



Administrationsvejledning til Cisco IP-konferencetelefon 8832-serien til Cisco Unified Communications Manager

Første gang udgivet: 2017-09-15

Senest ændret: 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

SPECIFIKATIONERNE OG OPLYSNINGERNE OM PRODUKTERNE I DENNE MANUAL KAN ÆNDRES UDEN VARSEL. ALLE ERKLÆRINGER, OPLYSNINGER OG ANBEFALINGER I DENNE MANUAL MENES AT VÆRE KORREKTE, MEN ER ANGIVET UDEN GARANTI AF NOGEN ART, HVERKEN UDTRYKTE ELLER UNDERFORSTÅEDE. BRUGERNE HAR DET FULDE ANSVAR FOR ANVENDELSEN AF PRODUKTERNE.

SOFTWARELICENSEN OG DEN BEGRÆNSEDE GARANTI FOR DET MEDFØLGENDE PRODUKT ER ANFØRT I DEN INFORMATIONSPAKKE, DER FØLGER MED PRODUKTET, OG ER INDFØJET HERI MED DENNE REFERENCE. HVIS DU IKKE KAN FINDE SOFTWARELICENSEN ELLER DEN BEGRÆNSEDE GARANTI, SKAL DU KONTAKTE EN REPRÆSENTANT FRA CISCO FOR AT FÅ EN KOPI.

Følgende oplysninger er for FCC-overholdelse for Klasse A-enheder: Dette udstyr er blevet afprøvet og fundet i overensstemmelse med grænserne for en digital Klasse A-enhed i henhold til afsnit 15 i FCC-reglerne. Disse grænseværdier er bestemt, for at give en rimelig beskyttelse imod skadelig interferens, når udstyret betjenes i et kommercielt miljø. Dette udstyr opretter, bruger og kan udsende radiofrekvensenergi, og hvis det ikke er installeret og anvendt i overensstemmelse med instruktionshåndbogen, kan der opstå skadelig interferens for radiokommunikationen. Betjening af dette udstyr i et boligområde kan med stor sandsynlighed skabe skadelig interferens, og i så fald må brugerne udbedre problemet for egen regning.

Følgende oplysninger er for FCC-overholdelse for Klasse B-enheder: Dette udstyr er blevet afprøvet og fundet i overensstemmelse med grænserne for en digital Klasse B-enhed i henhold til afsnit 15 i FCC-reglerne. Disse grænser er beregnet til at give en rimelig beskyttelse mod skadelig interferens i en privat installation. Dette udstyr genererer, anvender og kan udsende radiofrekvensenergi, og hvis udstyret ikke er installeret og anvendes i overensstemmelse med brugervejledningen, kan det gribe forstyrrende ind i radiokommunikation. Der gælder dog ingen garanti for, at der ikke vil opstå interferens med en bestemt type installation. Hvis udstyret griber forstyrrende ind i radio- eller tv-modtagelse, hvilket kan kontrolleres ved at slukke og tænde udstyret, opfordres brugeren til at forsøge at udbedre forholdene på en af følgende måder:

- Drej modtagerantennen, eller placer den et andet sted.
- Sørg for større afstand mellem udstyret og modtageren.
- Slut udstyret til en stikkontakt i et andet kredsløb, end det som modtageren er tilsluttet.
- Kontakt en forhandler eller en kvalificeret radio-/tv-tekniker for at få hjælp.

Ændringer af dette produkt, som ikke er godkendt af Cisco, kunne annullere FCC-godkendelsen og ophæve din ret til at anvende produktet.

Cisco-implementering af TCP-headerkomprimering er en ændring af et program, der er udviklet af University of California, Berkeley (UCB) som en del af UCB's offentlige domæneversion af UNIX-operativsystemet. Alle rettigheder forbeholdes. Copyright © 1981, Regents of the University of California.

UAGTET EVENTUELLE ANDRE GARANTIER HERI LEVERES ALLE DOKUMENTER OG SOFTWAREN FRA DISSE LEVERANDØRER "SOM DE FORELIGGER" INKLUSIVE EVENTUELLE FEJL. CISCO OG OVENNÆVNTE LEVERANDØRER FRALÆGGER SIG ALLE GARANTIER, UDTRYKTE ELLER UNDERFORSTÅEDE, HERUNDER, MEN UDEN BEGRÆNSNING, GARANTIER FOR SALGBARHED, EGNETHED TIL BESTEMTE FORMÅL ELLER GARANTIER I FORBINDELSE MED KØB, BRUG ELLER HANDELSPRAKSIS.

CISCO ELLER DENNES LEVERANDØRER FRASKRIVER SIG ETHVERT ERSTATNINGSANSVAR FOR EVENTUELLE FØLGESKADER, DIREKTE ELLER INDIREKTE SKADER, HERUNDER, UDEN BEGRÆNSNING, TAB AF FORVENTEDE INDTÆGTER ELLER TABTE DATA SOM FØLGE AF BRUG ELLER MANGLENDE MULIGHED FOR AT BRUGE DENNE MANUAL, SELV I DE TILFÆLDE HVOR CISCO ELLER DENNES LEVERANDØRER ER BLEVET GJORT OPMÆRKSOM PÅ MULIGHEDEN FOR, AT SÅDANNE SKADER KAN OPSTÅ.

Eventuelle IP-adresser (Internet Protocol) og telefonnumre i nærværende dokument er ikke faktiske adresser og telefonnumre. Alle eksempler, skærbilleder, netværkstopologidiagrammer og øvrige figurer, som er inkluderet i dette dokument, vises kun i illustrativt øjemed. Enhver brug af faktiske IP-adresser eller telefonnumre i det illustrative indhold er utilsigtet og tilfældigt.

Alle trykte kopier og identiske softwarekopier af dette dokument betragtes som ikke-kontrollerede. Se den aktuelle onlineversion for den seneste version.

Cisco har over 200 kontorer på verdensbasis. Adresser og telefonnumre står på Ciscos website på www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017–2023 Cisco Systems, Inc. Alle rettigheder forbeholdes.



INDHOLD

KAPITEL 1

Nye og ændrede oplysninger 1

| | |
|---|---|
| Nye og ændrede oplysninger til firmwarefrigivelse 14.2(1) | 1 |
| Nye og ændrede oplysninger til firmwareversion 14.1(1) | 1 |
| Nye og ændrede oplysninger til firmwareversion 14.0(1) | 2 |
| Nye og ændrede oplysninger til firmwarefrigivelse 12.8(1) | 2 |
| Nye og ændrede oplysninger til firmwarefrigivelse 12.7(1) | 2 |
| Nye og ændrede oplysninger til firmwarefrigivelse 12.6(1) | 2 |
| Nye og ændrede oplysninger til firmwareversion 12.5(1)SR3 | 2 |
| Nye og ændrede oplysninger til firmwareversion 12.5(1)SR2 | 3 |
| Nye og ændrede oplysninger til firmwareversion 12.5(1)SR1 | 3 |
| Nye og ændrede oplysninger til firmwarefrigivelse 12.5(1) | 3 |
| Nye og ændrede oplysninger til firmwarefrigivelse 12.1(1) | 4 |

DEL I:

Om Cisco IP-konferencetelefon 7

KAPITEL 2

Cisco IP-konferencetelefon-hardware 9

| | |
|--|----|
| Cisco IP-konferencetelefon 8832 | 9 |
| Taster og hardware for Cisco IP-konferencetelefon 8832 | 11 |
| Kablet udvidelsesmikrofon (kun 8832) | 12 |
| Trådløs udvidelsesmikrofon (kun 8832) | 13 |
| Relateret dokumentation | 14 |
| Cisco IP-konferencetelefon 8832 – dokumentation | 14 |
| Cisco Unified Communications Manager Dokumentation | 14 |
| Cisco Unified Communications Manager Express Dokumentation | 14 |
| Dokumentation til Cisco Hosted Collaboration Service | 14 |
| Dokumentation til Cisco Business Edition 4000 | 14 |

Dokumentation, support og sikkerhedsretningslinjer 14

 Oversigt over sikkerhed for Cisco-produkter 15

Terminologiske forskelle 15

KAPITEL 3

Tekniske oplysninger 17

 Specifikationer til det fysiske og driftsmæssige miljø 17

 Telefonens strømkrav 18

 Strømafbrudelse 19

 Reduktion af strømforbrug 19

 Netværksprotokoller 20

 Interaktion med Cisco Unified Communications Manager 22

 Cisco Unified Communications Manager Express-interaktion 22

 Interaktion med telefonsvarersystem 23

 Telefonkonfigurationsfiler 23

 Telefonens virkemåde i tilfælde af netværksforsinkelse 24

 API (Application Programming Interface) 24

DEL II:

Installation af Cisco IP-konferencetelefon 25

KAPITEL 4

Installation af telefon 27

 Kontrollér netværksopsætningen 27

 Onboarding af aktiveringskode til lokale telefoner 28

 Onboarding af aktiveringskode og mobil- og fjernadgang 29

 Aktivér automatisk registrering for telefoner 29

 Tilstand med seriel ledningsføring 31

 Installér konferencetelefon 31

 Sådan slutter du mødetelefonen til strøm 32

 Installér de kablede udvidelsesmikrofoner 35

 Installér de trådløse udvidelsesmikrofoner 36

 Installér opladningsholderen til den trådløse mikrofon 37

 Installér konferencetelefon i tilstand med seriel ledningsføring 38

 Genstart din conferencefonen fra backupafbildning 39

 Konfigurer telefonen ved hjælp af opsætningsmenuerne 40

 Anvend en telefonadgangskode 41

| | |
|--|----|
| Tekst- og menuindtastning fra telefonen | 41 |
| Konfigurer netværksindstillingerne | 42 |
| Felter til netværksopsætning | 42 |
| Indstil feltet Domænenavn | 46 |
| Aktivér trådløst LAN fra telefonen | 46 |
| Konfigurer det trådløse LAN fra Cisco Unified Communications Manager | 47 |
| Konfigurer trådløst LAN på telefonen | 48 |
| Angiv antallet af WLAN-godkendelsesforsøg | 49 |
| Aktivér WLAN-beskedtilstand | 50 |
| Konfigurer en Wi-Fi-profil ved hjælp af Cisco Unified Communications Manager | 50 |
| Konfigurer en Wi-Fi gruppe ved hjælp af Cisco Unified Communications Manager | 52 |
| Kontrollér start af telefon | 53 |
| Skift en brugers telefonmodel | 53 |

KAPITEL 5
Telefoninstallation med Cisco Unified Communications Manager 55

| | |
|---|----|
| Konfigurer en Cisco IP-konferencetelefon | 55 |
| Bestem telefonens MAC-adresse | 59 |
| Metoder til tilføjelse af telefoner | 60 |
| Tilføj telefoner individuelt | 60 |
| Tilføj telefoner ved hjælp af BAT-telefonskabelon | 61 |
| Føj brugere til Cisco Unified Communications Manager | 61 |
| Tilføj en bruger fra en ekstern LDAP-telefonbog | 62 |
| Føj bruger direkte til Cisco Unified Communications Manager | 62 |
| Føj bruger til en slutbrugergruppe | 63 |
| Tilknyt telefoner til brugere | 63 |
| Survivable Remote Site Telephony | 64 |

KAPITEL 6
Styring af selvbetjeningsportal 67

| | |
|--|----|
| Oversigt over selvbetjeningsportal | 67 |
| Konfigurer brugeradgang til selvbetjeningsportalen | 67 |
| Tilpas visning af selvbetjeningsportal | 68 |

DEL III:
Administration af Cisco IP-konferencetelefon 69

KAPITEL 7**Sikkerhed i Cisco IP-konferencetelefon 71**

- Oversigt over sikkerhed for Cisco IP-telefon 71
- Sikkerhedsforbedringer til dit telefonnetværk 72
- Understøttede sikkerhedsfunktioner 73
 - Konfigurer et certifikat, der lokalt er væsentligt 75
 - Aktivér FIPS-tilstand 76
 - Telefonopkaldssikkerhed 76
 - Sikker identifikation af konferenceopkald 77
 - Sikker identifikation af telefonopkald 78
 - Sørg for kryptering ved bryd ind 79
 - WLAN-sikkerhed 79
 - Sikkerhed på trådløst LAN 82
 - Administrationsside for Cisco IP-telefon 82
 - Konfiguration af SCEP 85
 - 802.1X authenticering 86

KAPITEL 8**Tilpasning af Cisco IP-konferencetelefon 87**

- Brugerdefinerede ringetoner på telefon 87
 - Konfigurer en brugerdefineret telefonringning 87
 - Brugerdefinerede formater til ringningsfiler 88
- Tilpas opkaldstonen 89

KAPITEL 9**Funktioner og konfiguration af Cisco IP-konferencetelefon 91**

- Brugersupport til Cisco IP-telefon 91
- Migration af din telefon til en multiplatformstelefon med det samme 92
- Konfigurer ny programtastskabelon 92
- Konfigurer telefontjenester for brugere 93
- Konfiguration af telefonfunktioner 93
 - Konfigurer telefonfunktioner for alle telefoner 94
 - Konfigurer telefonfunktioner for en gruppe telefoner 95
 - Konfigurer telefonfunktioner for en enkelt telefon 95
 - Produktspecifik konfiguration 95
 - Deaktiver TLS-kryptering (Transport Layer Security) 108

| | |
|---|-----|
| Planlæg strømbesparelse for Cisco IP-telefon | 108 |
| Planlæg EnergyWise på Cisco IP-telefon | 110 |
| Konfigurer DND (Forstyr ikke) | 113 |
| Konfigurer besked om viderestilling af opkald | 114 |
| Konfiguration af UCR 2008 | 115 |
| Konfigurer UCR 2008 med fælles enhedskonfiguration | 115 |
| Konfigurer UCR 2008 i Almindelig telefonprofil | 116 |
| Konfigurer UCR 2008 i konfiguration af firmatelefon | 116 |
| Konfigurer UCR 2008 i telefon | 116 |
| Mobil og fjernadgang via Expressway | 117 |
| Installationsscenerier | 118 |
| Konfigurer bevarelse af brugerlegitimationsoplysninger for Expressway-logon | 119 |
| Problemrapporteringsværktøj | 119 |
| Konfigurer en URL-adresse til overførsel ved kundesupport | 119 |
| Indstil etiket for en linje | 121 |

KAPITEL 10
Firmatelefonbog og personlig telefonbog 123

| | |
|-----------------------------------|-----|
| Opsætning af firmatelefonbog | 123 |
| Opsætning af personlig telefonbog | 123 |

DEL IV:
Fejlfinding af Cisco IP-konferencetelefon 125

KAPITEL 11
Overvågning af telefonsystemer 127

| | |
|--|-----|
| Oversigt over overvågning af telefonsystemer | 127 |
| Status for Cisco IP-telefon | 127 |
| Vis vinduet Telefonoplysninger | 128 |
| Vis menuen Status | 128 |
| Vis vinduet Statusmeddelelser | 128 |
| Vis vinduet Netværksstatistik | 133 |
| Vis vinduet Opkaldsstatistik | 136 |
| Cisco IP-telefon-webside | 138 |
| Gå til telefonens webside | 138 |
| Webside med enhedsoplysninger | 138 |
| Webside med netværksopsætning | 140 |

| | |
|---|-------------------------------------|
| Webside med Ethernet-oplysninger | 144 |
| Websider med netværk | 145 |
| Websider til konsollogfiler, kenedumps, statusmeddelelser og visning af fejl | 146 |
| Webside med streamingstatistik | 146 |
| Anmod om oplysninger fra telefonen i XML | 149 |
| Eksempel på CallInfo-output | 149 |
| Eksempel på LineInfo-output | 150 |
| Eksempel på ModeInfo-output | 151 |
| <hr/> | |
| KAPITEL 12 | Fejlfinding på telefonen 153 |
| Generelle fejlfindingsoplysninger | 153 |
| Problemer ved start | 154 |
| Cisco IP-telefon gennemgår ikke den normale startproces | 154 |
| Cisco IP-telefon registreres ikke hos Cisco Unified Communications Manager | 155 |
| Telefon viser fejlmeddelelser | 156 |
| Telefon kan ikke oprette forbindelse til TFTP-server eller til Cisco Unified Communications Manager | 156 |
| Telefon kan ikke oprette forbindelse til TFTP-server | 156 |
| Telefon kan ikke oprette forbindelse til server | 156 |
| Telefon kan ikke oprette forbindelse via DNS | 157 |
| Cisco Unified Communications Manager og TFTP-tjenester kører ikke | 157 |
| Beskadigelse af konfigurationsfil | 157 |
| Registrering med Cisco Unified Communications Manager | 157 |
| Cisco IP-telefon kan ikke hente IP-adresse | 158 |
| Problemer ved nulstilling af problemer | 158 |
| Telefon nulstilles pga. periodiske netværksnedbrud | 158 |
| Telefon nulstilles pga. fejl i DHCP-indstillinger | 159 |
| Telefon nulstilles pga. forkert statisk IP-adresse | 159 |
| Telefon nulstilles under kraftig brug af netværket | 159 |
| Telefon nulstilles pga. tilsigtet nulstilling | 159 |
| Telefon nulstilles pga. DNS- eller andre forbindelsesproblemer | 160 |
| Telefonen tændes ikke | 160 |
| Telefon kan ikke oprette forbindelse til LAN | 160 |
| Sikkerhedsproblemer med Cisco IP-telefon | 160 |

| | |
|---|-----|
| Problemer med CTL-fil | 161 |
| Godkendelsesfejl, telefon kan ikke godkende CTL-fil | 161 |
| Telefon kan ikke godkende CTL-fil | 161 |
| CTL-fil godkender, men andre konfigurationsfiler gør ikke | 161 |
| ITL-fil godkender, men andre konfigurationsfiler gør ikke | 161 |
| TFTP-autorisationen mislykkedes | 162 |
| Telefonen registreres ikke | 162 |
| Signerede konfigurationsfiler er ikke anmodet | 162 |
| Lydproblemer | 163 |
| Ingen talesti | 163 |
| Ujævn tale | 163 |
| En telefon i tilstand med seriel ledningsføring fungerer ikke | 163 |
| Generelle problemer med telefonopkald | 164 |
| Telefonopkald kan ikke foretages | 164 |
| Telefon genkender ikke DTMF-cifre, eller cifre er forsinket | 164 |
| Fejlfindingsprocedurer | 164 |
| Opret en telefonproblemrapport fra Cisco Unified Communications Manager | 165 |
| Kontrollér TFTP-indstillinger | 165 |
| Bestem DNS- eller forbindelsesproblemer | 165 |
| Kontrollér DHCP-indstillinger | 166 |
| Opret en ny telefonkonfigurationsfil | 166 |
| Kontrollér DNS-indstillinger | 167 |
| Start tjeneste | 168 |
| Kontrollér fejlfindingsoplysninger fra Cisco Unified Communications Manager | 168 |
| Yderligere fejlfindingsoplysninger | 169 |

KAPITEL 13
Vedligeholdelse 171

| | |
|---|-----|
| Genstart eller nulstil konferencetelefonen | 171 |
| Genstart konferencetelefonen | 171 |
| Nulstil indstillingerne for konferencetelefonen i telefonmenuen | 171 |
| Nulstil konferencetelefonen til fabriksindstillingerne fra tastaturet | 172 |
| Overvågning af talekvalitet | 172 |
| Fejlfindingstip til talekvalitet | 173 |
| Rengøring af Cisco IP-telefon | 174 |

KAPITEL 14

International brugersupport 175

Unified Communications Manager Endpoints Locale Installer **175**

Understøttelse af logføring af internationale opkald **175**

Sprogbegrænsning **176**



KAPITEL 1

Nye og ændrede oplysninger

- Nye og ændrede oplysninger til firmwarefrigivelse 14.2(1), på side 1
- Nye og ændrede oplysninger til firmwareversion 14.1(1), på side 1
- Nye og ændrede oplysninger til firmwareversion 14.0(1), på side 2
- Nye og ændrede oplysninger til firmwarefrigivelse 12.8(1), på side 2
- Nye og ændrede oplysninger til firmwarefrigivelse 12.7(1), på side 2
- Nye og ændrede oplysninger til firmwarefrigivelse 12.6(1), på side 2
- Nye og ændrede oplysninger til firmwareversion 12.5(1)SR3, på side 2
- Nye og ændrede oplysninger til firmwareversion 12.5(1)SR2, på side 3
- Nye og ændrede oplysninger til firmwareversion 12.5(1)SR1, på side 3
- Nye og ændrede oplysninger til firmwarefrigivelse 12.5(1), på side 3
- Nye og ændrede oplysninger til firmwarefrigivelse 12.1(1), på side 4

Nye og ændrede oplysninger til firmwarefrigivelse 14.2(1)

Følgende oplysninger er nye eller ændrede for firmwareversion 14.2(1).

| Funktion | Ny eller ændret |
|-------------------------------------|---|
| Understøttelse af SIP OAuth på SRST | Sikkerhedsforbedringer til dit telefonnetværk, på side 72 |

Nye og ændrede oplysninger til firmwareversion 14.1(1)

Følgende oplysninger er nye eller ændrede for firmwareversion 14.1(1).

| Funktion | Ny eller ændret |
|---|---|
| SIP OAuth til proxy-TFTP-understøttelse | Sikkerhedsforbedringer til dit telefonnetværk, på side 72 |
| Migrering af telefon uden overgangsindlæsning | Migration af din telefon til en multiplatformstelefon med det samme, på side 92 |

Nye og ændrede oplysninger til firmwareversion 14.0(1)

Tabel 1: Nye og ændrede oplysninger

| Funktion | Ny eller ændret |
|--|---|
| Udvidet overvågning af parkering af opkald | Produktspecifik konfiguration, på side 95 |
| SIP OAuth-forbedringer | Sikkerhedsforbedringer til dit telefonnetværk, på side 72 |
| OAuth-forbedringer for MRA | Mobil og fjernadgang via Expressway, på side 117 |
| Forbedringer af brugergrænseflade | Survivable Remote Site Telephony, på side 64 |

Fra og med firmwareversion 14.0 understøtter telefonerne DTLS 1.2. DTLS 1.2 kræver Cisco ASA (Adaptive Security Appliance) version 9.10 eller senere. Du kan konfigurere den mindste DTLS-version for en VPN-forbindelse i ASA. Hvis du ønsker yderligere oplysninger, kan du se *ASDM Bog 3: Konfigurationsvejledning til Cisco ASA-serie VPN ASDM* på <https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html>

Nye og ændrede oplysninger til firmwaredrigivelse 12.8(1)

Følgende oplysninger er nye eller ændrede for firmware version 12.8 (1).

| Funktion | Nyt eller ændret indhold |
|---|---|
| Telefondataoverførsel | Skift en brugers telefonmodel, på side 53 |
| Tilføj yderligere oplysninger om feltet Webadgang | Produktspecifik konfiguration, på side 95 |

Nye og ændrede oplysninger til firmwaredrigivelse 12.7(1)

Der kræves ingen opdateringer af administrationsvejledning for firmwareversion 12.7(1).

Nye og ændrede oplysninger til firmwaredrigivelse 12.6(1)

Der kræves ingen opdateringer af administrationsvejledning for firmwareversion 12.6(1).

Nye og ændrede oplysninger til firmwareversion 12.5(1)SR3

Alle referencer til Cisco Unified Communications Manager-dokumentationen er blevet opdateret for at understøtte alle versioner af Cisco Unified Communications Manager.

Tabel 2: Ændringer af administrationsvejledningen til Cisco IP-telefon 8832 for firmwareversion 12.5(1)SR3

| Revision | Opdateret afsnit |
|---|--|
| Understøttelse af aktivering af aktiveringskode og mobil-og fjernadgang | Onboarding af aktiveringskode og mobil- og fjernadgang, på side 29 |
| Understøttelse af brug af problemlapporteringsværktøj fra Cisco Unified Communications Manager. | Opret en telefonproblemlapport fra Cisco Unified Communications Manager, på side 165 |

Nye og ændrede oplysninger til firmwareversion 12.5(1)SR2

Der kræves ingen administrationsopdateringer for firmwareversion 12.5(1)SR2.

Firmwareversion 12.5(1)SR2 erstatter firmwareversion 12.5(1) og firmware 12.5(1)SR1. Firmwareversion 12.5 (1) og firmware release 12.5 (1) SR1 er blevet udskudt til fordel af firmware version 12.5 (1) SR2.

Nye og ændrede oplysninger til firmwareversion 12.5(1)SR1

Følgende tabel beskriver ændringer, der er foretaget i *Administrationsvejledning til Cisco IP-konferencetelefon 8832 til Cisco Unified Communications Manager* for at understøtte firmwareversion 12.5(1)SR1.

Tabel 3: Ændringer af Cisco IP-konferencetelefon 8832-administrationsvejledningen til firmwareversion 12.5(1)SR1

| Revision | Afsnit med nyt eller opdateret |
|----------------------------------|--|
| Understøttelse af Elliptic Curve | Understøttede sikkerhedsfunktioner, på side 73 |

Nye og ændrede oplysninger til firmwaredfrigivelse 12.5(1)

Følgende tabel beskriver ændringer, der er foretaget i *Administrationsvejledning til Cisco IP-konferencetelefon 8832 til Cisco Unified Communications Manager*, for at understøtte firmwareversion 12.5(1).

Tabel 4: Ændringer af Cisco IP-konferencetelefon 8832-administrationsvejledningen til firmwareversion 12.5(1)

| Revision | Afsnit med nyt eller opdateret |
|---|--|
| Understøttelse af Whisper-personsøgning på Cisco Unified Communications Manager Express | Cisco Unified Communications Manager Express-interaktion, på side 22 |
| Understøttelse af deaktivering af TLS-kryptering | Produktspecifik konfiguration, på side 95 |
| Understøttelse af Enbloc-opkald til forbedring af T.302-tidsindstilling mellem cifre. | Produktspecifik konfiguration, på side 95 |

Nye og ændrede oplysninger til firmwarefrigivelse 12.1(1)

Følgende tabel beskriver ændringer i *Administrationsvejledning til Cisco IP-konferencetelefon 8832 til Cisco Unified Communications Manager* for at understøtte firmwareversion 12.1 (1).

| Revision | Afsnit med nyt eller opdateret |
|--|--|
| Understøttelse af Cisco IP-konferencetelefon 8832 – PoE-injektor | <ul style="list-style-type: none"> • Telefonens strømkrav, på side 18 • Sådan slutter du mødetelefonen til strøm, på side 32 • Installér konferencetelefon, på side 31 |
| Understøttelse af trådløse mikrofoner | <ul style="list-style-type: none"> • Cisco IP-konferencetelefon 8832, på side 9 • Trådløs udvidelsesmikrofon (kun 8832), på side 13 • Installér de trådløse udvidelsesmikrofoner, på side 36 • Installér opladningsholderen til den trådløse mikrofon, på side 37 |
| Understøttelse af seriel ledningsføring | <ul style="list-style-type: none"> • Cisco IP-konferencetelefon 8832, på side 9 • Tilstand med seriel ledningsføring, på side 31 • Installér konferencetelefon i tilstand med seriel ledningsføring, på side 38 • En telefon i tilstand med seriel ledningsføring fungerer ikke, på side 163 |
| Understøttelse af Cisco IP-konferencetelefon 8832 – ikke-PoE Ethernet-injektor | <ul style="list-style-type: none"> • Installér konferencetelefon, på side 31 • Sådan slutter du mødetelefonen til strøm, på side 32 |

| Revision | Afsnit med nyt eller opdateret |
|---|---|
| Understøttelse af Wi-Fi | <ul style="list-style-type: none">• Installér konferencetelefon, på side 31• Sådan slutter du mødetelefonen til strøm, på side 32• Indstil feltet Domænenavn, på side 46• Aktivér trådløst LAN fra telefonen, på side 46• Konfigurer det trådløse LAN fra Cisco Unified Communications Manager, på side 47• Konfigurer trådløst LAN på telefonen, på side 48• Angiv antallet af WLAN-godkendelsesforsøg, på side 49• Aktivér WLAN-beskedtilstand, på side 50• Konfigurer en Wi-Fi-profil ved hjælp af Cisco Unified Communications Manager, på side 50• Konfigurer en Wi-Fi gruppe ved hjælp af Cisco Unified Communications Manager, på side 52 |
| Understøttelse af Mobile and Remote Access Through Expressway | <ul style="list-style-type: none">• Mobil og fjernadgang via Expressway, på side 117• Installationsscenerier, på side 118• Konfigurer bevarelse af brugerlegitimationsoplysninger for Expressway-logon, på side 119 |
| Understøttelse af aktivering eller deaktivering af TLS 1.2 til webserveradgang. | Produktspecifik konfiguration, på side 95 |
| Understøttelse af G722.2 AMR-WB-lydcodec | <ul style="list-style-type: none">• Cisco IP-konferencetelefon 8832, på side 9• Felter til opkaldsstatistik, på side 136 |



DEL **I**

Om Cisco IP-konferencetelefon

- [Cisco IP-konferencetelefon-hardware, på side 9](#)
- [Tekniske oplysninger, på side 17](#)



KAPITEL 2

Cisco IP-konferencetelefon-hardware

- [Cisco IP-konferencetelefon 8832, på side 9](#)
- [Taster og hardware for Cisco IP-konferencetelefon 8832, på side 11](#)
- [Relateret dokumentation, på side 14](#)
- [Dokumentation, support og sikkerhedsretningslinjer, på side 14](#)
- [Terminologiske forskelle, på side 15](#)

Cisco IP-konferencetelefon 8832

Cisco IP-konferencetelefon 8832 og 8832NR forbedrer personorienterede meddelelser. Den kombinerer suveræn HD-lydresultater (HD) og 360 graders dækning til mellemstore og store mødelokaler og bestyrelseslokaler. Det giver en lydvenlig oplevelse med tovejs bredbåndslud (G.722) og håndfri højttaler med fuld duplex. Denne telefon er en enkel løsning, der kan klare udfordringerne i de mest forskelligartede rum.

Figur 1: Cisco IP-konferencetelefon 8832



Konferencetelefonen har følsomme mikrofoner med 360 graders dækning. Denne dækning lader dig tale i normalt stemmeleje, og de kan høres op til 3 meter væk. Telefonen har også teknologi, der kan modstå forstyrrelser fra mobiltelefoner og andre trådløse enheder, hvilket sikrer levering af tydelig kommunikation uden distraherende elementer. Telefonen har en farveskærm og programtaster, der giver adgang til

brugerfunktioner. Med basisenheden alene giver telefonen en dækning i et lokale på op til 6,1 x 6,1 m og op til 10 personer.

To kablede udvidelsesmikrofoner er tilgængelige til brug med telefonen. Hvis udvidelsesmikrofonerne placeres væk fra basisenheden giver det bedre dækning i større konferencerum. Med basisenheden og de kablede udvidelsesmikrofoner giver konferencetelefonen en dækning i et lokale på op til 6,1 x 10 m og op til 22 personer.

Telefonen understøtter et valgfrit sæt af to trådløse udvidelsesmikrofoner. Med basisenheden og de trådløse udvidelsesmikrofoner giver konferencetelefonen en dækning i et lokale på op til 6,1 x 12,2 m og op til 26 personer. For at dække et lokale på 6,1 m x 12,2 m anbefaler vi, at du placerer hver mikrofonen i en maksimal afstand på 3 meter fra basisenheden.

Du kan forbinde to basisenheder for at øge dækningen for et lokale. Denne konfiguration kræver det valgfrie sæt til serielle ledningsføring og kan understøtte op til to udvidelsesmikrofoner (enten kablede eller trådløse, men ikke en blandet kombination). Hvis du bruger kablede mikrofoner med det valgfrie sæt til serielle ledningsføring, giver konfigurationen dækning for et lokale op til 6,1 x 15,2 m) og op til 38 personer. Hvis du bruger trådløse mikrofoner med det valgfrie sæt til serielle ledningsføring, omfatter konfigurationen dækning for et lokale op til 6,1 x 17,4 m og op til 42 personer.

Cisco IP-konferencetelefon 8832NR-versionen (ikke radio) understøtter ikke Wi-Fi, trådløse udvidelsesmikrofoner eller Bluetooth.

En Cisco IP-telefon kan som andre enheder konfigureres og styres. Disse telefoner koder og dekoder følgende codecs:

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



Advarsel Når du bruger en mobiltelefon, GSM-telefon eller tovejsradio i nærheden af en Cisco IP-telefon, kan der opstå interferens. Få flere oplysninger ved at se producentens dokumentation til den enhed, der giver interferens.

Cisco IP-telefoner har traditionel telefonifunktionalitet som f.eks. viderestilling af opkald og omstilling, hurtigopkald, conferenceopkald og adgang til telefonsvarersystem. Cisco IP-telefoner har også en række andre funktioner.

Som det gælder for andre netværksenheder, skal du konfigurere en Cisco IP-telefon, så den er klar til at få adgang til Cisco Unified Communications Manager og resten af IP-netværket. Når du bruger DHCP, har du færre indstillinger til at konfigurere en telefon. Hvis dit netværk kræver det, kan du imidlertid manuelt konfigurere oplysninger som f.eks.: oplysninger om en IP-adresse, TFTP-server og undernet.

Cisco IP-telefoner kan interagere med andre tjenester og enheder på dit IP-netværk, så du får en bedre funktionalitet. Du kan f.eks. integrere Cisco Unified Communications Manager med

LDAP3-standardfirmatelefonbogen (Lightweight Directory Access Protocol 3) for at give brugere mulighed for at søge efter kollegers kontaktoplysninger direkte fra deres IP-telefoner. Du kan også bruge XML til at give brugere mulighed for at få oplysninger som f.eks. vejret, aktier, dagens citat og andre webbaserede oplysninger.

Da Cisco IP-telefon er en netværksenhed, kan du derudover få detaljerede statusoplysninger direkte fra den. Disse oplysninger kan hjælpe dig med fejlfinding af problemer, som brugere kan støde på, når de bruger deres IP-telefoner. Du kan også få statistik om et aktivt opkald eller telefonens firmwareversioner.

For at kunne fungere på et IP-telefonnetværk skal Cisco IP-telefon oprette forbindelse til en netværksenhed som f.eks. en Cisco Catalyst-switch. Du skal også registrere Cisco IP-telefon i et Cisco Unified Communications Manager system-system, før der sendes og modtages opkald.

Taster og hardware for Cisco IP-konferencetelefon 8832

Følgende figur viser Cisco IP-konferencetelefon 8832.





Figur 2: Taster og funktioner for Cisco IP-konferencetelefon 8832



Følgende tabel beskriver knapperne på Cisco IP-konferencetelefon 8832.

Table 5: Knapper på Cisco IP-konferencetelefon 8832

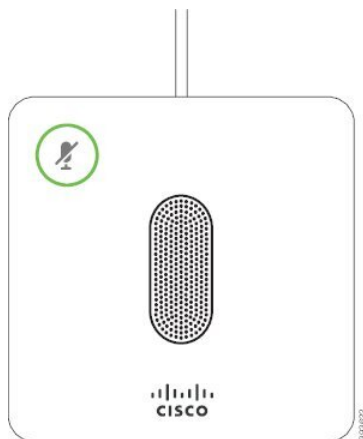
| | | |
|---|------------|--|
| 1 | LED-bjælke | <p>Indikerer opkaldstilstande:</p> <ul style="list-style-type: none"> • Grønt lys = aktivt opkald • Grønt blink = indgående opkald • Grønt, pulserende = parkeret opkald • Rødt lys = lydløst opkald |
|---|------------|--|


| | | |
|---|--------------------------------------|--|
| 2 | Port til udvidelsesmikrofon | Kabelstik til kablet udvidelsesport i porten. |
| 3 | Bjælken Slå lyd fra |  Slår mikrofonen til eller fra. Når mikrofonen er slået fra, lyser LED-bjælken rødt. |
| 4 | Programtaster |  Få adgang til funktioner og tjenester. |
| 5 | Navigationslinje og Vælg-knap |  Rul gennem menuer, marker elementer, og vælg det markerede element. |
| 6 | Lydstyrke-tast |  Juster lydstyrken for højtalertelefonen (løftet rør) og ringetonen (røret lagt på). Når du ændrer lydstyrken, lyser LED-bjælken hvidt for at vise ændringen i lydstyrken. |

Kablet udvidelsesmikrofon (kun 8832)

Cisco IP-konferencetelefon 8832 understøtter to kablede udvidelsesmikrofoner, der er tilgængelige i et valgfrit sæt. Brug udvidelsesmikrofonerne i større lokaler eller i et overfyldt lokale. For at få det bedste resultat anbefaler vi, at mikrofonerne placeres mellem 0,91 m og 2,1 m væk fra telefonen.

Figur 3: Kablet udvidelsesmikrofon



Når du er i gang med et opkald, lyser udvidelsesmikrofonens LED rundt om knappen **Slå lyd fra**  grønt. Når mikrofonens lyd er slået fra, lyser LED'en rødt. Når du trykker på knappen **Slå lyd fra**, slås lyden på telefonen og udvidelsesmikrofonerne fra.

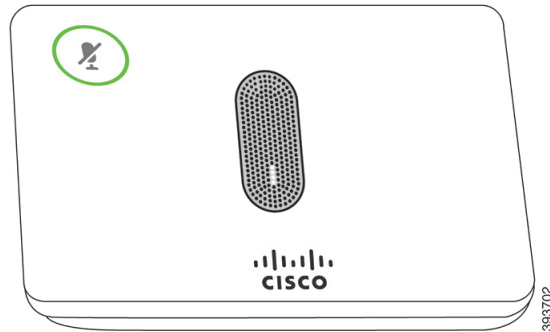
Lignende emner

[Installér de kablede udvidelsesmikrofoner](#), på side 35

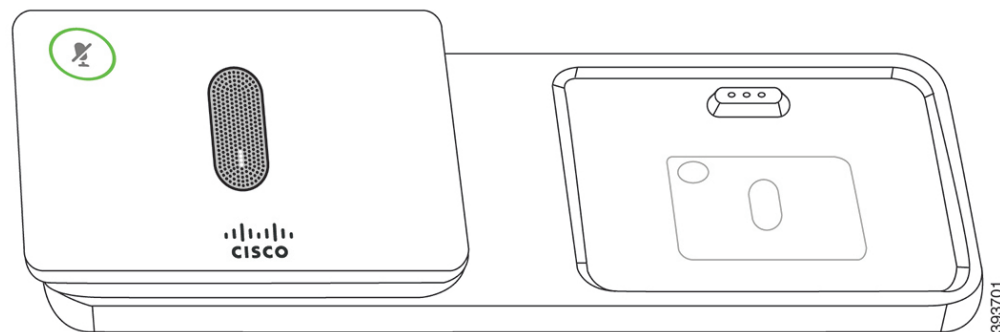
Trådløs udvidelsesmikrofon (kun 8832)


Cisco IP-konferencetelefon 8832 understøtter to kablede udvidelsesmikrofoner, der er tilgængelige med en opladningsholder i et valgfrit sæt. Når den trådløse mikrofon er placeret på opladningsholderen for at blive opladt, lyser LED'en på holderen hvidt.

Figur 4: Trådløs mikrofon



Figur 5: Trådløs mikrofon monteret på opladningsholderen



Når konferencetelefonen er i et opkald, lyser udvidelsesmikrofonens LED rundt om knappen **Slå lyd fra**  grønt.

Når mikrofonen er slået fra, lyser LED'en rødt. Når du trykker på knappen **Slå lyd fra**, slås lyden på telefonen og udvidelsesmikrofonerne fra.

Hvis telefonen er parret med en trådløs mikrofon (for eksempel trådløs mikrofon 1), og du tilslutter den trådløse mikrofon til opladeren, kan du se opladningsniveauet for den pågældende mikrofon ved at trykke på programtasten **Vis detaljer**.

Når telefonen er parret med en trådløs mikrofon og du tilslutter en kablede mikrofon, annulleres pardannelsen for den trådløse mikrofon, og telefonen parres med kablede mikrofon. Der vises en meddelelse på telefonskærmen, der angiver, at den kablede mikrofon er tilsluttet.

Lignende emner

[Installér de trådløse udvidelsesmikrofoner](#), på side 36

[Installér opladningsholderen til den trådløse mikrofon](#), på side 37

Relateret dokumentation

Du kan bruge følgende afsnit til at finde relaterede oplysninger.

Cisco IP-konferencetelefon 8832 – dokumentation

Find dokumentation, der er specifik for dit sprog, din telefonmodel og dit opkaldskontrolsystem på siden for [produktstøtte](#) for Cisco IP-telefon 7800-serien.

Cisco Unified Communications Manager Dokumentation

Se *Cisco Unified Communications Manager-dokumentationsvejledningen* og andre publikationer, der er specifikke for din version af Cisco Unified Communications Manager. Du kan starte med følgende URL til dokumentation:

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

Cisco Unified Communications Manager Express Dokumentation

Se de publikationer, der er specifikke for dit sprog, din telefonmodel og version af Cisco Unified Communications Manager Express. Du kan starte med følgende URL til dokumentation:

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

Dokumentation til Cisco Hosted Collaboration Service

Se *Cisco Hosted Collaboration Solution-dokumentationsvejledningen* og andre publikationer, der er specifikke for din version af Cisco Hosted Collaboration Solution. Du kan starte med følgende URL:

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

Dokumentation til Cisco Business Edition 4000

Se *Cisco Business Edition 4000-dokumentationsvejledningen* og andre publikationer, der er specifikke for din version af Cisco Business Edition 4000. Du kan starte med følgende URL:

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

Dokumentation, support og sikkerhedsretningslinjer

Få oplysninger om indhentning af dokumentation, indhentning af support, afgivelse af feedback om dokumentation, gennemgang af retningslinjer for sikkerhed og også anbefalede aliasser og generelle

Cisco-dokumenter i den månedlige udgivelse *What's New in Cisco Product Documentation* (Nyheder i Cisco-produktdokumentation), der også viser alt ny og revideret teknisk Cisco-dokumentation på:

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

Abonner på *What's New in Cisco Product Documentation* som et RSS (Really Simple Syndication)-feed, og indstil indholdet til at blive sendt direkte til din computer ved hjælp af et læserprogram. RSS-feeds er en gratis tjeneste, og Cisco understøtter p.t. RSS-version 2.0.

Oversigt over sikkerhed for Cisco-produkter

Dette produkt indeholder kryptografiske funktioner og er underlagt amerikansk lovgivning samt den lokale lovgivning i andre lande, for så vidt angår import, eksport, overførsel og brug. Levering af Ciscos kryptografiske produkter medfører ikke, at tredjemand har tilladelse til at importere, eksportere, distribuere eller anvende kryptering. Det er importørernes, eksportørernes, distributørernes og brugernes eget ansvar at sørge for, at de amerikanske eller lokale regler overholdes. Ved at tage dette produkt i brug erklærer du dig indforstået med at overholde de gældende love og regler. Hvis du ikke kan overholde de amerikanske eller lokale regler, bedes du returnere produktet med det samme.

Du kan finde yderligere oplysninger om amerikansk eksportregler på <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>.

Terminologiske forskelle

I dette dokument omfatter betegnelsen *Cisco IP-telefon* Cisco IP-konferencetelefon 8832.

Følgende tabel fremhæver nogle af terminologiforskellene i *Brugervejledning til Cisco IP-konferencetelefon 8832*, *Administrationsvejledning til Cisco IP-konferencetelefon 8832 for Cisco Unified Communications Manager* og Cisco Unified Communications Manager-dokumentationen.

Tabel 6: Terminologiske forskelle

| Brugervejledning | Administrationsvejledning |
|------------------------|---|
| Meddelelsesindikatorer | Indikator for ventende meddelelse (MWI) |
| Voicemail-system | Telefonsvarersystem |



KAPITEL 3

Tekniske oplysninger

- [Specifikationer til det fysiske og driftsmæssige miljø, på side 17](#)
- [Telefonens strømkrav, på side 18](#)
- [Netværksprotokoller, på side 20](#)
- [Interaktion med Cisco Unified Communications Manager, på side 22](#)
- [Cisco Unified Communications Manager Express-interaktion, på side 22](#)
- [Interaktion med telefonsvarersystem, på side 23](#)
- [Telefonkonfigurationsfiler, på side 23](#)
- [Telefonens virkemåde i tilfælde af netværksforsinkelse, på side 24](#)
- [API \(Application Programming Interface\), på side 24](#)

Specifikationer til det fysiske og driftsmæssige miljø

Følgende tabel viser specifikationerne til det fysiske og driftsmæssige miljø for konferencetelefonen.

