting](#), navigerer til telefonmodellen og velger lenken for Unified Communications Manager endepunkts språkinstallasjonsprogram.

Hvis du vil ha mer informasjon, kan du se dokumentasjonen for din spesifikke Cisco Unified Communications Manager versjon.



Merk Den nyeste versjonen av installasjonsprogrammet for språk er kanskje ikke tilgjengelig. Se etter oppdateringer på nettstedet regelmessig.

Beslektede emner

[Dokumentasjon Cisco Unified Communications Manager](#), på side 10

Støtte for logging av utenlandssamtaler

Hvis telefonsystemet er konfigurert for logging av utenlandssamtaler (normalisering for oppringer), kan det hende oppføringene i anropslogger, logger for ny oppringing eller samtalelogger viser et plusstegn (+). Dette plusstegnet representerer det internasjonale retningsnummeret der du befinner deg. Avhengig av konfigurasjonen for ditt telefonsystem, kan det hende plusstegnet blir erstattet med den riktige internasjonale ringekoden, eller

du må kanskje endre nummeret før du ringer for å erstatte plusstegnet manuelt med det internasjonale retningsnummeret for stedet du befinner deg. Anropsloggen eller katalogoppføringen viser kanskje i tillegg hele utenlandsnummeret for det mottatte anropet, mens telefonen kanskje viser den forkortede lokale versjonen av nummeret uten retningsnumre eller landsnumre.

Språkbegrensning

Det er ikke støtte for lokalisert inntasting av alfanumerisk tekst (KATE) for følgende asiatiske språk:

- Kinesisk (Kina)
- Kinesisk (Hongkong)
- Kinesisk (Taiwan)
- Japansk (Japan)
- Koreansk (Republikken Korea)

Standard engelsk (USA) blir presentert for brukeren som inntastingsspråk i stedet.

Telefonskjermen vil for eksempel vises teksten på koreansk, men **2** -tasten på tastaturet vil vise **en b c 2**
A B C.