Tabel 7: Fysiske og driftsmæssige specifikationer

| Specifikation | Værdi eller interval |
|---------------------------------|--|
| Driftstemperatur | 0 til 40 °C |
| Relativ luftfugtighed ved drift | 10 til 90 % (ingen kondensdannelse) |
| Opbevaringstemperatur | -10 til 60 °C |
| Højde | 278 mm |
| Bredde | 278 mm |
| Dybde | 61,3 mm |
| Vægt | 1852 g |
| Strøm | IEEE PoE-klasse 3 via en PoE-injektor. Telefonen er kompatibel med Discovery Protocol og Link Layer Discovery Protocol - Power over Ethernet. Andre indstillinger omfatter en PoE Ethernet-injektor, hvis de forberedes. En PoE Ethernet-injektor eller PoE-strømadapter er nødvendig ved Wi-Fi-installation. |

| Specifikation | Værdi eller interval |
|----------------------|---|
| Sikkerhedsfunktioner | Sikker start |
| Kabler | USB-C |
| Afstandskrav | Ethernet-specifikation antager, at den maksimale kabellængde mellem |

Få flere oplysninger i *dataarket til Cisco IP-konferencetelefon 8832*: <https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html>

Telefonens strømkrav

Cisco IP-konferencetelefon 8832 kan bruge disse strømkilder:

- PoE-installation (Power over Ethernet) med en Cisco IP-konferencetelefon 8832 – PoE-injektor
- Installationen uden PoE Ethernet med Cisco IP-konferencetelefon 8832 – ikke-PoE Ethernet-injektor
- En Cisco IP-konferencetelefon 8832-strømadapter er nødvendig ved Wi-Fi-installation.

Tabel 8: Retningslinjer for strøm til Cisco IP-konferencetelefon

| Strømtype | Retningslinjer |
|---|--|
| PoE-strøm - leveres af enten Cisco IP-konferencetelefon 8832 – PoE-injektor eller Cisco IP-konferencetelefon 8832 – Ethernet-injektor via det USB-C-kabel, der er tilsluttet telefonen. | <p>Hvis du bruger enten Cisco IP-konferencetelefon 8832 – PoE-injektor eller Cisco IP-konferencetelefon 8832 – Ethernet-injektor, skal du sikre, at switchen har en ekstra strømforsyning, så du kan bruge telefonen uden afbrydelser.</p> <p>Sørg for, at den CatOS eller IOS-version, der kører på din switch, understøtter din tilsigtede telefoninstallation. Se dokumentationen til din switch for at få oplysninger om operativsystemversioner.</p> <p>Når du installerer en telefon, der får strøm fra PoE, skal du tilslutte injektoren til LAN'et, før du kobler USB-C-kablet til telefonen. Når du fjerner en telefon, der benytter PoE, skal du tage USB-C-kablet ud af telefonen, før du fjerner strømmen fra adapteren.</p> |

| Strømtype | Retningslinjer |
|--|---|
| Ekstern strøm <ul style="list-style-type: none"> • Installationen uden PoE Ethernet med Cisco IP-konferencetelefon 8832 – ikke-PoE Ethernet-injektor • En Cisco IP-konferencetelefon 8832-strømadapter er nødvendig ved Wi-Fi-installation. • Ikke-PoE Ethernet-konfiguration med en Cisco IP-konferencetelefon 8832 – Ethernet-injektor og en Cisco IP-konferencetelefon 8832-strømadapter | Når du installerer en telefon, der får strøm fra en ekstern kilde, skal du forbinde injektoren til strømforsyningen og til Ethernet, før du kobler USB-C-kablet til telefonen. Når du fjerner en telefon, der benytter en ekstern strømkilde, skal du tage USB-C-kablet ud af telefonen, før du fjerner strømmen fra adapteren. |

Strømafbrydelse

Du kan kun foretage nødopkald fra telefonen, hvis den er tilsluttet strøm. Hvis der opstår strømafbrydelse, kan du ikke foretage service- og nødopkald, før der igen er strøm. I tilfælde af strømsvigt eller andre forstyrrelser kan du være nødt til at nulstille eller omkonfigurere udstyret, før du kan bruge service- og nødopkald igen.

Reduktion af strømforbrug

Du kan reducere den mængde energi, som Cisco IP-telefon forbruger, ved at bruge strømbesparelse eller EnergyWise-tilstanden (Power Save Plus).

Strømbesparelse

I tilstanden Strømbesparelse tændes skærmens baggrundsbelysning ikke, når telefonen ikke er i brug. Telefonen forbliver i strømbesparellestilstanden i den planlagte varighed, eller indtil brugeren trykker på en knap.

Strømbesparelse plus (EnergyWise)

Cisco IP-telefon understøtter Cisco EnergyWise-tilstanden (strømbesparelse plus). Når dit netværk har en EnergyWise-controller (EW) (f.eks. en Cisco-switch, hvor EnergyWise-funktionen er aktiveret), kan du konfigurere disse telefoner til at gå i dvale (strømforbrug ned) og vågne (strømforbrug op) efter en tidsplan for yderligere at reducere strømforbruget.

Indstil hver enkelt telefon til at aktivere eller deaktivere EnergyWise-indstillingerne. Hvis EnergyWise er aktiveret, kan du konfigurere en dvale- og opvågningstid samt andre parametre. Disse parametre sendes til telefonen som del af XML-filen til telefonkonfiguration.

Lignende emner

[Planlæg strømbesparelse for Cisco IP-telefon](#), på side 108

[Planlæg EnergyWise på Cisco IP-telefon](#), på side 110

Netværksprotokoller

Cisco IP-konferencetelefon 8832 understøtter adskillige branchestandarder og Cisco-netværksprotokoller, der kræves til talekommunikation. Følgende tabel indeholder en oversigt over netværksprotokoller, som telefonerne understøtter.

Tabel 9: Understøttede netværksprotokoller på Cisco IP-konferencetelefon

| Netværksprotokol | Formål | Forbrugsnoter |
|--|---|---|
| BootP (Bootstrap Protocol) | BootP gør det muligt for en netværksenhed, f.eks. telefonen, at opdage bestemte startoplysninger som f.eks. dens IP-adresse. | – |
| CDP (Cisco Discovery Protocol) | CDP er en protokol til registrering af enheder, der kører alt udstyr, som Cisco har fremstillet. En enhed kan bruge CDP til at give meddelelse om sin eksistens til andre enheder og modtage oplysninger om andre enheder på netværket. | Telefonen bruger CDP til at kommunikere oplysninger om konfigurationen af servicekvaliteter. |
| DHCP (Dynamic Host Configuration Protocol) | DHCP allokerer og tildeler dynamisk en IP-adresse til netværksenheder. DHCP gør det muligt at forbinde en IP-telefon med netværket og få telefonen til at virke uden manuelt at skulle tildele en IP-adresse eller konfigurere ekstra netværksparametre. | DHCP er aktiveret som standard. Hvis indstillingen gatewayen og en TFTP-server lokalt på hver telefon. Vi anbefaler, at du bruger den brugerdefinerede DHCP IP-adresse som indstillingsværdien. Du kan læse mere om den specifikke version af Cisco Unified Communications Manager. Bemærk Hvis du ikke kan bruge indstilling 150, |
| Hypertext Transfer Protocol (HTTP) | HTTP er standardprotokollen for overførsel af oplysninger og flytning af dokumenter på tværs af internettet. | Telefoner anvender HTTP til XML-tjenester, klargø |
| HTTPS (Hypertext Transfer Protocol Secure) | HTTPS (Hypertext Transfer Protocol Secure) er en kombination af Hypertext Transfer Protocol og SSL/TLS-protokollen, der sikrer kryptering og sikker serveridentifikation. | Webapplikationerne med både HTTP- og HTTPS-URL'erne. HTTPS, vælger HTTPS URL-adressen. Der vises et låseikon til brugeren, hvis forbindelse t |
| IEEE 802.1X | IEEE 802.1X-standarden definerer en klient-server-baseret adgangskontrol og godkendelsesprotokol, der begrænser uautoriserede klienter i at oprette forbindelse til et LAN via offentligt tilgængelige porte. Indtil klienten er godkendt, tillader 802.1x-adgangskontrol kun EAPOL (Extensible Authentication Protocol) over LAN-trafik gennem den port, som klienten er tilsluttet. Når godkendelsen er lykkedes, kan normal trafik passere gennem porten. | Telefonen implementerer IEEE 802.1X-standarden. Når 802.1X-godkendelse er aktiveret på telefonen, l |
| IP (Internet Protocol) | IP er en beskedprotokol, der håndterer og sender pakker på tværs af netværket. | For at kommunikere med IP skal netværksenheder h Identifikation af IP-adresser, undernet og gateway (Dynamic Host Configuration Protocol). Hvis du ikke bruger DHCP Telefonerne understøtter IPv6-adresser. Få flere oplysninger om Cisco Unified Communications Manager. |

| Netværksprotokol | Formål | Forbrugsnoter |
|---|---|---|
| LLDP (Link Layer Discovery Protocol) | LLDP er en standardiseret protokol til netværksregistrering (i lighed med CDP), der er understøttet på Cisco-enheder og tredjepartsenheder. | Telefonen understøtter LLDP på pc-porten. |
| Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED) | LLDP-MED er en udvidelse af LLDP-standarden, der er udviklet til taleprodukter. | Telefonen understøtter LLDP-MED på SW-porten. <ul style="list-style-type: none"> • Konfiguration af tale-VLAN • Enhedsregistrering • Strømstyring • Lagerstyring Få flere oplysninger om LLDP-MED-understøttede URL-adresse: https://www.cisco.com/en/US/tech/tk652/tk701/ |
| RP (Real-Time Transport Protocol) | RTP er en standardprotokol for transport af realtidsdata som f.eks. interaktiv tale og video over datanetværk. | Telefoner anvender RTP-protokollen til at sende |
| RTCP (Real-Time Control Protocol) | RTCP virker sammen med RTP for at levere QoS-data (f.eks. forvrængning, forsinkelse og forsinkelse for rundtur) på RTP-streams. | RTCP er aktiveret som standard. |
| SDP (Session Description Protocol) | SDP er del af SIP-protokollen, der bestemmer, hvilke parametre der er tilgængelige under en forbindelse mellem to slutpunkter. Konferencer oprettes ved kun at bruge de SDP-funktioner, som alle slutpunkter i konferencen understøtter. | SDP-funktioner såsom codec-typer, DTMF-registrering, Manager eller Media Gateway i drift. Nogle SIP |
| SIP (Session Initiation Protocol) | SIP er IETF-standarden (Internet Engineering Task Force) for multimediekonferencer over IP. SIP er en ASCII-baseret kontrolprotokol for programlag (defineret i RFC 3261), der kan bruges til at etablere, opretholde og afslutte opkald mellem to eller flere slutpunkter. | Lige som andre VoIP-protokoller er SIP designet til et pakketelefoninetsværk. Signaler gør det muligt for Sessionsadministration giver muligheden for at |
| SRTP (Secure Real-Time Transfer Protocol) | SRTP er en udvidelse af lyd-/videoprofilen for RTP (Real-Time Protocol) og sikrer integriteten af RTP- og RTCP-pakker, hvilket giver godkendelse, integritet og kryptering af mediepakker mellem to slutpunkter. | Telefoner anvender SRTP til mediekryptering. |
| TCP (Transmission Control Protocol) | TCP er en forbindelsesorienteret transportprotokol. | Telefoner anvender TCP til at oprette forbindelse |
| TLS (Transport Layer Security) | TLS er en standardprotokol til sikring og godkendelse af kommunikation. | Når sikkerhed er implementeret, anvender telefoner Manager. Få flere oplysninger i dokumentatione |
| TFTP (Trivial File Transfer Protocol) | TFTP gør det muligt at overføre filer over netværket. På telefonen gør TFTP det muligt at hente en konfigurationsfil, der er specifik for telefontypen. | TFTP kræver en TFTP-server på dit netværk, so skal anvende en anden TFTP-server end den, der ved at bruge menuen Netværksopsætning på tele Få flere oplysninger i dokumentationen til din sp |

| Netværksprotokol | Formål | Forbrugsnoter |
|------------------------------|--|--|
| UDP (User Datagram Protocol) | UDP er en forbindelsesløs beskedprotokol til levering af datapakker. | UDP bruges kun til RTP-streams. SIP-signaler på te |

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Interaktion med Cisco Unified Communications Manager

Cisco Unified Communications Manager er et åbent system til behandling af opkald og en industristandard. Cisco Unified Communications Manager-software konfigurerer og opdeler opkald mellem telefoner og integrerer traditionelle PBX-funktioner med firmaets IP-netværk. Cisco Unified Communications Manager administrerer komponenterne i IP-telefonisystemet som f.eks. de telefoner, adgangsgateways og ressourcer, der kræves til funktioner som f.eks. brug af opkaldskonference og ruteplanlægning. Cisco Unified Communications Manager har også:

- Firmware til telefoner
- CTL- (Certificate Trust List) og ITL-filer (Identity Trust List), der bruges i forbindelse med TFTP- og HTTP-tjenester
- Telefonregistrering
- Bevarelse af opkald, så mediesessionen fortsætter, selvom signalet mellem den primære kommunikationsstyring og en telefon går afbrydes

Få oplysninger om, hvordan du konfigurerer Cisco Unified Communications Manager til at virke sammen med de IP-telefoner, der er beskrevet i dette kapitel, ved at se dokumentationen til din specifikke version af Cisco Unified Communications Manager.

**Bemærk**

Hvis den telefonmodel, du vil konfigurere, ikke vises på rullelisten over telefontyper i Cisco Unified Communications Manager Administration, skal du installere den seneste enhedspakke til din version af Cisco Unified Communications Manager fra Cisco.com.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Cisco Unified Communications Manager Express-interaktion

Når din telefon bruges sammen med Cisco Unified Communications Manager Express (Unified CME), skal den være i CME-tilstand.

Når brugeren aktiverer konferencefunktionen, gør koden det muligt for telefonen at bruge enten en lokalt baseret eller netværksbaseret hardwarekonferencebro.

Telefonerne understøtter ikke følgende handlinger:

- Viderestilling – understøttes kun i scenarie med viderestilling af forbundet opkald.

- Konference – understøttes kun i scenarie med viderestilling af forbundet opkald.
- Deltag – understøttes ved brug af konferenceknappen eller Hookflash-adgang.
- Parkér – understøttes ved hjælp af parkeringsknappen.
- Bryd ind og flet – understøttes ikke.
- Direkte viderestilling – understøttes ikke.
- Vælg – understøttes ikke.

Brugerne kan ikke oprette konference og overføre opkald på tværs af linjer.

Unified CME understøtter samtaleanlægsopkald, også kendt som whisper-personsøgning. Men siden afvises af telefonen under opkald.

Interaktion med telefonsvarersystem

Cisco Unified Communications Manager gør det muligt at integrere med andre telefonsvarersystemer, herunder Cisco Unity Connection-telefonsvarersystemet. Da du kan integrere med forskellige systemer, skal du give brugerne oplysninger om, hvordan dit specifikke system skal bruges.

Hvis du vil aktivere muligheden for, at en bruger kan viderestille til voicemail, skal du konfigurere et *xxxxx-opkaldsmønster og konfigurere det som viderestil alle opkald til voicemail. Få flere oplysninger i dokumentationen til Cisco Unified Communications Manager.

Angiv følgende oplysninger for hver bruger:

- Hvordan du får adgang til kontoen til telefonsvarersystemet.
Sørg for, at du har brugt Cisco Unified Communications Manager til at konfigurere beskedknappen på Cisco IP-telefon.
- Indledende adgangskode for at få adgang til telefonsvarersystemet.
Konfigurer en standardadgangskode til voicemail-systemet for alle brugere.
- Hvordan telefonen angiver, at der venter beskeder på telefonsvarer.
Brug Cisco Unified Communications Manager til at konfigurere en MWI-metode (message waiting indicator).

Telefonkonfigurationsfiler

Konfigurationsfiler for en telefon er gemt på TFTP-serveren og definerer parametrene for at oprette forbindelse til Cisco Unified Communications Manager. Generelt er det sådan, at hver gang du foretager en ændring i Cisco Unified Communications Manager, der kræver, at telefonen skal nulstilles, foretages der automatisk en ændring af telefonkonfigurationsfilen.

Konfigurationsfiler indeholder også oplysninger om, hvilken afbildningsindlæsning telefonen skal køre. Hvis denne afbildningsindlæsning afviger fra den, der er indlæst på en telefon, kontakter telefonen TFTP-serveren for at anmode om de krævede indlæsningsfiler.

Hvis du konfigurerer sikkerhedsmæssige indstillinger i Cisco Unified Communications Manager Administration, indeholder telefonkonfigurationsfilen følsomme oplysninger. For at sikre fortroligheden af en konfigurationsfil skal du konfigurere den til kryptering. Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager. En telefon anmoder om en konfigurationsfil, når den nulstilles og registreres i Cisco Unified Communications Manager.

En telefon har adgang til en standardkonfigurationsfil, der hedder XmlDefault.cnf.xml, på TFTP-serveren, når følgende betingelser er opfyldt:

- Du har aktiveret automatisk registrering i Cisco Unified Communications Manager
- Telefonen ikke er blevet føjet til Cisco Unified Communications Manager-databasen
- Telefonen bliver registreret for første gang

Telefonens virkemåde i tilfælde af netværksforsinkelse

Alt, der nedsætter netværkets ydeevne, kan påvirke telefonens lyd og i visse tilfælde forårsage et afbrudt opkald. Kilder til nedsat netværksydeevne kan være, men er ikke begrænset til, følgende aktiviteter:

- Administrative opgaver, som f.eks. interne portscanninger eller sikkerhedsscanninger.
- Angreb på netværket i form af f.eks. Denial of Service-angreb.

API (Application Programming Interface)

Cisco understøtter tredjepartsprogrammernes brug af telefon-API, hvor disse programmer er blevet testet og certificeret gennem Cisco via tredjepartsprogramudvikleren. Alle telefonproblemer, der er relateret til ikke-certificeret programinteraktion, skal behandles af tredjeparten og vil ikke blive behandlet af Cisco.

Du kan finde flere oplysninger om supportmodellen for Cisco-certificerede tredjepartsprogrammer/-løsninger på webstedet for [Cisco Solution Partner Program](#).



DEL II

Installation af Cisco IP-konferencetelefon

- [Installation af telefon, på side 27](#)
- [Telefoninstallation med Cisco Unified Communications Manager, på side 55](#)
- [Styring af selvbetjeningsportal, på side 67](#)



KAPITEL 4

Installation af telefon

- Kontrollér netværksopsætningen, på side 27
- Onboarding af aktiveringskode til lokale telefoner, på side 28
- Onboarding af aktiveringskode og mobil- og fjernadgang, på side 29
- Aktivér automatisk registrering for telefoner, på side 29
- Tilstand med seriel ledningsføring, på side 31
- Installér konferencetelefon, på side 31
- Konfigurer telefonen ved hjælp af opsætningsmenuerne, på side 40
- Aktivér trådløst LAN fra telefonen, på side 46
- Kontrollér start af telefon, på side 53
- Skift en brugers telefonmodel, på side 53

Kontrollér netværksopsætningen

Ved implementering af et nyt IP-telefonisystem skal systemadministratorer og netværksadministratorer udføre flere indledende konfigurationsopgaver for at forberede netværket til IP-telefonitjeneste. Få oplysninger om og en tjekliste til indstilling og konfiguration af et Cisco IP-telefoninetwork i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Hvis telefonen skal kunne fungere som et slutpunkt i dit netværk, skal netværket overholde specifikke krav. Et krav er den relevante båndbredde. Telefonen kræver mere båndbredde end de anbefalede 32 kbps, når den registreres til Cisco Unified Communications Manager. Overvej dette højere båndbreddekrav, når du konfigurerer din QoS-båndbredde. Få yderligere oplysninger ved at se *Cisco Collaboration System 12.x Solution Reference Network Designs (SRND)* eller senere (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html).



Bemærk Telefonen viser datoen og klokkeslættet fra Cisco Unified Communications Manager. Det klokkeslæt, der vises på telefonen, kan være forskelligt fra Cisco Unified Communications Manager-klokkeslættet med op til 10 sekunder.

Fremgangsmåde

Trin 1 Konfigurer et VoIP-netværk, så det overholder følgende krav:

- VoIP er konfigureret på dine routere og gateways.
- Cisco Unified Communications Manager er installeret på dit netværk og konfigureret til at kunne håndtere behandling af opkald.

Trin 2 Konfigurer netværket, så det understøtter et af følgende:

- DHCP-understøttelse
- Manuel tildeling af IP-adresse, gateway og undernetmaske

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Onboarding af aktiveringskode til lokale telefoner

Du kan bruge aktiveringskoden ved onboarding til hurtigt at oprette nye telefoner uden automatisk registrering. Med denne metode kan du styre telefonens onboardingproces ved hjælp af en af følgende fremgangsmåder:

- Værktøjet Cisco Unified Communications Bulk Administration (BAT)
- Administrationsgrænseflade til Cisco Unified Communications Manager
- Administrative XML Web Service (AXL)

Aktiver denne funktion fra sektionen **Enhedsoplysninger** på siden Telefonkonfiguration. Vælg **Kræver aktiveringskode for onboarding**, hvis du ønsker, at denne funktion til at anvende en enkelt lokal telefon.

Brugere skal angive en aktiveringskode, før deres telefoner kan registreres. Aktiveringskode ved onboarding kan anvendes til individuelle telefoner, en gruppe af telefoner eller på tværs af hele netværket.

Det er en nem måde for brugere at onboarde deres telefoner på, fordi de kun skal angive en 16-cifret aktiveringskode. Hvis en telefon har et videokamera, indsendes koder enten manuelt eller med en QR-kode. Vi anbefaler, at du bruger en sikker metode til at give disse oplysninger til brugere. Men hvis en bruger er tildelt til en telefon, så oplysningerne er tilgængelige på selvbetjeningsportalen. Overvågningsloggen registrerer, når en bruger har adgang til koden fra portalen.

Aktiveringskoder kan kun bruges én gang, og de udløber som standard efter en uge. Hvis en kode udløber, skal du give brugeren en ny.

Du vil se, at denne fremgangsmåde er en nem måde at beskytte netværket på, da en telefon ikke kan registreres, før MIC (Manufacturing Installed Certificate) og aktiveringskode verificeres. Denne metode er også en nem måde at foretage en masseonboarding af telefoner på, da den ikke bruger TAPS (Tool for Auto-registered Phone Support) eller automatisk registrering. Hastigheden af onboarding er en telefon pr. sekund eller 3600 telefoner pr. time. Telefoner kan tilføjes med Cisco Unified Communications Manager Administrative, med Administrative XML Web Service (AXL) eller med BAT.

Eksisterende telefoner nulstilles, når de er konfigureret til onboarding med aktiveringskode. De registrerer ikke, før aktiveringskoden er angivet, og telefonens MIC er bekræftet. Informer aktuelle brugere om, du vil skifte til onboarding med aktiveringskode, før du implementerer den.

Få flere oplysninger i *Administrationsvejledning til Cisco Unified Communications Manager and IM and Presence Service, version 12.0(1)* eller senere.

Onboarding af aktiveringskode og mobil- og fjernadgang

Du kan bruge onboarding af aktiveringskode med mobil- og fjernadgang, når du installerer Cisco IP-telefon for fjernbrugere. Denne funktion er en sikker måde at implementere telefoner, når automatisk registrering ikke er påkrævet. Men du kan konfigurere en telefon til automatisk registrering, når du er på stedet, og aktiveringskoder, når du ikke er på stedet. Denne funktion svarer til onboarding af aktiveringskode til lokale telefoner, men den gør aktiveringskoden tilgængelig for telefoner, der ikke er lokale.

Onboarding af aktiveringskode til mobil- og fjernadgang kræver Cisco Unified Communications Manager 12.5(1)SU1 eller nyere og Cisco Expressway X12.5 eller nyere. Smart Licensing skal også aktiveres.

Du kan aktivere denne funktion fra Cisco Unified Communications Manager Administration, men du skal bemærke følgende:

- Aktiver denne funktion fra sektionen **Enhedsoplysninger** på siden Telefonkonfiguration.
- Vælg **Kræver aktiveringskode for onboarding**, hvis du ønsker, at denne funktion blot skal anvende en enkelt lokal telefon.
- Vælg **Tillad aktiveringskode via MRA**, og **Kræv aktiveringskode for Onboarding**, hvis du ønsker at bruge aktiverings indbygning for en enkelt lokal telefon. Hvis telefonen er lokal, skifter den til tilstanden for mobil og fjernadgang og bruger Expressway. Hvis telefonen ikke kan få forbindelse til Expressway, registreres den ikke, før den ikke længere er på stedet.

Se følgende dokumenter for at få flere oplysninger:

- *Administrationsvejledning til Cisco Unified Communications Manager and IM and Presence Service, version 12.0(1)*.
- *Mobil- og fjernadgang via Cisco Expressway* til Cisco Expressway X12.5 eller nyere

Aktivér automatisk registrering for telefoner

Cisco IP-telefon kræver, at Cisco Unified Communications Manager håndterer opkaldsbehandling. Se dokumentationen til din specifikke version af Cisco Unified Communications Manager eller den kontekstfølsomme hjælp i Cisco Unified Communications Manager Administration for at sikre, at Cisco Unified Communications Manager er konfigureret korrekt til at administrere telefonen og på korrekt vis viderestille og behandle opkald.

Før du installerer Cisco IP-telefon, skal du vælge en metode for tilføjelse af telefoner til Cisco Unified Communications Manager-databasen.

Ved at aktivere automatisk registrering, før du installerer telefonerne, kan du:

- Tilføje telefoner uden først at indhente MAC-adresserne fra telefonerne.
- Automatisk føje en Cisco IP-telefon til Cisco Unified Communications Manager-databasen, når du fysisk forbinder telefonen til dit IP-telefonnetværk. Ved automatisk registrering tildeler Cisco Unified Communications Manager det næste tilgængelige telefonnummer i rækkefølgen til telefonen.
- Hurtigt registrere telefoner i Cisco Unified Communications Manager-databasen og redigere indstillinger som f.eks. telefonnumrene fra Cisco Unified Communications Manager.

- Flytte automatisk registrerede telefoner til nye placering og tildele dem til forskellige enhedspuljer, uden at det påvirker deres telefonnumre.

Automatisk registrering er som standard deaktiveret. I nogle tilfælde vil du måske ikke bruge automatisk registrering, f.eks. hvis du vil tildele et specifikt telefonnummer til telefonen, eller hvis du vil bruge en sikker forbindelse med Cisco Unified Communications Manager. Få flere oplysninger om aktivering af automatisk registrering i dokumentationen til din specifikke version af Cisco Unified Communications Manager. Når du konfigurerer klyngen for blandet tilstand via Ciscos CTL-klient, er automatisk registrering deaktiveret automatisk, men du kan aktivere den. Når du konfigurerer klyngen for ikke-sikker tilstand via Ciscos CTL-klient, er automatisk registrering ikke deaktiveret automatisk.

Du kan tilføje telefoner med automatisk registrering og TAPS (Tool for AutoRegistered Phones Support) uden først at indhente MAC-adresser fra telefoner.

TAPS virker med BAT (Bulk Administration Tool) til at opdatere flere telefoner, der allerede var føjet til Cisco Unified Communications Manager-databasen med dummy MAC-adresser. Brug TAPS til at opdatere MAC-adresser og til at downloade foruddefinerede konfigurationer til telefoner.

Cisco anbefaler, at du bruger automatisk registrering og TAPS til at føje færre end 100 telefoner til dit netværk. Hvis du vil føje flere end 100 telefoner til dit netværk, skal du bruge BAT (Bulk Administration Tool).

For at implementere TAPS skal du eller slutbrugeren ringe til et TAPS-telefonnummer og følge talebeskederne. Når processen er færdig, indeholder telefonen telefonnummeret og andre indstillinger, og telefonen opdateres i Cisco Unified Communications Manager Administration med den korrekte MAC-adresse.

Bekræft, at automatisk registrering er aktiveret og korrekt konfigureret i Cisco Unified Communications Manager Administration, før du tilslutter en Cisco IP-telefon til netværket. Få flere oplysninger om aktivering og konfiguration af automatisk registrering i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Automatisk registrering skal være aktiveret i Cisco Unified Communications Manager Administration, for at TAPS virker.

Fremgangsmåde

-
- Trin 1** Klik på **System > Cisco Unified CM** i Cisco Unified Communications Manager Administration.
- Trin 2** Klik på **Find**, og vælg den krævede server.
- Trin 3** Konfigurer disse felter under **Oplysninger til automatisk registrering**.
- **Universel enhedsskabelon**
 - **Universel linjeskabelon**
 - **Starttelefonnummer**
 - **Sluttelefonnummer**
- Trin 4** Fjern markeringen i afkrydsningsfeltet **Automatisk registrering deaktiveret på Cisco Unified Communications Manager**.
- Trin 5** Klik på **Gem**.
- Trin 6** Klik på **Anvend konfig**.
-

Tilstand med seriel ledningsføring

Du kan tilslutte to konferencetelefoner ved hjælp af en Smart adapter og USB-C kabler, der leveres i sæt til seriel ledningsføring for at udvide lydækningsområdet i et lokale.

I tilstanden med seriel ledningsføring modtager begge enheder strøm gennem Smart-adapteren, der er tilsluttet en strømadapter. Du kan kun bruge én ekstern mikrofon pr. enhed. Du kan bruge et par kablede mikrofoner med enhederne eller et par af trådløse mikrofoner med enhederne, men ikke en blandet kombination af mikrofonerne. Når en kablet mikrofon forbindes til en af enhederne, annulleres dens parring med eventuelle trådløse mikrofoner, der er tilsluttet til samme enhed. Når der er et aktivt opkald, synkroniseres LED'erne og menuindstillingerne på telefonens skærm for begge enheder.

Lignende emner

[Installér konferencetelefon i tilstand med seriel ledningsføring](#), på side 38

[En telefon i tilstand med seriel ledningsføring fungerer ikke](#), på side 163

Installér konferencetelefon

Når telefonen har oprettet forbindelse til netværket, begynder processen til start af telefonen, og telefonen bliver registreret med Cisco Unified Communications Manager. Du skal konfigurere netværksindstillingerne på telefonen, hvis du deaktiverer DHCP-tjenesten.

Hvis du har anvendt automatisk registrering, skal du opdatere telefonens specifikke konfigurationsoplysninger som f.eks. at knytte telefonen til en bruger, ændre knaptabellen eller telefonbogsnummeret.

Når telefonen har forbindelse, bestemmer den, om der skal installeres en firmwarefil på telefonen.

Hvis du bruger konferencetelefonen i tilstand med seriel ledningsføring, skal du se under [Installér konferencetelefon i tilstand med seriel ledningsføring](#), på side 38.

Inden du begynder

Sørg for, at du har den nyeste firmwareversion installeret på din Cisco Unified Communications Manager. Søg efter opdaterede enhedspakker 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

Fremgangsmåde

Trin 1

Vælg telefonens strømkilde:

- PoE-installation (Power over Ethernet) med en Cisco IP-konferencetelefon 8832 – PoE-injektor
- Installationen uden PoE Ethernet med Cisco IP-konferencetelefon 8832 – ikke-PoE Ethernet-injektor
- En Cisco IP-konferencetelefon 8832-strømadapter er nødvendig ved Wi-Fi-installation.

Hvis du ønsker yderligere oplysninger, kan du se [Sådan slutter du mødetelefonen til strøm](#), på side 32.

Trin 2

Slut telefonen til switchen.

- Hvis du bruger PoE:
 1. Sæt Ethernet-kablet i LAN-porten.
 2. Sæt den anden ende af Ethernet-kablet i enten Cisco IP-konferencetelefon 8832 – PoE-injektor eller Cisco IP-konferencetelefon 8832 – Ethernet-injektor.
 3. Forbind injektoren til konferencetelefonen med USB-C-kablet.
- Hvis du ikke bruger PoE:
 1. Hvis du bruger Cisco IP-konferencetelefon 8832 – Ethernet-injektor, skal du sætte netadapteren i en stikkontakt.
 2. Slut strømadapteren til Ethernet-injektoren ved hjælp af et USB-C-kabel.
ELLER
Hvis du bruger den Cisco IP-konferencetelefon 8832 – ikke-PoE Ethernet-injektor, skal du sætte den i en stikkontakt.
 3. Sæt Ethernet-kablet ind i ikke-PoE-Ethernet-injektoren eller Ethernet-injektoren.
 4. Sæt Ethernet-kablet i LAN-porten.
 5. Forbind ikke-PoE-Ethernet-injektoren eller Ethernet-injektoren til konferencetelefonen med et USB-C-kabel.
- Hvis du bruger Wi-Fi:
 1. Sæt Cisco IP-konferencetelefon 8832-netadapteren i stikkontakten.
 2. Slut strømadapteren til konferencetelefonen ved hjælp af et USB-C-kabel.

Bemærk Du kan bruge ikke-PoE-Ethernet-injektoren til at forsyne telefonen med strøm. Du skal imidlertid trække LAN-kablet ud. Telefonen opretter kun forbindelse til Wi-Fi, når Ethernet-forbindelsen ikke er tilgængelig.

- Trin 3** Overvåg processen til start af telefonen. Dette trin kontrollerer, at telefonen er konfigureret korrekt.
- Trin 4** Hvis du ikke bruger automatisk registrering, skal du manuelt konfigurere sikkerhedsindstillingerne på telefonen.
- Trin 5** Giv telefonen mulighed for at opgradere til den aktuelle firmwareafbildning, der er gemt på din Cisco Unified Communications Manager.
- Trin 6** Foretag opkald med telefonen for at bekræfte, at telefonen og funktionerne virker korrekt.
- Trin 7** Angiv oplysninger til brugere om, hvordan de bruger deres telefoner, og hvordan de konfigurerer telefonens indstillingsmuligheder. Dette trin sikrer, at brugerne har tilstrækkelige oplysninger til at kunne bruge deres Cisco IP-telefon.

Sådan slutter du mødetelefonen til strøm

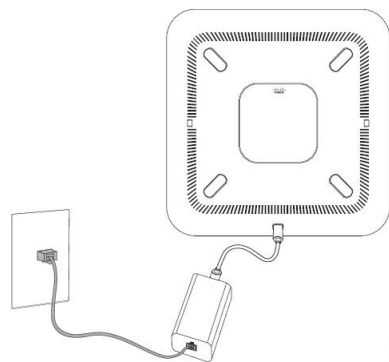
Din mødetelefon skal have strøm fra en af disse kilder:

- PoE (Power over Ethernet)

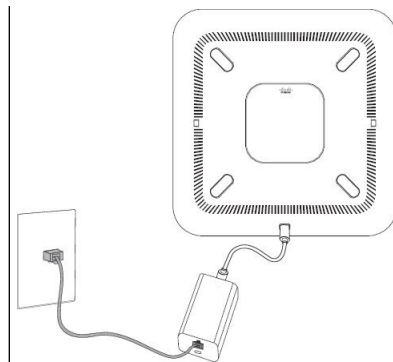
- Nordamerika
 - Cisco IP-konferencetelefon 8832 – PoE-injektor
 - Cisco IP-konferencetelefon 8832 – Ethernet-injektor
- Uden for Nordamerika – Cisco IP-konferencetelefon 8832 – PoE-injektor
- Ikke-PoE Ethernet
 - Nordamerika
 - Cisco IP-konferencetelefon 8832 – ikke-PoE Ethernet-injektor
 - Cisco IP-konferencetelefon 8832 – Ethernet-injektor med en Cisco IP-konferencetelefon 8832-strømadapter forbundet til en stikkontakt.
 - Uden for Nordamerika – Cisco IP-konferencetelefon 8832 – ikke-PoE Ethernet-injektor
- Wi-Fi – Brug Cisco IP-konferencetelefon 8832-strømadapteren forbundet til en stikkontakt.

Figur 6: PoE-strømmuligheder til konferencetelefon

Følgende figur viser de to PoE-strømmuligheder.



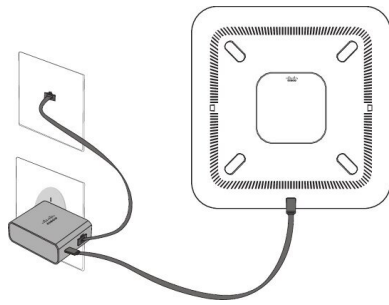
Cisco IP-konferencetelefon 8832 – PoE-injektor med PoE-strømmuligheden



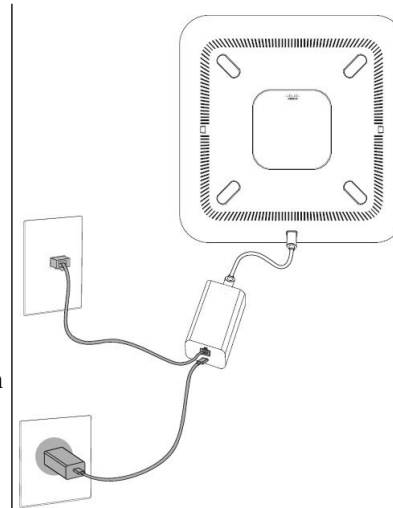
Cisco IP-konferencetelefon 8832 – Ethernet-injektor med PoE-strømmuligheden

Figur 7: Ethernet-strømmuligheder til mødetelefon

Følgende figur viser de to Ethernet-strømmuligheder.

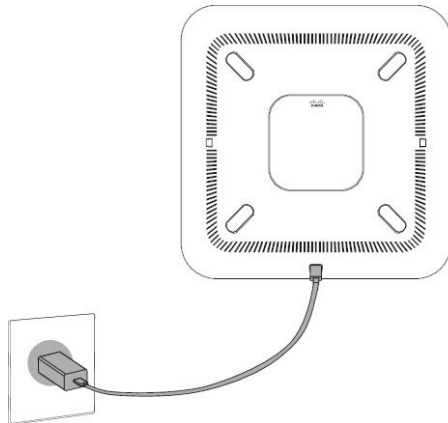


Cisco IP-konferencetelefon 8832 – ikke-PoE
Ethernet-injektor med Ethernet-strømmuligheden



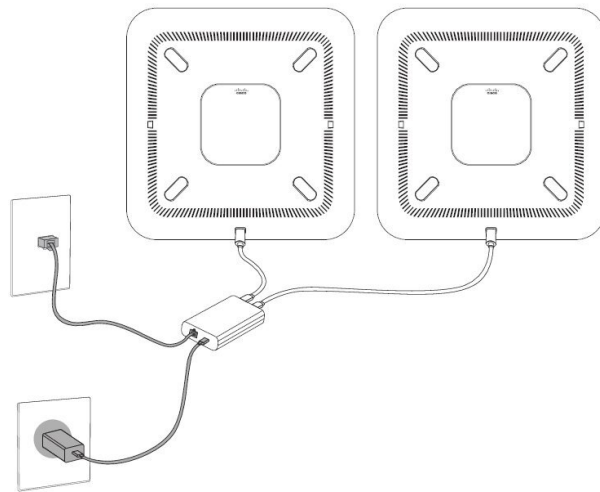
Cisco IP-konferencetelefon 8832 – Ethernet-injektor med
Ethernet-strømmuligheden

Figur 8: Strømmuligheden for konferencetelefon ved tilslutning til et Wi-Fi-netværk



Figur 9: Strømmuligheder for konferencetelefon med seriel ledningsføring

Følgende figur viser strømmuligheden, når telefonen er tilsluttet i tilstand med seriel ledningsføring.



Installér de kablede udvidelsesmikrofoner

Telefonen understøtter et valgfrit sæt med to kablede udvidelsesmikrofoner. Du kan udvide mikrofonerne op til 2,13 m fra telefonen. Du får de bedste resultater ved at anbringe mikrofonerne mellem 0,91 m og 2,1 m fra telefonen.

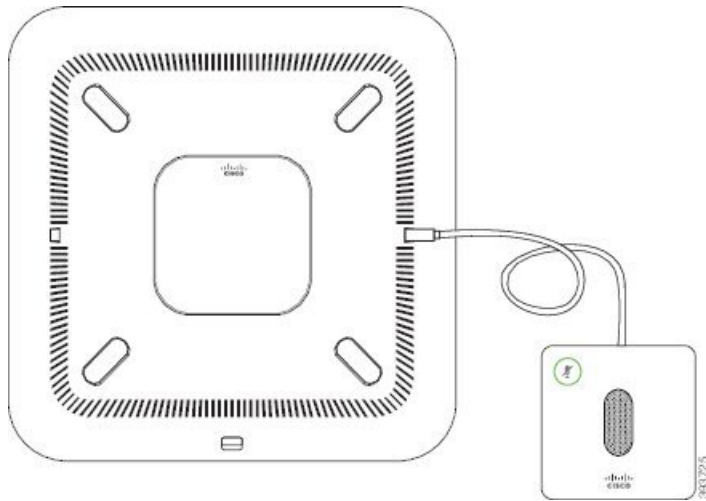
Fremgangsmåde

Trin 1 Slut endestykket af mikrofonkablet til porten på siden af telefonen.

Trin 2 Forlæng mikrofonkablet til den ønskede position.

Følgende figur viser installation af en kablet udvidelsesmikrofon.

Figur 10: Installation af kablet udvidelsesmikrofon



Installér de trådløse udvidelsesmikrofoner

Konferencetelefonen giver mulighed for at forbinde to trådløse udvidelsesmikrofoner.



Bemærk Du skal bruge enten to kablede mikrofoner eller to trådløse mikrofoner med telefonen, men ikke en blandet kombination.

Når konferencetelefonen er i et opkald, lyser LED'en på udvidelsesmikrofonen grønt. Hvis du vil slå lyden fra for udvidelsesmikrofonen, skal du trykke på tasten **Slå lyd fra**. Når mikrofonen er slået fra, lyser LED'en rødt. Når batteriet i mikrofonen næsten er opbrugt, blinker LED'en hurtigt.

Inden du begynder

Frakobl de kablede udvidelsesmikrofoner, før du installerer trådløse udvidelsesmikrofoner. Du kan ikke bruge både kablede og trådløse udvidelsesmikrofoner på samme tid.

Fremgangsmåde

- Trin 1** Placer bordmonteringspladen på det sted på bordets overflade, hvor du vil placere mikrofonen.
- Trin 2** Fjern klæbearbejdet for den dobbelthæftende tape på bunden af bordets monteringsplade. Placer bordets monteringsplade, så den hæftes fast på bordoverfladen.
- Trin 3** Sæt mikrofonen i bordets monteringsplade. Magneter er integreret i mikrofonen, så enheden fastgøres på sin plads.

Du kan flytte mikrofonen og den tilknyttede bordmontering til en anden placering på bordets overflade, hvis det er nødvendigt. Vær forsigtig under bevægelse for at beskytte enheden.

Lignende emner

[Trådløs udvidelsesmikrofon \(kun 8832\)](#), på side 13

[Installér opladningsholderen til den trådløse mikrofon](#), på side 37

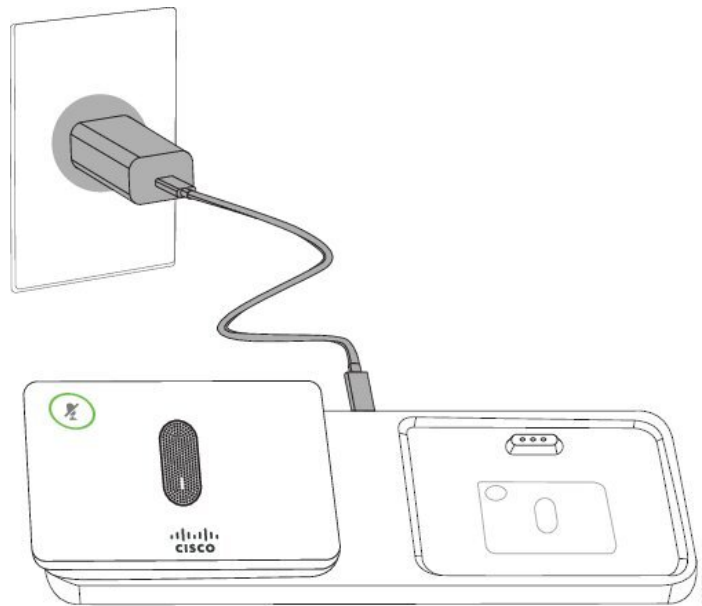
Installér opladningsholderen til den trådløse mikrofon

Du kan bruge opladningsholderen til at oplade batteriet til den trådløse mikrofon.

Fremgangsmåde

- Trin 1** Sæt netadapteren til opladningsholderen i stikkontakten.
- Trin 2** Slut den ene ende af USB-C-kablet til opladningsholderen og anden ende til strømadapteren.
- Følgende figur viser installation af en opladningsholder til trådløs mikrofon.

Figur 11: Installation af opladningsholder til trådløs mikrofon



Lignende emner

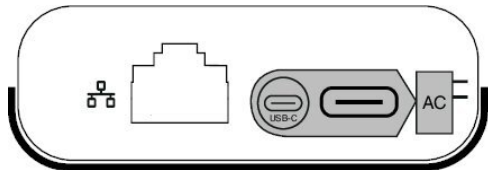
[Trådløs udvidelsesmikrofon \(kun 8832\)](#), på side 13

[Installér de trådløse udvidelsesmikrofoner](#), på side 36

Installér konferencetelefon i tilstand med seriel ledningsføring

Sættet til seriel ledningsføring indeholder en Smart adapter, et kort LAN-kabel, to lange, tykkere USB-C-kabler og et kortere, tyndere USB-C-kabel. I tilstanden med seriel ledningsføring kræver konferencetelefoner ekstern strøm fra en stikkontakt. Du skal bruge Smart adapter til at forbinde telefoner til hinanden. De lange USB-C kabler går til telefonen, og det korte går til netadapteren. Se følgende figur, når du tilslutter netadapteren og LAN-porten til Smart adapter.

Figur 12: Smart Adapter-strømport og LAN-port



Du kan kun bruge én mikrofon pr. enhed.



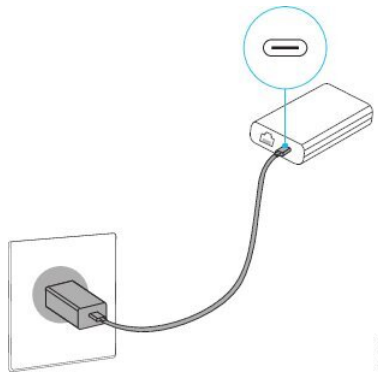
Bemærk Du skal bruge enten to kablede mikrofoner eller to trådløse mikrofoner med telefonen, men ikke en blandet kombination.

USB-C kablet til netadapteren er tyndere end de USB-C kabler, der er tilsluttet telefonen.

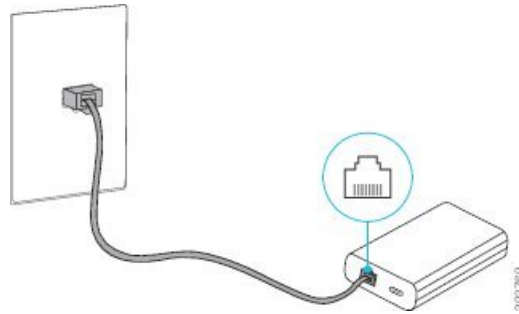
Fremgangsmåde

- Trin 1** Slut nedadapteren til stikkontakten.
- Trin 2** Tilslut det korte, tyndere USB-C-kabel fra netadapteren til Smart adapter.

Figur 13: Smart Adapter-USB-port forbundet til stikkontakten



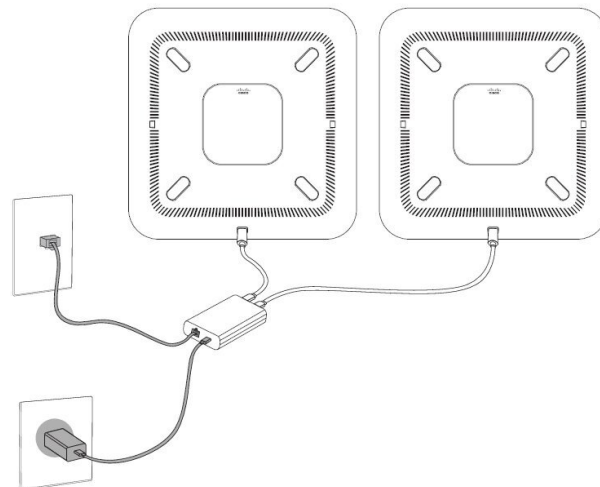
- Trin 3** Påkrævet: Tilslut Ethernet-kablet til Smart adapter og LAN-porten.

Figur 14: Smart Adapter-LAN-port tilsluttet til LAN-porten i stikkontakten på væggen

Trin 4 Tilslut den første telefon til Smart adapter med det længere, tykkere USB-C-kabel.

Trin 5 Forbind den anden telefon til Smart adapter med et andet USB-C-kabel.

Følgende figur viser installation af konferencetelefonen i tilstanden med seriel ledningsføring.

Figur 15: Installation af konferencetelefon i tilstand med seriel ledningsføring

Lignende emner

[Tilstand med seriel ledningsføring](#), på side 31

[En telefon i tilstand med seriel ledningsføring fungerer ikke](#), på side 163

Genstart din konferencefonen fra backupafbildning

Din Cisco IP-konferencetelefon 8832 har en anden afbildning, der fungerer som backup, og som gør det muligt at genoprette telefonen, når standardafbildningen er blevet kompromitteret.

Benyt følgende fremgangsmåde for at genstarte telefonen fra afbildningen.

Fremgangsmåde

Trin 1 Hold tasten * nede, mens du tilslutter strømmen til konferencetelefonen.

- Trin 2** Når LED-bjælken tændes og lyser grønt og derefter slukkes, kan du slippe tasten *.
- Trin 3** Konferencetelefonen genstarter fra backupafbildningen.

Konfigurer telefonen ved hjælp af opsætningsmenuerne

Telefonen har mange netværksindstillinger, der kan konfigureres, og som det kan være nødvendigt at ændre, før telefonen kan bruges af dine brugere. Du kan få adgang til disse indstillinger og ændre nogle dem via telefonens menuer.

Telefonen omfatter følgende opsætningsmenuer:

- **Netværksopsætning:** har indstillinger til visning og konfiguration af en række forskellige netværksindstillinger.
 - **IPv4-opsætning:** Denne undermenu har yderligere netværksindstillinger.
 - **IPv6-opsætning:** Denne undermenu har yderligere netværksindstillinger.
- **Sikkerhedsopsætning:** har indstillinger til visning og konfiguration af en række forskellige sikkerhedsindstillinger.



Bemærk

Du kan kontrollere, om en telefon har adgang til indstillingsmenuen eller til indstillinger i denne menu. Brug feltet **Adgang til indstillinger** i vinduet Cisco Unified Communications Manager Administration Telefonkonfiguration til at få styre adgangen. Feltet **Adgang til indstillinger** accepterer disse værdier:


- **Aktiveret:** Giver adgang til menuen Indstillinger.
- **Deaktiveret:** Forhindrer adgang til de fleste poster i menuen Indstillinger. Brugeren kan stadig få adgang til **Indstillinger > Status**.
- **Begrænset:** Giver adgang til menuen Brugerpræferencer og menupunkter i menuen Status og gør det muligt at lagre ændringer i lydstyrke. Forhindrer adgang til andre indstillingsmuligheder i menuen Indstillinger.

Hvis du ikke kan få adgang til en indstillingsmulighed i menuen Administrationsindstillinger, skal du markere feltet **Adgang til indstillinger**.

Du konfigurerer indstillinger, der er skrivebeskyttet på telefonen, i Cisco Unified Communications Manager Administration.

Fremgangsmåde

- Trin 1** Tryk på **Indstillinger**.
- Trin 2** Vælg **Administratorindstillinger**.
- Trin 3** Angiv adgangskode, hvis den kræves, og klik derefter på **Log på**.
- Trin 4** Vælg **Netværksopsætning** eller **Sikkerhedsopsætning**.

- Trin 5** Udfør en af følgende handlinger for at få vist den ønskede menu:
- Brug navigationspilene til at vælge den ønskede menu, og tryk derefter på **Vælg**.
 - Brug telefonens tastatur til at angive det nummer, der svarer til menuen.
- Trin 6** Vis en undermenu ved at gentage trin 5.
- Trin 7** Afslut en menu ved at trykke på **Tilbage** .

Lignende emner

[Genstart eller nulstil konferencetelefonen](#), på side 171

[Konfigurer netværksindstillingerne](#), på side 42

[Konfigurer sikkerhedsindstillingerne](#)


Anvend en telefonadgangskode

Fremgangsmåde

- Trin 1** Gå til vinduet Konfiguration af almindelig telefonprofil i Cisco Unified Communications Manager Administration (**Enhed > Enhedsindstillinger > Almindelig telefonprofil**).
- Trin 2** Angiv en adgangskode i indstillingen Lokal adgangskode til oplåsning af telefon.
- Trin 3** Anvend adgangskoden til den almindelige telefonprofil, som telefonen bruger.
-

Tekst- og menuindtastning fra telefonen

Når du redigerer værdien af en indstilling, skal du følge disse retningslinjer:

- Brug pilene på navigationstastaturet for at markere det felt, du vil redigere. Tryk på **Vælg** på navigationspladen for at aktivere feltet. Når feltet er aktiveret, kan du angive værdier.
- Brug tasterne på tastaturet til at angive tal og bogstaver.
- Hvis du vil angive bogstaver ved hjælp af tastaturet, skal du bruge en tilhørende taltast. Tryk på tasten en eller flere gange for at få vist et bestemt bogstav. Tryk f.eks. på **2**-tasten én gang for "a," to gange hurtigt for "b" og tre gange hurtigt for "c." Når du stopper, går markøren automatisk frem, så du kan indtaste det næste bogstav.
- Tryk på programtasten , hvis du laver en fejl. Denne programtast sletter tegnet til venstre for markøren.
- Tryk på **Gendan**, før du trykker på **Anvend** for at kassere de ændringer, du foretager.
- Hvis du vil angive et punktum (f.eks. i en IP-adresse), skal du trykke på * på tastaturet.
- Hvis du vil angive et kolon til en IPv6-adresse, skal du trykke på * på tastaturet.



Bemærk Cisco IP-telefon har flere metoder, du kan bruge til at nulstille eller gendanne indstillinger, hvis det er nødvendigt.

Konfigurer netværksindstillingerne

Fremgangsmåde

- Trin 1** Tryk på **Indstillinger**.
- Trin 2** Vælg **Administratorindstillinger > Netværksopsætning > Ethernet-opsætning**.
- Trin 3** Indstil felterne som beskrevet i [Felter til netværksopsætning, på side 42](#). Når du har angivet felterne, skal du genstarte telefonen.

Felter til netværksopsætning

Menuen Netværksopsætning indeholder felter og undermenuer til IPv4 og IPv6.

Hvis du vil ændre nogle af felterne, skal du deaktivere DHCP.

Tabel 10: Menu til netværksopsætning

| Indtastning | Type | Standard | Beskrivelse |
|---------------------|--------|----------|---|
| IPv4-opsætning | Menu | | Se tabellen “Undermenu i IPv4-opsætning”. Denne indstilling vises kun i tostakstilstanden. |
| IPv6-opsætning | Menu | | Se tabellen “Undermenu i IPv6-opsætning”. |
| Værtsnavn | Streng | | Telefonens værtsnavn. Hvis du bruger DHCP, tildeles dette navn automatisk. |
| Domænenavn | Streng | | Navnet på DNS-domænet (Domain Name System), som telefonen er i. Hvis du vil ændre dette felt, skal du deaktivere DHCP. |
| Operationel VLAN-id | | | Et VLAN (Virtual Local Area Network) i brug, der er konfigureret på en Cisco Catalyst-switch, som telefonen er medlem af. |
| Admin VLAN-id | | | Ekstra VLAN, som telefonen er medlem af. |

| Indtastning | Type | Standard | Beskrivelse |
|-------------------|--|------------------------|--|
| SW-portopsætning | Automatisk forhandling 10 med halv dupleks 10 med fuld dupleks 100 med halv dupleks 100 med fuld dupleks | Automatisk forhandling | Switchportens hastighed og dupleks, hvor: <ul style="list-style-type: none"> • 10 Halv = 10-BaseT/halv dupleks • 10 Fuld = 10-BaseT/fuld dupleks • 100 Halv = 100-BaseT/halv dupleks • 100 Fuld = 100-BaseT/fuld dupleks |
| LLDP-MED: SW-port | Deaktiveret Aktiveret | Aktiveret | Angiver om LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) er aktiveret på switchporten. |

Tabel 11: Undermenuen IPv4-opsætning

| Indtastning | Type | Standard | Beskrivelse |
|------------------|--------------------------|-----------|--|
| DHCP | Deaktiveret Aktiveret | Aktiveret | Aktiverer eller deaktiverer brugen af DHCP. |
| IP-adresse | | | Telefonens IP-adresse (IPv4). Hvis du vil ændre dette felt, skal du deaktivere DHCP. |
| Undernetmaske | | | Den undernetmaske, telefonen bruger. Hvis du vil ændre dette felt, skal du deaktivere DHCP. |
| Standardrouter 1 | | | Anvendt standardrouter, som telefonen bruger. Hvis du vil ændre dette felt, skal du deaktivere DHCP. |
| DNS-server 1 | | | Primær DNS-server (Domain Name System) (DNS-server 1), som telefonen bruger. Hvis du vil ændre dette felt, skal du deaktivere DHCP. |
| DNS-server 2 | | | Primær DNS-server (Domain Name System) (DNS-server 2), som telefonen bruger. |

| Indtastning | Type | Standard | Beskrivelse |
|-----------------------|-----------|----------|--|
| DNS-server 3 | | | Primær DNS-server (Domain Name System) (DNS-server 3), som telefonen bruger. |
| Alternativ TFTP | Nej Ja | Nej | Angiver, om telefonen bruger en alternativ TFTP-server. |
| TFTP-server 1 | | | Anvendt primær TFTP-server (Trivial File Transfer Protocol), som telefonen bruger. Hvis du aktiverer indstillingen alternativ TFTP, skal du angive en værdi, der ikke er nul, for indstillingen TFTP-Server 1. Hvis hverken den primære TFTP-server eller den ekstra TFTP-server vises i CTL- eller ITL-filen på telefonen, skal du låse filen op, før du kan gemme ændringerne til indstillingen TFTP Server 1. I dette tilfælde sletter telefonen filen, når du gemmer ændringer til indstillingen TFTP-Server 1. En ny CTL- eller ITL-fil hentes fra den nye TFTP-Server 1-adresse. Se TFTP-noterne efter den sidste tabel. |
| TFTP-server 2 | | | Sekundær TFTP-server, som telefonen bruger. Hvis hverken den primære TFTP-server eller den ekstra TFTP-server vises i CTL- eller ITL-filen på telefonen, skal du låse filen op, før du kan gemme ændringerne til indstillingen TFTP Server 2. I dette tilfælde sletter telefonen filen, når du gemmer ændringer til indstillingen TFTP-Server 2. En ny CTL- eller ITL-fil hentes fra den nye TFTP-Server 2-adresse. Se afsnittet om TFTP-noter efter den sidste tabel. |
| DHCP-Adresse Frigivet | Nej Ja | Nej | |

Tabel 12: Undermenuen IPv6-opsætning

| Indtastning | Type | Standard | Beskrivelse |
|-----------------------|--------------------------|-----------|--|
| DHCPv6 aktiveret | Deaktiveret Aktiveret | Aktiveret | Aktiverer eller deaktiverer brugen af IPv6 DHCP. |
| IPv6-adresse | | | Telefonens IPv6-adresse. Hvis du vil ændre dette felt, skal du deaktivere DHCP. |
| IPv6-præfiks længde | | | Længden af IPv6-adressen. Hvis du vil ændre dette felt, skal du deaktivere DHCP. |
| IPv6 standardrouter 1 | | | Standardrouter-IPv6. Hvis du vil ændre dette felt, skal du deaktivere DHCP. |
| IPv6 DNS-server 1 | | | Primær IPv6 DNS-server Hvis du vil ændre dette felt, skal du deaktivere DHCP. |
| IPv6 alternativ TFTP | Nej Ja | Nej | Angiver, om telefonen bruger en alternativ IPv6 TFTP-server. |
| IPv6 TFTP-server 1 | | | Primær IPv6 TFTP-server, der bruges, og som telefonen bruger. Se afsnittet om TFTP-noter efter den denne tabel. |
| IPv6 TFTP-server 2 | | | Sekundær IPv6 TFTP-server, der bruges, og som telefonen bruger. Se afsnittet om TFTP-noter efter den denne tabel. |
| IPv6-adresse frigivet | Nej Ja | Nej | |

Før indstillinger af IPv6-opsætningen kan konfigureres på din enhed, skal IPv6 være aktiveret og konfigureret i Cisco Unified Communication Administration. Følgende felter til enhedskonfiguration gælder for IPv6-konfiguration:

- IP-adresseringstilstand
- IP-adressetilstand til signal

Hvis IPv6 er aktiveret i Unified-klyngen, er standardindstillingen for IP-adressetilstanden IPv4 og IPv6. I denne adresetilstand vil telefonen hente og bruge en IPv4-adresse og en IPv6-adresse. Den kan bruge IPv4-

og IPv6-adressen, alt efter hvad kræves for medie. Telefonen bruger enten IPv4- eller IPv6-adressen til opkaldsstyringssignal.

Få flere oplysninger om IPv6 under:

- “Fælles enhedskonfiguration” i *Vejledning i funktioner og tjenester for Cisco Unified Communications Manager* i kapitlet “IPv6-understøttelse i Cisco Unified Communications-enheder”.
- *IPv6-installationsvejledning til Cisco Collaboration Systems version 12.0* findes her: <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html>

TFTP-bemærkninger

Når telefonen søger efter TFTP-serveren, prioriterer telefonen manuelt tildelte TFTP-servere, uanset protokollen. Hvis din konfiguration omfatter både IPv6- og IPv4 TFTP-servere, prioriterer telefonen den rækkefølge, den søger efter TFTP-serveren på, ved at prioritere manuelt tildelte IPv6 TFTP-servere og IPv4 TFTP-servere. Telefonen søger efter TFTP-serveren i denne rækkefølge:

1. Alle manuelt tildelte IPv4 TFTP-servere
2. Alle manuelt tildelte IPv6-servere
3. DHCP-tildelte TFTP-servere
4. DHCPv6-tildelte TFTP-servere

Få oplysninger om CTL- og ITL-filerne i *sikkerhedsvejledningen til Cisco Unified Communications Manager*.

Indstil feltet Domænenavn

Fremgangsmåde

-
- Trin 1** Angiv indstillingen DHCP aktiveret til **Nej**.
- Trin 2** Rul til indstillingen Domænenavn, tryk på **Vælg**, og angiv et nyt domænenavn.
- Trin 3** Tryk på **Anvend**.
-

Aktivér trådløst LAN fra telefonen

Sørg for, at Wi-Fi dækningen på den placering, hvor det trådløse LAN er installeret, er egnet til afsendelse af talepakker.

En hurtig og sikker roamingmetode anbefales til Wi-Fi-brugere. Vi anbefaler, at du bruger 802.11r (FT).

Få alle konfigurationsoplysningerne ved at se *Vejledning i implementering af trådløst LAN til Cisco IP-telefon 8832-serien* på denne placering:

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

Vejledning i implementering af trådløst LAN til Cisco IP-telefon 8832-serien omfatter følgende konfigurationsoplysninger:

- Konfiguration af trådløst netværk
- Konfiguration af trådløst netværk i Cisco Unified Communications Manager Administration
- Konfiguration af trådløst netværk på Cisco IP-telefon

Inden du begynder

Sørg for, at Wi-Fi er aktiveret på telefonen, og at Ethernet-kablet er afbrudt.

Fremgangsmåde

-
- Trin 1** Hvis du vil aktivere programmet, skal du trykke på **Indstillinger**.
- Trin 2** Gå til **Administratorindstillinger > Netværksopsætning > Opsætning af Wi-Fi-klient > Trådløs**.
- Trin 3** Tryk på **Til**.
-

Konfigurer det trådløse LAN fra Cisco Unified Communications Manager

I Cisco Unified Communications Manager Administration skal du aktivere en parameter, der hedder “Wi-Fi” for konferencetelefonen.



-
- Bemærk** I vinduet telefonkonfiguration i Cisco Unified Communications Manager Administration (**Enhed > Telefon**) skal du bruge den kablede linje med MAC-adresse, når du konfigurerer MAC-adressen. Cisco Unified Communications Manager-registrering bruger ikke den trådløse MAC-adresse.
-

Benyt følgende fremgangsmåde i Cisco Unified Communications Manager Administration.

Fremgangsmåde

-
- Trin 1** Hvis du vil aktivere det trådløse LAN på en bestemt telefon, skal du gøre følgende:
- a) Vælg **Enhed > Telefon**.
 - b) Find den ønskede telefon.
 - c) Vælg indstillingen **Aktiveret** for Wi-Fi-parametere i afsnittet Produktspecifikt konfigurationslayout.
 - d) Marker afkrydsningsfeltet **Tilsidesæt almindelige indstillinger**.
- Trin 2** Hvis du vil aktivere trådløst LAN for en gruppe telefoner:
- a) Vælg **Enhed > Enhedsindstillinger > Almindelig telefonprofil**.
 - b) Vælg indstillingen **Aktiveret** for Wi-Fi-parametere.

- Bemærk** For at sikre, at konfigurationen i dette trin fungerer, skal du fjerne markeringen af afkrydsningsfeltet **Tilsidesæt almindelige indstillinger**, der er nævnt i trin 1d.

- c) Marker afkrydsningsfeltet **Tilsidesæt almindelige indstillinger**.
- d) Tilknyt telefonerne til den almindelige telefonprofil ved hjælp af **Enhed > Telefon**.

Trin 3 Hvis du vil aktivere trådløst LAN for WLAN-kompatible alle telefoner i dit netværk:

- a) Vælg **System > Konfiguration af firmatelefon**.
- b) Vælg indstillingen **Aktiveret** for Wi-Fi-parametereen.

Bemærk For at sikre, at konfigurationen i dette trin fungerer, skal du fjerne markeringen af afkrydsningsfeltet **Tilsidesæt almindelige indstillinger**, der er nævnt i trin 1d og 2c.

- c) Marker afkrydsningsfeltet **Tilsidesæt almindelige indstillinger**.

Konfigurer trådløst LAN på telefonen

Før Cisco IP-telefon kan oprette forbindelse til WLAN'et, skal du konfigurere telefonens netværksprofil med de relevante WLAN-indstillinger. Du kan bruge menuen **Netværksopsætning** på telefonen for at få adgang til undermenuen **Konfiguration af Wi-Fi-klient** og angive WLAN-konfigurationen.



Bemærk Indstillingen **Konfiguration af Wi-Fi-klient** vises ikke i menuen **Netværksopsætning**, når Wi-Fi er deaktiveret på Cisco Unified Communications Manager.

Få flere oplysninger i *Implementeringsvejledningen til Cisco IP-konferencetelefon 8832-serien*, som du finder her: <http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>.

Inden du begynder

Konfigurer trådløst LAN fra Cisco Unified Communications Manager.

Fremgangsmåde

Trin 1 Tryk på **Indstillinger**.

Trin 2 Vælg **Administratorindstillinger > Netværksopsætning > Konfiguration af Wi-Fi-klient**.

Trin 3 Konfigurer den trådløse konfiguration som beskrevet i tabellen nedenfor.

Table 13: Indstillinger i menuen Konfiguration af Wi-Fi-klient

| Indstilling | Beskrivelse | Hvis du vil ændre |
|--------------|--|---|
| Trådløs | Aktiverer eller deaktiverer den trådløse radio på Cisco IP-telefon. | Rul til indstillingen Trådløs , og brug til/fra-knappen til at ændre indstillingen til og fra. |
| Netværksnavn | Gør det muligt at oprette forbindelse til et trådløst netværk ved hjælp af vinduet Vælg et netværk . Dette vindue har to programtaster - Tilbage og Andet . | I vinduet Vælg et netværk skal du vælge et netværk, du vil oprette forbindelse til. |

| Indstilling | Beskrivelse | Hvis du vil ændre |
|-------------------|--|--|
| Wi-Fi-loginadgang | Aktiverer visning af Wi-Fi-loginvinduet. | Rul til indstillingen Wi-Fi-login , og tryk på til/fra-knappen til at ændre indstillingen til og fra. |
| IPv4-opsætning | I undermenuen til IPv4-konfiguration kan du gøre følgende: <ul style="list-style-type: none"> • Aktivere eller deaktivere telefonen til at bruge den IP-adresse, som DHCP-serveren tildeler. • Manuelt indstille IP-adressen, undernetmasken, standardrouterne, DNS-serveren og alternative TFTP-servere. Få yderligere oplysninger om IPv4-adressefelterne i tabellen "Undermenu til IPv4-opsætning". | Rul til IPv4-opsætning , og tryk på |
| IPv6-opsætning | I undermenuen til IPv6-konfiguration kan du gøre følgende: <ul style="list-style-type: none"> • Aktivere eller deaktivere telefonens mulighed for at bruge den IPv6-adresse, der er tildelt af DHCPv6-serveren eller erhvervet med SLAAC via en IPv6-aktiveret router. • Manuelt indstille IPv6-adressen, præfikslængden, standardrouterne, DNS-serveren og alternative TFTP-servere. Få yderligere oplysninger om IPv6-adressefelterne i tabellen "Undermenu til IPv6-opsætning". | Rul til IPv6-opsætning , og tryk på |
| MAC-adresse | Entydig MAC-adresse (Media Access Control) for telefonen. | Kun til skærmsvisning. Kan ikke ændres. |
| Domænenavn | Navnet på DNS-domænet (Domain Name System), som telefonen er i. | Se Indstil feltet Domænenavn , på |

Trin 4 Tryk på **Gem** for at foretage ændringer, eller tryk på **Gendan** for at kassere forbindelsen.

Angiv antallet af WLAN-godkendelsesforsøg

En anmodning om godkendelse er en bekræftelse på brugerens logonlegitimationsoplysninger. Det sker, når en telefon, der allerede er tilsluttet et Wi-Fi-netværk, forsøger at oprette forbindelse til Wi-Fi-serveren. Det kan f.eks. være, når der er timeout for en Wi-Fi-session, eller en Wi-Fi-forbindelse mistes og derefter oprettes igen.

Du kan konfigurere det antal gange en Wi-Fi-telefon sender en godkendelsesansøgning til Wi-Fi-serveren. Standardantallet af forsøg er 2, men du kan indstille denne parameter fra 1 til 3. Hvis en telefon ikke kan godkendes, bliver brugeren bedt om at logge på igen.

Du kan anvende WLAN-godkendelsesforsøg for individuelle telefoner, for en gruppe af telefoner eller for alle Wi-Fi-telefonerne i dit netværk.

Fremgangsmåde

- Trin 1** Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration, og find telefonen.
 - Trin 2** Gå til området Produktspecifik konfiguration, og indstil feltet **WLAN-godkendelsesforsøg**.
 - Trin 3** Vælg **Gem**.
 - Trin 4** Vælg **Anvend konfig**.
 - Trin 5** Genstart telefonen.
-

Aktivér WLAN-beskedtilstand

Aktivér WLAN-profil 1 – beskedtilstand, hvis du ønsker, at en bruger skal logge på Wi-Fi-netværket, når deres telefon startes eller nulstilles.

Fremgangsmåde

- Trin 1** Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration.
 - Trin 2** Find den telefon, du skal konfigurere.
 - Trin 3** Gå til området Produktivspecifik konfigurationsområde, og indstil feltet **WLAN-profil 1– beskedtilstand til Aktivér**.
 - Trin 4** Vælg **Gem**.
 - Trin 5** Vælg **Anvend konfig**.
 - Trin 6** Genstart telefonen.
-

Konfigurer en Wi-Fi-profil ved hjælp af Cisco Unified Communications Manager

Du kan konfigurere en Wi-Fi-profil og derefter tildele en profil til de telefoner, der understøtter Wi-Fi. Profilen indeholder de parametre, der kræves for, at telefoner kan oprette forbindelse til Cisco Unified Communications Manager med Wi-Fi. Når du opretter og bruger en Wi-Fi-profil, behøver du eller dine brugere ikke konfigurere det trådløse netværk for individuelle telefoner.

Wi-Fi-profiler er understøttet på Cisco Unified Communications Manager-version 10.5 (2) eller nyere. EAP-FAST, PEAP-GTC og PEAP-MSCHAPv2 understøttes i Cisco Unified Communications Manager version 10.0 og senere. EAP-TLS understøttes i Cisco Unified Communications Manager version 11.0 og senere.

En Wi-Fi-profil giver dig mulighed at forhindre eller begrænse ændringer af Wi-Fi-konfigurationen på telefonen efter brugeren.

Vi anbefaler, at du bruger en sikker profil med TFTP-kryptering aktiveret for at beskytte nøgler og adgangskoder, når du bruger en Wi-Fi-profil.

Når du konfigurerer telefoner til at bruge EAP-FAST-, PEAP-MSCHAPv2- eller PEAP-GTC-godkendelse, skal dine brugere have individuelle bruger-id'er og adgangskoder for at kunne logge på telefonen.

Telefonerne understøtter kun ét servercertifikat, der kan installeres enten med SCEP eller den manuelle installationsmetode, men ikke med begge metoder. Telefonerne understøtter ikke metoden TFTP for certifikatinstallationen.

Fremgangsmåde

-
- Trin 1** Vælg **Enhed > Enhedsindstillinger > Trådløs LAN-profil** i Cisco Unified Communications Manager Administration.
- Trin 2** Klik på **Tilføj ny**.
- Trin 3** Angiv parametrene i **Oplysninger om trådløs LAN-profil**:
- **Navn** – angiv et entydigt navn på Wi-Fi-profilen. Dette navn vises på telefonen.
 - **Beskrivelse** – angiv en beskrivelse af Wi-Fi-profilen, så du kan skelne denne profil fra andre Wi-Fi-profiler.
 - **Kan redigeres af bruger** – vælg en indstilling:
 - **Tilladt** – angiver, at brugerne kan foretage ændringer af Wi-Fi-indstillingerne på deres telefon. Denne indstilling vælges som standard.
 - **Ikke tilladt** – angiver, at brugerne ikke kan foretage ændringer af Wi-Fi-indstillingerne på deres telefon.
 - **Begrænset** – angiver, at brugerne kan ændre Wi-Fi-brugernavnet og adgangskoden på deres telefon. Men brugere må ikke foretage ændringer af andre Wi-Fi-indstillingerne på telefonen.
- Trin 4** Indstil parameterværdierne i sektionen **Trådløse indstillinger**:
- **SSID (netværksnavn)** – Angiv det netværksnavn, der er tilgængeligt i det brugermiljø, som telefonen kan tilsluttes. Dette navn vises på listen over tilgængelige netværk på telefonen, og telefonen har forbindelse til dette trådløse netværk.
 - **Frekvensbånd** – de mulige indstillinger er automatisk, 2,4 GHz og 5 GHz. Dette felt angiver det frekvensbånd, den trådløse forbindelse bruger. Hvis du vælger automatisk, forsøger telefonen at bruge 5 GHz båndet først og bruger kun 2,4 GHz, når 5 GHz ikke er tilgængeligt.
- Trin 5** I sektionen **Godkendelsesindstillinger** skal du indstille **Godkendelsesmetode** til en af disse godkendelsesmetoder: EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP og Ingen.
- Når du har angivet dette felt, kan du muligvis se flere felter, du skal konfigurere.
- **Brugercertifikat** – kræves til EAP-TLS-godkendelse. Vælg **Produktionsinstalleret** eller **Brugerinstalleret**. Telefonen kræver, at der er installeret et certifikat, enten automatisk fra SCEP eller manuelt fra administrationssiden på telefonen.
 - **PSK-adgangskode** – påkrævet for PSK-godkendelse. Angiv adgangskoden på 8-63 ASCII-tegn eller 64 hex-tegn.
 - **WEP-nøgle** – påkrævet for WEP-godkendelse. Indtast 40/102 eller 64/128 ASCII eller Hex WEP-nøglen.
 - 40/104 ASCII er 5 tegn.

- 64/128 ASCII er 13 tegn.
- 40/104 HEX er 10 tegn.
- 64/128 HEX er 26 tegn.

- **Angiv delte legitimationsoplysninger:** påkrævet til EAP-FAST PEAP MSCHAPv2- og PEAP GTC-godkendelse.
 - Hvis brugeren administrerer brugernavn og adgangskode, skal felterne **Brugernavn** og **Adgangskode** være tomme.
 - Hvis alle dine brugere deler den samme brugernavn og adgangskode, kan du angive oplysningerne i felterne **Brugernavn** og **Adgangskode**.
 - Angiv en beskrivelse i feltet **Beskrivelse af adgangskode**.

Bemærk Hvis du skal knytte et entydigt brugernavn og en entydig adgangskode til hver bruger, skal du oprette en profil for hver bruger.

Trin 6 Klik på **Gem**.

Næste trin

Anvend WLAN-profilgruppen på en enhedspulje (**System > Enhedspulje**) eller direkte på telefonen (**Enhed > Telefon**).

Konfigurer en Wi-Fi gruppe ved hjælp af Cisco Unified Communications Manager

Du kan oprette en trådløs LAN-profilgruppe og føje en trådløs LAN-profil til denne gruppe. Profilgruppen kan derefter tildeles til telefonen, når du konfigurerer telefonen.

Fremgangsmåde

- Trin 1** Vælg **Enhed > Enhedsindstillinger > Profilgruppe for trådløst LAN** i Cisco Unified Communications Administration.
- Du kan også definere den profilgruppe for trådløst LAN fra **System > Enhedspulje**.
- Trin 2** Klik på **Tilføj ny**.
- Trin 3** Angiv et gruppenavn og en beskrivelse i sektionen **Oplysninger om gruppeprofil for trådløst LAN**.
- Trin 4** I sektionen **Profile for denne profilgruppe for trådløst LAN** skal du vælge en tilgængelig profil fra listen **Tilgængelige profiler** og flytte den valgte profil til listen **Valgte profiler**.
- Når mere end en trådløse LAN-profil er valgt, bruger telefonen kun den første trådløse LAN-profil.
- Trin 5** Klik på **Gem**.

Kontrollér start af telefon

Når telefonen er blevet tilsluttet strøm, går den automatisk gennem en diagnosticeringsproces i starten.

Fremgangsmåde

Sæt strøm til telefonen.

Når hovedskærmen vises, er den startet korrekt.

Skift en brugers telefonmodel

Du eller din bruger kan ændre en brugers telefonmodel. Ændringen kan være nødvendig af et antal grunde, f.eks. hvis:

- Du har opdateret din Cisco Unified Communications Manager (Unified CM) til en softwareversion, der ikke understøtter telefonmodellen.
- Brugeren ønsker en anden telefonmodel end den aktuelle model.
- Telefonen kræver reparation eller udskiftning.

Unified CM identificerer den gamle telefon og bruger den gamle telefonens MAC-adresse til at identificere den gamle telefonkonfiguration. Unified CM kopierer den gamle telefonkonfiguration til posten for den nye telefon. Den nye telefon har derefter samme konfiguration som den gamle telefon.

Begrænsning : Hvis den gamle telefon har flere linjer eller linjetaster end den nye telefon, har den nye telefon ingen ekstra linjer eller linjetaster konfigureret.

Telefonen genstarter, når konfigurationen er fuldført.

Inden du begynder

Konfigurer Cisco Unified Communications Manager ifølge instruktionerne i *Funktionskonfigurationsvejledningen til Cisco Unified Communications Manager*.

Du skal bruge en ny, ubenyttet telefon, der leveres forudinstalleret med firmware version 12.8 (1) eller senere.

Fremgangsmåde

- | | |
|---------------|---|
| Trin 1 | Sluk for den gamle telefon. |
| Trin 2 | Tænd den nye telefon. |
| Trin 3 | Vælg Erstat en eksisterende telefon på den nye telefon. |
| Trin 4 | Angiv det primære lokalnummer for den gamle telefon. |
| Trin 5 | Hvis den gamle telefon har angivet en pinkode, skal du angive pinkoden. |
| Trin 6 | Tryk på Send . |

Trin 7 Hvis der er mere end én enhed til brugeren, skal du vælge den enhed, der skal erstattes, og trykke på **Fortsæt**.



KAPITEL 5

Telefoninstallation med Cisco Unified Communications Manager

- [Konfigurer en Cisco IP-konferencetelefon, på side 55](#)
- [Bestem telefonens MAC-adresse, på side 59](#)
- [Metoder til tilføjelse af telefoner, på side 60](#)
- [Føj brugere til Cisco Unified Communications Manager, på side 61](#)
- [Føj bruger til en slutbrugergruppe, på side 63](#)
- [Tilknyt telefoner til brugere, på side 63](#)
- [Survivable Remote Site Telephony, på side 64](#)

Konfigurer en Cisco IP-konferencetelefon

Hvis automatisk registrering ikke er aktiveret, og telefonen ikke findes i Cisco Unified Communications Manager-databasen, skal du konfigurere Cisco IP-telefon manuelt i Cisco Unified Communications Manager Administration. Visse opgaver i denne procedure er valgfrie. Det afhænger af dit system og brugernes behov.

Få flere oplysninger om disse trin i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Udfør konfigurationstrinnene i følgende procedure ved hjælp af Cisco Unified Communications Manager Administration.

Fremgangsmåde

Trin 1

Indsaml følgende oplysninger om telefonen:

- Telefonmodel
- MAC-adresse: se [Bestem telefonens MAC-adresse, på side 59](#)
- Fysisk placering af telefonen
- Navn eller bruger-id for telefonens bruger
- Enhedspulje
- Partition, opkaldssøgeområde og oplysninger om placering

- Telefonnummer (DN) til at tildele til telefonen
- Cisco Unified Communications Manager-bruger, der skal knyttes til telefonen
- Oplysninger om brug af telefonen, der påvirker programtastskabelonen, telefonfunktionerne, IP-telefontjenesterne eller telefonapplikationerne

Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager, og se de relaterede links.

Trin 2 Kontrollér, at du har det tilstrækkelige antal enhedslicenser til din telefon.

Få flere oplysninger ved at se licensdokumentet til din specifikke version af Cisco Unified Communications Manager.

Trin 3 Definer enhedspuljerne. Vælg **System > Enhedspulje**.

Enhedspuljer definerer fælles egenskaber for enheder, f.eks. område dato/klokkeslæt-gruppe og programtastskabelon.

Trin 4 Definer den almindelige telefonprofil. Vælg **Enhed > Enhedsindstillinger > Almindelig telefonprofil**.

Almindelig telefonprofiler giver de data, som Cisco TFTP-serveren kræver samt almindelige telefonindstillinger som f.eks. Forstyr ikke og indstillinger til styring af funktioner.

Trin 5 Definer et opkaldssøgeområde. Klik på **Distribution af opkald > Styringsklasse > Opkaldssøgeområde** i Cisco Unified Communications Manager Administration.

Et opkaldssøgeområde er en samling partitioner, der søges i for at finde ud af, hvordan et kaldt nummer er blevet distribueret. Opkaldssøgeområdet for enheden og opkaldssøgeområdet for telefonbogsnummeret bruges sammen. Telefonbogsnummerets CSS har forrang i forhold til telefonens CSS.

Trin 6 Konfigurer en sikkerhedsprofil for enhedstype og -protokol. Vælg **System > Sikkerhed > Telefonsikkerhedsprofil**.

Trin 7 Konfigurer telefonen. Vælg **Enhed > Telefon**.

- Find den telefon, du vil ændre, eller tilføj en ny telefon.
- Konfigurer telefonen ved at udføre de krævede felter i ruden Enhedsinformation i vinduet Telefonkonfiguration.

- MAC-adresse (krævet): Sørg for, at værdien omfatter 12 hexadecimalte tegn.
- Beskrivelse: Angiv en nyttig beskrivelse, der kan hjælpe dig, hvis du skal søge efter oplysninger om denne bruger.
- Enhedspulje (krævet)
- Almindelig telefonprofiler
- CSS (Class of Control)
- Sted
- Ejer (bruger eller anonym), og hvis brugeren er markeret, ejerens bruger-id

Enheden og dens standardindstillinger føjes til Cisco Unified Communications Manager-database.

Få oplysninger om produktspecifikke konfigurationsfelter i “?” Knaphjælp i vinduet Telefonkonfiguration og det relaterede link.

Bemærk Hvis du vil føje både telefonen og brugeren til Cisco Unified Communications Manager-databasen på samme tid, skal du se i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

- c) Vælg en enhedssikkerhedsprofil i området med protokolspecifikke oplysninger, og indstil sikkerhedstilstanden.

Bemærk Vælg en sikkerhedsprofil, der er baseret på firmaets overordnede sikkerhedsstrategi. Hvis telefonen ikke understøtter sikkerhed, skal du vælge en profil, der ikke er sikker.

- d) Markér afkrydsningsfeltet Aktivér Extension Mobility i Oplysninger om lokalnummer, hvis telefonen understøtter Cisco Extension Mobility.

- e) Klik på **Gem**.

Trin 8 Vælg **Enhed > Enhedsindstillinger > SIP-profil** til konfiguration af SIP-parametre.

Trin 9 Vælg **Enhed > Telefon** for at konfigurere telefonbogsnumre (linjer) på telefonen for at udfylde de krævede felter i vinduet Directory Number Configuration (Konfiguration af nummer).

- a) Find telefonen.

- b) Klik på linje 1 i vinduet Telefonkonfiguration i vinduets venstre rude.

Konferencetelefoner har kun én linje.

- c) Angiv et gyldigt nummer, der kan ringes til i feltet Telefonnummer.

Bemærk Dette felt skal indeholde det samme nummer, der vises i feltet Telefonnummer i vinduet Konfiguration af slutbrugere.

- d) Vælg den partition, som telefonnummeret hører til, på rullelisten Rutepartition. Hvis du ikke vil begrænse adgangen til telefonnummeret, skal du vælge <None> for partitionen.

- e) Vælg det relevante opkaldssøgeområde på rullelisten Opkaldssøgeområde. Den værdi, du vælger, gælder for alle enheder, der bruger dette telefonnummer.

- f) Vælg elementerne og tilhørende destinationer, som opkald skal sendes til, i området Indstillinger for besvarelse af opkald og viderestilling af opkald (f.eks. Medflyt, Viderestil ved optaget internt).

Eksempel:

Hvis indgående og eksterne opkald, der modtager et optaget signal, skal viderestilles til voicemailen for denne linje, skal du markere afkrydsningsfeltet Voicemail ud for Forward Busy Internal- og Forward Busy External-elementer i den venstre kolonne i området Indstillinger for besvarelse af opkald og viderestilling af opkald.

- g) Konfigurer følgende felter i linje 1 i ruden Enhed:

- Visning (Internt opkalder-id): Du kan angive brugerens fornavn og efternavn for denne enhed, så dette navn vises for alle interne opkald. Lad feltet være tomt, så systemet viser telefonens lokalnummer.
- Ekstern telefonnummermaske: Angiv telefonnummer (eller maske), der bruges til at sende oplysninger om opkalder-ID, når et opkald foretages fra denne linje. Du kan angive maksimalt 24 numeriske og "X" tegn. X'er repræsenterer telefonnummeret og skal vises efter mønstret.

Eksempel:

Hvis du angiver masken 408902XXXX, viser et eksternt opkald fra lokalnummer 6640 opkalds-ID-nummeret 4089026640.

Denne indstilling gælder kun for den aktuelle enhed, medmindre du skal markere afkrydsningsfeltet til højre (Update Shared Device Settings), og klik på **Udfyld valgte**. Afkrydsningsfeltet til højre vises kun, hvis andre enheder deler dette telefonnummer.

h) Vælg **Gem**.

Få flere oplysninger om telefonnumre i dokumentationen til din specifikke version af Cisco Unified Communications Manager, og se de relaterede links.

Trin 10 (Valgfri) Tilknyt brugeren til en telefon. Klik på **Tilknyt slutbrugere** nederst i vinduet Telefonkonfiguration for at knytte en bruger til den linje, der konfigureres.

- a) Brug **Find** sammen med søgefelterne for at finde brugeren.
- b) Markér afkrydsningsfeltet ud for brugernavnet, og klik på **Tilføj valgte**.

Brugernavnet og bruger-ID'et vises i ruden Brugere tilknyttet til i vinduet Konfiguration af telefonnummer.

c) Vælg **Gem**.

Brugeren er nu knyttet til linje 1 på telefonen.

Trin 11 (Valgfri) Tilknyt brugeren til enheden:

- a) Vælg **Brugeradministration > Slutbrugere**.
- b) Brug søgefelterne og **Find** til at finde den bruger, du har tilføjet.
- c) Klik på bruger-id'et.
- d) Indstil det primære lokalnummer på rullelisten i skærmområdet Tilknytninger af telefonnumre.
- e) (Valgfri) Markér feltet Aktivér mobilitet i området Mobilitetsoplysninger.
- f) Brug knapperne **Føj til adgangskontrolgruppe** i området Oplysninger om tilladelser til at føje denne bruger til brugergrupper.

Det kunne f.eks. være, at du vil føje brugeren til en gruppe, der er defineret som en standard-CCM-slutbrugergruppe.

- g) Få vist oplysningerne om en gruppe ved at vælge den og klikke på **Vis detaljer**.
- h) Markér feltet Aktivér Extension Mobility Cross Cluster i området Extension Mobility, hvis brugeren kan bruge Extension Mobility Cross Cluster-tjenesten.
- i) Klik på **Enhedstilknævninger** i området Enhedsinformation.
- j) Brug søgefelterne og **Find** for at finde den enhed, du vil knytte til brugeren.
- k) Vælg enheden, og klik på **Gem valgte/ændringer**.
- l) Klik på **Gå** ud for det relaterede link "Tilbage til bruger" i skærmens øverste højre hjørne.
- m) Vælg **Gem**.

Trin 12 Tilpas programtastskabelonerne. Vælg **Enhed > Enhedsindstillinger > Programtastskabelon**.

Brug siden til at tilføje, slette eller ændre rækkefølgen af programtastfunktioner, der vises på brugerens telefon, så de overholder kravene til brugen af funktionerne.

Konferencetelefonen har af særlige krav for programtaster. Se de relaterede links for at få flere oplysninger.

Trin 13 Konfigurer Cisco IP-telefon-tjenesterne, og tildel tjenester. Vælg **Enhed > Enhedsindstillinger > Telefontjenester**.

Leverer IP-telefontjenester til telefonen.

Bemærk Brugere kan tilføje eller ændre tjenester på deres telefoner ved hjælp af selvbetjeningsportalen til Cisco Unified Communications.

Trin 14 (Valgfri) Føj brugeroplysninger til den globale telefonbog for Cisco Unified Communications Manager. Vælg **Brugeradministration > Slutbruger**, og klik derefter på **Tilføj ny**, og konfigurér de krævede felter. Obligatoriske felter er angivet med en stjerne (*).

Bemærk Hvis dit firma bruger en LDAP-telefonbog (Lightweight Directory Access Protocol) til at lagre oplysninger om brugerne, kan du installere og konfigurere Cisco Unified Communications til at bruge din eksisterende LDAP-telefon. Se [Opsætning af firmatelefonbog, på side 123](#). Når feltet Enable Synchronization from the LDAP Server (Aktivér synkronisering fra LDAP-server) er blevet aktiveret, kan du ikke tilføje flere brugere fra Cisco Unified Communications Manager Administration.

- Indstil felterne for bruger-id og efternavn.
- Tildel en adgangskode (til selvbetjeningsportal).
- Tildel en pinkode (til Cisco Extension Mobility og personlig telefonbog).
- Tilknyt brugeren til en telefon.

Giver brugerne kontrol over deres telefon som f.eks. viderestilling af opkald eller tilføjelse af hurtigopkaldsnumre eller -tjenester.

Bemærk Visse telefon som f.eks. dem i konferencerum, har ikke en tilknyttet bruger.

Trin 15 (Valgfri) Tilknyt en bruger til en brugergruppe. Vælg **Brugeradministration > Brugerindstillinger > Adgangskontrolgruppe**.

Tildel brugerne en fælles liste over roller og tilladelser, der gælder for alle brugerne i en brugergruppe. Administratorer kan styre brugergrupper, roller og tilladelser, så de kan styre adgangsniveauet (og derfor sikkerhedsniveauet) for systembrugere.

Hvis slutbrugere skal have adgang til selvbetjeningsportalen til Cisco Unified Communications, skal du føje brugere til standardgruppen af slutbrugere i Cisco Communications Manager.

Lignende emner

- [Produktspecifik konfiguration](#), på side 95
- [Funktioner og konfiguration af Cisco IP-konferencetelefon](#), på side 91
- [Cisco Unified Communications Manager Dokumentation](#), på side 14
- [Konfigurer ny programtastskabelon](#), på side 92

Bestem telefonens MAC-adresse

For at føje telefoner til Cisco Unified Communications Manager skal du først bestemme MAC-adressen til en telefon.

Fremgangsmåde

Udfør en af følgende handlinger:

- Tryk på **Indstillinger > Telefonoplysninger** på telefonen, og se efter feltet MAC-adresse.
- Se efter MAC-etiketten bag på telefonen.

- Vis websiden for telefonen, og klik på **Enhedsoplysninger**.
-

Metoder til tilføjelse af telefoner

Når du har installeret Cisco IP-telefon, kan du vælge en af følgende valgmuligheder til at føje telefoner til Cisco Unified Communications Manager-databasen.

- Brug Cisco Unified Communications Manager Administration til at tilføje telefoner individuelt
- Brug BAT (Bulk Administration Tool) til at tilføje flere telefoner
- Automatisk registrering
- BAT og TAPS (Tool for Auto-Registered Phones Support)

Før du kan tilføje telefoner individuelt eller med BAT, skal du bruge telefonens MAC-adresse. Hvis du ønsker yderligere oplysninger, kan du se [Bestem telefonens MAC-adresse, på side 59](#).

Få flere oplysninger om BAT (Bulk Administration Tool) i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Tilføj telefoner individuelt

Indsaml oplysningerne om MAC-adressen og telefonen for den telefon, du vil føje til Cisco Unified Communications Manager.

Fremgangsmåde

Trin 1 Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration.

Trin 2 Klik på **Tilføj ny**.

Trin 3 Vælg telefontypen.

Trin 4 Vælg **Næste**.

Trin 5 Fuldfør oplysningerne om telefonen, herunder MAC-adressen.

Få de fuldstændige og begrebsmæssige oplysninger om Cisco Unified Communications Manager i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Trin 6 Vælg **Gem**.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Tilføj telefoner ved hjælp af BAT-telefonskabelon

Cisco Unified Communications Bulk Administration Tool (BAT) gør det muligt at udføre batchhandling, herunder registrering af flere telefoner.

Hvis du vil tilføje telefoner udelukkende ved hjælp af BAT (ikke i forbindelse med TAPS), skal du få fat i den relevante MAC-adresse for hver telefon.

Få flere oplysninger om brugen af BAT i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Fremgangsmåde

- Trin 1** Vælg **Masseadministration > Telefoner > Telefonskabelon** i Cisco Unified Communications Administration.
- Trin 2** Klik på **Tilføj ny**.
- Trin 3** Vælg en telefontype, og klik på **Næste**.
- Trin 4** Angiv oplysningerne til de telefonspecifikke parametre, f.eks. enhedspulje, telefonknapskabelon og enhedssikkerhedsprofil.
- Trin 5** Klik på **Gem**.
- Trin 6** Vælg **Enhed > Telefon > Tilføj ny** for at tilføje en telefon ved hjælp af BAT-telefonskabelonen.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Føj brugere til Cisco Unified Communications Manager

Du kan vise og bevare oplysninger om de brugere, der er registreret i Cisco Unified Communications Manager. Cisco Unified Communications Manager giver også hver bruger mulighed for at udføre disse opgaver:

- Få adgang til firmatelefonbogen og andre tilpassede telefonbøger fra en Cisco IP-telefon.
- Opret en personlig telefonbog
- Konfigurer hurtigopkald og numre til viderestilling af opkald.
- Abonner på tjenester, der er tilgængelige fra en Cisco IP-telefon.

Fremgangsmåde

- Trin 1** Læs om tilføjelse af enkelte brugere under [Føj bruger direkte til Cisco Unified Communications Manager](#), på side 62.
 - Trin 2** Hvis du vil tilføje brugere i batches, skal du bruge BAT (Bulk Administration Tool). Med denne metode kan du også indstille en identisk standardadgangskode for alle brugere.
Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.
-

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Tilføj en bruger fra en ekstern LDAP-telefonbog

Hvis du har føjet en bruger til en LDAP-telefonbog (en telefonbog, der ikke er relateret til Cisco Unified Communications Server), kan du øjeblikkeligt synkronisere LDAP-telefonbogen med den Cisco Unified Communications Manager, på hvilken du tilføjer brugeren og brugertelefonen.



Bemærk Hvis du ikke synkroniserer LDAP-telefonbogen med Cisco Unified Communications Manager med det samme, bestemmer tidsplanen for synkronisering af LDAP-telefonbogen i vinduet for LDAP-telefonbogen, hvornår den næste automatiske synkronisering planlægges til. Synkronisering skal forekomme, før du kan tilknytte en ny bruger til en enhed.

Fremgangsmåde

- Trin 1** Log på Cisco Unified Communications Manager Administration.
- Trin 2** Vælg **System > LDAP > LDAP-telefonbog**.
- Trin 3** Brug **Find** til at finde din LDAP-telefonbog.
- Trin 4** Klik på navnet på LDAP-telefonbogen.
- Trin 5** Klik på **Udfør fuld synkronisering nu**.

Føj bruger direkte til Cisco Unified Communications Manager

Hvis du ikke bruger en LDAP-telefonbog (Lightweight Directory Access Protocol), kan du tilføje en bruger direkte ved hjælp af Cisco Unified Communications Manager Administration ved at følge disse trin.



Bemærk Hvis LDAP er synkroniseret, kan du ikke tilføje en bruger med Cisco Unified Communications Manager Administration.

Fremgangsmåde

- Trin 1** Vælg **Brugeradministration > Slutbruger** i Cisco Unified Communications Manager Administration.
- Trin 2** Klik på **Tilføj ny**.
- Trin 3** Angiv følgende i ruden med brugeroplysninger:
 - Bruger-id: Angiv slutbrugers id-navn. Cisco Unified Communications Manager tillader ikke redigering af bruger-id'et, efter at det er oprettet. Du kan bruge følgende specialtegn: =, +, <, >, #,;, \, " og mellemrumstegn. **Eksempel:** johndoe

- Adgangskode og Bekræft adgangskode: Angiv fem eller flere alfanumeriske tegn eller specialtegn som adgangskode for slutbruger. Du kan bruge følgende specialtegn: =, +, <, >, #, ;, \, , " og mellemrumstegn.
- Efternavn: Angiv slutbrugerens efter navn. Du kan bruge følgende specialtegn: =, +, <, >, #, ;, \, , " og mellemrumstegn. **Eksempel:** doe
- Telefonnummer: Angiv det primære telefonbogsnummer for slutbrugeren. Slutbrugere kan have flere linjer på deres telefoner. **Eksempel:** 26640 (John Does interne firmatelefonnummer)

Trin 4 Klik på **Gem**.

Føj bruger til en slutbrugergruppe

Hvis du vil føje en bruger til standardslutbrugergruppen i Cisco Unified Communications Manager, skal du foretage disse trin:

Fremgangsmåde

- Trin 1** Vælg **Brugeradministration > Brugerindstillinger > Adgangskontrolgruppe** i Cisco Unified Communications Manager Administration.
- Vinduet Find og vis brugere vises.
- Trin 2** Angiv de relevante søgekriterier, og klik på **Find**.
- Trin 3** Vælg linket **Standard-CCM-slutbrugere**. Vinduet Konfiguration af brugergruppe til standard-CCM-slutbrugere vises.
- Trin 4** Vælg **Føj slutbrugere til gruppe**. Vinduet Find og vis brugere vises.
- Trin 5** Brug felterne på rullelisten Find bruger til at finde de brugere, du vil tilføje, og klik på **Find**.
- Der vises en liste over de brugere, der matcher dine søgekriterier.
- Trin 6** Klik på afkrydsningsfeltet ud for de brugere, du vil føje til denne brugergruppe, på listen over poster. Hvis listen er lang, kan du bruge linksene nederst til at se flere resultater.
- Bemærk** Listen over søgeresultater viser ikke brugere, der allerede tilhører brugergruppen.
- Trin 7** Vælg **Tilføj valgt**.
-

Tilknyt telefoner til brugere

Du kan tilknytte telefoner til brugere i vinduet Slutbruger i Cisco Unified Communications Manager.

Fremgangsmåde

-
- Trin 1** Vælg **Brugeradministration > Slutbruger** i Cisco Unified Communications Manager Administration. Vinduet Find og vis brugere vises.
- Trin 2** Angiv de relevante søgekriterier, og klik på **Find**.
- Trin 3** Vælg linket til brugeren på den liste over poster, der vises.
- Trin 4** Vælg **Enhedstilknytning**.
Vinduet Tilknytning af brugerenheder.
- Trin 5** Angiv de relevante søgekriterier, og klik på **Find**.
- Trin 6** Vælg den enhed, du vil knytte til brugeren, ved at markere feltet til venstre for enheden.
- Trin 7** Vælg **Gem valgte/ændringer** for at knytte enheden til brugeren.
- Trin 8** Vælg **Tilbage til bruger**, og klik på **Gå** på rullelisten Relaterede links i øverste højre hjørne af vinduet. Vinduet Konfiguration af slutbrugere, og de tilknyttede enheder, du har valgt, vises i ruden Styrede enheder.
- Trin 9** Vælg **Gem valgte/ændringer**.
-

Survivable Remote Site Telephony

SRST (Survivable Remote Site Telephony) sikrer, at telefonens basisfunktioner forbliver tilgængelige, når kommunikation med den styrende Cisco Unified Communications Manager er ødelagt. I dette scenarie kan telefonen holde et igangværende opkald aktivt, og brugeren kan få adgang til et undersæt af tilgængelige funktioner. Når der opstår failover, modtager brugeren en meddelelse på telefonen.

Få oplysninger om SRST under <https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html>

Følgende tabel beskriver tilgængeligheden af funktioner under failover.

Tabel 14: Understøttelse af SRST-funktion

| Funktion | Understøttet | Bemærkninger |
|---------------|--------------|-------------------------------|
| Nyt opk | Ja | |
| Afslut opkald | Ja | |
| Gentag | Ja | |
| Besvar | Ja | |
| Hold | Ja | |
| Genoptag | Ja | |
| Konference | Ja | Kun 3-vejs og lokal blanding. |

| Funktion | Understøttet | Bemærkninger |
|---|--------------|--|
| Konferenceliste | Nej | |
| Omstilling | Ja | Kun rådgivning. |
| Omstil til Aktive opkald (direkte overførsel) | Nej | |
| Autosvar | Ja | |
| Ventende opkald | Ja | |
| Opkalder | Ja | |
| Præsentation af forenet session | Ja | Konference er den eneste understøttede funktion pga. andre funktionsbegrænsninger. |
| Voicemail | Ja | Voicemail synkroniseres ikke med andre brugere i Cisco Unified Communications Manager-klyngen. |
| Viderestil alle | Ja | Viderestillingstilstanden er kun tilgængelig på den telefon, der indstiller viderestilling, da der ikke er nogen delt linje i SRST-tilstand. Indstillingerne for Viderestil alle opkald bevares ikke på failover til SRST fra Cisco Unified Communications Manager eller fra SRST fail-back til Communications Manager. Enhver original Viderestil alle opkald, der stadig er på Communications Manager, bør indikeres, når enheden genetablerer forbindelsen til Communications Manager efter failover. |
| Hurtigkald | Ja | |
| Til voicemail (IDivert) | Nej | Programtasten IDivert vises ikke. |
| Linjefiltre | Delvis | Linjer understøttes, men kan ikke deles. |
| Overvåget parkering | Nej | Programtasten Parker vises ikke. |
| Udvidet indikator for ventende meddelelse | Ja | Felter med antal meddelelser vises på telefonskærmen. |
| Direkte parkering | Nej | Programtasten vises ikke. |
| Retur fra Hold | Ja | |
| Fjernopkald i vente-position | Nej | Opkald vises som opkald i lokal vente-position. |
| Mød Mig | Nej | Programtasten Mød mig vises ikke. |

| Funktion | Understøttet | Bemærkninger |
|-------------------------------|---------------------|---|
| GrSvar | Ja | |
| Gruppesvar | Nej | Programtasten vises ikke. |
| Gruppesvar, tilknyttet gruppe | Nej | Programtasten vises ikke. |
| Id for ondsindede opkald | Ja | |
| QRT | Ja | |
| Søgegruppe | Nej | Programtasten vises ikke. |
| Mobilitet | Nej | Programtasten vises ikke. |
| Privat | Nej | Programtasten vises ikke. |
| Ring tilb. | Nej | Programtasten Notering vises ikke. |
| Tjeneste URL | Ja | Den programmerbare linje nøgle med en tjeneste-URL, der er tildelt, vises ikke. |



KAPITEL 6

Styring af selvbetjeningsportal

- [Oversigt over selvbetjeningsportal, på side 67](#)
- [Konfigurer brugeradgang til selvbetjeningsportalen, på side 67](#)
- [Tilpas visning af selvbetjeningsportal, på side 68](#)

Oversigt over selvbetjeningsportal

Brugerne kan fra selvbetjeningsportalen i Cisco Unified Communications tilpasse og styre telefonfunktioner og -indstillinger.

Som administratoren kan du styre adgangen til selvbetjeningsportalen. Du skal også angive oplysninger til dine brugere, så de har adgang til selvbetjeningsportalen.

Før en bruger kan få adgang til Cisco Unified Communications-selvbetjeningsportalen, skal du bruge Cisco Unified Communications Manager Administration til at føje brugeren til en Cisco Unified Communications Manager-standardgruppe for slutbrugere.

Du skal også give slutbrugere følgende oplysninger om selvbetjeningsportalen:

- URL-adressen til at få adgang til programmet. Denne URL-adresse er:
`https://<server_name:portnummer>/ucmuser/`, hvor servernavnet er den vært, som webserveren er installeret på, og portnummeret er portnummeret på den pågældende vært.
- Et bruger-id og en standardadgangskode til at få adgang til programmet.
- En oversigt over de opgaver, som brugerne kan løse med portalen.

Disse indstillinger svarer til de værdier, du angav, da du føjede brugeren til Cisco Unified Communications Manager.

Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Konfigurer brugeradgang til selvbetjeningsportalen

Før en bruger kan få adgang til selvbetjeningsportalen, skal du godkende adgangen.

Fremgangsmåde

- Trin 1** Gå til Cisco Unified Communications Manager Administration, og vælg **Brugeradministration > Slutbruger**.
 - Trin 2** Søg efter brugeren.
 - Trin 3** Klik på linket bruger-id.
 - Trin 4** Sørg for, at brugeren har en adgangskode og pinkode konfigureret.
 - Trin 5** I afsnittet Tilladelsesoplysninger skal du sikre dig, at listen Grupper indeholder **Standard-CCM-slutbrugere**.
 - Trin 6** Vælg **Gem**.
-

Tilpas visning af selvbetjeningsportal

De fleste indstillinger vises på selvbetjeningsportalen. Du skal imidlertid indstille følgende valgmuligheder ved hjælp af indstillingerne af Konfiguration af virksomhedsparametre i Cisco Unified Communications Manager Administration:

- Vis indstillinger for ringninger
- Vis indstillinger for linjemærkater



Bemærk Indstillingerne gælder for alle selvbetjeningsportalens sider på dit websted.

Fremgangsmåde

- Trin 1** Vælg **System > Virksomhedsparametre** i Cisco Unified Communications Manager Administration.
 - Trin 2** Indstil feltet **Standardserver til selvbetjeningsportal** i selvbetjeningsportalens område.
 - Trin 3** Aktivér eller deaktiver de parametre, brugerne kan få adgang til i portalen.
 - Trin 4** Vælg **Gem**.
-



DEL III

Administration af Cisco IP-konferencetelefon

- [Sikkerhed i Cisco IP-konferencetelefon, på side 71](#)
- [Tilpasning af Cisco IP-konferencetelefon, på side 87](#)
- [Funktioner og konfiguration af Cisco IP-konferencetelefon, på side 91](#)
- [Firmatelefonbog og personlig telefonbog, på side 123](#)



KAPITEL 7

Sikkerhed i Cisco IP-konferencetelefon

- [Oversigt over sikkerhed for Cisco IP-telefon, på side 71](#)
- [Sikkerhedsforbedringer til dit telefonnetværk, på side 72](#)
- [Understøttede sikkerhedsfunktioner, på side 73](#)

Oversigt over sikkerhed for Cisco IP-telefon

Sikkerhedsfunktionerne beskytter mod flere trusler, herunder trusler i forhold til identiteten af telefonen og dataene. Disse funktioner etablerer og opretholder godkendte kommunikationsstrømme mellem telefonen og Cisco Unified Communications Manager-servere og sikrer, at telefonen kun bruger filer, der er signeret digitalt.

Cisco Unified Communications Manager Release 8.5(1) og senere omfatter Security by Default, der giver følgende sikkerhedsfunktioner for Cisco IP-telefon, uden at køre CTL-klienten:

- Signering af telefonkonfigurationsfilerne
- Kryptering af telefonkonfigurationsfiler
- HTTPS med Tomcat og andre webtjenester



Bemærk Sikre signalerings- og mediefunktioner kræver stadig, at du kører CTL-klienten og bruger hardware-eTokens.

Få flere oplysninger om disse sikkerhedsfunktioner i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Et lokalt LSC (Locally Significant Certificate) installeres på telefoner, når du har udført de nødvendige opgaver, der er knyttet til CAPF (Certificate Authority Proxy Function). Du kan også bruge Cisco Unified Communications Manager Administration til at konfigurere en LSC. Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

En LSC kan ikke bruges som brugercertifikatet til EAP-TLS med WLAN-godkendelse.

Du kan også starte installationen af en LSC fra telefonens menu til sikkerhedsopsætning. I denne menu kan du også opdatere eller fjerne en LSC.

Cisco IP-konferencetelefon 8832 overholder FIPS (Federal Information Processing Standard). For at kunne fungere korrekt kræver FIPS-tilstanden en RSA-nøgle på 2048 bit eller mere. Hvis RSA-servercertifikatet ikke er på 2048 bit eller mere, registreres telefonen ikke i Cisco Unified Communications Manager, og

telefonen kan ikke registreres. Størrelsen på certificeringsnøglen er ikke FIPS-kompatibel vises i telefonens statusmeddelelser.

Du kan ikke bruge private nøgler (LSC eller MIC) i FIPS-tilstand.

Hvis telefonen har en eksisterende LSC, der er mindre end 2048 bit, skal du opdatere størrelsen af LSC-nøglen til 2048 bit eller mere, før FIPS aktiveres.

Lignende emner

- [Konfigurer et certifikat, der lokalt er væsentligt](#), på side 75
- [Cisco Unified Communications Manager Dokumentation](#), på side 14

Sikkerhedsforbedringer til dit telefonnetværk

Du kan aktivere Cisco Unified Communications Manager 11.5(1) og 12.0(1), så den fungerer i miljø med udvidet sikkerhed. Disse forbedringer gør, at dit telefonnetværk skal overholde et sæt strenge sikkerheds- og risikostyringskontroller, så du og dine brugere er beskyttet.

Cisco Unified Communications Manager 12.5 (1) understøtter ikke et forbedret sikkerhedsmiljø. Deaktiver FIPS før opgradering til Cisco Unified Communications Manager 12.5 (1), eller også vil din TFTP- og andre tjenester ikke fungere korrekt.

Det forbedrede sikkerhedsmiljø indeholder følgende funktioner:

- Autorisation af kontaktsøgning.
- TCP som standardprotokol til ekstern revisionslogføring.
- FIPS-tilstand.
- En forbedret politik om legitimationsoplysninger.
- Understøttelse af SHA-2-serien af hastværdier til digitale signaturer.
- Understøttelse af RSA-nøglestørrelse på 512 og 4096 bit.

Med Cisco Unified Communications Manager version 14.0 og firmwareversion 14.0 og senere til Cisco IP-telefon, understøtter telefonerne SIP OAuth-godkendelse.

OAuth understøttes for proxy-TFTP (Proxy Trivial File Transfer Protocol) med Cisco Unified Communications Managerversion 14.0(1) SU1 eller nyere og firmwareversion 14.1(1) til Cisco IP-telefon. Proxy-TFTP og OAuth til proxy-TFTP understøttes ikke på MRA (Mobile Remote Access).

Få yderligere oplysninger om sikkerhed under følgende:

- *Vejledning i systemkonfiguration til Cisco Unified Communications Manager*, version 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>).
- *Sikkerhedsvejledning til Cisco Unified Communications Manager* (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>)
- SIP OAuth: *Vejledning i funktionskonfiguration til Cisco Unified Communications Manager* (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>)



Bemærk Cisco IP-telefonen kan kun lagre et begrænset antal ITL-filer (Identity Trust List). ITL-filer kan ikke overskride grænsen på 64K på telefonen, så begræns antallet af filer, som Cisco Unified Communications Manager sender til telefonen.

Understøttede sikkerhedsfunktioner

Sikkerhedsfunktionerne beskytter mod flere trusler, herunder trusler i forhold til identiteten af telefonen og dataene. Disse funktioner etablerer og opretholder godkendte kommunikationsstrømme mellem telefonen og Cisco Unified Communications Manager-servere og sikrer, at telefonen kun bruger filer, der er signeret digitalt.

Cisco Unified Communications Manager Release 8.5(1) og senere omfatter Security by Default, der giver følgende sikkerhedsfunktioner for Cisco IP-telefon, uden at køre CTL-klienten:

- Signering af telefonkonfigurationsfilerne
- Kryptering af telefonkonfigurationsfiler
- HTTPS med Tomcat og andre webtjenester



Bemærk Sikre signalerings- og mediefunktioner kræver stadig, at du kører CTL-klienten og bruger hardware-eTokens.

Implementering af sikkerheden i Cisco Unified Communications Manager-systemet forhindrer identitetstyveri på telefonen, og Cisco Unified Communications Manager-serveren forhindrer datamanipulation og forhindrer manipulation af opkaldssignaler og mediestreams.

For at afhjælpe disse trusler etablerer og opretholder Cisco IP-telefon-netværket sikre (krypterede) kommunikationsstrømme mellem en telefon og serveren, signerer filer digitalt, før de overføres til en telefon, og krypterer mediestreams og opkaldssignaler mellem Cisco IP-telefon.

Et lokalt LSC (Locally Significant Certificate) installeres på telefoner, når du har udført de nødvendige opgaver, der er knyttet til CAPF (Certificate Authority Proxy Function). Du kan bruge Cisco Unified Communications Manager Administration til at konfigurere en LSC, sådan som det er beskrevet i Cisco Unified Communications Manager Security Guide. Du kan også starte installationen af en LSC fra telefonens menu til sikkerhedsopsætning. I denne menu kan du også opdatere eller fjerne en LSC.

En LSC kan ikke bruges som brugercertifikatet til EAP-TLS med WLAN-godkendelse.

Telefonerne bruger telefonsikkerhedsprofilen, der definerer, om enheden er sikker eller sikker. Få oplysninger om anvendelse af sikkerhedsprofilen på telefonen i dokumentationen til din specifikke version af Cisco Unified Communications Manager

Hvis du konfigurerer sikkerhedsmæssige indstillinger i Cisco Unified Communications Manager Administration, indeholder telefonkonfigurationsfilen følsomme oplysninger. For at sikre fortroligheden af en konfigurationsfil skal du konfigurere den til kryptering. Få mere detaljerede oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Implementering af sikkerheden i Cisco Unified Communications Manager-systemet forhindrer identitetstyveri på telefonen, og Cisco Unified Communications Manager-serveren forhindrer datamanipulation og forhindrer manipulation af opkaldssignaler og mediestreams.

Følgende tabel indeholder en oversigt over de sikkerhedsfunktioner, som Cisco IP-konferencetelefon 8832-serien understøtter. Få oplysninger om disse funktioner og om Cisco Unified Communications Manager og Cisco IP-telefon-sikkerhed ved at se i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Tabel 15: Oversigt over sikkerhedsfunktioner

| Funktion | Beskrivelse |
|--|---|
| Godkendelse af afbildning | Signerede binære filer (med filtype .sbn) forhindrer manipulation. Hvis afbildningen bliver manipuleret, får det telefonen til at give fejl under godkendelse. |
| Installation af certifikat på kundewebsted | Hver enkelt telefon understøttet et unikt certifikat for enhedsgodkendelse. For ekstra sikkerhed kan du i Cisco Unified Communications Manager konfigurere CAPF (Certificate Authority Proxy Function). Du kan også vælge at konfigurere Sikkerhedskonfiguration på telefonen. |
| Enhedsgodkendelse | Skaber forbindelse mellem Cisco Unified Communications Manager-servere og telefoner. Bestemmer, om en sikker forbindelse mellem telefon og en Cisco Unified Communications Manager-server mellem enhederne ved hjælp af TLS-protokollen, hvis det er nødvendigt. Hvis ikke, medmindre de er godkendt af Cisco Unified Communications Manager. |
| Filgodkendelse | Validerer digitalt signerede filer, som telefonen downloader. Telefonen tjekker filen efter oprettelse af filen. Filer, der ikke kan godkendes, skrives til log og kræver yderligere behandling. |
| Godkendelse af signaler | Bruger TLS-protokollen til at validere, at signalpakker ikke er blevet manipuleret. |
| Produktionsinstalleret certifikat | Hver enkelt telefon indeholder et unikt MIC (manufacturing integrity code) og entydigt bevis på telefonens identitet og giver Cisco Unified Communications Manager adgang til at validere telefonens identitet. |
| Sikker SRST-reference | Når du har konfigureret en SRST-reference af sikkerhedsmæssig betydning i Cisco Unified Communications Manager Administration, følger TFTP-serveren referencen til den sikre SRST. Derefter bruger en sikker telefon en TLS-forbindelse for at interagere med SRST-serveren. |
| Mediekryptering | Bruger SRTP til at sikre, mediestreams mellem understøttede enheder. Omfatter oprettelse af et mediehovednøglerpar for enheder og en nøgle, når nøglerne transporteres. |
| CAPF (Certificate Authority Proxy Function) | Implementerer dele af proceduren til oprettelse af certifikat, der er nødvendigt i forhold til oprettelse af nøgler og installation af certifikater. CAPF kan konfigureres på vegne af telefonen, eller den kan konfigureres til at oprette certifikater på telefonen. |
| Sikkerhedsprofiler | Definerer, om telefonen ikke er sikker, godkendt, krypteret eller sikker. |
| Krypterede konfigurationsfiler | Giver dig mulighed for at sikre fortroligheden af telefonkonfigurationsfiler. |
| Valgfri deaktivering af telefonens webserverfunktion | Du kan forhindre adgang til en telefonwebsted, der viser en række af telefonens indstillinger. |
| Telefonhærdning | Ekstra sikkerhedsindstillinger, du kan styre fra Cisco Unified Communications Manager Administration. <ul style="list-style-type: none"> Deaktiver adgang til websider for en telefon <p>Bemærk Du kan se de aktuelle indstillinger for Pc-GARP på telefonen.</p> |

| Funktion | Beskrivelse |
|---|---|
| 802.1X autentificering | Telefonen kan bruge 802.1X-godkendelse til at anmode om |
| AES 256-kryptering | Når telefonerne har forbindelse til Cisco Unified Communications Manager, er der tilgængelig 256-krypteringsunderstøttelse for TLS og SIP for brug af sig (Secure Internet Protocol). TLS 1.2-forbindelser ved hjælp af AES-256-baserede koder (Advanced Encryption Standard Information Processing Standards). De nye koder er: <ul style="list-style-type: none"> • For TLS-forbindelser: <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>Få flere oplysninger i dokumentationen til Cisco Unified Communications Manager.</p> |
| ECDSA-certifikater (Elliptic Curve Digital Signature Algorithm) | Som del af CC-certificeringen (Common Criteria) certificering, er der tilgængelig version 11.0. Dette påvirker alle VOS-produkter (Voice Operating System). |

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Konfigurer et certifikat, der lokalt er væsentligt

Denne opgave anvendes til at konfigurere en LSC med godkendelsesstrengmetoden.

Inden du begynder

Sørg for, at de rigtige sikkerhedskonfigurationer af Cisco Unified Communications Manager og Certificate Authority Proxy Function (CAPF) er angivet:

- CTL- eller ITL-filen har et CAPF-certifikat.
- Bekræft, at CAPF-certifikatet er installeret i Cisco Unified Communications Operating System Administration.
- CAPF kører og er konfigureret.

Få flere oplysninger om disse indstillinger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Fremgangsmåde

-
- Trin 1** Få den CAPF-godkendelseskode, der blev indstillet, da CAPF blev konfigureret.
- Trin 2** Gå til telefonen, og vælg **Indstillinger**.

Trin 3 Vælg **Administratorindstillinger > Sikkerhedsopsætning**.

Bemærk Du kan kontrollere adgang til menuen Indstillinger ved at bruge feltet Adgang til indstillinger i vinduet Cisco Unified Communications Manager Administration Phone Configuration.

Trin 4 Vælg **LSC**, og tryk på **Vælg** eller **Opdater**.

Telefonen beder om en godkendelsesstreng.

Trin 5 Angiv godkendelseskode, og tryk på **Send**.

Telefonen begynder at installere, opdatere eller fjerne LSC'en, afhængigt af hvordan CAPF er konfigureret. Under proceduren vises en række meddelelser i indstillingsfeltet LSC i menuen Sikkerhedskonfiguration, så du kan overvåge statussen. Når proceduren er fuldført, vises Installeret eller Ikke installeret på telefonen.

Processen til installation, opdatering eller fjernelse af LSC kan tage lang tid at fuldføre.

Når proceduren til installation af telefonen er gennemført, vises meddelelsen *Installeret*. Hvis telefonen viser *Ikke installeret*, kan godkendelsesstrengen være forkert, eller telefonopgraderingen er muligvis ikke aktiveret. Hvis CAPF-handlingen sletter LSC, viser telefonen *Ikke installeret* for at angive, at handlingen er gennemført. CAPF-serveren logfører fejlmeddelelserne. Se i dokumentationen til CAPF-serveren for at finde logfilerne og for at forstå, hvad fejlmeddelelserne betyder.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Aktivér FIPS-tilstand

Fremgangsmåde

Trin 1 Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration, og find telefonen.

Trin 2 Gå til området Produktspecifikt konfigurationslayout.

Trin 3 Indstil feltet **FIPS-tilstand** til aktiveret.


Trin 4 Vælg **Anvend konfig**.

Trin 5 Vælg **Gem**.

Trin 6 Genstart telefonen.

Telefonopkaldssikkerhed

Når der implementeres sikkerhed for en telefon, kan du identificere sikre telefonopkald på ikoner på telefonskærmen. Du kan også bestemme, om den tilsluttede telefon er sikker og beskyttet, hvis der afspilles en sikkerhedstone i begyndelsen af opkaldet.

I et sikkert opkald krypteres alle signal- og mediestreams. Et sikkert opkald tilbyder et højt niveau af sikkerhed med integritet og beskyttelse af personlige oplysninger ved opkaldet. Når et igangværende opkald er krypteret, skifter opkaldsstatusikonet til højre for opkaldsvarighedstimeren på telefonskærmen til følgende ikon: .



Bemærk Hvis opkaldet sendes gennem ikke-IP-opkaldslogge, f.eks. PSTN, er opkaldet muligvis ikke-sikkert, selvom det er krypteret på IP-netværket og har et låseikon tilknyttet.

I et sikkert opkald afspilles der en sikkerhedstone i begyndelsen af et opkald for at angive, at den anden tilsluttede telefon også modtager og sender sikker lyd. Hvis dit opkald forbinder til en ikke-sikker telefon, afspilles sikkerhedstonen ikke.




Bemærk Sikre opkald understøttes mellem to telefoner. Sikker konference, Cisco Extension Mobility og delte linjer kan konfigureres af en sikker konferencebro.

Når en telefon er konfigureret som sikker (krypteret og pålidelig) i Cisco Unified Communications Manager, kan den få tildelt en "beskyttet"-status. Derefter kan den beskyttede telefon konfigureres til at afspille en indikationstone i begyndelsen af et opkald:

- Beskyttet enhed: Hvis du vil ændre en sikker telefons status til beskyttet, skal du markere afkrydsningsfeltet Beskyttet enhed i vinduet Telefonkonfiguration i Cisco Unified Communications Manager Administration (**Enhed > Telefon**).
- Afspil sikker indikationstone: Hvis den beskyttede telefon skal afspille en sikker eller ikke-sikker indikationstone, skal du sætte indstillingen Afspil sikker indikationstone til Sand. Afspil sikker indikationstone er som standard indstillet til Falsk. Du angiver denne indstilling i Cisco Unified Communications Manager Administration (**System > Serviceparametre**). Vælg serveren og derefter tjenesten Unified Communications Manager. I vinduet Konfiguration af serviceparametre skal du vælge indstillingen i området Funktion - Sikker tone. Er som standard Falsk.

Sikker identifikation af konferenceopkald

Du kan starte et sikkert konferenceopkald og overvåge deltagerens sikkerhedsniveau. Sådan etablerer du et sikkert konferenceopkald:

1. En bruger starter konferencen fra en sikker telefon.
2. Cisco Unified Communications Manager tildeler en sikker konferencebro til opkaldet.
3. Efterhånden som deltagere tilføjes, bekræfter Cisco Unified Communications Manager sikkerhedstilstanden for hver telefon og beholder det sikre niveau for konferencen.
4. Telefonen viser konferenceopkaldets sikkerhedsniveau. En sikker konference viser ikonet  for sikkert opkald til højre for **Konference** på telefonskærmen.



Bemærk Sikre opkald understøttes mellem to telefoner. For beskyttede telefoner er visse funktioner, f.eks. konferenceopkald, delte linjer og Extension Mobility, ikke tilgængelige, når sikre opkald er konfigureret.

Følgende tabel indeholder oplysninger om ændringer af konferencens sikkerhedsniveauer afhængigt af igangsætterens telefonsikkerhedsniveau, deltagerens sikkerhedsniveau og tilgængeligheden af sikre konferencebroer.


Tabel 16: Sikkerhedsbegrænsninger med konferenceopkald

| Igangsætterens telefonsikkerhedsniveau | Anvendt funktion | Deltagernes sikkerhedsniveau | Resultater af handling |
|--|------------------|--|--|
| Ikke-sikker | Konference | Sikker | Ikke-sikker konferencebro Ikke-sikker konference |
| Sikker | Konference | Mindst ét medlem er ikke-sikkert. | Sikker konferencebro Ikke-sikker konference |
| Sikker | Konference | Sikker | Sikker konferencebro Sikker og krypteret konference |
| Ikke-sikker | Mød Mig | Det minimale sikkerhedsniveau er krypteret. | Igangsætteren får beskeden Opfylder ikke sikkerhedsniveauet, opkald afvist |
| Sikker | Mød Mig | Det minimale sikkerhedsniveau er ikke-sikkert. | Sikker konferencebro Konferencen accepterer alle opkald. |

Sikker identifikation af telefonopkald

Et sikkert opkald etableres, når din telefon og telefonen i den anden ende er konfigureret til sikre opkald. Den anden telefon kan være på samme Cisco IP-netværk eller på et netværk uden for IP-netværket. Sikre opkald kan kun foretages mellem to telefoner. Konferenceopkald bør understøtte sikre opkald, efter en sikker konferencebro er konfigureret.

Et sikret opkald etableres ved hjælp af denne proces:

1. En bruger starter opkaldet fra en sikret telefon (sikret sikkerhedstilstand).
2. Telefonen viser ikonet  for sikkert opkald på telefonens skærm. Dette ikon angiver, at telefonen er konfigureret til sikre opkald, men dette betyder ikke, at den anden tilsluttede telefon også er sikret.
3. Brugeren hører en sikkerhedstone, hvis opkaldet opretter forbindelse til en anden sikret telefon, hvilket angiver, at begge ender af samtalen er krypteret og sikret. Hvis opkaldet opretter forbindelse til en ikke-sikret telefon, vil brugere ikke høre sikkerhedstone.



Bemærk Sikre opkald understøttes mellem to telefoner. For beskyttede telefoner er visse funktioner, f.eks. konferenceopkald, delte linjer og Extension Mobility, ikke tilgængelige, når sikre opkald er konfigureret.

Kun beskyttede telefoner afspiller disse sikre eller ikke-sikre indikationstøner. Ikke-beskyttede telefoner afspiller aldrig tønner. Hvis den generelle opkaldsstatus ændrer sig under opkaldet, ændres indikationstone, og den beskyttede telefon afspiller den passende tone.

En beskyttet telefon afspiller en tone (eller ikke) under følgende omstændigheder:

- Når indstillingen Afspil sikker indikationstone er aktiveret:

- Når sikkert end-to-end-medie er etableret, og opkaldsstatussen er sikker, afspiller telefonen den sikre indikationstone (tre lange bip med pauser).
- Når ikke-sikkert end-to-end-medie er etableret, og opkaldsstatussen er ikke-sikker, afspiller telefonen den ikke-sikre indikationstone (seks korte bip med korte pauser).

Hvis indstillingen Afspil sikker indikationstone er deaktiveret, afspilles der ingen tone.

Sørg for kryptering ved bryd ind

Cisco Unified Communications Manager kontrollerer telefonens sikkerhedsstatus, når der er etableret konferencer, og ændrer sikkerhedsangivelse for konferencen eller blokerer afslutningen af opkaldet for at sikre systemets integritet og sikkerhed.

En bruger kan ikke bryde ind i et krypteret opkald, hvis den telefon, der bruges til at bryde ind med, ikke er konfigureret til kryptering. Når bryd ind-handlingen mislykkes i dette tilfælde, afspilles en omorganiseringstone (hurtig optaget) på den telefon, hvor bryd ind blev startet.

Hvis den startende telefon er konfigureret til kryptering, kan den, der starter bryd ind-handlingen, bryde ind i et ikke-sikkert opkald fra den krypterede telefon. Når bryd ind-handlingen er sket, klassificerer Cisco Unified Communications Manager opkaldet som ikke-sikkert.

Hvis den startende telefon er konfigureret til kryptering, kan den, der starter bryd ind-handlingen, bryde ind i et krypteret opkald, og telefonen angiver, at opkaldet er krypteret.

WLAN-sikkerhed

Da alle WLAN-enheder, der er inden for rækkevidde, kan modtage alle andres WLAN-trafik, er beskyttelse af talekommunikation vigtigt i WLAN. For at sikre, at folk med uautoriseret adgang ikke manipulerer eller opfanger taletrafikken, understøtter Cisco SAFE Security-arkitekturen Cisco IP-telefon og Cisco Aironet AP'er. Få flere oplysninger om sikkerhed i netværk under http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

Ciscos løsning til trådløs IP-telefoni giver sikkerhed for trådløst netværk, der forhindrer uautoriseret logon og kompromitteret kommunikation ved hjælp af følgende godkendelsesmetoder, der understøtter den trådløse Cisco IP-telefon:

- Åben godkendelse: Trådløse enheder kan anmode om godkendelse i et åbent system. Det AP, der modtager anmodningen, kan give godkendelse til en person eller kun de anmodere, der findes på en liste over brugere. Kommunikation mellem den trådløse enhed og AP kunne være uden kryptering, eller enheder kan bruge WEP-nøgler (Wired Equivalent Privacy) til at give sikkerhed. Enheder, der bruger WEP, forsøger kun at godkende med en AP, der bruger WEP.
- EAP-FAST-godkendelse (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling): Denne klient/server-sikkerhedsarkitektur krypterer EAP-transaktioner inden i en LTS-tunnel (Transport Level Security) mellem AP'et og RADIUS-serveren, f.eks. Cisco Access Control Server (ACS).

TLS-tunnelen bruger PAC'er (Protected Access Credentials) til godkendelse mellem klienten (telefon) og RADIUS-serveren. Serveren sender et AID (Authority ID) til klienten (telefonen), som gengæld vælger det relevante PAC. Klienten (telefonen) returnerer en PAC-Opaque til RADIUS-serveren. Serveren dekrypterer PAC med masternøglen. Begge slutpunkter indeholder nu PAC-nøglen, og der oprettes en TLS-tunnel. EAP-FAST understøtter automatisk PAC-klargøring, men du skal aktivere det på RADIUS-serveren.



Bemærk I Cisco ACS udløber PAC som standard i løbet af en uge. Hvis telefonen har en udløbet PAC, tager en godkendelse med RADIUS-serveren længere tid, mens telefonen får en ny PAC. For at undgå forsinkelser pga. PAC-klargøring skal du indstille PAC-udløbsperioden til 90 dage eller længere på ACS'en eller RADIUS-serveren.

- EAP-TLS-godkendelse (Extensible Authentication Protocol-Transport Layer Security): EAP-TLS kræver et klientcertifikat til godkendelse og netværksadgang. Når det gælder kablet EAP-TLS, kan klientcertifikatet enten være telefonens MIC eller en LSC. LSC er det anbefalede klientgodkendelsescertifikat for kablet EAP-TLS.
- PEAP (Protected Extensible Authentication Protocol): Ciscos beskyttede adgangskodebaserede gensidige godkendelsesmetode mellem klienten (telefonen) og en RADIUS-server. Cisco IP-telefon kan bruge PEAP til godkendelse med det trådløse netværk. Kun PEAP MSCHAPV2 understøttes. PEAP-GTC understøttes ikke.

Følgende godkendelsesmetode bruger RADIUS-serveren til at administrere godkendelsesnøgler:

- WPA/WPA2: Bruger RADIUS-serveroplysninger til at generere entydige nøgler til godkendelse. Da disse nøgler genereres på den centrale RADIUS-server, giver WPA/WPA2 mere sikkerhed end forhåndsdelte WPA-nøgler, der er gemt på AP'en og telefonen.
- Hurtig sikker roaming: Bruger oplysninger om RADIUS-server og en trådløs domæneserver (WDS) for at administrere og godkende nøgler. WDS opretter en cache med sikkerhedsmæssige legitimationsoplysninger for CCKM-aktiverede klientenheder for at få en hurtig og sikker fornyelse af godkendelse. Cisco IP-telefon i 8800-serien understøtter 802.11r (FT). Begge 11r (FT) og CCKM understøttes for at tillade hurtig og sikker roaming. Men Cisco anbefaler på det kraftigste at bruge den trådløse 802.11r (FT)-metode.

Med WPA WPA2/og CCKM angives krypteringsnøgler ikke på telefonen, men afledes automatisk mellem AP'en og telefonen. Men det EAP-brugernavn og den adgangskode, der bruges til godkendelse, skal angives på hver enkelt telefon.

For at sørge for, at taletrafikken er sikker, understøtter Cisco IP-telefon WEP TKIP og AES (Advanced Encryption Standards) for kryptering. Når disse mekanismer bruges til kryptering, krypteres både signal-SIP-pakker og RTP-talepakker (Real-Time Transport Protocol) mellem AP'en og Cisco IP-telefon.

WEP

Når WEP bruges i det trådløse netværk, sker godkendelse på AP'en ved at bruge åben godkendelse eller godkendelse med delt nøgle. Den WEP-nøgle, der er konfigureret på telefonen, skal matche den WEP-nøgle, der er konfigureret på AP'en, for at forbindelserne kan oprettes. Cisco IP-telefon understøtter WEP-nøgler, der bruger 40-bit kryptering eller en 128-bit kryptering og forbliver statiske på telefonen og AP'en.

EAP- og CCKM-godkendelse kan bruge WEP-nøgler til kryptering. RADIUS-serveren administrerer WEP-nøglen og sender en entydig nøgle til AP efter godkendelse for at kryptere alle talepakker. Disse WEP-nøgler kan ændres ved hver godkendelse.

TKIP

WPA og CCKM bruger TKIP-kryptering, der er bedre på flere områder i forhold til WEP. TKIP giver nøglekryptering med pr. pakke og længere initialiseringsvektorer, der styrker kryptering. Desuden sikrer

et MIC (message integrity check), at krypterede pakker ikke ændres. TKIP fjerner forudsigeligheden ved WEP, der hjælper personer med uautoriseret adgang med at tyde WEP-nøglen.

AES

En krypteringsmetode, der bruges til WPA2-godkendelse. Denne nationale standard for kryptering bruger en symmetrisk algoritme, der har den samme nøgle til kryptering og dekryptering. AES CBC-kryptering (Cipher Blocking Chain) i 128-bit størrelse, der som minimum understøtter nøglestørrelser på 128, 192 og 256 bit. Cisco IP-telefon understøtter en nøglestørrelse på 256 bit.



Bemærk Cisco IP-telefon understøtter ikke Cisco Key Integrity Protocol (CKIP) med CMIC.

Godkendelses- og krypteringsmetoder konfigureres inden for det trådløse LAN. VLAN'er konfigureres i netværket og på AP'er og angiver forskellige kombinationer af godkendelse og kryptering. Et SSID er knyttet til et VLAN og det specifikke godkendelses- og krypteringsmetode. For at klientenheder med trådløs forbindelse kan godkendes, skal du konfigurere de samme SSID'er med deres godkendelses- og krypteringsmetoder på AP'erne og på Cisco IP-telefon.

Visse godkendelsesmetoder kræver bestemte typer kryptering. Med åben godkendelse kan du bruge statisk WEP til kryptering, hvilket giver ekstra sikkerhed. Men hvis du bruger godkendelse med delt nøgle, skal du angive angive statisk WEP til kryptering, og du skal konfigurere en WEP-nøgle på telefonen.



- Bemærk**
- Når du bruger forhåndsdelte WPA-nøgle eller forhåndsdelte WPA2-nøgle, skal den forhåndsdelte nøgle være indstillet statisk på telefonen. Disse nøgler skal matche de nøgler, der er i AP'en.
 - Cisco IP-telefon understøtter ikke automatisk EAP-forhandling. Hvis du vil bruge EAP-FAST-tilstand, skal du angive den.

Følgende tabel indeholder en liste over godkendelses og krypteringsmetoder, der er konfigureret på Cisco Aironet AP'er, og som Cisco IP-telefon understøtter. Tabellen viser netværkskonfigurationsindstillingen for den telefon, der svarer til konfigurationen af AP.

Tabel 17: Godkendelses- og krypteringsmetoder

| Konfiguration af Cisco IP-telefon | AP-konfiguration | | | |
|-----------------------------------|------------------|-------------|------------|----------------|
| | Sikkerhed | Taststyring | Kryptering | Hurtig roaming |
| Ingen | Ingen | Ingen | Ingen | I/A |
| WEP | Statisk WEP | Statisk | WEP | I/A |
| PSK | PSK | WPA | TKIP | Ingen |
| | | WPA2 | AES | FT |

| Konfiguration af Cisco IP-telefon | AP-konfiguration | | | |
|-----------------------------------|------------------|----------|--------|----------|
| | EAP-FAST | EAP-FAST | 802.1x | WEP |
| WPA | | | TKIP | CCKM |
| WPA2 | | | AES | FT, CCKM |
| EAP-TLS | EAP-TLS | 802.1x | WEP | CCKM |
| | | WPA | TKIP | CCKM |
| | | WPA2 | AES | FT, CCKM |
| PEAP-MSCHAPV2 | PEAP-MSCHAPV2 | 802.1x | WEP | CCKM |
| | | WPA | TKIP | CCKM |
| | | WPA2 | AES | FT, CCKM |

Få flere oplysninger om konfiguration af godkendelses- og krypteringsmetoder på AP'er under *Konfigurationsvejledning til Cisco Aironet* for din model og version på følgende URL-adresse:

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

Sikkerhed på trådløst LAN

Cisco-telefoner, der understøtter Wi-Fi, er underlagt flere sikkerhedskrav og kræver ekstra konfiguration. Disse ekstra trin omfatter installation af certifikater og konfigurere sikkerhed på telefonerne og på Cisco Unified Communications Manager.

Få flere oplysninger i *Sikkerhedsvejledning til Cisco Unified Communications Manager*.

Administrationsside for Cisco IP-telefon

Cisco-telefoner, der understøtter Wi-Fi, har specialwebsider, der er forskellige fra andre telefoners sider. Du anvender disse specialwebsider til at konfigurere telefonsikkerheden, når SCEP (Simple Certificate Enrollment Protocol) ikke er tilgængelig. Brug disse sider til manuelt at installere sikkerhedscertifikater på en telefon, til at downloade et sikkerhedscertifikat eller til manuelt at konfigurere telefonens dato og klokkeslæt.

Disse websider viser også de samme oplysninger, som du ser på andre telefoners websider, herunder oplysninger om enheden, netværkskonfiguration, logge og statistiske oplysninger.

Konfigurer administrationssiden for telefon

Administrationswebsiden er aktiveret, når telefonen leveres fra fabrikken, og adgangskoden er indstillet til Cisco. Men hvis en telefon registreres med Cisco Unified Communications Manager, skal administrationswebsiden være aktiveret, og der skal konfigureres en ny adgangskode.

Aktiver denne webside, og Indstil legitimationsoplysningerne for logon, før du bruger websiden for første gang, efter at telefonen er registreret.

Når administrationswebsiden er aktiveret, er den tilgængelig på HTTPS-port 8443 (<https://x.x.x.x:8443>, hvor x.x.x.x er en telefon-IP-adresse).

Inden du begynder

Bestem dig for en adgangskode, før du aktiverer administrationswebsiden. Adgangskoden kan være en kombination af bogstaver og tal, men den skal være på mellem 8 og 127 tegn.

Dit brugernavn er permanent angivet som administrator.

Fremgangsmåde

- Trin 1** Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration.
 - Trin 2** Find telefonen.
 - Trin 3** I sektionen **Produktspecifikt konfigurationslayout** skal du indstille parameteren **Web-admin** til **Aktiveret**.
 - Trin 4** Angiv en adgangskode i feltet **Administratoradgangskode**.
 - Trin 5** Vælg **Gem**, og klik på **OK**.
 - Trin 6** Vælg **Anvend konfig**, og klik på **OK**.
 - Trin 7** Genstart telefonen.
-

Gå til websiden til telefonadministration

Når du ønsker at få adgang til administrationswebsiderne, skal du angive administrationsporten.

Fremgangsmåde

- Trin 1** Bestem telefonens IP-adresse:
 - Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration, og find telefonen. Telefoner, der er registreret med Cisco Unified Communications Manager, viser IP-adressen i vinduet **Søg efter og vis telefoner** øverst i vinduet **Telefonkonfiguration**.
 - Trin 2** Åbn en webbrowser, og angiv følgende URL-adresse, hvor *IP_adresse* er IP-adressen til Cisco IP-telefon:
https://<IP_adresse>:8443
 - Trin 3** Indtast adgangskoden i feltet Adgangskode.
 - Trin 4** Klik på **Send**.
-

Installér et brugercertifikat fra websiden til telefonadministration

Du kan manuelt installere et brugercertifikat på telefonen, hvis SCEP (Simple Certificate Enrollment Protocol) ikke er tilgængeligt.

Det forhåndsinstallerede MIC (Manufacturing Installed Certificate) kan anvendes som brugercertifikat for EAP-TLS.

Når brugercertifikatet er installeret, skal du føje det til RADIUS-serverens tillidsliste.

Inden du begynder

Før du kan installere et brugercertifikat for en telefon, skal du have:

Installér et godkendelsesservercertifikat fra websiden til telefonadministration

- Et brugercertifikat gemt på din pc. Certifikatet skal have formatet PKCS nr. 12.
- Certifikatets udtrukne adgangskode.

Fremgangsmåde

-
- Trin 1** Vælg **Certifikater** på websiden for telefonsadministration.
 - Trin 2** Gå til certifikatet på din pc.
 - Trin 3** I feltet **Udtræk adgangskode** skal du angive certifikatudtræksadgangskode.
 - Trin 4** Klik på **Upload**.
 - Trin 5** Genstart telefonen, når overførslen er fuldført.
-

Installér et godkendelsesservercertifikat fra websiden til telefonadministration

Du kan manuelt installere et godkendelsesservercertifikat på telefonen, hvis SCEP (Simple Certificate Enrollment Protocol) ikke er tilgængeligt.

Rod CA-certifikatet, der udstedte RADIUS-servercertifikatet, skal være installeret for EAP-TLS.

Inden du begynder

Før du kan installere et certifikat på en telefon, skal du have en godkendelsesservercertifikat, der er gemt på din pc. Certifikatet skal kodes i PEM (base-64) eller DER.

Fremgangsmåde

-
- Trin 1** Vælg **Certifikater** på websiden for telefonsadministration.
 - Trin 2** Find feltet **Godkendelsesserveren CA (administratorwebseite)**, og klik på **Installér**.
 - Trin 3** Gå til certifikatet på din pc.
 - Trin 4** Klik på **Upload**.
 - Trin 5** Genstart telefonen, når overførslen er fuldført.
- Hvis du installerer mere end ét certifikat, skal du installere alle certifikaterne, før du genstarter telefonen.
-

Fjern manuelt et sikkerhedscertifikat fra websiden til telefonadministration

Du kan manuelt fjerne et sikkerhedscertifikat fra en telefon, hvis SCEP (Enrollment Protocol SCEP) ikke er tilgængeligt.

Fremgangsmåde

-
- Trin 1** Vælg **Certifikater** på websiden for telefonsadministration.
 - Trin 2** Find certifikatet på siden **Certifikater**.
 - Trin 3** Klik på **Slet**.

Trin 4 Genstart telefonen, når sletningen er fuldført.

Konfigurer telefonens dato og klokkeslæt manuelt

Med certifikatbaseret godkendelse skal telefonen vise den korrekte dato og det korrekte klokkeslæt. En godkendelsesserveren kontrollerer telefonens dato og klokkeslæt i forhold til certifikatets udløbsdato. Hvis telefonens og serverens datoer og klokkeslæt ikke stemmer overens, holder telefonen op med at fungere.

Brug denne procedure til manuelt for at indstille datoen og klokkeslættet på telefonen, hvis telefonen ikke modtager de korrekte oplysninger fra dit netværk.

Fremgangsmåde

Trin 1 Rul til **Dato og klokkeslæt** fra websiden til telefonadministration.

Trin 2 Udfør en af følgende muligheder:

- Klik på **Indstil telefon til lokal dato og klokkeslæt** for at synkronisere telefonen med en lokal server.
 - I feltet **Angiv dato og klokkeslæt** skal du vælge måned, dag, år, time, minut og sekund ved hjælp af menuerne og klikke på **Indstil telefonen til bestemt dato og klokkeslæt**.
-

Konfiguration af SCEP

SCEP (Simple Certificate Enrollment Protocol) er standarden til automatisk anskaffelse og fornyelse af certifikater. Den gør det muligt at undgå manuel installation af certifikater på dine telefoner.

Konfigurer parametrene for produktspecifikt konfigurationslayout for SCEP

Du skal konfigurere følgende SCEP-parametre på din telefonwebseite

- RA IP-adresse
- SHA-1- eller SHA-256-fingeraftryk af CA-rodcertifikatet til SCEP-serveren

Cisco IOS Registration Authority (RA) fungerer som en proxy i forhold til SCEP-serveren. SCEP-klienten på telefonen bruger de parametre, der er hentet fra Cisco Unified Communication Manager. Når du har konfigureret parametrene, sender telefonen en SCEP `getcs`-anmodning til RA, og rod-CA-certifikatet valideres ved hjælp af det definerede fingeraftryk.

Fremgangsmåde

Trin 1 Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration.

Trin 2 Find telefonen.

Trin 3 Rul til området **Produktspecifikt konfigurationslayout**.

Trin 4 Markér afkrydsningsfeltet **WLAN SCEP-server** for at aktivere SCEP-parameteren.

- Trin 5** Markér afkrydsningsfeltet **WLAN-rod-CA-fingeraftryk (SHA256 eller SHA1)** for at aktivere SCEP QED-parameteren.

Understøttelse af SCEP-server (Simple Certificate Enrollment Protocol)

Hvis du bruger en SCEP-server (Simple Certificate Enrollment Protocol), kan serveren automatisk vedligeholde dine bruger- og certifikater. På SCEP-serveren skal du konfigurere SCEP-registreringsagenten til at:

- Fungerere som et PKI-tillidspunkt
- Fungerere som en PKI-registreringsagent
- Udføre enhedsgodkendelse ved hjælp af en RADIUS-server

Du kan finde flere oplysninger i dokumentationen til din SCEP-server.

802.1X authenticering

Cisco IP-telefon understøtter 802.1X-godkendelse.

Cisco IP-telefon og Cisco Catalyst-switches bruger traditionelt set Cisco Discovery Protocol (CDP) til at identificere hinanden og bestemme parametre som f.eks. VLAN-tildeling og integreret strømkrav.

Understøttelse af 802.1X-godkendelse kræver flere komponenter:

- Cisco IP-telefon: Telefonen starter anmodningen for at få adgang til netværket. Telefoner indeholder en 802.1X-supplikant. Denne supplikant giver netværksadministratorer kontrol over forbindelsen mellem IP-telefoner og porte på LAN-switch. Den aktuelle version af telefonens 802.1X-supplikant bruger EAP-FAST- og EAP-TLS-indstillingerne til netværksgodkendelse.
- Cisco Catalyst-switch (eller en anden tredjepartsswitch): Switchen skal understøtte 802.1X, så den kan fungere som godkendelsesfunktion og sende meddelelserne mellem telefonen og godkendesserveren. Når udvekslingen er fuldført, giver eller afviser switchen at give telefonen adgang til netværket.

Du skal udføre følgende handlinger for at konfigurere 802.1X.

- Konfigurer de andre komponenter, før du aktiverer 802.1X-godkendelse på telefonen.
- Konfigurer tale-VLAN – Da 802.1X-standarden ikke tager højde for VLAN'er, skal du konfigurere denne indstilling ud fra switchunderstøttelsen.
 - Aktiveret – Hvis du bruger en switch, der understøtter godkendelse på flere domæner, kan du fortsat bruge tale-VLAN'et.
 - Deaktiveret – Hvis switchen ikke understøtter godkendelse på flere domæner, skal du deaktivere tale VLAN'et og overveje at tildele porten til det indbyggede VLAN.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14



KAPITEL 8

Tilpasning af Cisco IP-konferencetelefon

- [Brugerdefinerede ringetoner på telefon, på side 87](#)
- [Tilpas opkaldstonen, på side 89](#)

Brugerdefinerede ringetoner på telefon

Cisco IP-telefon leveres med to indbyggede ringetoner, der er implementeret i hardwaren: Chirp1 og Chirp2. Cisco Unified Communications Manager indeholder også et standardsæt af yderligere ringetoner, der er implementeret i softwaren som PCM-filer (Pulse Code Modulation). PCM-filerne sammen med en XML-fil, der beskriver de tilgængelige ringetoner på dit websted, findes i TFTP-telefonbogen på hver Cisco Unified Communications Manager-server.



Bemærk Der skelnes mellem store og små bogstaver i alle filnavne. Hvis du ikke bruger de rigtige store og små bogstaver til filnavnet, vil telefonen ikke anvende dine ændringer.

Få yderligere oplysninger i kapitlet "Brugerdefinerede telefonringing og baggrunde" [Vejledning i konfiguration af funktioner til Cisco Unified Communications Manager](#).

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Konfigurer en brugerdefineret telefonringning

Fremgangsmåde

- Trin 1** Opret en PCM-fil for hver brugerdefineret ringetone (én ringetone pr. fil).
Sørg for, at PCM-filerne overholder de retningslinjer for format, der er angivet i afsnittet [Brugerdefinerede formater til ringningsfiler](#).
- Trin 2** Overfør de nye PCM-filer, du har oprettet til Cisco TFTP-serveren for hver Cisco Unified Communications Manager i din klynge.
Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Trin 3 Gem dine ændringer, og luk Ringlist-wb-filen.

Trin 4 Sådancachelagres den nye Ringlist-wb-fil:

- Stort og start TFTP-tjenesten ved hjælp af Cisco Unified Serviceability
- Deaktiver og genaktiver TFTP-tjenesteparameteren "Aktiver cachelagring af konstanter og binfiler ved start", der findes i området Avancerede serviceparametre.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Brugerdefinerede formater til ringningsfiler

Filen Ringlist-wb.xml file definerer et XML-objekt, der indeholder en liste over telefonringningstyper. Denne fil omfatter op til 50 ringningstyper. Hver ringningstype indeholder en markør til den PCM-fil, der bruges til den pågældende ringningstype, og den tekst, der vises på menuen Ring Type (Ringningstype) på en Cisco IP-telefon for den pågældende ringning. Cisco TFTP-serveren for hver Cisco Unified Communications Manager indeholder denne fil.

CiscoIPPhoneRinglist XML-objektet bruger følgende enkle kodesæt til at beskrive oplysningerne:

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

Følgende tegn gælder for definitionsnavnene. Du skal medtage det krævede DisplayName og FileName for hver type af telefonringning.

- DisplayName angiver navnet på den brugerdefinerede ringning for den tilknyttede PCM-fil, der vises på menuen Ring Type (Ringningstype) for Cisco IP-telefon.
- FileName angiver navnet på PCM-filen for den brugerdefinerede ringning, der skal knyttes til DisplayName.



Bemærk Felterne DisplayName og FileName må højst være på 25 tegn.

Dette eksempel viser en Ringlist-wb.xml-fil, der definerer to typer af telefonringninger:

```
<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-filerne til ringningerne skal overholde følgende krav til korrekt afspilning på Cisco IP-telefon:

- Raw PCM (ingen header)

- 8000 samplinger pr. sekund
- 8 bit pr. sampling
- Mu-law-komprimering
- Maksimal ringningsstørrelse = 16080 samplinger
- Mindste ringningsstørrelse = 240 samplinger
- Antal samplinger i ringningen = multipel af 240.
- Start og slut af ringning ved nul krydsning.

Hvis du vil oprette PCM-filer til brugerdefinerede telefonringninger, skal du bruge en standardlydredigeringspakke, der understøtter disse krav til filformat.

Tilpas opkaldstonen

Du kan konfigurere dine telefoner, så brugerne hører forskellige opkaldstoner ved interne og eksterne opkald. Afhængigt af hvad du har brug for, kan du vælge mellem tre opkaldstoneindstillinger:

- Standard: en forskellig opkaldstone for interne og eksterne opkald.
- Intern: Den interne opkaldstone bruges til alle opkald.
- Ekstern: Den eksterne opkaldstone bruges til alle opkald.

Brug altid opkaldstone er et obligatorisk felt i Cisco Unified Communications Manager.

Fremgangsmåde

- Trin 1** Vælg **System** > **Serviceparametre** i Cisco Unified Communications Manager Administration.
 - Trin 2** Vælg den relevante server.
 - Trin 3** Vælg **Cisco CallManager** som tjenesten.
 - Trin 4** Rul til ruden for klyngeparametre.
 - Trin 5** Indstil **Brug altid opkaldstone** til en af følgende:
 - Ekstern
 - Intern
 - Standard
 - Trin 6** Vælg **Gem**.
 - Trin 7** Genstart dine telefoner.
-



KAPITEL 9

Funktioner og konfiguration af Cisco IP-konferencetelefon

- [Brugersupport til Cisco IP-telefon, på side 91](#)
- [Migration af din telefon til en multiplatformstelefon med det samme, på side 92](#)
- [Konfigurer ny programtastskabelon, på side 92](#)
- [Konfigurer telefontjenester for brugere, på side 93](#)
- [Konfiguration af telefonfunktioner, på side 93](#)

Brugersupport til Cisco IP-telefon

Hvis du er en systemadministrator, er du sandsynligvis brugernes primære kilde til oplysninger vedrørende Cisco IP-telefon i dit netværk eller firma. Det er vigtigt at angive aktuelle og grundige oplysninger til slutbrugere.

Hvis du vil være i stand til at bruge nogle af funktionerne på Cisco IP-telefon (herunder valgmuligheder for tjenester og voicemail), skal brugerne modtage oplysninger fra dig eller dit netværksteam eller være i stand til at kontakte dig, hvis de har brug for hjælp. Sørg for at give brugerne kontaktoplysninger på personer, der kan kontaktes ved brug for hjælp, og med instruktioner i, hvordan disse personer kontaktes.

Vi anbefaler, at du opretter en webside på dit interne supportwebsted, der giver slutbrugerne vigtige oplysninger om deres Cisco IP-telefon.

Overvej at medtage følgende typer oplysninger på dette websted:

- Brugervejledninger til alle de Cisco IP-telefon-modeller, du understøtter
- Oplysninger, om hvordan man får adgang til selvbetjeningsportalen til Cisco Unified Communications
- Liste over understøttede funktioner
- Brugervejledning eller opslagsværk til dit voicemail-system

Migration af din telefon til en multiplatformstelefon med det samme

Du kan nemt migrere din virksomhedstelefon til en multiplatformstelefon med ét trin uden at bruge indlæsning af overgangsfirmware. Det eneste, du behøver, er at få fat i og godkende migreringslicensen fra serveren.

Hvis du ønsker yderligere oplysninger, kan du se under 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

Konfigurer ny programtastskabelon

Du skal føje programtaster til en programtastskabelon for at give brugere adgang til visse funktioner. Hvis du ønsker, at brugerne skal kunne vælge forstyr ikke, skal du aktivere programtasten. Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Det kan være en god ide at oprette flere skabeloner. Det kan f.eks. være en god ide at have en skabelon til telefonen i et mødelokale og en anden skabelon til en telefon på en ledende medarbejders kontor.

Denne procedure fører dig gennem trinnene til at oprette en ny programtastskabelon og tildele den til en bestemt telefon. Ligesom andre telefonfunktioner kan du også bruge skabelonen til alle dine konferencetelefoner eller en gruppe af telefoner.

Fremgangsmåde

-
- Trin 1** Log på Cisco Unified Communications Manager Administration som administrator.
- Trin 2** Vælg **Enhed > Enhedsindstillinger > Programtastskabelon**.
- Trin 3** Klik på **Find**.
- Trin 4** Vælg en af følgende indstillinger:
- Cisco Unified Communications Manager 11.5 og tidligere versioner – **Standardbruger**
 - Cisco Unified Communications Manager 12.0 og tidligere versioner – **Personlig konferencebruger** eller **Offentlig konferencebruger**.
- Trin 5** Klik på **Kopier**
- Trin 6** Skift navnet på skabelonen.
- Det kunne f.eks. være 8832-mødelokaleskabelon.
- Trin 7** Klik på **Gem**.
- Trin 8** Gå til siden **Konfigurer layout af programtast** i menuen øverst til højre.
- Trin 9** For hver opkaldstilstand skal du indstille de funktioner, der skal vises.
- Trin 10** Klik på **Gem**.
- Trin 11** Gå tilbage til **skærbilledet Søg/liste** i menuen øverst til højre.
- Du ser din nye skabelon på listen over skabeloner.
- Trin 12** Vælg **Enhed > Telefon**.

- Trin 13** Find den telefonen, der skal have nye skabelon, og vælg den.
- Trin 14** Vælg den nye programtastskabelon i feltet **Programtastskabelon**.
- Trin 15** Klik på **Gem** og **Anvend konfig**.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Konfigurer telefontjenester for brugere

Du kan give brugere adgang til Cisco IP-telefon-tjenester på IP-telefonen. Du kan også tildele en knap til andre telefontjenester. IP-telefonen administrerer hver enkelt tjeneste som et separat program.

Før en bruger kan få adgang til en tjeneste:

- Brug Cisco Unified Communications Manager Administration til at konfigurere tjenester, der ikke er til stede som standard.
- Brugeren skal abonnere på tjenester ved at bruge Selvbetjeningsportal til Cisco Unified Communications. Dette webbaserede program har en grafisk brugergrænseflade, der giver mulighed for, at slutbrugere i begrænset omfang kan konfigurere IP-telefonprogrammer. En bruger kan imidlertid ikke abonnere på en tjeneste, som du konfigurerer som et virksomhedsabonnement.

Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Før du konfigurerer tjenester, skal du indsamle URL-adresser til de websteder, du vil konfigurere, og kontrollere, at brugere kan få adgang til disse websteder fra dit firmas IP-telefonnetværk. Denne aktivitet gælder ikke for de standardtjenester, som Cisco leverer.

Fremgangsmåde

-
- Trin 1** I Cisco Unified Communications Manager Administration skal du vælge **Enhed > Enhedsindstillinger > Telefontjenester**.
- Trin 2** Kontrollér, at brugerne kan få adgang til Selvbetjeningsportal til Cisco Unified Communications, hvorfra de kan vælge og abonnere på konfigurerede tjenester.
- Se [Oversigt over selvbetjeningsportal, på side 67](#) for at få en oversigt over de oplysninger, du skal give til slutbrugere.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Konfiguration af telefonfunktioner

Du kan indstille telefoner til at få en række forskellige funktioner, der er baseret på dine brugeres behov. Du kan anvende funktioner på alle telefoner, en gruppe af telefoner og til individuelle telefoner.

Når du konfigurerer funktioner, viser vinduet Cisco Unified Communications Manager Administration oplysninger, der gælder for alle telefoner og oplysninger, der gælder for telefonmodellen. De oplysninger, der er specifikke for telefonmodellen, er i området Produktspecifikt konfigurationslayout i vinduet.

Få flere oplysninger om de felter, der gælder for alle telefonmodeller, i dokumentationen til Cisco Unified Communications Manager.

Når du indstiller et felt, er det vindue, du indstiller feltet i, vigtigt, fordi vinduerne bliver prioriteret. Prioritetsrækkefølgen er:

1. Individuelle telefoner (højeste prioritet)
2. Gruppe af telefoner
3. Alle telefoner (laveste prioritet)

Hvis du f.eks. ikke ønsker, at et bestemt sæt brugere skal have adgang til telefonwebsider, mens resten af brugerne godt må, skal du gøre følgende:

1. Aktivér adgang til telefonwebsider for alle brugere.
2. Deaktiver adgang til telefonwebsider for hver enkelt bruger, eller konfigurer en brugergruppe, og deaktiver adgang til telefonwebsider for gruppen af brugere.
3. Hvis en bestemt bruger i brugergruppen ikke havde brug for adgang til telefonwebsiderne, skal du aktivere denne indstilling for den pågældende bruger.

Lignende emner

[Konfigurer bevarelse af brugerlegitimationsoplysninger for Expressway-logon](#), på side 119

Konfigurer telefonfunktioner for alle telefoner

Fremgangsmåde

- Trin 1** Log på Cisco Unified Communications Manager Administration som administrator.
- Trin 2** Vælg **System > Konfiguration af firmatelefon**.
- Trin 3** Angiv de felter, du vil ændre.
- Trin 4** Markér afkrydsningsfeltet **Tilsidesæt virksomhedsindstillinger** for eventuelt ændrede felter.
- Trin 5** Klik på **Gem**.
- Trin 6** Klik på **Anvend konfig**.
- Trin 7** Genstart telefonerne.

Bemærk Dette vil påvirke alle telefoner i din organisation.

Lignende emner

[Produktspecifik konfiguration](#), på side 95

Konfigurer telefonfunktioner for en gruppe telefoner

Fremgangsmåde

- Trin 1** Log på Cisco Unified Communications Manager Administration som administrator.
 - Trin 2** Vælg **Enhed > Enhedsindstillinger > Almindelig telefonprofil**.
 - Trin 3** Find profilen.
 - Trin 4** Gå til ruden Produktspecifikt konfigurationslayout, og indstil felterne.
 - Trin 5** Markér afkrydsningsfeltet **Tilsidesæt virksomhedsindstillinger** for eventuelt ændrede felter.
 - Trin 6** Klik på **Gem**.
 - Trin 7** Klik på **Anvend konfig**.
 - Trin 8** Genstart telefonerne.
-

Lignende emner

[Produktspecifik konfiguration](#), på side 95

Konfigurer telefonfunktioner for en enkelt telefon

Fremgangsmåde

- Trin 1** Log på Cisco Unified Communications Manager Administration som administrator.
 - Trin 2** Vælg **Enhed > Telefon**
 - Trin 3** Find den telefon, der er knyttet til brugeren.
 - Trin 4** Gå til ruden Produktspecifikt konfigurationslayout, og indstil felterne.
 - Trin 5** Markér afkrydsningsfeltet **Tilsidesæt almindelige indstillinger** for de felter, der måtte være ændret.
 - Trin 6** Klik på **Gem**.
 - Trin 7** Klik på **Anvend konfig**.
 - Trin 8** Genstart telefonen.
-

Lignende emner

[Produktspecifik konfiguration](#), på side 95

Produktspecifik konfiguration

Følgende tabel beskriver felterne i ruden til produktspecifik konfigurationslayout. Nogle felter i denne tabel vises kun på siden **Enhed > Telefon**.

Tabel 18: Felter til produktspecifik konfiguration

| Felt navn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|--|---------------------------------------|-------------|--|
| Adgang til indstillinger | Deaktiveret Aktiveret Begrænset | Aktiveret | Aktiverer, deaktiverer eller begrænser adgang til lokale indstillinger for konfiguration i appen Indstillinger. Med begrænset adgang er der mulighed for at tilgå menuerne Præferencer og Systemoplysninger. Nogle af indstillingerne i menuen Wi-Fi er også tilgængelige. Med deaktiveret adgang viser menuen Indstillinger ingen valgmuligheder. |
| Gratis ARP | Deaktiveret Aktiveret | Deaktiveret | Aktiverer eller deaktiverer muligheden for, at telefonen kan få MAC-adresser fra Gratuitous ARP. Denne funktion er krævet for at kunne overvåge eller optage videostrømme. |
| Webadgang | Deaktiveret Aktiveret | Deaktiveret | Aktiverer eller deaktiverer adgang til telefonwebsider via en webbrowser. Advarsel Hvis du aktiverer dette felt, kan du vise følsomme oplysninger om telefonen. |
| Deaktiver TLS 1.0 og TLS 1.1 for WebAccess | Deaktiveret Aktiveret | Aktiveret | Styrer brugen af TLS 1.2 for en webserverforbindelse. <ul style="list-style-type: none"> • Deaktiveret – en telefon, der er konfigureret til TLS1.0, TLS 1.1 eller TLS1.2, kan fungere som en HTTPS-server. • Aktiveret – Kun en telefon, der er konfigureret til TLS1.2, kan fungere som en HTTPS-server. |
| Enbloc-opkald | Deaktiveret Aktiveret | Deaktiveret | Styrer opkaldsmetoden. <ul style="list-style-type: none"> • Deaktiveret – Cisco Unified Communications Manager venter på, at tidsindstilling mellem cifre udløber, når en opkaldsplan eller et rutemønster overlapper. • Aktiveret – hele opkaldsstrengen sendes til Cisco Unified Communications Manager, når opkaldet er afsluttet. For at undgå timeout for T.302-tidsindstillingen anbefaler vi, at du aktiverer Enbloc-opkald, når en opkaldsplan eller et rutemønster overlapper. <p>Obligatoriske godkendelseskoder og klientårsagskoder understøtter ikke Enbloc-opkald. Hvis du bruger obligatoriske godkendelseskoder eller klientårsagskoder, kan du ikke bruge denne funktion.</p> |

| Felt navn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|------------------------------|----------------------------------|----------|--|
| Dage baggrundslys er inaktiv | Ugedage | | <p>Definerer de dage, hvor baggrundslyset ikke tændes automatisk på det tidspunkt, der er angivet i feltet Baggrundslys tænder klokken.</p> <p>Vælg dagen eller dagene på rullelisten. Hvis du vil vælge mere end én dag, skal du bruge Ctrl+klik på de ønskede dage.</p> <p>Se Planlæg strømbesparelse for Cisco IP-telefon, på side 108.</p> |
| Baggrundslys tænder klokken | tt:mm | | <p>Definerer det klokkeslæt hver dag, hvor baggrundslyset tændes automatisk (undtagen på de dage, der er angivet i feltet Backlight Display Not Active (Visning af baggrundslys ikke aktiv)).</p> <p>Angiv tiden i dette felt ved brug af 24-timers formatet, hvor 0:00 er midnat.</p> <p>Hvis du f.eks. automatisk vil tænde baggrundslyset kl. 07:00 om morgenen (0700), skal du angive 07:00. Hvis du vil tænde baggrundslyset kl. 2 om eftermiddagen (1400), skal du angive 14:00.</p> <p>Hvis dette felt er tomt, tændes baggrundslyset automatisk kl. 0:00.</p> <p>Se Planlæg strømbesparelse for Cisco IP-telefon, på side 108.</p> |
| Baggrundslys tændt varighed | tt:mm | | <p>Definerer længden af den tid, som baggrundslyset er tændt, efter at det er blevet tændt på det tidspunkt, der er angivet i feltet Baggrundslys tænder klokken.</p> <p>Hvis du f.eks. vil lade baggrundslyset være tændt i 4 timer og 30 timer, efter at det er blevet tændt automatisk, skal du angive 04:30.</p> <p>Hvis dette felt er tomt, slukkes telefonen, når dagen er gået (0:00).</p> <p>Hvis Baggrundslyset tænder klokken er 0:00, og Baggrundslys tændt varighed er tom (eller 24:00), tændes baggrundslyset ikke.</p> <p>Se Planlæg strømbesparelse for Cisco IP-telefon, på side 108.</p> |

| Feltnavn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|---|----------------------------------|-----------|--|
| Baggrundslys udløbstid | tt:mm | | <p>Definerer længden af den tid, som telefonen er inaktiv, før baggrundslyset slukkes. Gælder kun, når baggrundslyset blev slukket efter planen, og tændt af en bruger (ved at trykke på en knap på telefonen eller løfte håndsættet).</p> <p>Hvis du f.eks. vil slukke baggrundslyset, når telefonen har været inaktiv i 1 time og 30 minutter, når en bruger tænder baggrundslyset, skal du angive 01:30.</p> <p>Se Planlæg strømbesparelse for Cisco IP-telefon, på side 108.</p> |
| Baggrundslys tændt ved indgående opkald | Deaktiveret Aktiveret | Aktiveret | Tænder baggrundslyset, når der er et indgående opkald. |

| Feltnavn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|--|----------------------------------|----------|--|
| Enable Power Save Plus (Aktiver strømsparefunktion plus) | Ugedage | | <p>Definerer tidsplanen for de dage, hvor telefonen er slukket.</p> <p>Vælg dagen eller dagene på rullelisten. Hvis du vil vælge mere end én dag, skal du bruge Ctrl+klik på de ønskede dage.</p> <p>Når Strømsparefunktion plus er aktiveret, modtager du en meddelelse, der advarer om nødforhold (e911).</p> <p>Advarsel Mens strømsparefunktionen ("tilstanden") er aktiveret, bliver slutpunkter, der er konfigureret til den tilstand, deaktiveret ved nødopkald og modtagelse af indgående opkald. Ved at vælge denne tilstand accepterer du følgende: (i) Du påtager dig det fulde ansvar for at sikre alternative metoder til nødopkald og modtagelse af opkald, når denne tilstand er aktiveret; (ii) Cisco er ikke ansvarlig for dit valg af denne tilstand, og alt ansvar i forbindelse med aktivering af denne tilstand påhviler dig; og (iii) Du giver brugerne alle oplysninger om virkningen af tilstanden ved opkald, foretagelse af opkald og på anden vis.</p> <p>Hvis du vil deaktivere strømsparefunktionen, skal du fjerne markeringen af afkrydsningsfeltet Tillad EnergyWise-tilsidesættelser. Hvis Tillad EnergyWise-tilsidesættelser forbliver markeret, men der ikke er valgt nogen dage i feltet Aktiver strømsparefunktion plus, er strømsparefunktionen ikke aktiveret.</p> <p>Se Planlæg EnergyWise på Cisco IP-telefon, på side 110.</p> |

| Felt navn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|-----------------------------------|----------------------------------|----------|---|
| Tidspunkt for tænding af telefon | tt:mm | | <p>Bestemmer, hvornår telefonen automatisk tændes på de dage, der er angivet i feltet Aktivér Power Save Plus.</p> <p>Angiv tiden i dette felt ved brug af 24-timers formatet, hvor 00:00 er midnat.</p> <p>Hvis du f.eks. vil tænde telefonen kl. 07:00 om morgenen (0700), skal du angive 07:00. Hvis du vil tænde telefonen kl. 02:00 om eftermiddagen (1400), angiv 14:00.</p> <p>Standardværdien er tom, hvilket betyder 00:00.</p> <p>Tidspunkt for tænding af telefon skal være mindst 20 minutter senere end Tidspunkt for slukning af telefon. Hvis f.eks. Tidspunkt for slukning af telefon er 7:00, må Tidspunkt for tænding af telefon ikke være tidligere end 7:20.</p> <p>Se Planlæg EnergyWise på Cisco IP-telefon, på side 110.</p> |
| Tidspunkt for slukning af telefon | tt:mm | | <p>Definerer det tidspunkt på dagen, hvor telefonen slukkes, for de dage, der er angivet i feltet Enable Power Save Plus (Aktiver strømsparefunktion plus). Hvis felterne Tidspunkt for tænding af telefon og Tidspunkt for slukning af telefon indeholder den samme værdi, slukkes telefonen ikke.</p> <p>Angiv tiden i dette felt ved brug af 24-timers formatet, hvor 00:00 er midnat.</p> <p>Hvis du f.eks. vil slukke telefonen kl. 7:00 om morgenen (0700), skal du angive 7:00. Hvis du vil slukke telefonen kl. 2:00 om eftermiddagen (1400), angiv 14:00.</p> <p>Standardværdien er tom, hvilket betyder 00:00.</p> <p>Tidspunkt for tænding af telefon skal være mindst 20 minutter senere end Tidspunkt for slukning af telefon. Hvis f.eks. Tidspunkt for slukning af telefon er 7:00, må Tidspunkt for tænding af telefon ikke være tidligere end 7:20.</p> <p>Se Planlæg EnergyWise på Cisco IP-telefon, på side 110.</p> |

| Felt navn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|---|----------------------------------|---------------|---|
| Timeout for telefon slukket ved inaktivitet | tt:mm | | <p>Angiver det tidsrum, hvori telefonen skal være inaktiv, før telefonen slukkes.</p> <p>Timeouten sker under følgende betingelser:</p> <ul style="list-style-type: none"> • Når telefonen som planlagt er i tilstanden strømsparefunktion plus, og når den går ud af strømsparefunktion plus, fordi brugeren af telefonen har trykket på tasten Vælg. • Når telefonen får strøm igen fra den påsatte switch. • Når Tidspunkt for slukning af telefon nås, men telefonen er i brug. <p>Se Planlæg EnergyWise på Cisco IP-telefon, på side 110.</p> |
| Aktivér lydbesked | Afkrydsningsfelt. | Ikke markeret | <p>Når denne indstilling er aktiveret, får telefonen besked om at afspille en lydbesked, der starter 10 minutter før det tidspunkt, der er angivet i feltet Tidspunkt for slukning af telefon.</p> <p>Dette afkrydsningsfelt gælder kun, hvis listefeltet Aktiver strømsparefunktion plus indeholder en eller flere af de valgte dage.</p> <p>Se Planlæg EnergyWise på Cisco IP-telefon, på side 110.</p> |
| EnergyWise Domæne | Op til 127 tegn | | <p>Identificerer det EnergyWise-domæne, telefonen er i.</p> <p>Se Planlæg EnergyWise på Cisco IP-telefon, på side 110.</p> |
| EnergyWise-hemmelighed | Op til 127 tegn | | <p>Identificerer den hemmelige sikkerhedsadgangskode, der bruges til at kommunikere på EnergyWise-domænet.</p> <p>Se Planlæg EnergyWise på Cisco IP-telefon, på side 110.</p> |

| Felt navn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|------------------------------------|----------------------------------|---------------|---|
| Tillad EnergyWise-tilsidesættelser | Afkrydsningsfelt | Ikke markeret | <p>Angiver, om du tillader, at politikken for EnergyWise-domænecontrolleren kan sende opdateringer om strømniveau til telefonerne. Følgende betingelser gælder:</p> <ul style="list-style-type: none"> • Der skal være valgt en eller flere dage i feltet Aktiver strømsparefunktion plus. • Indstillingerne i Cisco Unified Communications Manager Administration aktiveres efter planen, også selvom EnergyWise sender en tilsidesættelse. <p>Hvis det f.eks. antages, at Tidspunkt for slukning af telefon indstilles til 22:00 (10:00 om aftenen), værdien i feltet Tidspunkt for tænding af telefon er 06:00 (6:00 om morgenen), og en eller flere dage er valgt for Aktiver strømsparefunktion plus.</p> <ul style="list-style-type: none"> • Hvis EnergyWise angiver, at telefonen skal slukkes kl. 20:00 (8:00 om aftenen), vil den angivelse gælde (forudsat at brugeren af telefonen ikke gør noget) indtil 6:00 a.m., som er konfigureret for Tidspunkt for tænding af telefon. • Kl. 6:00 om morgenen tændes telefonen og fortsætter med at modtage ændringerne i strømniveauet fra indstillingerne i Cisco Unified Communications Manager Administration. • For at ændre strømniveauet på telefonen igen skal EnergyWise udstede en ny kommando om ændring af strømniveau. <p>Hvis du vil deaktivere strømsparefunktionen, skal du fjerne markeringen af afkrydsningsfeltet Tillad EnergyWise-tilsidesættelser. Hvis Tillad EnergyWise-tilsidesættelser forbliver markeret, men der ikke er valgt nogen dage i feltet Aktiver strømsparefunktion plus, er strømsparefunktionen ikke aktiveret.</p> <p>Se Planlæg EnergyWise på Cisco IP-telefon, på side 110.</p> |

| Felt navn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|--|--|---|---|
| Politik for deltagelse og direkte omstilling | På samme linje aktiveret På samme linje deaktiveret | Samme linje, på tværs af linjer aktiveret | Styrer en brugers mulighed for at deltage i og omstille opkald. <ul style="list-style-type: none"> • På samme linje aktiveret – brugerne kan direkte omstille til, eller deltage i, aktuel linje for et andet opkald på den samme linje. • Samme linje deaktiveret – brugerne kan ikke deltage i eller omstille opkald på den samme linje. Funktioner til deltagelse og omstilling er deaktiveret, og brugeren kan ikke bruge funktionen til direkte omstilling eller deltagelse. |
| Optagertone | Deaktiveret Aktiveret | Deaktiveret | Styrer afspilningen af tonen, når brugeren optager et opkald |
| Optagertone-lokallydstyrke | Heltal 0-100 | 100 | Styrer lydstyrken af optagertonen for den lokale bruger. |
| Optagertone-fjernlydstyrke | Heltal 0-100 | 50 | Styrer lydstyrken af optagertonen for den eksterne bruger. |
| Optagertone varighed | Heltal 1-3000 millisekunder | | Styrer varigheden af optagertonen. |
| Log server | Streng på op til 256 tegn | | Identificerer IPv4 syslog-serveren for telefonfejlfindingsoutput. Adressen har følgende format: adresse : <port>@@base=<0-7>;pfs=<0-1> |
| Ekstern logfil | Deaktiveret Aktiveret | Deaktiveret | Styrer muligheden for at sende logfiler til syslog-serveren. |

| Feltnavn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|--|---|-------------|---|
| Logprofil | Standard Fast Telefoni- SIP UI Netværk Medier Opgradering Tilbehør Sikkerhed Energywise MobileRemoteAccess | Fast | Angiver den foruddefinerede logføeringsprofil. <ul style="list-style-type: none"> • Standard – standardniveau for logføring ved fejlfinding • Fast – overskriver ikke telefonens lokale indstilling for logføring ved fejlfinding • Telefoni – logfører oplysninger om telefoni eller opkaldsfunktioner • SIP – logfører oplysninger om brug af SIP-signaler • UI – logfører oplysninger om telefonens brugergrænseflade • Netværk – logfører netværksoplysninger • Medier – logfører medieoplysninger • Opgradering – logfører opgraderingsoplysninger • Tilbehør – logfører tilbehørsoplysninger • Sikkerhed – logfører sikkerhedsoplysninger • Energywise – logfører oplysninger om energisparefunktion • MobileRemoteAccess – logfører mobiladgang og ekstern adgang via Expressway-oplysninger |
| IPv6-log server | Streng på op til 256 tegn | | Identificerer IPv6 syslog-serveren for telefonfejlfindingsoutput. |
| CDP (Cisco Discovery Protocol): switchport | Deaktiveret Aktiveret | Aktiveret | Styrer Cisco Discovery Protocol på telefonen. |
| LLDP_MED (Link Layer Discovery Protocol - Media Endpoint Discover): switchport | Deaktiveret Aktiveret | Aktiveret | Aktiverer LLDP-MED på SW-porten. |
| LLDP-aktiv-ID | Streng, op til 32 tegn | | Identificerer det aktiv-ID, der er knyttet til telefonen i forbindelse med lagerstyring. |
| Energy Efficient Ethernet (EEE): switchport | Deaktiveret Aktiveret | Deaktiveret | Styrer EEE på switchporten. |

| Felt navn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|--|---|--------------------|--|
| LLDP Power Priority | Ukendt Lav Ofte Kritisk | Ukendt | Tildeler en telefonstrømsprioritet til switchen, der gør det muligt for switchen at levere den rigtige strøm til telefonerne. |
| 802.1X-godkendelse | Brugerkontrolleret Deaktiveret Aktiveret | Brugerkontrolleret | Angiver statussen for 802.1x-godkendelsesfunktionen. <ul style="list-style-type: none"> • Brugerkontrolleret – brugeren kan konfigurere 802.1x på telefonen. • Deaktiveret – 802.1x-godkendelse anvendes ikke. • Aktiveret – 802.1x-godkendelse bruges, og du kan konfigurere godkendelsen for telefonerne. |
| Ekstern konfiguration af switch-port | Deaktiveret Automatisk forhandling 10 med halv dupleks 10 med fuld dupleks 100 med halv dupleks 100 med fuld dupleks | Deaktiveret | Gør det muligt eksternt at konfigurere hastigheden og dupleksfunktionen på telefonens SW-port. Dette forbedrer ydelsen ved store installationer med specifikke portindstillinger. Hvis SW-portene konfigureres til ekstern portkonfiguration i Cisco Unified Communications Manager, kan dataene ikke ændres på telefonen. |
| SSH-adgang | Deaktiveret Aktiveret | Deaktiveret | Styrer adgangen til SSH-daemon via port 22. Hvis du lader port 22 være åben, er telefonen sårbar over for DoS-angreb (denial of Service). |
| Landstandard for ringning | Standard Japan | Standard | Styrer ringningsmønstret. |
| Timer for TLS-genoptagelse | Heltal 0-3600 sekunder | 3600 | Styrer muligheden for at genoptage en TLS-session uden at gentage hele TLS-godkendelsesprocessen. Hvis feltet er indstillet til 0, så er genoptagelse af TLS-sessionen deaktiveret. |
| FIPS-tilstand | Deaktiveret Aktiveret | Deaktiveret | Aktiverer eller deaktiverer FIPS-tilstanden (Federal Information Processing Standards) på telefonen. |
| Registrer opkaldslogfil fra delt linje | Deaktiveret Aktiveret | Deaktiveret | Angiver om, du vil registrere opkaldslog fra en delt linje. |
| Minimumlydstyrke ved ringning | 0-stilhed 1-15 | 0-stilhed | Styrer telefonens minimumlydstyrke ved ringning. |

| Feltnavn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|---------------------------------------|----------------------------------|-----------|--|
| Peer-firmwaredeling | Deaktiveret Aktiveret | Aktiveret | <p>Lader telefonen finde andre telefoner i samme model på undernettet og dele opdaterede firmwarefiler. Hvis telefonen har fået en ny firmware, kan den dele firmware med de andre telefoner. Hvis en af de andre telefoner har en ny firmware, kan telefonen downloade den fra den anden telefon i stedet for fra TFTP-serveren.</p> <p>Peer-firmwaredeling:</p> <ul style="list-style-type: none"> • Begrænser overbelastning på TFTP-overførsler til centraliserede eksterne TFTP-servere. • Fjerner behovet for manuelt at styre firmwareopgraderinger. • Reducerer telefonens nedetid under opgradering, når et stort antal telefoner nulstilles samtidigt. • Er en hjælp under opgradering af firmware i scenarier med installation på afdelingskontorer eller fjernkontorer, der foretages via WAN-forbindelser med bredbåndsbegrænsning. |
| Belastningsserver | Streng på op til 256 tegn | | Identificerer den alternative IPv4-server, som telefonen bruger til at hente firmwarefiler og -opgraderinger. |
| IPv6-belastningsserver | Streng på op til 256 tegn | | Identificerer den alternative IPv6-server, som telefonen bruger til at hente firmwarefiler og -opgraderinger. |
| Registrer Unified CM-forbindelsesfejl | Normal Forsinket | Normal | <p>Bestemmer den følsomhed, telefonen har i forhold til at registrere en forbindelsesfejl til Cisco Unified Communications Manager (Unified CM), der er det første trin, før enheden har en failover til en ekstra Unified CM/SRST.</p> <p>Gyldige værdier angiver Normal (registrering af en Unified CM-forbindelsesfejl sker ved standardssystemhastighed) eller Forsinket (registrering af en Unified CM-forbindelsesfejl sker omtrent fire gange langsommere end Normal).</p> <p>Vælg Normal for at få en hurtigere genkendelse af en Unified CM-forbindelsesfejl. Hvis du foretrækker, at failoveren bliver en smule forsinket, så forbindelsen har mulighed for at blive genoprettet, skal du vælge Forsinket</p> <p>Den nøjagtige tidsforskel mellem registrering af Normal og Forsinket forbindelsesfejl afhænger af, hvor mange variabler der hele tiden ændrer sig.</p> |

| Felt navn | Felttype Eller valgmuligheder | Standard | Beskrivelse |
|---|---|-------------------------|--|
| Special Requirement ID (Særligt kravs-ID) | Streng | | Styrer brugerdefinerede funktioner fra ES-filer (Engineering Special). |
| HTTPS-server | http og https aktiveret kun https | http og https aktiveret | Styrer typen af kommunikation til telefonen. Hvis du kun vælger HTTPS, er telefonkommunikation mere sikker. |
| Brugerlegitimationsoplysninger bevares for Expressway-logon | Deaktiveret Aktiveret | Deaktiveret | <p>Styrer, om telefonen lagrer brugerens logonlegitimationsoplysninger. Når indstillingen er deaktiveret, ser brugeren altid meddelelsen om at logge på Expressway-serveren for MRA (Mobile and Remote Access).</p> <p>Hvis du gerne vil gøre det nemmere for brugerne at logge på, skal du aktivere dette felt, så legitimationsoplysningerne til Expressway-logon bevares. Derefter skal brugeren kun angive sine logonoplysninger den første gang. På et hvilket som helst tidspunkt efter det (når telefonen er tændt på eksternt sted), udfyldes logonoplysningerne automatisk på logonskærmen.</p> <p>Du kan få yderligere oplysninger i Konfigurer bevarelse af brugerlegitimationsoplysninger for Expressway-logon, på side 119.</p> |
| URL-adressen til overførsel ved kundesupport | Streng, op til 256 tegn | | <p>Angiver URL-adressen til PRT (Problem Report Tool).</p> <p>Hvis du installerer enheder med mobil- og fjernadgang via Expressway, skal du også føje PRT-serveradressen til tilladelseslisten for HTTP-serveren på Expressway-serveren.</p> <p>Du kan få yderligere oplysninger i Konfigurer bevarelse af brugerlegitimationsoplysninger for Expressway-logon, på side 119.</p> |
| Deaktiver TLS-kryptering | Se Deaktiver TLS-kryptering (Transport Layer Security), på side 108 . | Ingen | <p>Deaktiverer den valgte TLS-kryptering.</p> <p>Deaktiver mere end én krypteringspakke ved at vælge og holde Ctrl nede på computerens tastatur.</p> |
| Dedikere en linje til parkering af opkald | Deaktiveret Aktiveret | Aktiveret | <p>Styrer, om et parkeret opkald optager en linje eller ej.</p> <p>Få flere oplysninger i dokumentationen til Cisco Unified Communications Manager.</p> |

Lignende emner

[Konfigurer bevarelse af brugerlegitimationsoplysninger for Expressway-logon, på side 119](#)

Deaktiver TLS-kryptering (Transport Layer Security)

Du kan deaktivere TLS-koder (Transport Layer Security) med parameteren **Deaktiver TLS-kryptering**. Dette gør det muligt at tilpasse din sikkerhed i forhold til kendte sikkerhedsproblemer og få dit netværk til at følge din virksomheds politikker for kryptering.

Ingen er standardindstillingen.

Deaktiver mere end én krypteringspakke ved at vælge og holde **Ctrl** nede på computerens tastatur. Hvis du vælger alle telefonkrypteringer, påvirkes TLS-telefontjenesten. Dine muligheder 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

Få flere oplysninger om telefonens sikkerhed under *Hvidbog med sikkerhedsoversigt over 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>).

Planlæg strømbesparelse for Cisco IP-telefon

For at spare strøm og sikre en langtidsholdbar telefonskærm kan du indstille skærmen til at slukke, når den ikke skal bruges.

Du kan konfigurere indstillingerne i Cisco Unified Communications Manager Administration til at slukke for skærmen på et bestemt tidspunkt på nogle dage og hele dagen på andre dage. Du kan f.eks. vælge at slukke for skærmen efter kontortid på hverdage og hele dagen på lørdage og søndage.

Du kan udføre en af følgende handlinger for at tænde når som helst, hvis den er slukket:

- Tryk på en knap på telefonen.
Telefonen udfører den handling, der er angivet af den pågældende knap, for at tænde skærmen.
- Løft røret.

Når du tænder skærmen, forbliver den tændt, indtil telefonen har været inaktiv i et angivet tidsrum, hvorefter den slukker automatisk.

Fremgangsmåde

Trin 1 Vælg **Enhed** > **Telefon** i Cisco Unified Communications Manager Administration.

Trin 2 Find den telefon, du skal konfigurere.

Trin 3 Gå til det produktspecifikke konfigurationsområde, og indstil følgende felter:

- Dage skærm er inaktiv
- Skærm tænder klokken
- Skærm tændt varighed
- Skærm inaktiv timeout

Tabel 19: Felter til konfiguration af strømbesparelse

| Felt | Beskrivelse |
|-----------------------|---|
| Dage skærm er inaktiv | De dage, hvor skærmen ikke tændes automatisk på det tidspunkt, der er angivet i feltet Skærm tænder klokken. Vælg dagen eller dagene på rullelisten. Hvis du vil vælge mere end én dag, skal du bruge Ctrl+klik på de ønskede dage. |
| Skærm tænder klokken | Det klokkeslæt hver dag, hvor skærmen tændes automatisk (undtagen på de dage, der er angivet i feltet Dage skærm er inaktiv). Angiv tiden i dette felt ved brug af 24-timers formatet, hvor 00:00 er midnat. Hvis du f.eks. automatisk vil tænde skærmen kl. 07:00 om morgenen (0700), skal du angive 07:00 . Hvis du vil tænde skærmen kl. 14.00 om eftermiddagen (1400), skal du angive 14:00 . Hvis dette felt er tomt, tændes skærmen automatisk kl. 0:00. |
| Skærm tændt varighed | Længden af den tid, som skærmen er tændt, efter at det er blevet tændt på det tidspunkt, der er angivet i feltet Skærm tænder klokken. Angiv værdien i dette felt i formatet <i>timer:minutter</i> . Hvis du f.eks. vil lade skærmen være tændt i 4 timer og 30 minutter, efter at det er blevet tændt automatisk, skal du angive 04:30 . Hvis dette felt er tomt, slukkes telefonen, når dagen er gået (0:00). Bemærk Hvis Skærm tænder klokken er 0:00, og varigheden af skærm tænder er tom (eller 24:00), slukkes skærmen ikke. |
| Skærm inaktiv timeout | Længden af den tid, som telefonen er inaktiv, før skærmen slukkes. Gælder kun, når skærmen blev slukket efter planen, og tændt af en bruger (ved at trykke på en knap på telefonen eller løfte håndsættet). Angiv værdien i dette felt i formatet <i>timer:minutter</i> . Hvis du f.eks. vil slukke skærmen, når telefonen har været inaktiv i 1 time og 30 minutter, når en bruger tænder skærmen, skal du angive 01:30 . Standardværdien er 01:00. |

Trin 4 Vælg **Gem**.

Trin 5 Vælg **Anvend konfig**.

Trin 6 Genstart telefonen.

Planlæg EnergyWise på Cisco IP-telefon

Hvis du vil reducere strømforbruget, kan du konfigurere telefonen til dvale (slukkes) og opvågning (tændes), hvis dit system omfatter en EnergyWise-controller.

Du konfigurerer indstillingerne i Cisco Unified Communications Manager Administration for at aktivere EnergyWise og konfigurere tidspunkter for dvale og opvågning. Disse parametre er tæt forbundne med parametrene til konfigurationen af telefonvisningen.

Når EnergyWise er aktiveret, og der er indstillet en dvaletimer, sender telefonen en anmodning til switchen for at vække den på det konfigurerede tidspunkt. Switchen returnerer enten en accept eller afvisning af anmodningen. Hvis switchen afviser anmodningen, eller hvis switchen ikke svarer, slukkes telefonen ikke. Hvis switchen accepterer anmodningen, går den inaktive telefon i dvale og reducerer dermed strømforbruget til et forudbestemt niveau. En telefon, der ikke er inaktiv, indstiller en timer for inaktivitet og går i dvale, når timeren for inaktivitet udløber.

Tryk på Vælg for at vække Telefonen. På det planlagte opvågningstidspunkt genopretter systemet strømmen til telefonen, så den vågner.

Fremgangsmåde

Trin 1 Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration.

Trin 2 Find den telefon, du skal konfigurere.

Trin 3 Gå til det produktspecifikke konfigurationsområde, og indstil følgende felter.

- Enable Power Save Plus (Aktiver strømsparefunktion plus)
- Tidspunkt for tænding af telefon
- Tidspunkt for slukning af telefon
- Timeout for telefon slukket ved inaktivitet
- Aktivér lydbesked
- EnergyWise Domæne
- EnergyWise-hemmelighed
- Tillad EnergyWise-tilsidesættelser

Tabel 20: EnergyWise-konfigurationsfelter

| Felt | Beskrivelse |
|--|---|
| Enable Power Save Plus (Aktiver strømsparefunktion plus) | <p>Vælger tidsplanen for de dage, hvor telefonen er slukket. Vælg flere dage ved at trykke på og holde Ctrl-tasten nede, mens du klikker på dagene i tidsplanen.</p> <p>Som standard er ingen dage valgt.</p> <p>Når Aktiver strømsparefunktion plus er markeret, modtager du en meddelelse, der advarer om nødforhold (e911).</p> <p>Advarsel Mens strømsparefunktionen ("tilstanden") er aktiveret, bliver slutpunkter, der er konfigureret til den tilstand, deaktiveret ved nødopkald og modtagelse af indgående opkald. Ved at vælge denne tilstand accepterer du følgende: (i) Du påtager dig det fulde ansvar for at sikre alternative metoder til nødopkald og modtagelse af opkald, når denne tilstand er aktiveret; (ii) Cisco er ikke ansvarlig for dit valg af denne tilstand, og alt ansvar i forbindelse med aktivering af denne tilstand påhviler dig; og (iii) Du giver brugerne alle oplysninger om virkningen af tilstanden ved opkald, foretagelse af opkald og på anden vis.</p> <p>Bemærk Hvis du vil deaktivere strømsparefunktionen, skal du fjerne markeringen af afkrydsningsfeltet Tillad EnergyWise-tilsidesættelser. Hvis Tillad EnergyWise-tilsidesættelser forbliver markeret, men der ikke er valgt nogen dage i feltet Aktiver strømsparefunktion plus, er strømsparefunktionen ikke aktiveret.</p> |
| Tidspunkt for tænding af telefon | <p>Bestemmer, hvornår telefonen automatisk tændes på de dage, der er angivet i feltet Aktivér Power Save Plus.</p> <p>Angiv tiden i dette felt ved brug af 24-timers formatet, hvor 00:00 er midnat.</p> <p>Hvis du f.eks. vil tænde telefonen kl. 07:00 om morgenen (0700), skal du angive 07:00. Hvis du vil tænde telefonen kl. 02:00 om eftermiddagen (1400), angiv 14:00.</p> <p>Standardværdien er tom, hvilket betyder 00:00.</p> <p>Bemærk Tidspunkt for tænding af telefon skal være mindst 20 minutter senere end Tidspunkt for slukning af telefon. Hvis f.eks. Tidspunkt for slukning af telefon er 7:00, må Tidspunkt for tænding af telefon ikke være tidligere end 7:20.</p> |
| Tidspunkt for slukning af telefon | <p>Det tidspunkt på dagen, hvor telefonen slukkes, for de dage, der er angivet i feltet Aktivér strømsparefunktion plus. Hvis felterne Tidspunkt for tænding af telefon og Tidspunkt for slukning af telefon indeholder den samme værdi, slukkes telefonen ikke.</p> <p>Angiv tiden i dette felt ved brug af 24-timers formatet, hvor 00:00 er midnat.</p> <p>Hvis du f.eks. vil slukke telefonen kl. 7:00 om morgenen (0700), skal du angive 7:00. Hvis du vil slukke telefonen kl. 2:00 om eftermiddagen (1400), angiv 14:00.</p> <p>Standardværdien er tom, hvilket betyder 00:00.</p> <p>Bemærk Tidspunkt for tænding af telefon skal være mindst 20 minutter senere end Tidspunkt for slukning af telefon. Hvis f.eks. Tidspunkt for slukning af telefon er 7:00, må Tidspunkt for tænding af telefon ikke være tidligere end 7:20.</p> |

| Felt | Beskrivelse |
|---|---|
| Timeout for telefon slukket ved inaktivitet | <p>Det tidsrum, hvori telefonen skal være inaktiv, før telefonen slukkes.</p> <p>Timeouten sker under følgende betingelser:</p> <ul style="list-style-type: none"> • Når telefonen som planlagt er i tilstanden strømsparefunktion plus, og når den går ud af strømsparefunktion plus, fordi brugeren af telefonen har trykket på tasten Vælg. • Når telefonen får strøm igen fra den påsatte switch. • Når Tidspunkt for slukning af telefon nås, men telefonen er i brug. <p>Feltets område er 20 til 1440 minutter.</p> <p>Standardværdien er 60 minutter.</p> |
| Aktivér lydbesked | <p>Når denne indstilling er aktiveret, får telefonen besked om at afspille en lydbesked, der starter 10 minutter før det tidspunkt, der er angivet i feltet Tidspunkt for slukning af telefon.</p> <p>Lydsignalet bruger telefonringetonen, der afspilles kortvarigt på bestemte tidspunkter i 10 minutters beskedperioden. Beskedringetonen afspilles med den brugerangivne lydstyrke. Tidsplan for hørbar besked er:</p> <ul style="list-style-type: none"> • 10 minutter før sluk afspilles ringetonen fire gange. • 7 minutter før sluk afspilles ringetonen fire gange. • 4 minutter før sluk afspilles ringetonen fire gange. • 30 sekunder før sluk afspilles ringetonen 15 gange, eller indtil telefonen slukker. <p>Dette afkrydsningsfelt gælder kun, hvis listefeltet Aktiver strømsparefunktion plus indeholder en eller flere af de valgte dage.</p> |
| EnergyWise Domæne | <p>Det EnergyWise-domæne, telefonen er i.</p> <p>Den maksimale længde på dette felt er 127 tegn.</p> |
| EnergyWise-hemmelighed | <p>Den hemmelige sikkerhedsadgangskode, der bruges til at kommunikere på EnergyWise-domænet.</p> <p>Den maksimale længde på dette felt er 127 tegn.</p> |

| Felt | Beskrivelse |
|------------------------------------|---|
| Tillad EnergyWise-tilsidesættelser | <p>Dette afkrydsningsfelt angiver, om du tillader, at politikken for EnergyWise-domænecontrolleren kan sende opdateringer om strømniveau til telefonerne. Følgende betingelser gælder:</p> <ul style="list-style-type: none"> • Der skal være valgt en eller flere dage i feltet Aktiver strømsparefunktion plus. • Indstillingerne i Cisco Unified Communications Manager Administration aktiveres efter planen, også selvom EnergyWise sender en tilsidesættelse. <p>Hvis det f.eks. antages, at Tidspunkt for slukning af telefon indstilles til 22:00 (10:00 om aftenen), værdien i feltet Tidspunkt for tænding af telefon er 06:00 (6:00 om morgenen), og en eller flere dage er valgt for Aktiver strømsparefunktion plus.</p> <ul style="list-style-type: none"> • Hvis EnergyWise angiver, at telefonen skal slukkes kl. 20:00 (8:00 om aftenen), vil den angivelse gælde (forudsat at brugeren af telefonen ikke gør noget) indtil 6:00 a.m., som er konfigureret for Tidspunkt for tænding af telefon. • Kl. 6:00 om morgenen tændes telefonen og fortsætter med at modtage ændringerne i strømniveauet fra indstillingerne i Unified Communications Manager Administration. • For at ændre strømniveauet på telefonen igen skal EnergyWise udstede en ny kommando om ændring af strømniveau. <p>Bemærk Hvis du vil deaktivere strømsparefunktionen, skal du fjerne markeringen af afkrydsningsfeltet Tillad EnergyWise-tilsidesættelser. Hvis Tillad EnergyWise-tilsidesættelser forbliver markeret, men der ikke er valgt nogen dage i feltet Aktiver strømsparefunktion plus, er strømsparefunktionen ikke aktiveret.</p> |

- Trin 4** Vælg **Gem**.
- Trin 5** Vælg **Anvend konfig**.
- Trin 6** Genstart telefonen.

Konfigurer DND (Forstyr ikke)

Når Ring ikke (DND) er aktiveret, bliver hoveddelen på konferencetelefonen rød.

Få flere oplysninger i oplysningerne om Forstyr ikke i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Fremgangsmåde

- Trin 1** Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration.
- Trin 2** Find den telefon, der skal konfigureres.
- Trin 3** Indstil følgende parametre.
- Do Not Disturb: Med dette afkrydsningsfelt kan du aktivere DND på telefonen.
 - DND-indstilling: Ring af, Afvist opkald eller brug almindelig telefonprofilindstilling.

- Alarm om indgående opkald ved DND: Vælg den type alarm, om nogen, der skal afspilles på en telefon ved indgående opkald, når DND er aktiv.

Bemærk Denne parameter findes i vinduet Almindelig telefonprofil og vinduet Telefonkonfiguration. Vinduesværdien Telefonkonfiguration har højere prioritet.

Trin 4 Vælg **Gem**.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Konfigurer besked om viderestilling af opkald

Du kan justere indstillingerne for viderestilling af opkald.

Fremgangsmåde

Trin 1 Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration.

Trin 2 Find den telefon, der skal konfigureres.

Trin 3 Konfigurer felterne Besked om viderestil opkald.

| Felt | Beskrivelse |
|------------------------------|--|
| Opkalders navn | Når dette afkrydsningsfelt er markeret, vises navnet på den person, der ringer op, i beskedvinduet. Dette afkrydsningsfelt er som standard markeret. |
| Caller Number | Når dette afkrydsningsfelt er markeret, vises opkalderens nummer i beskedvinduet. Dette afkrydsningsfelt er som standard ikke markeret. |
| Viderestillet nummer | Når dette afkrydsningsfelt er markeret, vises oplysninger om den opkalder, der sidst viderestillede opkaldet, i beskedvinduet. Eksempel: Hvis Opkalder A ringer til B, men B har viderestillet alle opkald til C, og C har viderestillet alle opkald til D, indeholder den beskedboks, som D ser, telefonoplysningerne for opkalder C. Dette afkrydsningsfelt er som standard ikke markeret. |
| Nummer, der er ringet op til | Når dette afkrydsningsfelt er markeret, vises oplysninger om den originale modtager af opkaldet i beskedvinduet. Eksempel: Hvis Opkalder A ringer til B, men B har viderestillet alle opkald til C, og C har viderestillet alle opkald til D, indeholder den beskedboks, som D ser, telefonoplysningerne for opkalder B. Dette afkrydsningsfelt er som standard markeret. |

Trin 4 Vælg **Gem**.

Konfiguration af UCR 2008

Parametrene, der understøtter UCR 2008, findes i Cisco Unified Communications Manager Administration. Følgende tabel beskriver parametrene og angiver stien til at ændre indstillingen.

Tabel 21: Placering af UCR 2008-parameteren

| Parameter | Administrationssti |
|--|--|
| FIPS-tilstand | Enhed > Enhedsindstillinger > Almindelig telefonprofil |
| | System > Konfiguration af firmatelefon |
| | Enhed > Telefoner |
| SSH-adgang | Enhed > Telefon |
| | Enhed > Enhedsindstillinger > Almindelig telefonprofil |
| Webadgang | Enhed > Telefon |
| | System > Konfiguration af firmatelefon |
| | Enhed > Enhedsindstillinger > Almindelig telefonprofil |
| System > Konfiguration af firmatelefon | |
| IP-adresseringstilstand | Enhed > Enhedsindstillinger > Fælles enhedskonfiguration |
| IP-adressetilstand til signal | Enhed > Enhedsindstillinger > Fælles enhedskonfiguration |

Konfigurer UCR 2008 med fælles enhedskonfiguration

Brug denne procedure til at indstille følgende UCR 2008-parametre:

- IP-adresseringstilstand
- IP-adressetilstand til signal

Fremgangsmåde

- Trin 1** Vælg **Enhed > Enhedsindstillinger > Fælles enhedskonfiguration** i Cisco Unified Communications Manager Administration.
- Trin 2** Indstil parameteren for tilstand af IP-adresse.
- Trin 3** Angiv indstilling af tilstand for IP-adresse for signalparameter.

Trin 4 Vælg **Gem**.

Konfigurer UCR 2008 i Almindelig telefonprofil

Brug denne procedure til at indstille følgende UCR 2008-parametre:

- FIPS-tilstand
- SSH-adgang
- Webadgang

Fremgangsmåde

- Trin 1** Vælg **Enhed > Enhedsindstillinger > Almindelig telefonprofil** i Cisco Unified Communications Manager Administration.
- Trin 2** Indstil FIPS-tilstandsparameteren til **Aktiveret**.
- Trin 3** Indstil SSH-adgangsparameteren til **Deaktiveret**.
- Trin 4** Indstil webadgangsparameteren til **Deaktiveret**.
- Trin 5** Indstil 80-bit SRTCP-parameteren til **Aktiveret**.
- Trin 6** Vælg **Gem**.
-

Konfigurer UCR 2008 i konfiguration af firmatelefon

Brug denne procedure til at indstille følgende UCR 2008-parametre:

- FIPS-tilstand
- Webadgang

Fremgangsmåde

- Trin 1** Vælg **System > Konfiguration af firmatelefon** i Cisco Unified Communications Manager Administration.
- Trin 2** Indstil FIPS-tilstandsparameteren til **Aktiveret**.
- Trin 3** Indstil webadgangsparameteren til **Deaktiveret**.
- Trin 4** Vælg **Gem**.
-

Konfigurer UCR 2008 i telefon

Brug denne procedure til at indstille følgende UCR 2008-parametre:

- FIPS-tilstand
- SSH-adgang
- Webadgang

Fremgangsmåde

- Trin 1** Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration.
- Trin 2** Indstil SSH-adgangsparameteren til **Deaktiveret**.
- Trin 3** Indstil FIPS-tilstandsparameteren til **Aktiveret**.
- Trin 4** Indstil webadgangsparameteren til **Deaktiveret**.
- Trin 5** Vælg **Gem**.
-

Mobil og fjernadgang via Expressway

Mobil og fjernadgang via Expressway (MRA) giver fjernarbejdere mulighed for nemt og sikkert at oprette forbindelse til firmaets netværk uden at bruge en VPN-klienttunnel (virtual private network). Expressway anvender TLS (Transport Layer Security) til at beskytte netværkstrafikken. Hvis en telefon skal kunne godkende et Expressway-certifikat og oprette en TLS-session, skal et offentligt nøglecenter, som telefonens firmware har tillid til, signere Expressway-certifikatet. Det er ikke muligt at installere eller have tillid til andre CA-certifikater på telefoner til godkendelse af et Expressway-certifikat.

Listen over CA-certifikater, der er integreret i telefonens firmware, er tilgængelig på <http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html>.

Mobil og fjernadgang via Expressway (MRA) fungerer sammen med Cisco Expressway. Du skal kende dokumentationen til Cisco Expressway documentation, herunder *Administratorvejledningen til Cisco Expressway Administrator* og *Vejledningen i grundlæggende konfiguration og installation af Cisco Expressway*. Cisco Expressway-dokumentationen findes på <http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html>.

Det er kun IPv4-protokollen, der understøttes for brugere af Mobil og fjernadgang via Expressway.

Få yderligere oplysninger om, hvordan du bruger Mobil og fjernadgang via Expressway, ved at se:

- *Cisco Preferred Architecture for Enterprise Collaboration, designoversigt*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD*
- *Installationsvejledning til Unified Communications Mobile og fjernadgang via Cisco VCS*
- *Cisco TelePresence Video Communication Server (VCS), konfigurationsvejledninger*
- *Implementeringsvejledning til Mobile and Remote Access via Cisco Expressway*

Mens processen til registrering af telefonen er i gang, synkroniserer telefonen den viste dato og det viste klokkeslæt med NTP-serveren (Network Time Protocol). Med MRA bruges DHCP-indstillingskode 42 til at finde IP-adresserne på de NTP-servere, der er angivet til synkronisering af klokkeslæt og dato. Hvis koden DHCP-indstilling 42 ikke er i konfigurationsoplysningerne, leder telefonen efter koden 0.tandberg.pool.ntp.org for at identificere NTP-serverne.

Når registreringen er færdig, bruger telefonen oplysningerne fra SIP-meddelelsen til at synkronisere den viste dato og det viste klokkeslæt, medmindre en NTP-server er konfigureret i Cisco Unified Communications Manager-telefonkonfigurationen.



Bemærk Hvis indstillingen TFTP Encrypted Config (TFTP-krypteret konfig.) er markeret i telefonsikkerhedsprofilen for en af dine telefoner, kan du ikke bruge telefonen med mobil og fjernadgang. MRA-løsningen understøtter ikke enhedsinteraktion med CAPE (Certificate Authority Proxy Function).

SIP OAuth-tilstand understøttes for MRA. Denne tilstand giver dig mulighed for at bruge OAuth-adgangstokens til godkendelse i sikre miljøer.



Bemærk I forbindelse med SIP OAuth i MRA-tilstand (Mobile and Remote Access) må du kun bruge aktiveringskode, der er indbygget i mobil- og fjernadgang, når du installerer telefonen. Aktivering med et brugernavn og en adgangskode understøttes ikke.

SIP OAuth-tilstand kræver Expressway x14.0(1) og nyere eller Cisco Unified Communications Manager 14.0(1) og nyere.

Få flere oplysninger om SIP OAuth-tilstand i *Vejledning i funktionskonfiguration til Cisco Unified Communications Manager*, version 14.0(1) eller nyere.

Installationsscenerier

Følgende tabel viser forskellige installationsscenerier for Mobil og fjernadgang via Expressway.

| Scenarie | Handlinger |
|--|--|
| Lokal bruger logger på firmanetværket efter installation af Mobil og fjernadgang via Expressway. | Firmanetværket detekteres, og telefonen registreres med Cisco Unified Communications Manager, som den normalt vil. |
| Ekstern bruger logger på firmanetværket med Mobil og fjernadgang via Expressway. | <p>Telefonen detekterer, at den er i ekstern tilstand, Mobil og fjernadgang via Expressway-logonvinduet vises, og brugeren opretter forbindelse til firmanetværket.</p> <p>Brugere skal have et gyldigt tjenesteanavn, brugernavn og adgangskode for at oprette forbindelse til netværket.</p> <p>Brugere skal også nulstille tjenestetilstanden for at rydde indstillingen for den alternative TFTP, før de kan få adgang til firmaets netværk. Dette rydder indstillingen for den alternative TFTP-server, så telefonen registrerer netværk uden for virksomheden.</p> <p>Hvis en telefon installeres direkte fra kassen, behøver brugere ikke at nulstille netværksindstillingerne.</p> <p>Hvis brugere har DHCP-indstilling 150 eller indstilling 66 aktiveret på deres netværksrouter, kan de muligvis ikke logge på firmanetværket. Brugere bør deaktivere disse DHCP-indstillinger eller konfigurere deres statiske IP-adresse direkte.</p> |

Konfigurer bevarelse af brugerlegitimationsoplysninger for Expressway-logon

Når en bruger logger på netværket med Mobil og fjernadgang via Expressway, bedes brugeren angive tjenestedomæne, brugernavn og adgangskode. Hvis du aktiverer parameteren for bevarelse af brugerlegitimationsoplysninger for Expressway-logon, gemmes brugerens logonoplysninger, så det ikke er nødvendigt at indtaste disse oplysninger igen. Denne parameter er deaktiveret som standard.

Du kan konfigurere legitimationsoplysninger, der skal bevares, for en enkelt telefon, en gruppe af telefoner eller alle telefoner.

Lignende emner

[Konfiguration af telefonfunktioner](#), på side 93

[Produktspecifik konfiguration](#), på side 95

Problemrapporteringsværktøj

Brugerne sender problemrapport til dig ved hjælp af problemrapporteringsværktøjet.



Bemærk Cisco TAC skal bruge logfilerne fra problemrapporteringsværktøj ved fejlfinding af problemer. Logfilerne ryddes, hvis du genstarter telefonen. Indsaml logfilerne, før du genstarter telefonerne.

For at oprette en problemrapport skal brugerne åbne problemrapporteringsværktøjet og angive dato og klokkeslæt for, hvornår problemet opstod, samt en beskrivelse af problemet.

Hvis PRT-overførslen mislykkes, kan du få adgang til PRT-filen for telefonen fra URL-adressen **http://<phone-ip-address>/FS/<prt-file-name>**. Denne URL-adresse vises på telefonen i disse tilfælde:

- Hvis telefonens tilstand er fabriktilstand. URL'en er aktiv i 1 time. Når der er gået 1 time, skal brugeren forsøge at sende telefonens logfiler igen.
- Hvis telefonen har downloadet en konfigurationsfil, og opkaldskontrolsystemet giver webadgang til telefonen.

Du skal føje en serveradresse til feltet **URL-adressen til overførsel ved kundesupport** på Cisco Unified Communications Manager.

Hvis du installerer enheder med Mobile and Remote Access Through Expressway, skal du også føje PRT-serveradressen til tilladelseslisten for HTTP-serveren på Expressway-serveren.

Konfigurer en URL-adresse til overførsel ved kundesupport

Du skal bruge en server med et overførselsscript for at modtage PRT-filer. PRT bruger en HTTP POST-mekanisme, hvor følgende parametre indgår i overførslen (brug af MIME-kodning i flere dele):

- devicename (eksempel: "SEP001122334455")
- serialno (eksempel: "FCH12345ABC")
- brugernavn (det brugernavn, der er konfigureret i Cisco Unified Communications Manager, enhedens ejer)
- prt_file (eksempel: "probrep-20141021-162840.tar.gz")

Herunder vises et eksempel på script. Script er kun tiltænkt som reference. Cisco yder ikke support for de overførselsscript, der er installeret på en kundes server.

```
<?php

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

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

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

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

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

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

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

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

?>
```



Bemærk Telefonerne understøtter kun HTTP-baserede URL-adresser.

Fremgangsmåde

- Trin 1** Konfigurer en server, der kan køre dit PRT-overførselsscript
- Trin 2** Skriv et script, der kan håndtere de parametre, der er angivet herover, eller rediger det angivne scripteksempel, så det passer til dit behov.
- Trin 3** Overfør dit script til din server.
- Trin 4** I Cisco Unified Communications Manager skal du gå til området Produktspecifikt konfigurationslayout i vinduet til konfiguration af den enkelte enhed, vinduet Almindelig telefonprofil eller vinduet Konfiguration af firmatelefon.
- Trin 5** Markér **URL-adressen til overførsel ved kundesupport**, og angiv URL-adressen til overførsel til din server.

Eksempel:

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

- Trin 6** Gem dine ændringer.

Indstil etiket for en linje

Du kan konfigurere en telefon til at vise en tekstetiket i stedet for telefonnummeret. Brug denne etiket til at identificere linjen efter navn eller funktion. Hvis din bruger f.eks. deler linjer på telefonen, kunne du identificere linjen med navnet på den person, der deler linjen.

Når du tilføjer en etiket til et tastudvidelsesmodul, vises kun de første 25 tegn på en linje.

Fremgangsmåde

- Trin 1** Vælg **Enhed > Telefon** i Cisco Unified Communications Manager Administration.
 - Trin 2** Find den telefon, der skal konfigureres.
 - Trin 3** Find linjeforekomsten, og indstil feltet Linjetekstetiket.
 - Trin 4** (Valgfri) Hvis etiketten skal anvendes på andre enheder, der deler linjen, skal afkrydsningsfeltet Opdater indstillinger for delt enhed markeres. Klik derefter på **Udfyldning valgt**.
 - Trin 5** Vælg **Gem**.
-



KAPITEL 10

Firmatelefonbog og personlig telefonbog

- [Opsætning af firmatelefonbog, på side 123](#)
- [Opsætning af personlig telefonbog, på side 123](#)

Opsætning af firmatelefonbog

Firmatelefonbogen giver en bruger mulighed for at slå kollegernes telefonnumre op. Hvis den funktion skal understøttes, skal du konfigurere firmatelefonbøger.

Cisco Unified Communications Manager bruger et LDAPkatalog (Lightweight Directory Access Protocol LDAP) til at gemme godkendelses- og autorisationsoplysninger om brugere af Cisco Unified Communications Manager-programmer, der har en brugergrænseflade med Cisco Unified Communications Manager. Godkendelse giver brugerrettigheder til at få adgang til systemet. Autorisation identificerer telefonressourcer, som en bruger har tilladelse til at bruge, f.eks. et bestemt telefonlokalnummer.

Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Når du har fuldført konfigurationen af LDAP-telefonbogen, kan brugerne anvende firmatelefonbogstjenesten på deres telefon til at slå brugere op i firmatelefonbogen.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Opsætning af personlig telefonbog

Den personlige telefonbog giver en bruger mulighed for at lagre et sæt personlige numre.

Den personlige telefonbog har følgende funktioner:

- Personligt adressekartotek (PAB)
- Hurtigkald

Brugerne kan bruge disse metoder til at få adgang til funktioner i den personlige telefonbog:

- Fra en webbrowser - brugerne kan få adgang til PAB- og hurtigopkaldsfunktionerne fra selvbetjeningsportalen til Cisco Unified Communications.
- Gå til Cisco IP-telefon – og vælg **Kontakter** for at søge i firmatelefonbogen eller brugerens personlige telefonbog.

Hvis du vil konfigurere den personlige telefonbog fra en webbrowser, skal brugerne gå til deres selvbetjeningsportal. Du skal give brugerne en URL-adresse og logonoplysninger.



DEL **IV**

Fejlfinding af Cisco IP-konferencetelefon

- [Overvågning af telefonsystemer, på side 127](#)
- [Fejlfinding på telefonen, på side 153](#)
- [Vedligeholdelse, på side 171](#)
- [International brugersupport, på side 175](#)



KAPITEL 11

Overvågning af telefonsystemer

- [Oversigt over overvågning af telefonsystemer, på side 127](#)
- [Status for Cisco IP-telefon, på side 127](#)
- [Cisco IP-telefon-webside, på side 138](#)
- [Anmod om oplysninger fra telefonen i XML, på side 149](#)

Oversigt over overvågning af telefonsystemer

Du kan få vist en række forskellige oplysninger om telefonen ved hjælp af telefonstatusmenuen på telefonen og telefonens websider. Disse oplysninger omfatter:

- Enhedsoplysninger
- Oplysninger om netværksopsætning
- Netværksstatistik
- Enhedslogs
- Streaming-statistik

Dette kapitel beskriver de oplysninger, du kan få fra telefonens webside. Du kan bruge disse oplysninger til at fjernovervåge betjeningen af en telefon og til at hjælpe med fejlfinding.

Lignende emner

[Fejlfinding på telefonen](#), på side 153

Status for Cisco IP-telefon

De følgende afsnit beskriver, hvordan du kan få vist modeloplysninger, statusmeddelelser og netværksstatistik på Cisco IP-telefon.

- Modeloplysninger: viser oplysninger om telefonens hardware og software.
- Menuen Status: giver adgang til skærme, der viser statusmeddelelser, netværksstatistik og statistik for det aktuelle opkald.

Du kan bruge de oplysninger, der vises på disse skærme, til at overvåge betjeningen af en telefon og til at hjælpe med fejlfinding.

Du kan også få mange af disse oplysninger og andre relaterede oplysninger eksternt ved hjælp af telefonens webside.

Vis vinduet Telefonoplysninger

Fremgangsmåde

-
- Trin 1** Tryk på **Indstillinger** > **Systemoplysninger**.
- Trin 2** Afslut menuen ved at trykke på **Afslut**.
-

Vis menuen Status

Fremgangsmåde

-
- Trin 1** Tryk på **Indstillinger** > **Status**.
- Trin 2** Afslut menuen ved at trykke på **Afslut**.
-

Vis vinduet Statusmeddelelser

Fremgangsmåde

-
- Trin 1** Tryk på **Indstillinger** > **Status** > **Statusmeddelelser**.
- Trin 2** Afslut menuen ved at trykke på **Afslut**.
-

Felter til statusmeddelelser

Følgende tabel beskriver de statusmeddelelser, der vises på skærmen Statusmeddelelser på telefonen.

Tabel 22: Statusmeddelelser på Cisco IP-telefon

| Meddelelse | Beskrivelse | Mulig forklaring og handling |
|--|---|---|
| Der kunne ikke hentes en IP-adresse fra DHCP | Telefonen har ikke tidligere fået en IP-adresse fra en DHCP-server. Dette kan forekomme, når du foretager en nulstilling med det samme eller en fabriksnulstilling. | Bekræft, at DHCP-serveren er tilgængelig og har den rigtige IP-adresse til telefonen. |
| TFTP-størrelsesfejl | Konfigurationsfilen er for stor til telefonens filsystem. | Genstart telefonen. |

| Meddelelse | Beskrivelse | Mulig forklaring og handling |
|------------------------------------|--|---|
| ROM checksumfejl | Downloadet softwarefil er beskadiget. | Få en ny kopi af telefonens firmware og TFTPPath-mappen. Du bør kun kopiere den, når TFTP-serversoftware er lukket og ikke er beskadiget. |
| IP-dublet | En anden enhed bruger den IP-adresse, der er tildelt telefonen. | Hvis telefonen har en statisk IP-adresse, skal du kontrollere den dupliserede IP-adresse. Hvis du bruger DHCP, skal du kontrollere den DHCP-serveren. |
| Sletter CTL- og ITL-filer | Sletter CTL- og ITL-fil. | Ingen. Denne meddelelse er kun til information. |
| Fejl u opdater. af brugersprog | En eller flere lokaliseringsfiler blev ikke fundet i TFTP-stimappen eller var ikke gyldige. Landstandard blev ikke ændret. | I Cisco Unified Operating System skal du kontrollere, at følgende filer findes i TFTP-filstyringen: <ul style="list-style-type: none"> • Findes i undermappe med samme navn som netværkslandestandarden: <ul style="list-style-type: none"> • tones.xml • Findes i undermappe med samme navn som brugerstandarden: <ul style="list-style-type: none"> • glyphs.xml • dictionary.xml • kate.xml |
| Fil blev ikke fundet <Cfg File> | Den navnebaserede konfigurationsfil og standardkonfigurationsfilen blev ikke fundet på TFTP-serveren. | Konfigurationsfilen til en telefon oprettes af Cisco Unified Communications Manager. Hvis telefonen ikke findes i Cisco Unified Communications Manager-databasen, genererer TFTP-serveren blev ikke fundet . <ul style="list-style-type: none"> • Telefon er ikke registreret med Cisco Unified Communications Manager. Du skal manuelt føje telefonen til Cisco Unified Communications Manager, hvis den ikke kan registreres automatisk. • Hvis du bruger DHCP, skal du kontrollere den DHCP-serveren peger på den telefon. • Hvis du bruger en statisk IP-adresse, skal du kontrollere konfigurationen af TFTP-serveren. |
| Fil blev ikke fundet <CTLFile.tlv> | Denne meddelelse vises på telefonen, når Cisco Unified Communications Manager-klyngen ikke er i sikker tilstand. | Ingen påvirkning. Telefonen kan starte Cisco Unified Communications Manager. |

| Meddelelse | Beskrivelse | Mulig forklaring og handling |
|----------------------|--|---|
| IP-adresse frigivet | Telefonen er konfigureret til at frigive IP-adressen. | Telefonen forbliver inaktiv, indtil den efterfølgende nulstiller DHCP-adressen. |
| IPv4 DHCP-timeout | IPv4 DHCP-server svarede ikke. | <p>Netværk er optaget: Fejlene skal løses og netværksbelastningen reduceres.</p> <p>Ingen netværksforbindelse mellem IPv4 telefonen: Kontrollér netværksforbindelsen.</p> <p>IPv4 DHCP-server er nede: Kontrollér DHCP-serveren.</p> <p>Fejl fortsætter: Overvej at tildele en statisk IP-adresse.</p> |
| IPv6 DHCP-timeout | IPv6 DHCP-server svarede ikke. | <p>Netværk er optaget – fejlene skal løses og netværksbelastningen reduceres.</p> <p>Ingen netværksforbindelse mellem IPv6 telefonen: Kontrollér netværksforbindelsen.</p> <p>IPv6 DHCP-server er nede: Kontrollér DHCP-serveren.</p> <p>Fejl fortsætter: Overvej at tildele en statisk IP-adresse.</p> |
| IPv4DNS-timeout | IPv4 DNS-server svarede ikke. | <p>Netværk er optaget: Fejlene skal løses og netværksbelastningen reduceres.</p> <p>Ingen netværksforbindelse mellem IPv4 telefonen: Kontrollér netværksforbindelsen.</p> <p>IPv4 DNS-server er nede: Kontrollér DNS-serveren.</p> |
| IPv6 DNS-timeout | IPv6 DNS-server svarede ikke. | <p>Netværk er optaget: Fejlene skal løses og netværksbelastningen reduceres.</p> <p>Ingen netværksforbindelse mellem IPv6 telefonen: Kontrollér netværksforbindelsen.</p> <p>IPv6 DNS-server er nede: Kontrollér DNS-serveren.</p> |
| DNS ukendt IPv4-vært | IPv4 DNS kunne ikke fortolke navnet på TFTP-serveren eller Cisco Unified Communications Manager. | <p>Kontrollér, at værtsnavnene for TFTP-serveren og Cisco Unified Communications Manager er konfigureret korrekt.</p> <p>Overvej at bruge IPv4-adresser i stedet for domænenavne.</p> |
| DNS ukendt IPv6-vært | IPv6 DNS kunne ikke fortolke navnet på TFTP-serveren eller Cisco Unified Communications Manager. | <p>Kontrollér, at værtsnavnene for TFTP-serveren og Cisco Unified Communications Manager er konfigureret korrekt.</p> <p>Overvej at bruge IPv6-adresser i stedet for domænenavne.</p> |

| Meddelelse | Beskrivelse | Mulig forklaring og handling |
|---|---|--|
| Load Rejected HC | Det program, der blev downloadet, er ikke kompatibelt med telefonens hardware. | Det sker, hvis du forsøger at installere et program på denne telefon, der ikke understøttes af denne telefon. Kontrollér det indlæsnings-id, der tildelles til den enhed. Enhed > Telefon i Cisco Unified Communications Manager. Angiv den indlæsning, der vises på skærmen. |
| Ingen standardrouter | DHCP eller statisk konfiguration angav ikke en standardrouter. | Hvis telefonen har en statisk IP-adresse, er den standardrouteren er konfigureret. Hvis du bruger DHCP, har DHCP-serveren en standardrouter. Kontrollér konfigurationen af DHCP-serveren. |
| Ingen IPv4DNS-server | Der blev angivet et navn, men DHCP eller konfigurationen af den statiske IP angav ikke en IPv4 DNS-serveradresse. | Hvis telefonen har en statisk IP-adresse, er IPv4 DNS-serveren er konfigureret. Hvis du bruger DHCP, har DHCP-serveren en DNS-server. Kontrollér konfigurationen af DHCP-serveren. |
| Ingen IPv6 DNS-server | Der blev angivet et navn, men DHCP eller konfigurationen af den statiske IP angav ikke en IPv6 DNS-serveradresse. | Hvis telefonen har en statisk IP-adresse, er IPv6 DNS-serveren er konfigureret. Hvis du bruger DHCP, har DHCP-serveren en DNS-server. Kontrollér konfigurationen af DHCP-serveren. |
| Ingen tillidsliste installeret | CTL- eller ITL-filen er ikke installeret på telefonen. | Tillidslisten er ikke konfigureret i Cisco Unified Communications Manager, der ikke som standard understøttes. Tillidslisten er ikke konfigureret. Få flere oplysninger om tillidslister og hvordan du installerer en specifik version af Cisco Unified Communications Manager. |
| Telefonen kunne ikke registreres. Størrelsen på certificeringsnøglen er ikke FIPS-kompatibel. | FIPS kræver, at RSA-servercertifikatet er på 2048 bit eller mere. | Opdater certifikatet. |
| Cisco Unified Communications Manager har anmodet om genstart | Telefonen genstartes på grund af en anmodning fra Cisco Unified Communications Manager. | Der er sandsynligvis blevet foretaget en genstart af telefonen i Cisco Unified Communications Manager. Tryk på Anvend konfiguration for at genstarte telefonen. |
| TFTP-adgangsfejl | TFTP-server peger på en mappe, der ikke findes. | Hvis du bruger DHCP, skal du kontrollere, at DHCP-serveren peger på den rigtige TFTP-server. Hvis du bruger en statisk IP-adresse, skal du kontrollere konfigurationen af TFTP-serveren. |
| TFTP-fejl | Telefonen genkender ikke en fejlkode fra TFTP-serveren. | Kontakt Cisco TAC. |

| Meddelelse | Beskrivelse | Mulig forklaring og handling |
|--|--|---|
| TFTP-timeout | TFTP-server svarede ikke. | <p>Netværk er optaget: Fejlene skal løses netværksbelastningen reduceres.</p> <p>Ingen netværksforbindelse mellem TFTP-server og switch. Kontrollér netværksforbindelserne.</p> <p>TFTP-server er nede: Kontrollér konfigurationen af TFTP-serveren.</p> |
| Fik timeout | Supplikant har forsøgt 802.1X-transaktion, men fik timeout på grund af manglende godkendelsesfunktion. | Der er typisk timeout for godkendelse, hvis den er konfigureret på switchen. |
| Opdatering af tillidsliste mislykkedes | Opdatering af CTL- og ITL-filer mislykkedes. | <p>Telefon har CTL- og ITL-filer installeret, men ikke opdatere de nye CTL- og ITL-filer.</p> <p>Mulige årsager til fejl:</p> <ul style="list-style-type: none"> • Der er opstået en netværksfejl. • TFTP-server var nede. • Den nye sikkerhedstoken, der blev installeret i CTL-filen, og TFTP-certifikatet, der blev installeret i ITL-filen, er introduceret, men ikke er installeret på de aktuelle CTL- og ITL-filer på telefonen. • Der er opstået en intern telefonfejl. <p>Mulige løsninger:</p> <ul style="list-style-type: none"> • Kontrollér netværksforbindelsen. • Kontrollér, om TFTP-serveren er opstartet. • Hvis TVS-serveren (Transactional Voice Service) understøttes i Cisco Unified Communications Manager, skal du kontrollere, om TVS-serveren er opstartet normalt. • Kontrollér, om sikkerhedstokenen er gyldig. <p>Slet CTL- og ITL-filerne manuelt, hvis de er installeret. Løsninger ikke kan bruges. Nulstil telefonen.</p> <p>Få flere oplysninger om tillidslister i den aktuelle version af Cisco Unified Communications Manager.</p> |
| Tillidsliste blev opdateret | CTL-filen, ITL-filen eller begge filer opdateres. | <p>Ingen. Denne meddelelse er kun til orientering.</p> <p>Få flere oplysninger om tillidslister i den aktuelle version af Cisco Unified Communications Manager.</p> |
| Versionsfejl | Navnet på telefonindlæsningsfilen er forkert. | Sørg for, at telefonindlæsningsfilen har det korrekte navn. |
| XmlDefault.cnf.xml eller cnf.xml svarende til telefonenhedens navn | Navn på konfigurationsfilen. | Ingen. Denne meddelelse angiver navnet på konfigurationsfilen. |

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Vis vinduet Netværksstatistik

Fremgangsmåde

- Trin 1** Tryk på **Indstillinger > Status > Netværksstatistik**.
- Trin 2** Afslut menuen ved at trykke på **Afslut**.

Felter til netværksstatistik

Følgende tabel beskriver oplysningerne på skærmen Netværksstatistik.

Tablet 23: Felter til netværksstatistik

| Element | Beskrivelse |
|-------------------------|---|
| Tx Frames | Antal pakker, som telefonen har sendt |
| Tx broadcast | Antal udsendelsespakker, som telefonen har sendt |
| Tx unicast | Det samlede antal unicast-pakker, som telefonen har sendt. |
| Rx Frames | Antal pakker, som telefonen har modtaget |
| Rx broadcast | Antal udsendelsespakker, som telefonen har modtaget |
| Rx unicast | Det samlede antal unicast-pakker, som telefonen har modtaget. |
| CDP Neighbor Device ID | Id'et for en enhed, der er forbundet til denne port, som CDP-protokollen har registreret. |
| CDP Neighbor IP Address | Id'et for en enhed, der er forbundet til denne port, som CDP-protokollen har registreret ved hjælp af IP. |
| CDP Neighbor Port | Id'et for en enhed, der er forbundet til denne port, som CDP-protokollen har registreret. |

| Element | Beskrivelse |
|---|--|
| <p>Årsag til genstart: en af disse værdier:</p> <ul style="list-style-type: none"> • Nulstilling af hardware (nulstilling ved tænding) • Nulstilling af software (hukommelsescontroller nulstilles også) • Nulstilling af software (hukommelsescontroller nulstilles ikke) • Nulstilling af Watchdog • Initialiseret • Ukendt | Årsag til den seneste nulstilling af telefonen |
| Port 1 | Netværksportens forbindelsestilstand og forbindelse (100 Full betyder f.eks., at pc-porten er i forbindelsestilstanden og automatisk har forhandlet en 100 Mbps forbindelse med fuld dupleks) |
| IPv4 | <p>Oplysninger om DHCP-statussen. Dette omfatter følgende tilstande:</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>Oplysninger om DHCP-statussen. Dette omfatter følgende tilstande:</p> <ul style="list-style-type: none"> • CDP INIT • DHCP6 BOUND • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DISABLED DUPLICATE IPV6 • DHCP6 DECLINED DUPLICATE IP • ROUTER ADVERTISE • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT CANNOT RESTORE • IPV6 STACK TURNED OFF • ROUTER ADVERTISE • ROUTER ADVERTISE • UNRECOGNIZED MANAGED BY • ILLEGAL IPV6 STATE |

Vis vinduet Opkaldsstatistik

Fremgangsmåde

Trin 1 Tryk på **Indstillinger > Status > Opkaldsstatistik**.

Trin 2 Afslut menuen ved at trykke på **Afslut**,

Felter til opkaldsstatistik

Følgende tabel beskriver elementerne på skærmen Opkaldsstatistik.

Tabel 24: Elementer i opkaldsstatistik

| Element | Beskrivelse |
|--------------------|---|
| Modtager-codec | Type af modtaget talestream (RTP-streaminglyd fra codec): <ul style="list-style-type: none"> • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS |
| Afsender Codec | Type af sendt talestream (RTP-streaminglyd fra codec): <ul style="list-style-type: none"> • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS |
| Modtagerstørrelse | Størrelse af talepakker, i millisekunder, i den modtagne talestream (RTP-streaminglyd). |
| Afsender størrelse | Størrelse af talepakker, i millisekunder, i den afsendte talestream (RTP-streaminglyd). |

| Element | Beskrivelse |
|---------------------------------|---|
| Modtager pakker | <p>Antal RTP-talepakker, der er modtaget, siden talestreamen blev åbnet.</p> <p>Bemærk Dette antal er ikke nødvendigvis identisk med det antal RTP-talepakker, der var modtaget, da opkaldet gik i gang, fordi opkaldet kan være sat i venteposition.</p> |
| Afsender pakker | <p>Antal RTP-talepakker, der er sendt, siden talestreamen blev åbnet.</p> <p>Bemærk Dette antal er ikke nødvendigvis identisk med det antal RTP-talepakker, der er blevet sendt, da opkaldet gik i gang, fordi opkaldet kan være sat i venteposition.</p> |
| Gns. forvrængning | Den estimerede gennemsnitlige RTP-pakkeforvrængning (dynamisk forsinkelse, som en pakke udsættes for, når den bevæger sig gennem netværket), i millisekunder, som blev observeret fra åbningen af den modtagne talestream. |
| Maks. forvrængning | Maksimumforvrængning, i millisekunder, der blev observeret fra åbningen af den modtagne talestream. |
| Modtager kasseret | <p>Det antal RTP-pakker i den modtagne talestream, der blev kasseret (forkerte pakker, forsinkede osv.).</p> <p>Bemærk Telefonen kasserer nyttelast med komfortstøj af datatype 19, som Cisco-gateways genererer, fordi de øger værdien af denne tæller.</p> |
| Modtager tabte pakker | Manglende RTP-pakker (mistet undervejs). |
| Måletal for talekvalitet | |
| Kumulativ Conceal ratio | Samlet antal af skjulningsframes delt med det samlede antal taleframes, der blev modtaget fra starten af talestreamen. |
| Interval for Conceal ratio | Antal skjulningsframes i forhold til taleframes i det foregående 3-sekunders interval af aktiv tale. Hvis der bruges VAD (voice activity detection), kræves der muligvis et længere interval til at akkumulere 3 sekunder med aktiv tale. |
| Maks Conceal Ratio | Højeste interval af skjulningsrate fra starten af talestreamen. |
| Conceal sek. | Antal sekunder, der har skjulningshændelser (mistede frames) fra starten af talestrømmen (inkluderer stærkt skjulningssekunder). |
| Severely Conceal sek. | Antal sekunder, der har mere end 5 procent skjulningshændelser (tabte frames) fra starten af talestrømmen. |
| Latenstid | Estimat af netværksforsinkelsen udtrykt i millisekunder. Repræsenterer et kørende gennemsnit af forsinkelsen for rundtur, der måles, når RTCP-modtagerrapportblokke modtages. |

Cisco IP-telefon-webside

Alle Cisco IP-telefon har en webside, hvor du kan se en række forskellige oplysninger om telefonen, herunder:

- Enhedsoplysninger: Viser enhedens indstillinger og relaterede oplysninger for telefonen.
- Netværksopsætning: viser oplysninger om netværksopsætning og oplysninger om andre telefonindstillinger.
- Netværksstatistikker: Viser hyperlinks, der angiver oplysninger om netværkstrafik.
- Enhedslogfiler: Viser hyperlinks, der angiver oplysninger, du kan bruge til fejlfinding.
- Streamingstatistikker: Viser hyperlinks til en række forskellige streamingstatistikker.

Dette afsnit beskriver de oplysninger, du kan få fra telefonens webside. Du kan bruge disse oplysninger til at fjernovervåge betjeningen af en telefon og til at hjælpe med fejlfinding.

Du kan også få mange af disse oplysninger direkte fra en telefon.

Gå til telefonens webside



Bemærk Hvis du ikke kan få adgang til websiden, er den muligvis deaktiveret som standard.

Fremgangsmåde

-
- Trin 1** Få IP-adressen til Cisco IP-telefon ved hjælp af en af disse metoder:
- a) Søg efter telefonen i Cisco Unified Communications Manager Administration ved at vælge **Enhed > Telefon**. Telefoner, der er registreret med Cisco Unified Communications Manager, viser IP-adressen i vinduet Søg efter og vis telefoner øverst i vinduet Telefonkonfiguration.
 - b) Gå til telefonen, tryk på **Indstillinger > Systemoplysninger**, og rul derefter til feltet IPv4-adresse.
- Trin 2** Åbn en webbrowser, og angiv følgende URL-adresse, hvor *IP_adresse* er IP-adressen til Cisco IP-telefon:
- http://<IP_adresse>**
-

Webside med enhedsoplysninger

Området Enhedsoplysninger på en telefons webside viser enhedsindstillinger og relaterede oplysninger for telefonen. Følgende tabel beskriver disse elementer.

For at få vist området Enhedsoplysninger skal du åbne websiden til telefonen og derefter klikke på linket **Enhedsoplysninger**.

Tabel 25: Felter på webside med enhedsoplysninger

| Felt | Beskrivelse |
|------------------------|---|
| Tjenestetilstand | Telefonens tjenestemodel. |
| Tjenestens domæne | Tjenestens domæne. |
| Tjenestetilstand | Tjenestens aktuelle tilstand. |
| MAC-adresse | Telefonens MAC-adresse. |
| Værtsnavn | Entydigt, fast navn, der automatisk tildeles til telefonen baseret på MAC-adressen. |
| Telefon DN | Telefonnummer, der er tildelt telefonen. |
| App-Loader ID | Identificerer programmets indlæsningsversion. |
| Start indlæsning af ID | Identificerer version af startindlæsningen. |
| Version | Identikator af telefonens firmware. |
| Hardware revision | Mindre revisionsværdi af telefonens hardware. |
| Serienummer | Telefonens entydige serienummer. |
| Modelnummer | Telefonens modelnummer. |
| Meddelelse venter | Indikerer, om en talemeddelelse venter på den primære linje for denne telefon. |
| UDI | Viser følgende Cisco UDI-oplysninger (Unique Device Identifier) om telefonen: <ul style="list-style-type: none"> • Hardwaretype • Telefonens modelnavn • Produkt-id • Versions-id (VID) – angiver det større hardwareversionsnummer. • Serienummer |
| Tid | Tidspunkt for den Dato-/klokkeslætsgruppe, som telefonen tilhører. Disse oplysninger kommer fra Cisco Unified Communications Manager. |
| Tidszone | Tidszone for den Dato-/klokkeslætsgruppe, som telefonen tilhører. Disse oplysninger kommer fra Cisco Unified Communications Manager. |
| Dato | Dato for den dato-/klokkeslætsgruppe, som telefonen tilhører. Disse oplysninger kommer fra Cisco Unified Communications Manager. |
| System Free Memory | Mængde af tilgængelig systemhukommelse. |
| Java Heap Free Memory | Mængde af ledig hukommelse til Java-heapen. |
| Java Pool Free Memory | Mængde af ledig hukommelse til Java-puljen. |

| Felt | Beskrivelse |
|-------------------------|---|
| FIPS-tilstand aktiveret | Indikerer, om FIPS-tilstanden (Federal Information processing Standard) er aktiveret. |

Webside med netværksopsætning

Området Netværksopsætning på en telefonwebseite viser oplysninger om netværksopsætningen og oplysninger om andre telefonindstillinger. Følgende tabel beskriver disse elementer.

Du kan få vist og indstille mange af disse elementer i menuen Netværksopsætning på Cisco IP-telefon.

For at få vist området Netværksopsætning skal du gå til telefonens webseite og derefter klikke på hyperlinket **Netværksopsætning**.

Tabel 26: Elementer i området Netværksopsætning

| Element | Beskrivelse |
|-----------------------|---|
| MAC-adresse | Telefonens MAC-adresse. |
| Værtsnavn | Værtsnavn, som DHCP-serveren har tildelt telefonen. |
| Domænenavn | Navnet på DNS-domænet (Domain Name System), som telefonen er i. |
| DHCP-server | IP-adressen for DHCP-serveren (Dynamic Host Configuration Protocol), hvorfra telefonen IP-adressen. |
| BOOTP-server: | Angiver, om telefonen får konfigurationen fra en BootP-server (Bootstrap Protocol). |
| DHCP | Angiver, om telefonen bruger DHCP. |
| IP-adresse | Telefonens IP-adresse (internetprotokol). |
| Undernetmaske | Den undernetmaske, telefonen bruger. |
| Standardrouter 1 | Anvendt standardrouter, som telefonen bruger. |
| DNS-server 1-3 | Primær DNS-server (Domain Name System) (DNS-server 1) og valgfrie ekstra DNS-servere (DNS-server 2 og 3), som telefonen bruger. |
| Alternativ TFTP | Angiver, om telefonen bruger en alternativ TFTP-server. |
| TFTP-server 1 | Anvendt primær TFTP-server (Trivial File Transfer Protocol), som telefonen bruger. |
| TFTP-server 2 | Ekstra TFTP-server (Trivial File Transfer Protocol), som telefonen bruger. |
| DHCP-Adresse Frigivet | Angiver indstillingen af valgmuligheden DHCP-adresse frigivet. |
| Operationel VLAN-id | Et VLAN (Virtual Local Area Network) i brug, der er konfigureret på en Cisco Catalyst-switch, som telefonen er medlem af. |
| Admin VLAN-id | Ekstra VLAN, som telefonen er medlem af. |

| Element | Beskrivelse |
|------------------|--|
| Unified CM 1-5 | <p>Værtsnavne eller IP-adresser i prioriteret rækkefølgen for Cisco Unified Communications Manager-servere, som telefonen kan registreres med. Et element kan også vise IP-adressen for en SRST-router, der kan give en begrænset Cisco Unified Communications Manager-funktionalitet, hvis sådan router er tilgængelig.</p> <p>Når det gælder en tilgængelig server, viser Cisco Unified Communications Manager-serveren følgende tilstande:</p> <ul style="list-style-type: none"> • Aktiv: Cisco Unified Communications Manager-serveren, hvorfra telefonen i øjeblikket henter services, der behandler opkald • Standby: Cisco Unified Communications Manager-serveren, som telefonen skifter til, hvis den aktuelle server bliver tilgængelig • Tom: Hvis der ikke er en aktuell forbindelse til denne Cisco Unified Communications Manager-server <p>Et element kan også omfatte SRST-angivelsen (Survivable Remote Site Telephony), der refererer til en SRST-router, der har Cisco Unified Communications Manager-funktionalitet med et begrænset funktionssæt. Denne router overtager kontrollen med behandlingen af opkald, hvis alle Cisco Unified Communications Manager-servere ikke er tilgængelige. SRST Cisco Unified Communications Manager vises altid sidst på listen over servere, også selvom den er aktiv. Du kan konfigurere SRST-routeradressen i afsnittet Enhedspulje i vinduet Cisco Unified Communications Manager Configuration.</p> |
| Information URL | URL-adressen til den hjælpe tekst, der vises på telefonen. |
| Telefonbøger URL | URL-adressen til den server, som telefonen henter telefonbogsoplysninger fra. |
| Meddelelser URL | URL-adressen til den server, som telefonen henter meddelelsservices fra. |
| Tjenester URL | URL-adressen til den server, som telefonen henter Cisco IP-telefon-tjenester fra. |
| Inaktiv URL | Den URL-adresse, som telefonen viser, når telefonen er inaktiv, i det tidsrum, som feltet Inaktiv URL tid angiver, og ingen menu er åbnet. |
| Inaktiv URL tid | Det antal sekunder, telefonen er inaktiv, og ingen menu er åben, før den XML-service, som er angivet i URL-adresse angiver, aktiveres. |
| Proxy-server URL | URL-adresse til proxyserver, der foretager HTTP-anmodninger til ikke-lokale værtsadresser af telefonens HTTP-klient og giver svar fra den ikke-lokale vært til telefonens HTTP-klient. |
| Godkendelses-URL | Den URL-adresse, som telefonen bruger til at validere anmodninger, der foretages til telefonens webserver. |
| SW-portopsætning | <p>Switchportens hastighed og dupleks, hvor:</p> <ul style="list-style-type: none"> • A = Automatisk forhandling • 10H = 10-BaseT/halv dupleks • 10F = 10-BaseT/fuld dupleks • 100H = 100-BaseT/halv dupleks • 100F = 100-BaseT/fuld dupleks • 1000F = 1000-BaseT/fuld dupleks • Intet link = Ingen forbindelse til switchporten |

| Element | Beskrivelse |
|--------------------------------|--|
| Brugersprog | Brugerlandestandard, der er knyttet til telefonens bruger. Identificerer et sæt detaljerede oplysninger for at understøtte brugere, herunder sprog, skrifttype, format af dato og klokkeslæt og oplysninger om alfanumerisk tekst på tastatur. |
| Netværksbrugersprog | Netværkslandestandard, der er knyttet til telefonens bruger. Identificerer et sæt detaljerede oplysninger for at understøtte telefonen på et bestemt sted, herunder definitionerne af tonerne og den kadence telefonen bruger. |
| Lokal brugerversion | Version af den brugerlandestandard, som er indlæst på telefonen. |
| Lokal netværksversion | Version af den netværkslandestandard, som er indlæst på telefonen. |
| Højtaler aktiveret | Angiver, om højttalertelefonen aktiveret på telefonen. |
| Medlyt | Angiver, om gruppefunktioner er aktiveret på telefonen. Gruppelisten gør det muligt at få hjælp af håndsættet og lytte til højttaleren samtidigt. |
| GARP aktiveret | Angiver, om telefonen får MAC-adresser fra Gratuitous ARP-svar. |
| Automatisk linjevalg aktiveret | Angiver, om telefonen skifter opkaldsfokusset for indgående opkald på alle linjer. |
| DSCP til opkaldskontrol | DSCP IP-klassificering til styring af opkaldssignaler. |
| DSCP til konfiguration | DSCP IP-klassificering for enhver overførsel af telefonkonfigurationer. |
| DSCP til tjenester | DSCP IP-klassificering for telefonbaserede services. |
| Sikkerhedstilstand | Sikkerhedstilstand, der er indstillet for telefonen. |
| Web-adgang aktiveret | Angiver, om webadgang er aktiveret (Ja) eller deaktiveret (Nej) for telefonen. |
| Web-adgang aktiveret | Angiver, om telefonen accepterer eller blokerer SSH-forbindelserne. |
| CDP: SW-port | Angiver, om der er CDP-understøttelse til switchporten (standard er aktiveret). Aktiver CDP på switchporten for VLAN-tildeling for telefonen, strømforhandlingen, QoS-tilstand og 802.1x-sikkerheden. Aktiver CDP på switchporten, når telefonen opretter forbindelse til en Cisco-switch. Når CDP er deaktiveret i Cisco Unified Communications Manager, vises en advarsel, der angiver, at CDP kun skal deaktiveres på switchporten, hvis telefonen opretter forbindelse til en switch, der er fra Cisco. De aktuelle CDP-værdier for pc og switchport vises i menuen Indstillinger. |
| LLDP-MED: SW-port | Angiver om LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) er aktiveret på switchporten. |

| Element | Beskrivelse |
|---|--|
| LLDP Power Priority | Meddeler telefonstrømsprioritet til switchen, der gør det muligt for switchen at levere den til telefonerne. Indstillinger omfatter: <ul style="list-style-type: none"> • Ukendt: Dette er standardværdien. • Lav • Ofte • Kritisk |
| LLDP-aktiv-ID | Identificerer det aktiv-ID, der er knyttet til telefonen i forbindelse med lagerstyring. |
| CTL-fil | Identificerer CTL-filen. |
| ITL-fil | ITL-filen indeholder den første tillidsliste. |
| CTL-signatur | Øger sikkerheden ved at bruge SHA-1 (secure hash algorithm) i CTL- og ITL-filerne. |
| CAPF-server | Navnet på den CAPF-server, telefonen bruger. |
| TVS | Hoveddelen i Security by Default (Sikkerhed som standard). TVS (Trust Verification Service) giver Cisco Unified IP-telefon mulighed for at godkende programservere som f.eks. EM-service og MIDlet ved hjælp af HTTPS-oprettelse. |
| TFTP-server | Navnet på den TFTP-server, telefonen bruger. |
| Automatisk synkronisering af port | Synkroniserer portene til den laveste hastighed, som forhindrer pakketab. |
| Ekstern konfiguration af switch-port | Giver administratoren mulighed for at konfigurere hastigheden og funktionen af Cisco Discovery Protocol (CDP) Collaboration Experience-porten eksternt ved hjælp af Cisco Unified Communications Manager Administration. |
| Ekstern konfiguration af pc-port | Angiver, om en ekstern portkonfiguration af hastighed og duplekstilstand for pc-porten er aktiveret eller deaktiveret. |
| IP-adresseringstilstand | Viser, at IP-adressetilstanden er tilgængelig på telefonen. |
| IP-præferencestyling | Angiver den version af IP-adressen, som telefon bruger under signalering med Cisco Unified Communications Manager, når både IPv4 og IPv6 er tilgængelige på telefonen. |
| IP-præferencetilstand for medie | Angiver, at enheden i forhold til medie bruger en IPv4-adresse til at oprette forbindelse til Cisco Unified Communications Manager. |
| Automatisk IPv6-konfig. | Viser, om den automatiske konfiguration er aktiveret eller deaktiveret på telefonen. |
| IPv6 DAD | Viser, hvor unikke de nye IPv6-adresser for unicast er, før adresserne tildeles til grænsefladen. |
| IPv6 Accepter omdirigeringsmeddelelser | Angiver, om telefonen accepterer omdirigeringsmeddelelser fra den samme router, der bruger det samme modtagernummeret. |
| IPv6 Besvar anmodning om Multicast Echo | Angiver, at telefonen sender en Echo Reply-meddelelse som svar på en Echo Request-meddelelse, der er sendt til en IPv6-adresse. |

| Element | Beskrivelse |
|------------------------|---|
| IPv6-belastningsserver | Bruges til at optimere installationstiden for telefonens opgraderinger og aflaste WAN'et ved at afbildninger lokalt og forhandle behovet for at krydse WAN-linket ved telefonopgradering. |
| IPv6-log server | Angiver IP-adressen og porten for den eksterne logføringsmaskine, som telefonen sender logme til. |
| IPv6 CAPF-server | Fælles navn (fra Cisco Unified Communications Manager-certifikat) for den CAPF, telefon b |
| DHCPv6 | DHCP (Dynamic Host Configuration Protocol) tildeler automatisk IPv6-adresser til enheder, forbinder dem til netværket. Cisco Unified IP-telefoner aktiverer DHCP som standard. |
| IPv6-adresse | Viser telefonens aktuelle IPv6-adresse eller giver brugeren mulighed for at angive en ny IPv6 |
| IPv6-præfiks længde | Viser den aktuelle præfikslængde for undernettet eller tillader, at brugeren kan angive en ny præfikslængde. |
| IPv6 standardrouter 1 | Viser den standardrouter, telefonen bruger, eller giver brugeren mulighed for at angive en ny IPv6-standardrouter. |
| IPv6 DNS-server 1 | Viser den primære DNSv6-server, telefonen bruger, eller giver brugeren mulighed for at ang server. |
| IPv6 DNS-server 2 | Viser den sekundære DNSv6-server, telefonen bruger, eller giver brugeren mulighed for at an ny sekundær DNSv6-server. |
| IPv6 alternativ TFTP | Giver brugeren mulighed for at aktivere brugen af en alternativ (sekundær) IPv6 TFTP-server |
| IPv6 TFTP-server 1 | Viser den primære IPv6 TFTP-server, telefonen bruger, eller giver brugeren mulighed for at a ny primær TFTP-server. |
| IPv6 TFTP-server 2 | Viser den sekundære IPv6 TFTP-server, der bruges, hvis den primære IPv6 TFTP-server ikke tilgængelig, eller giver brugeren mulighed for at angive en ny sekundær TFTP-server. |
| IPv6-adresse frigivet | Giver brugeren for at frigive IPv6-relaterede oplysninger. |
| EnergyWise-strømniveau | Et mål for den energi, der bruges af enheder i et EnergyWise-netværk. |
| EnergyWise-domæne | En administrativ gruppering af enheder, der har til formålet at overvåge og styre strømmen. |

Webside med Ethernet-oplysninger

Følgende tabel beskriver indeholdet på websiden med Ethernet-oplysninger.

Tabel 27: Oplysningslementer om Ethernet

| Element | Beskrivelse |
|--------------|--|
| Tx Frames | Det samlede antal pakker, som telefonen sender. |
| Tx broadcast | Det samlede antal udsendelsespakker, som telefonen sender. |
| Tx multicast | Det samlede antal multicast-pakker, som telefonen sender. |

| Element | Beskrivelse |
|----------------|--|
| Tx unicast | Det samlede antal unicast-pakker, som telefonen sender. |
| Rx Frames | Det samlede antal pakker, som telefonen har modtaget. |
| Rx broadcast | Det samlede antal udsendelsespakker, som telefonen modtager. |
| Rx multicast | Det samlede antal multicast-pakker, som telefonen modtager. |
| Rx unicast | Det samlede antal unicast-pakker, som telefonen modtager. |
| Rx PacketNoDes | Det samlede antal kasserede pakker, som mangel på DMA-beskrivelse (Direct Memory Access) medfører. |

Websider med netværk

Følgende tabel beskriver oplysningerne på websiderne for netværksområdet.



Bemærk Når du klikker på linket **Netværk** under Netværksstatistik, hedder siden "Portoplysninger".

Tablet 28: Elementer i netværksområde

| Element | Beskrivelse |
|---------------------------|--|
| Rx totalPkt | Det samlede antal pakker, som telefonen har modtaget. |
| Rx multicast | Det samlede antal multicast-pakker, som telefonen har modtaget. |
| Rx broadcast | Det samlede antal udsendelsespakker, som telefonen har modtaget. |
| Rx unicast | Det samlede antal unicast-pakker, som telefonen har modtaget. |
| Rx tokenDrop | Det samlede antal pakker, der blev kasseret på grund af manglende ressourcer (f.eks. FIFO-overløb). |
| Tx totalGoodPkt | Det samlede pakker uden fejl (multicast, udsendelse og unicast), som telefonen har modtaget. |
| Tx broadcast | Det samlede antal udsendelsespakker, som telefonen har sendt. |
| Tx multicast | Det samlede antal multicast-pakker, som telefonen har sendt. |
| LLDP FramesOutTotal | Det samlede antal LLDP-frames, som telefonen har sendt. |
| LLDP AgeoutsTotal | Det samlede antal LLDP-frames, som har haft timeout i cachen. |
| LLDP FramesDiscardedTotal | Det samlede antal LLDP-frames, der blev kasseret, når en af de obligatoriske TLV'er mangler, ikke virker eller har en strenglængde, der ligger uden for intervallet. |

| Element | Beskrivelse |
|----------------------------|---|
| LLDP FramesInErrorsTotal | Det samlede antal LLDP-frames, der blev modtaget med en eller flere registrerbare fejl. |
| LLDP FramesInTotal | Det samlede antal LLDP-frames, som telefonen modtager. |
| LLDP TLVDiscardedTotal | Det samlede antal LLDP-TLV'er, der er kasseret. |
| LLDP TLVUnrecognizedTotal | Det samlede antal LLDP-TLV'er, der ikke genkendes på telefonen. |
| CDP Neighbor Device ID | Id'et for en enhed, der er forbundet til denne port, som CDP har registreret. |
| CDP Neighbor IP Address | IP-adresse på den registrerede naboenhed, som CDP har registreret. |
| CDP Neighbor IPv6 Address | IPv6-adresse på den registrerede naboenhed, som CDP har registreret. |
| CDP Neighbor Port | Naboenhedsport, som telefonen er tilsluttet, som CDP har registreret. |
| LLDP Neighbor Device ID | Id'et for en enhed, der er forbundet til denne port, som LLDP har registreret. |
| LLDP Neighbor IP Address | IP-adresse på den naboenhed, som LLDP har registreret. |
| LLDP Neighbor IPv6 Address | IPv6-adresse på den naboenhed, som CDP har registreret. |
| LLDP Neighbor Port | Naboenhedsport, som telefonen er tilsluttet, og som LLDP har registreret. |
| Portinformation | Oplysninger om hastighed og duplex. |

Websider til konsollogfiler, kernedumps, statusmeddelelser og visning af fejl

Under overskriften Enhedslogs giver links til konsollogfiler, kernedumps, statusmeddelelser og fejlfindingsvisninger, der gør det muligt at overvåge og foretage fejlfinding på telefonen.

- Konsollogfiler – omfatter hyperlinks til individuelle logfiler. Konsollogfilerne omfatter fejlfindings- og fejlmeddelelser, som telefonen modtager.
- Kernedumps – omfatter hyperlinks til individuelle dumpfiler. Kernedumpfilerne omfatter data fra et telefonnedbrud.
- Statusmeddelelser – viser de 10 seneste statusmeddelelser, som telefonen har oprettet, siden den sidst blev tændt. Du kan også få disse oplysninger på skærmen Statusmeddelelser på telefonen.
- Fejlfindingsvisning – viser fejlfindingsmeddelelser, der kan være nyttige for Cisco TAC, hvis du har brug for hjælp til fejlfinding.

Webside med streamingstatistik

En Cisco IP-telefon kan streame oplysninger til og fra op til fem enheder samtidigt. En telefon streamer oplysninger, når den er på et opkald eller kører en tjeneste, der sender eller modtager lyd eller data.

Områderne med streamingstatistik på en telefonwebside giver oplysninger om streamsene.

For at få vist et område med streamingstatistik skal du åbne websiden til telefonen og derefter klikke på et **streamlink**.

Følgende tabel beskriver elementerne i områderne med streamingstatistik.

Table 29: Felter til streamingstatistik

| Element | Beskrivelse |
|--|---|
| Ekstern adresse | Streamdestinationens IP-adresse og UDP-port. |
| Lokaladresse | Telefonens IP-adresse og UPD-port. |
| Starttid | Det interne tidsstempel angiver, hvornår Cisco Unified Communications Manager a om, at telefonen skal starte pakkeoverførsel. |
| Streamstatus | Indikation af, om streaming er aktiv eller ej. |
| Værtsnavn | Entydigt, fast navn, der automatisk tildeles til telefonen baseret på MAC-adressen. |
| Afsender pakker | Samlet antal RTP-datapakker, som telefonen overførte, siden den startede denne for Værdien er 0, hvis forbindelsen er indstillet til kun at modtage. |
| Afsender oktetter | Samlet antal dataoktetter, som telefonen overførte i RTP-datapakker, siden den start forbindelse. Værdien er 0, hvis forbindelsen er indstillet til kun at modtage. |
| Afsender Codec | Type af lydkodning, som er til den overførte stream. |
| Afsenderrapporter afsendt (se note) | Antallet af gange, som RTCP-afsenderrapport er blevet sendt. |
| Afsenderrapport afsend.tidspkt (se note) | Internt tidsstempel, der angiver, hvornår den seneste RTCP-afsenderrapport blev se |
| Modtager tabte pakker | Samlet antal RTP-datapakker, som gik tabt, siden datamodtagelsen startede på denne f Defineret som antallet af forventede pakker minus antallet af pakker, der faktisk mo hvor antallet af modtagne pakker omfatter alle, der er forsinkede eller dubletter. Væ 0, hvis forbindelsen var indstillet til kun at sende. |
| Gns. forvrængning | Estimat af middelfvigelse af mellem RTP-datapakkeankomster pr. millisekund. Væ 0, hvis forbindelsen var indstillet til kun at sende. |
| Modtager-codec | Type af lydkodning, som bruges til den modtagne stream. |
| Modtagerrapporter afsendt (se note) | Antallet af gange, som RTCP-modtagerrapporter er blevet sendt. |
| Modtagerrapport afsend.tidspkt. (se note) | Internt tidsstempel, der angiver, hvornår en RTCP-modtagerrapport blev sendt. |
| Modtager pakker | Samlet antal RTP-datapakker, som telefonen har modtaget, siden datamodtagelsen s denne forbindelse. Indeholder pakker, der blev modtaget fra forskellige kilder, hvis d er et multicast-opkald. Værdien viser 0, hvis forbindelsen var indstillet til kun at se |

| Element | Beskrivelse |
|---|---|
| Modtager oktetter | Samlet antal dataoktetter, som enheden modtog i RTP-datapakker, siden modtagelsen startede på forbindelsen. Indeholder pakker, der blev modtaget fra forskellige kilder, hvis dette er et multicast-opkald. Værdien viser 0, hvis forbindelsen var indstillet til kun at sende. |
| Kumulativ Conceal ratio | Samlet antal af skjulningsframes delt med det samlede antal taleframes, der blev modtaget fra starten af talestrømmen. |
| Interval for Conceal ratio | Antal skjulningsframes i forhold til taleframes i det foregående 3-sekunders interval af tale. Hvis VAD (voice activity detection) er i brug, kræves der muligvis et længere interval for at akkumulere tre sekunder af aktiv tale. |
| Maks Conceal Ratio | Højeste interval af skjulningsforhold fra starten af talestrømmen. |
| Conceal sek. | Antal sekunder, der har skjulningshændelser (mistede frames) fra starten af talestrømmen (inkluderer stærkt skjulningssekunder). |
| Severely Conceal sek. | Antal sekunder, der har mere end fem procent skjulningshændelser (mistede frames) fra starten af talestrømmen. |
| Latenstid (se note) | Estimat af netværksforsinkelsen udtrykt i millisekunder. Repræsenterer et kørende gennemsnit af forsinkelsen for rundtur, der måles, når RTCP-modtagerrapportblokke modtages. |
| Maks. forvrængning | Maksimal værdi af øjeblikkelig forvrængning i millisekunder. |
| Afsender størrelse | RTP-pakkestørrelse i millisekunder for den overførte stream. |
| Afsenderrapporter modtaget (se note) | Antal gange, som RTCP-afsenderrapporter er blevet modtaget. |
| Afsenderrapport modtage.tidspkt (se note) | Seneste tidspunkt, hvor en RTCP-afsenderrapport blev modtaget. |
| Modtagerstørrelse | RTP-pakkestørrelse i millisekunder for den modtagne stream. |
| Modtager kasseret | RTP-pakker, der blev modtaget fra netværket, men som blev fjernet fra forvrængningsbufferen. |
| Modtagerrapporter modtaget (se note) | Antal gange, som RTCP-modtagerrapporter er blevet modtaget. |
| Modtagerrapport modtage.tidspkt. (se note) | Seneste tidspunkt, hvor en RTCP-modtagerrapport blev modtaget. |



Bemærk Når RTP-kontrolprotokol er deaktiveret, genereres der ingen data for dette felt, og derfor vises den som 0.

Anmod om oplysninger fra telefonen i XML

Ved fejlfinding kan du anmode om oplysninger fra telefonen. De oplysninger, du får, er i XML-format. Følgende oplysninger er tilgængelige:

- CallInfo er oplysninger om opkaldssession for en bestemt linje.
- LineInfo er oplysninger om linjekonfiguration for telefonen.
- ModeInfo er oplysninger om telefontilstand.

Inden du begynder

Webadgang skal være aktiveret for at få oplysningerne.

Telefonen skal være knyttet til en bruger.

Fremgangsmåde

Trin 1 Få opkaldsoplysninger ved at angive følgende URL-adresse i en browser: **http://<phone ip address>/CGI/Java/CallInfo<x>**

hvor

- *<phone ip address>* er telefonens IP-adresse
- *<x>* er det linjenummer, du får oplysninger om.

Kommandoen returnerer et XML-dokument.

Trin 2 Få linjeoplysninger ved at angive følgende URL-adresse i en browser: **http://<phone ip address>/CGI/Java/LineInfo**

hvor

- *<phone ip address>* er telefonens IP-adresse

Kommandoen returnerer et XML-dokument.

Trin 3 Få modeloplysninger ved at angive følgende URL-adresse i en browser: **http://<phone ip address>/CGI/Java/ModeInfo**

hvor

- *<phone ip address>* er telefonens IP-adresse

Kommandoen returnerer et XML-dokument.

Eksempel på CallInfo-output

Følgende XML-kode er et eksempel på output 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>

```

Eksempel på LineInfo-output

Følgende XML-kode er et eksempel på output 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>
```

Eksempel på ModelInfo-output

Følgende XML-kode er et eksempel på output 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>
```




KAPITEL 12

Fejlfinding på telefonen

- Generelle fejlfindingsoplysninger, på side 153
- Problemer ved start, på side 154
- Problemer ved nulstilling af problemer, på side 158
- Telefon kan ikke oprette forbindelse til LAN, på side 160
- Sikkerhedsproblemer med Cisco IP-telefon, på side 160
- Lydproblemer, på side 163
- Generelle problemer med telefonopkald, på side 164
- Fejlfindingsprocedurer, på side 164
- Kontrollér fejlfindingsoplysninger fra Cisco Unified Communications Manager, på side 168
- Yderligere fejlfindingsoplysninger, på side 169

Generelle fejlfindingsoplysninger

Følgende tabel indeholder generelle fejlfindingsoplysninger for Cisco IP-telefon.

Tabel 30: Fejlfinding af Cisco IP-telefon

| Resumé | Forklaring |
|---|--|
| Længere udsendelsesstørrelse får IP-telefoner til at nulstille eller til ikke at kunne foretage eller besvare et opkald | En forlænget udsendelsesstørrelse Lag 2 (der varer flere minutter) på tale- eller tekstkonferencer får IP-telefoner til at nulstilles, miste et aktivt opkald eller til ikke at kunne besvare et opkald. Telefoner vises muligvis ikke, før en udsendelsesstørrelse er afsluttet. |
| Flytning af en netværksforbindelse fra telefonen til en arbejdsstation | Hvis din telefon får strøm via netværksforbindelsen, skal du være forsigtig, når du afbryder telefonens netværksforbindelse og sætter ledningen i en stationær computer. Advarsel Netværkskortet i computeren kan ikke modtage strøm via netværksforbindelsen. Hvis der kommer strøm gennem forbrugsnetværkskortet, skal du trække netværkskortet ud af computeren og sætte det i stationær computer. For at beskytte netværkskortet skal du vente i mindst 10 sekunder eller længere, efter du har trukket telefonledningen ud af computeren. Denne forsinkelse giver switchet tid til at registrere, at der ikke længere er en telefon på linjen, og derefter med at sende strøm gennem ledningen. |

| Resumé | Forklaring |
|--|---|
| Ændring af telefonens konfiguration | <p>Indstillingerne for administratorens adgangskode er som standard låst for at brugere i at foretage ændringer, der kan påvirke deres netværksforbindelse. Låse op for indstillingerne for administratorens adgangskode, før du kan køre dem.</p> <p>Se Anvend en telefonadgangskode, på side 41 for at få yderligere oplysninger.</p> <p>Bemærk Hvis administratorens adgangskode ikke er indstillet i den aktuelle telefonprofil, kan brugeren ændre netværksindstillingerne.</p> |
| Kodeksmismatch mellem telefonen og den anden enhed | <p>Statistikken for RxType og TxType viser det kodeks, der bruges til en samtale mellem denne Cisco IP-telefon og den anden enhed. Værdierne af disse statistikker skal være ens. Hvis ikke, skal du bekræfte, at den anden enhed kan håndtere kodekset eller at der er en transcoder, der kan håndtere tjenesten. Se Vis vinduet Opkaldsstatistik, på side 136 for at få yderligere oplysninger.</p> |
| Lydprøvemismatch mellem telefonen og den anden enhed | <p>Statistikken for RxSize og TxSize viser størrelsen på de talepakker, der bruges til en samtale mellem denne Cisco IP-telefon og den anden enhed. Værdierne af disse statistikker skal være ens. Se Vis vinduet Opkaldsstatistik, på side 136 for at få yderligere oplysninger.</p> |
| Loopback-tilstand | <p>Der kan opstå en loopback-betingelse, når følgende betingelser er opfyldt:</p> <ul style="list-style-type: none"> • Indstillingen SW-portkonfiguration på telefonen er indstillet til 10 Half-Duplex (10-BaseT/half duplex). • Telefonen får strøm fra en ekstern strømforsyning. • Telefonen slukkes (strømforsyningen frakobles). <p>I dette tilfælde deaktiveres switchporten på telefonen, og følgende besked vises i switchens konsollogfil:</p> <pre>HALF_DUX_COLLISION_EXCEED_THRESHOLD</pre> <p>Du kan løse problemet ved at genaktivere porten fra switchen.</p> |

Problemer ved start

Når du har installeret en telefon på dit netværk og føjet den til Cisco Unified Communications Manager, skal telefonen starte, sådan som det er beskrevet i det relaterede emne herunder.

Hvis telefonen ikke starter korrekt, skal du se i følgende afsnit for at finde fejlfindingsoplysninger.

Lignende emner

[Kontrollér start af telefon](#), på side 53

Cisco IP-telefon gennemgår ikke den normale startproces

Problem

Når du tilslutter en Cisco IP-telefon til netværksporten, gennemgår telefonen ikke den normale startproces som beskrevet i det relaterede emne, og telefonskærmen viser ikke oplysninger.

Årsag

Hvis telefonen ikke gennemgår startprocessen, kan det skyldes defekte kabler, dårlige forbindelser, netværksnedbrud, strømmangel, eller telefonen virker muligvis ikke.

Løsning

For at afgøre, om telefonen virker, skal du bruge følgende forslag til at eliminere andre mulige problemer.

- Bekræft, at netværksporten virker:
 - Udskift Ethernet-kablerne med de kabler, som, du ved, virker.
 - Fjern en Cisco IP-telefon, der virker, fra en anden port, og tilslut den til denne netværksport for at bekræfte, at porten er aktiv.
 - Tilslut den Cisco IP-telefon, der ikke starter med en anden netværksport, der er kendt som velfungerende.
 - Tilslut den Cisco IP-telefon, der ikke starter op direkte med porten på switchen, så patchpanelforbindelsen på kontoret elimineres.
- Bekræft, at telefonen får strøm:
 - Hvis du bruger ekstern strøm, skal du bekræfte, at stikkontakten virker.
 - Hvis du bruger integreret strøm, skal du bruge den eksterne strømforsyning i stedet.
 - Hvis du bruger den eksterne strømforsyning, skal du udskifte den med en enhed, som, du ved, virker.
- Hvis telefonen stadig ikke starter korrekt, skal du oplade telefonen med sikkerhedskopien af softwareafbildningen.
- Hvis telefonen stadig ikke starter korrekt, skal du udføre en fabriksnulstilling af telefonen.
- Hvis telefonskærmen på Cisco IP-telefon ikke viser nogen tegn efter mindst 5 minutter, efter du har prøvet disse løsninger, skal du kontakte en teknisk supportmedarbejder fra Cisco for at få yderligere hjælp.

Lignende emner

[Kontrollér start af telefon](#), på side 53

Cisco IP-telefon registreres ikke hos Cisco Unified Communications Manager

Hvis telefonen fortsætter efter den første fase i startprocessen (blink fra LED-knapper tændes og slukkes), men fortsætter med at gå gennem de meddelelser, der vises på telefonskærmen, starter telefonen ikke korrekt. Telefonen kan ikke startes, medmindre den har forbindelse til Ethernet-netværket, og den registreres med en Cisco Unified Communications Manager-server.

Derudover kan problemer med sikkerheden forhindre, at telefonen starter korrekt. Se [Fejlfindingsprocedurer, på side 164](#) for at få flere oplysninger.

Telefon viser fejlmeddelelser

Problem

Statusmeddelelser viser fejl under start.

Løsning

Når telefonen går igennem startprocessen, kan du få adgang til statusmeddelelser, der muligvis kan give dig oplysninger om årsagen til problemet. Se afsnittet om “Vinduet Vis statusmeddelelser” for at få instruktioner i, hvordan du får adgang til statusmeddelelser, og en liste over mulige fejl, forklaringer på dem, og hvordan de kan løses.

Lignende emner

[Vis vinduet Statusmeddelelser](#), på side 128

Telefon kan ikke oprette forbindelse til TFTP-server eller til Cisco Unified Communications Manager

Problem

Hvis netværket er nede mellem telefonen og enten TFTP-serveren eller Cisco Unified Communications Manager, kan telefonen ikke startes korrekt.

Løsning

Sørg for, at netværket kører i øjeblikket.

Telefon kan ikke oprette forbindelse til TFTP-server

Problem

TFTP-serverindstillingerne er muligvis ikke korrekte.

Løsning

Kontrollér TFTP-indstillingerne.

Lignende emner

[Kontrollér TFTP-indstillinger](#), på side 165

Telefon kan ikke oprette forbindelse til server

Problem

IP-adresser og distributionsfelter er muligvis ikke konfigureret korrekt.

Løsning

Du skal kontrollere indstillingerne for IP-adresserne og distribution på telefonen. Hvis du bruger DHCP, skal DHCP-serveren angive disse værdier. Hvis du har tildelt telefonen en statisk IP-adresse, skal du manuelt angive disse værdier.

Lignende emner

[Kontrollér DHCP-indstillinger](#), på side 166

Telefon kan ikke oprette forbindelse via DNS

Problem

DNS-indstillingerne kan være forkerte.

Løsning

Hvis du bruger DNS til at få adgang til TFTP-serveren eller Cisco Unified Communications Manager, skal du sikre dig, at du angiver en DNS-server.

Lignende emner

[Kontrollér DNS-indstillinger](#), på side 167

Cisco Unified Communications Manager og TFTP-tjenester kører ikke

Problem

Hvis Cisco Unified Communications Manager eller TFTP-tjenester ikke kører, kan telefoner muligvis ikke startes korrekt. Hvis det sker, er der sandsynligvis en fejl i hele systemet, og andre telefoner og enheder vil ikke kunne startes korrekt.

Løsning

Hvis Cisco Unified Communications Manager-tjenesten ikke kører, påvirkes alle de enheder, der bruger den til at foretage telefonopkald. Hvis TFTP-tjenesten ikke kører, kan mange enheder ikke startes. Hvis du ønsker yderligere oplysninger, kan du se [Start tjeneste, på side 168](#).

Beskadigelse af konfigurationsfil

Problem

Hvis du fortsat har problemer med en bestemt telefon, som andre forslag i dette afsnit ikke kan løse, kan konfigurationsfilen være beskadiget.

Løsning

Opret en ny telefonkonfigurationsfil.

Lignende emner

[Opret en ny telefonkonfigurationsfil](#), på side 166

Registrering med Cisco Unified Communications Manager

Problem

Telefonen er ikke registreret med Cisco Unified Communications Manager

Løsning

En Cisco IP-telefon kan kun registreres med en Cisco Unified Communications Manager-server, hvis telefonen er føjet til serveren, eller hvis automatisk registrering er aktiveret. Gennemse oplysningerne og procedurerne i [Metoder til tilføjelse af telefoner, på side 60](#) for at sikre, at telefonen er føjet til Cisco Unified Communications Manager-databasen.

Hvis du vil kontrollere, at telefonen er i Cisco Unified Communications Manager-databasen, skal du vælge **Enhed > Telefon** i Cisco Unified Communications Manager Administration. Klik på **Find** for at søge efter telefonen ud fra MAC-adressen. Få oplysninger om, hvordan du bestemmer en MAC-adresse, under [Bestem telefonens MAC-adresse, på side 59](#).

Hvis telefonen allerede er i Cisco Unified Communications Manager-databasen, kan konfigurationsfilen være beskadiget. Se [Beskadigelse af konfigurationsfil, på side 157](#) for at få hjælp.

Cisco IP-telefon kan ikke hente IP-adresse

Problem

Hvis en telefon ikke kan hente en IP-adresse, når den starter, er telefonen muligvis ikke på det samme netværk eller VLAN som DHCP-serveren, eller også kan den switchport, som telefonen forbinder til, være deaktiveret.

Løsning

Sørg for, at det netværk eller VLAN, som telefonen opretter forbindelse til, har adgang til DHCP-serveren, og sørg for, at den switchport er aktiveret.

Problemer ved nulstilling af problemer

Hvis brugerne rapporterer, at deres telefoner bliver nulstillet under opkald, eller når telefonerne er ledige, skal du undersøge årsagen. Hvis netværksforbindelsen og Cisco Unified Communications Manager-forbindelsen er stabil, burde en telefon ikke blive nulstillet.

Når en telefon nulstilles, skyldes det typisk, at den har problemer med at oprette forbindelse til netværket eller Cisco Unified Communications Manager.

Telefon nulstilles pga. periodiske netværksnedbrud

Problem

Dit netværk kan få periodiske nedbrud.

Løsning

Periodiske netværksafbrydelser påvirker data- og taletrafikken på forskellig måde. Dit netværk kan få periodiske nedbrud uden registrering. Hvis det er tilfældet, kan datatrafikken gensende mistede pakker og kontrollere, at pakker modtages og overføres. Taletrafik kan dog ikke gensende mistede pakker. I stedet for at sende en mistet netværksforbindelse igen bliver telefonen nulstillet, og den forsøger at oprette forbindelse til netværket igen. Kontakt systemadministratoren for at få oplysninger om kendte problemer i talenetværket.

Telefon nulstilles pga. fejl i DHCP-indstillinger

Problem

DHCP-indstillingerne kan være forkerte.

Løsning

Bekræft, at du på korrekt vis har konfigureret telefonen til at bruge DHCP. Bekræft, at DHCP-serveren er konfigureret korrekt. Bekræft varigheden af DHCP-lease. Vi anbefaler, at du indstiller lease-varigheden til 8 dage.

Lignende emner

[Kontrollér DHCP-indstillinger](#), på side 166

Telefon nulstilles pga. forkert statisk IP-adresse

Problem

Den statiske IP-adresse, der er tildelt til telefonen, kan være forkert.

Løsning

Hvis telefonen er tildelt en statisk IP-adresse, skal du kontrollere, at du har angivet de rigtige indstillinger.

Telefon nulstilles under kraftig brug af netværket

Problem

Hvis telefonen virker til at blive nulstillet under kraftig brug af netværket, skyldes det sandsynligvis, at du ikke har konfigureret et tale-VLAN.

Løsning

Hvis telefonerne isoleres på et separat VLAN, bliver kvaliteten af taletrafikken bedre.

Telefon nulstilles pga. tilsigtet nulstilling

Problem

Hvis du ikke er den eneste administrator, der har adgang til Cisco Unified Communications Manager, skal du bekræfte, at ingen anden har nulstillet telefonerne med vilje.

Løsning

Du kan kontrollere, om en Cisco IP-telefon har modtaget en kommando fra Cisco Unified Communications Manager om at nulstille ved at trykke på **Indstillinger** på telefonen og vælge **Admin-indstillinger > Status > Netværksstatistik**.

- Hvis feltet Årsag til genstart viser Nulstil–Nulstil, modtager telefonen Nulstil fra Cisco Unified Communications Manager Administration.
- Hvis feltet Årsag til genstart viser Genstart–Genstart, lukkede telefonen, fordi den modtog Nulstil/Genstart fra Cisco Unified Communications Manager Administration.

Telefon nulstilles pga. DNS- eller andre forbindelsesproblemer

Problem

Nulstillingen af telefonen fortsætter, og du har mistanke om problemer med DNS eller andre forbindelsesproblemer.

Løsning

Hvis telefonen bliver ved med at nulstille, skal du eliminere DNS-fejl eller andre forbindelsesfejl ved at følge proceduren i [Bestem DNS- eller forbindelsesproblemer, på side 165](#).

Telefonen tændes ikke

Problem

Telefon virker ikke til at blive tændt.

Løsning

I de fleste tilfælde genstarter telefonen, hvis den får strøm fra en ekstern kilde, men mister den forbindelse og skifter til PoE. En telefon kan ligeledes genstartes, hvis den får strøm ved hjælp af PoE og derefter opretter forbindelse til en ekstern strømforsyning.

Telefon kan ikke oprette forbindelse til LAN

Problem

Den fysiske forbindelse til LAN'et kan være afbrudt.

Løsning

Kontrollér, at den Ethernet-forbindelse, som Cisco IP-telefon opretter forbindelse til, fungerer. Kontrollér f.eks. om den specifikke port eller switch, som telefonen opretter forbindelse til, er nede, og at switchen ikke genstarter. Sørg også for, at der ikke er brud på nogen kabler.

Sikkerhedsproblemer med Cisco IP-telefon

I de følgende afsnit er der fejlfindingsoplysninger for sikkerhedsfunktionerne på Cisco IP-telefon. Få oplysninger om løsningerne på disse problemer og flere fejlfindingsoplysninger om sikkerhed under *Cisco Unified Communications Manager Security Guide*.

Problemer med CTL-fil

Følgende afsnit beskriver fejlfinding af problemer med CTL-filen.

Godkendelsesfejl, telefon kan ikke godkende CTL-fil

Problem

Der er opstået en fejl ved godkendelse af enhed.

Årsag

CTL-filen har ikke et Cisco Unified Communications Manager-certifikat, eller certifikatet er forkert.

Løsning

Installér et korrekt certifikat.

Telefon kan ikke godkende CTL-fil

Problem

Telefon kan ikke godkende CTL-filen.

Årsag

Sikkerhedstokenen, der signerede den opdaterede CTL-fil, findes ikke i CTL-filen på telefonen.

Løsning

Skift sikkerhedstokenen i CTL-filen, og installér den nye fil på telefonen.

CTL-fil godkender, men andre konfigurationsfiler gør ikke

Problem

Telefon kan ikke godkende andre konfigurationsfiler end CTL-filen.

Årsag

Der findes en forkert TFTP-post, eller også er konfigurationsfilen muligvis ikke signeret af det tilhørende certifikat på telefonens tillidsliste.

Løsning

Kontrollér TFTP-posten og certifikatet på tillidslisten.

ITL-fil godkender, men andre konfigurationsfiler gør ikke

Problem

Telefon kan ikke godkende andre konfigurationsfiler end ITL-filen.

Årsag

Konfigurationsfilen er muligvis ikke signeret af det tilhørende certifikat på tillidslisten for telefoner.

Løsning

Signer konfigurationsfilen ved at bruge det rigtige certifikat.

TFTP-autorisationen mislykkedes**Problem**

Telefonen rapporterer fejl ved TFTP-autorisation.

Årsag

TFTP-adressen til telefonen findes ikke i CTL-filen.

Hvis du oprettede en ny CTL-fil med en ny TFTP-post, indeholder den eksisterende CTL-fil muligvis ikke en post til den nye TFTP-server.

Løsning

Kontrollér konfigurationen af TFTP-adressen i telefonens CTL-fil.

Telefonen registreres ikke**Problem**

Telefonen registreres ikke med Cisco Unified Communications Manager.

Årsag

CTL-filen indeholder ikke de korrekte oplysninger for Cisco Unified Communications Manager-serveren.

Løsning

Rediger Cisco Unified Communications Manager-serveroplysningerne i CTL-filen.

Signerede konfigurationsfiler er ikke anmodet**Problem**

Telefon anmoder ikke om signerede konfigurationsfiler.

Årsag

CTL-filen indeholder ikke nogen TFTP-poster med certifikater.

Løsning

Konfigurer TFTP-poster med certifikater i CTL-filen.

Lydproblemer

I følgende afsnit beskrives det, hvordan du løser lydproblemer.

Ingen talesti

Problem

En eller flere personer har ingen lyd under et opkald.

Løsning

Hvis mindst én person i et opkald ikke kan høre lyd, er der ikke IP-forbindelse mellem telefonerne. Kontrollér konfigurationen af routere og switches for at sikre, at IP-forbindelsen er konfigureret korrekt.

Ujævn tale

Problem

En bruger klager over ujævn tale under et opkald.

Årsag

Der kan være et mismatch i forvrængningskonfigurationen.

Løsning

Kontrollér statistikken for AvgJtr og MaxJtr. En stor varians mellem disse statistikker kan indikere et problem med forvrængning på netværket eller periodiske høje niveauer af netværksaktivitet.

En telefon i tilstand med seriel ledningsføring fungerer ikke

Problem

I tilstanden med seriel ledningsføring fungerer en af konferencetelefoner ikke.

Løsning

Kontrollér, om kablerne er tilsluttet Smart Adapter korrekt. De to tykkere kabler tilslutter telefonerne til Smart Adapter. Det tyndere kabel tilslutter Smart Adapter til netadapteren.

Lignende emner

[Tilstand med seriel ledningsføring](#), på side 31

[Installer konferencetelefon i tilstand med seriel ledningsføring](#), på side 38

Generelle problemer med telefonopkald

Følgende afsnit indeholder hjælp til fejlfinding af generelle problemer med telefonopkald.

Telefonopkald kan ikke foretages

Problem

En bruger klager over ikke at kunne foretage et opkald.

Årsag

Telefonen har ikke en DHCP IP-adresse og kan ikke registreres i Cisco Unified Communications Manager. Telefoner med en LCD-skærm viser meddelelsen *Configuring IP* (Konfiguration af IP) eller *Registering* (Registrering). Telefoner uden en LCD-skærm afspiller omorganiseringstonen (i stedet for opkaldstonen) på håndsættet, når brugeren forsøger at foretage et opkald.

Løsning

1. Kontrollér følgende:
 1. Ethernet-kablet er sat i.
 2. Cisco CallManager-tjenesten kører på Cisco Unified Communications Manager-serveren.
 3. Begge telefoner er registreret i samme Cisco Unified Communications Manager.
2. Logfiler til fejlfinding og registrering af lydserver er aktiveret for begge telefoner. Aktivér Java-fejlfinding, hvis det er nødvendigt.

Telefon genkender ikke DTMF-cifre, eller cifre er forsinket

Problem

Brugeren klager over, at tal mangler eller er forsinket, når tastaturet bruges.

Årsag

Hvis du trykker for hurtigt på tasterne, kan det medføre, at tal mangler eller er forsinket.

Løsning

Du må ikke trykke hurtigt ned på tasterne.

Fejlfindingsprocedurer

Disse procedurer kan bruges til at identificere og løse problemer.

Opret en telefonproblemrapport fra Cisco Unified Communications Manager

Du kan generere en problemrapport for telefonerne fra Cisco Unified Communications Manager. Denne handling resulterer i de samme oplysninger, som programtasten PRT (problemrapportværktøjet) genererer på telefonen.

Problemrapporten indeholder oplysninger om telefonen og hovedtelefonerne.

Fremgangsmåde

- Trin 1** Vælg **Enhed > Telefon** i Cisco Unified CM Administration.
 - Trin 2** Klik **Find**, og vælg en eller flere Cisco IP-telefoner.
 - Trin 3** Klik på **Generer PRT for valgte** for at indsamle PRT-logfiler for de hovedtelefoner, der bruges på de valgte Cisco IP-telefoner.
-

Kontrollér TFTP-indstillinger

Fremgangsmåde

- Trin 1** Markér afkrydsningsfeltet TFTP-server 1.

Hvis du har tildelt telefonen en statisk IP-adresse, skal du manuelt angive en indstilling for TFTP-server 1-indstillingsmuligheden.

Hvis du bruger DHCP, får telefonen adressen til TFTP-serveren fra DHCP-serveren. Kontrollér, at IP-adressen er konfigureret i indstilling 150.
 - Trin 2** Du kan også give telefonen mulighed for at bruge en anden TFTP-server. En sådan indstilling er især nyttig, hvis telefonen for nylig er flyttet fra ét sted til et andet.
 - Trin 3** Hvis den lokale DHCP ikke har den rigtige TFTP-adresse, skal du give telefonen mulighed for at bruge en anden TFTP-server.

Dette er ofte nødvendigt, hvis der bruges VPN.
-

Bestem DNS- eller forbindelsesproblemer

Fremgangsmåde

- Trin 1** Brug menuen Nulstil indstillinger til at nulstille telefonindstillinger til deres standardværdier.
- Trin 2** Rediger DHCP- og IP-indstillinger:
 - a) Deaktiver DHCP.

- b) Tildel telefonen statiske IP-værdier. Brug den samme standardrouterindstilling, som andre funktioner, der virker, bruger.
- c) Tildel en TFTP-server. Brug den samme TFTP-server, som andre funktioner, der virker, bruger.

- Trin 3** Kontrollér, at de lokale værtsfiler på Cisco Unified Communications Manager-serveren har det rigtige Cisco Unified Communications Manager-servernavn tilknyttet til den rigtige IP-adresse.
- Trin 4** Vælg **System > Server** i Cisco Unified Communications Manager, og kontrollér, at der er en reference til serveren ved hjælp af IP-adressen og ikke DNS-navnet.
- Trin 5** Vælg **Enhed > Telefon** i Cisco Unified Communications Manager. Klik på **Find** for at søge efter denne telefon. Kontrollér, at du har tildelt den korrekte MAC-adresse til denne Cisco IP-telefon.
- Trin 6** Genstart telefonen.

Lignende emner

[Bestem telefonens MAC-adresse](#), på side 59

[Genstart eller nulstil konferencetelefonen](#), på side 171

Kontrollér DHCP-indstillinger

Fremgangsmåde

- Trin 1** Tryk på **Indstillinger** på telefonen.
- Trin 2** Vælg **Administratorindstillinger > Ethernet-opsætning > IPv4-opsætning**.
- Trin 3** Markér afkrydsningsfeltet DHCP-server.
- Hvis du har tildelt en statisk IP-adresse til telefonen, er det ikke nødvendigt at angive en værdi for indstillingen DHCP-server. Hvis du imidlertid bruger en DHCP-server, skal denne indstilling have en værdi. Hvis der ikke findes en værdi, skal du kontrollere din IP-routing og VLAN-konfiguration. Se dokumentet *Fejlfinding af switchport og grænsefladeproblemer*, der er tilgængeligt på denne URL-adresse:
- https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html
- Trin 4** Markér felterne IP-adresse, Undernetmaske og Standardrouter.
- Hvis du tildeler en statisk IP-adresse til telefonen, skal du manuelt angive indstillinger for disse valgmuligheder.
- Trin 5** Hvis du bruger DHCP, skal du kontrollere de IP-adresser, som din DHCP-server fordele.
- Se dokumentet *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* (Forståelse og fejlfinding af DHCP i Catalysts-switchnetværk eller firmanetværk), der er tilgængeligt på denne URL-adresse:
- https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml
-

Opret en ny telefonkonfigurationsfil

Når du fjerner en telefon fra Cisco Unified Communications Manager-databasen, slettes konfigurationsfilen fra Cisco Unified Communications Manager TFTP-serveren. Telefonbogsnummeret eller -numrene bliver i Cisco Unified Communications Manager-databasen. De kaldes for utildelte DN'er og kan bruges til andre

enheder. Hvis utildelte DN'er ikke bruges af andre enheder, skal du slette disse DN'er fra Cisco Unified Communications Manager-databasen. Du kan bruge ruteplansrapporten til at se og slette utildelte referencenumre. Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.

Hvis knapperne på en telefonknapskabelon ændres, eller der tildeles en anden telefonknapskabelon til en telefon, kan det resultere i telefonbogsnumre, der ikke længere er tilgængelige fra telefonen. Telefonbogsnumrene er stadig tildelt telefonen i Cisco Unified Communications Manager-databasen, men telefonen har ingen knap på telefonen, som opkald kan besvares med. Disse telefonbogsnumre bør fjernes fra telefonen og om nødvendigt slettes.

Fremgangsmåde

Trin 1 Vælg **Enhed** > **Telefon** i Cisco Unified Communications Manager, og klik på **Find** for at identificere den telefon, der har problemer.

Trin 2 Vælg **Slet** for at fjerne telefonen fra Cisco Unified Communications Manager-databasen.

Bemærk Når du fjerner en telefon fra Cisco Unified Communications Manager-databasen, slettes konfigurationsfilen fra Cisco Unified Communications Manager TFTP-serveren. Telefonbogsnummeret eller -numrene bliver i Cisco Unified Communications Manager-databasen. De kaldes for utildelte DN'er og kan bruges til andre enheder. Hvis utildelte DN'er ikke bruges af andre enheder, skal du slette disse DN'er fra Cisco Unified Communications Manager-databasen. Du kan bruge ruteplansrapporten til at se og slette utildelte referencenumre.

Trin 3 Føj telefonen tilbage til Cisco Unified Communications Manager-databasen.

Trin 4 Genstart telefonen.

Lignende emner

[Metoder til tilføjelse af telefoner](#), på side 60

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Kontrollér DNS-indstillinger

Fremgangsmåde

Trin 1 Tryk på **Indstillinger** på telefonen.

Trin 2 Vælg **Administratorindstillinger** > **Ethernet-opsætning** > **IPv4-opsætning**.

Trin 3 Kontrollér, at feltet DNS-server 1 er indstillet korrekt.

Trin 4 Du skal også kontrollere, at en CNAME-post blev angivet på DNS-serveren for TFTP-serveren og Cisco Unified Communications Manager-systemet.

Du skal også sikre dig, at DNS er konfigureret til at foretage modsatte opslag.

Start tjeneste

En tjeneste skal aktiveres, før den kan startes eller stoppes.

Fremgangsmåde

-
- Trin 1** Vælg **Cisco Unified Serviceability** i navigationsrullelisten, og klik på **Gå** i Cisco Unified Communications Manager Administration.
- Trin 2** Vælg **Funktioner > Kontrolcenter – funktionstjenester**.
- Trin 3** Vælg den primære Cisco Unified Communications Manager-server fra serverrullelisten.
- Vinduet viser tjenestens navne for den server, du vælger, statussen på tjenesterne og et tjenestekontrolpanel til at starte eller stoppe en tjeneste.
- Trin 4** Hvis en tjeneste er stoppet, skal du klikke på den tilhørende alternativknap og derefter klikke på **Start**. Symbolet for tjenestens status ændres fra en firkant til en pil.
-

Kontrollér fejlfindingsoplysninger fra Cisco Unified Communications Manager

Hvis du har problemer med telefonen, du ikke kan få løst, kan du få hjælp fra Cisco TAC. Du skal aktivere fejlfinding på telefonen, genskabe problemet, deaktivere fejlfindingen og derefter sende logfilerne til TAC, så de kan blive analyseret.

Da der under fejlfindingen registreres oplysninger, kan kommunikationstrafikken gøre telefonen langsommere, så den reagerer dårligere. Når du har registreret logfilerne, skal du deaktivere fejlfindingen, så telefonen kan bruges.

Fejlfindingsoplysningerne kan omfatte en encifret kode, der viser, hvor alvorlig situationen er. Situationer klassificeres på følgende måde:

- 0 – Nødsituation
- 1 – Alert
- 2 – Kritisk
- 3 – Fejl
- 4 – Warn
- 5 – Besked
- 6 – Oplysninger
- 7 – Fejlfinding

Kontakt Cisco TAC for at få flere oplysninger og hjælp.

Fremgangsmåde

Trin 1 I Cisco Unified Communications Manager Administration skal du vælge et af følgende vinduer:

- **Enhed > Enhedsindstillinger > Almindelig telefonprofil**
- **System > Konfiguration af firmatelefon**
- **Enhed > Telefon**

Trin 2 Indstil følgende parametre:

- Logprofil – værdier: Fast (standard), Standard, Telefoni, SIP, UI, Netværk, Medier, Opgradering, Tilbehør, Sikkerhed, Energywise, MobileRemoteAccess
- Ekstern logfil – værdier: Deaktiver (standard), Aktivér
- IPv6-logserver eller logserver – IP-adresse (IPv4- eller IPv6-adresse)

Bemærk Når der ikke kan oprettes forbindelse til logserveren, holder telefonen op med at sende fejlfindingsmeddelelser.

- Formatet på adressen til IPv4-logserveren er **adresse:<port>@@base=<0-7>;pfs=<0-1>**
 - Formatet på adressen til IPv6-logserveren er **[adresse]:<port>@@base=<0-7>;pfs=<0-1>**
 - Hvor:
 - IPv4 -adressen adskilles med et punktum (.)
 - IPv6 -adressen adskilles med et kolon (:)
-

Yderligere fejlfindingsoplysninger

Hvis du har yderligere spørgsmål om fejlfinding af din telefon, skal du gå til følgende Cisco-websted og navigere til den ønskede telefonmodel:

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



KAPITEL 13

Vedligeholdelse

- [Genstart eller nulstil konferencetelefonen, på side 171](#)
- [Overvågning af talekvalitet, på side 172](#)
- [Rengøring af Cisco IP-telefon, på side 174](#)

Genstart eller nulstil konferencetelefonen

Du kan udføre en grundlæggende nulstilling af en telefon for at genoprette den, hvis telefonen får en fejl. Du kan også gendanne konfigurations- og sikkerhedsindstillinger til fabriksindstillingerne.

Genstart konferencetelefonen

Når du genstarter telefonen, mistes eventuelle ændringer i brugere og netværk, der ikke er gemt i flash-hukommelse på telefonen.

Fremgangsmåde

Tryk på **Indstillinger** > **Administratorindstillinger** > **Nulstil indstillinger** > **Nulstill enhed**.

Lignende emner

[Tekst- og menuindtastning fra telefonen](#), på side 41

Nulstil indstillingerne for konferencetelefonen i telefonmenuen

Fremgangsmåde

- Trin 1** Tryk på **Indstillinger**.
- Trin 2** Vælg **Administratorindstillinger** > **Nulstil indstillinger**.
- Trin 3** Vælg nulstillingstypen.
- **Alle** – gendanner fabriksindstillingerne.
 - **Nulstil enhed** – nulstiller enheden. De eksisterende indstillinger ændres ikke.

- **Netværk**– nulstiller netværkskonfigurationen til standardindstillinger.
- **Tjenestetilstand**– rydder den aktuelle tjenestetilstand, deaktiverer VPN og genstarter telefonen.
- **Sikkerhed** – nulstiller sikkerhedskonfigurationen til standardindstillinger. Denne indstilling sletter CTL-filen.

Trin 4 Tryk på **Nulstil** eller **Annuller**.

Lignende emner

[Tekst- og menuindtastning fra telefonen](#), på side 41

Nulstil konferencetelefonen til fabriksindstillingerne fra tastaturet

Når du nulstiller telefonen fra det tastaturet, vender telefonen tilbage til fabriksindstillingerne.

Fremgangsmåde

Trin 1 Frakobl telefonen:

- Hvis du bruger PoE, skal du trække LAN-kablet ud.
- Hvis du bruger en adapter, skal du frakoble den.

Trin 2 Vent 5 sekunder.

Trin 3 Hold # nede, og tilslut telefonen igen.

Trin 4 Når telefonen starter, lyser LED-strimlen op. Så snart LED-striben tændes, skal du trykke på **123456789*0#** i rækkefølge.

Efter du trykker på disse knapper, starter processen med at nulstille telefonens fabriksindstillinger.

Hvis du trykker på knapperne i en anden rækkefølge, tænder telefonen på normal vis.

Advarsel Sluk ikke telefonen, før nulstillingen af dens fabriksindstillinger er færdig, og hovedskærmen vises.

Lignende emner

[Tekst- og menuindtastning fra telefonen](#), på side 41

Overvågning af talekvalitet

Hvis du vil måle talekvaliteten af opkald, der er blevet sendt og modtaget inden for netværket, bruger Cisco IP-telefoner disse statistiske måletal, der er baseret på skjulningshændelser. DSP afspiller skjulningsframes for at maskere tab af frames i talepakke-streamen.

- Måletal for skjultningsrate – Vis raten af skjulningsframes i forhold til det samlede antal taleframes. En intervalbaseret skjultningsrate bliver beregnet hver 3. sekund.
- Måletal for skjulte sekunder – Vis det antal sekunder, hvor DSP afspiller skjulningsframes pga. tab af frames. Et markant “skjult sekund” er et sekund, hvor DSP afspiller mere end fem procent skjulningsframes.



Bemærk Skjulningsrate og skjulningssekunder er primære målinger baseret på tab af frames. En skjulningsrate på nul indikerer, at IP-netværket leverer frames og pakker til tiden uden tab.

Du kan få adgang til måletal for talekvalitet fra Cisco IP-telefon ved hjælp af skærmen Opkaldsstatistik eller eksternt ved hjælp af streamingstatistik.

Fejlfindingstip til talekvalitet

Når du bemærker væsentlige og vedblivende ændringer i måletallene, skal du bruge følgende tabel til generelle fejlfindingsoplysninger.

Tabel 31: Ændringer i måletal for talekvalitet

| Ændring i måletal | Tilstand |
|---|---|
| Skjulningsrate og skjulningssekunder øges væsentligt | Netværksforringelse på grund af pakketab eller stor forvrængning. |
| Skjulningsrate er tæt på nul, men talekvaliteten er dårlig. | <ul style="list-style-type: none"> • Støj eller forvrængning i lydkanalen som f.eks. ekko eller lyd niveauer. • Forbundne opkald, der bliver kodet/afkodet flere gange, som f.eks. opkald til et mobilnetværk eller netværk til forudbetalte kort. • Akustiske problemer fra en højttalertelefon, håndfri mobiltelefon eller trådløse hovedtelefoner. <p>Kontrollér tællerne for pakkeafsendelse (TxCnt) og pakkemodtagelse (RxCnt) for at bekræfte, at talepakkerne flyder.</p> |
| MOS LQK-resultater falder væsentligt | <p>Netværksforringelse på grund af pakketab eller højre forvrængningsniveauer:</p> <ul style="list-style-type: none"> • Gennemsnitlige fald i MOS LQK kan angive omfattende og ensartet forringelse. • Individuelt fald i MOS LQK kan angive forringelse pga. af udfald. <p>Krydstjek skjulningsraten og skjulningssekunder for at finde tegn på tab af pakker og forvrængning.</p> |
| MOS LQK-resultater øges væsentligt | <ul style="list-style-type: none"> • Kontrollér, om telefonen bruger et andet codec end forventet (RxType og TxType). • Kontrollér, om MOS LQK-versionen er blevet ændret efter en opgradering af firmwaren. |



Bemærk Måletallene for talekvalitet tager ikke højde for støj eller forvrængning, kun tab af frames.

Rengøring af Cisco IP-telefon

Hvis du vil rengøre din Cisco IP-telefon, må du kun bruge en blød klud til forsigtigt at aftørre telefonen og telefonskærmen. Hæld ikke væsker eller pulver direkte på telefonen. Som det gælder med al elektronik, der ikke er vejrbestandig, kan væske og pulver beskadige komponenterne og give fejl.

Når telefonen er i slumretilstand, er skærmen tom, og knappen Vælg lyser ikke. Når telefonen er i denne tilstand, kan du rense skærmen, så længe du ved, at telefonen vil forblive i slumretilstand, indtil du afslutter rensningen.



KAPITEL 14

International brugersupport

- [Unified Communications Manager Endpoints Locale Installer](#), på side 175
- [Understøttelse af logføring af internationale opkald](#), på side 175
- [Sprogbegrænsning](#), på side 176

Unified Communications Manager Endpoints Locale Installer

Cisco IP-telefon er som standard konfigureret til engelsk (amerikansk). For at bruge Cisco IP-telefoner på andre sprog skal du installere den sprogspecifikke version af det lokale installationsprogram til Unified Communications Manager-slutpunkter på hver Cisco Unified Communications Manager-server i klyngen. Locale Installer installerer den senest oversatte tekst til telefonens brugergrænseflade og landespecifikke telefonlyde på dit system, så de er tilgængelige for Cisco IP-telefon.

For at få adgang til det lokale installationsprogram, der kræves til en version, skal du gå til siden [Software Download](#), finde din telefonmodel og vælge linket Installationsprogram til Unified Communications Manager-landestandarder for slutpunkter.

Få flere oplysninger i dokumentationen til din specifikke version af Cisco Unified Communications Manager.



Bemærk Den seneste Locale Installer er muligvis ikke øjeblikkeligt tilgængelig. Fortsæt for at søge efter opdateringer på webstedet.

Lignende emner

[Cisco Unified Communications Manager Dokumentation](#), på side 14

Understøttelse af logføring af internationale opkald

Hvis dit telefonsystem er konfigureret til logføring af internationale opkald (normalisering af den kaldende part), viser opkaldslogfiler, genopringning, eller poster i opkaldskatalog et plus tegn (+), der repræsenterer den internationale escape-kode for dit sted. Afhængigt af konfigurationen af dit telefonsystem kan + blive erstattet med den korrekte internationale opkaldskode, eller du er muligvis nødt til at redigere nummeret før opkald for manuelt at udskifte + med den internationale escape-kode for dit sted. Derudover er det sådan, at selvom opkaldslogfilen eller telefonbogsposten viser det fulde internationale nummer for det modtagne

nummer, viser telefonen måske kun den forkortede lokale version af nummeret uden internationale koder eller landekoder.

Sprogbegrænsning

Der er ingen oversat understøttelse af KATE (Keyboard Alphanumeric Text Entry) for følgende asiatiske landestandarder:

- Kinesisk (Kina)
- Kinesisk (Hongkong)
- Kinesisk (Taiwan)
- Japansk (Japan)
- Koreansk (Den Koreanske Republik)

Brugeren ser i stedet KATE på standardengelsk (USA).

Telefonskærmen viser f.eks. viser tekst på koreansk, men **2**-tasten på tastaturet viser **a b c 2 A B C**.