



## **Cisco IP-Konferenztelefon 8832 – Administratorhandbuch für Cisco Unified Communications Manager**

**Erste Veröffentlichung:** 15. September 2017

**Letzte Änderung:** 16. Juni 2023

### **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

DIE SPEZIFIKATIONEN UND INFORMATIONEN ZU DEN PRODUKTEN IN DIESEM HANDBUCH KÖNNEN OHNE VORHERIGE ANKÜNDIGUNG GEÄNDERT WERDEN. ALLE ANGABEN, INFORMATIONEN UND EMPFEHLUNGEN IN DIESEM HANDBUCH WURDEN IN DER ANNAHME ZUR VERFÜGUNG GESTELLT, DASS SIE KORREKT SIND. JEDE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNG IST JEDOCH AUSGESCHLOSSEN. DIE ALLEINIGE VERANTWORTUNG FÜR DIE ANWENDUNG DER PRODUKTE LIEGT BEI DEN BENUTZERN.

DIE SOFTWARELIZENZ UND BESCHRÄNKTE GEWÄHRLEISTUNG FÜR DAS BEILIEGENDE PRODUKT SIND IM INFORMATIONSPAKET FÜR DAS PRODUKT ENTHALTEN UND WERDEN DURCH DIESE BEZUGNAHME IN DIE VORLIEGENDEN BESTIMMUNGEN EINGESCHLOSSEN. WENN SIE DIE SOFTWARELIZENZ ODER BESCHRÄNKTE GARANTIE NICHT FINDEN KÖNNEN, WENDEN SIE SICH AN EINEN VERTRETER VON CISCO, UM EINE KOPIE ZU ERHALTEN.

Die folgenden Informationen beziehen sich auf die Einhaltung der FCC-Richtlinien für Geräte der Klasse A: Dieses Gerät wurde getestet und erfüllt die Grenzwerte für digitale Geräte der Klasse A gemäß Teil 15 der FCC-Richtlinien. Diese Anforderungen ermöglichen einen angemessenen Schutz gegen elektromagnetische Störungen, wenn das Gerät in einem gewerblichen Umfeld eingesetzt wird. Dieses Gerät erzeugt und verwendet Hochfrequenzsignale und kann diese abstrahlen. Wenn dieses Gerät nicht gemäß der Bedienungsanleitung installiert und betrieben wird, kann es Funkstörungen verursachen. Der Betrieb dieses Geräts in einem Wohngebiet kann unter Umständen zu funktechnischen Störungen führen. In diesem Fall muss der Benutzer diese Störungen auf eigene Kosten beheben.

Die folgenden Informationen betreffen FCC-konforme Geräte der Klasse B: Dieses Gerät wurde getestet und erfüllt die Anforderungen für digitale Geräte der Klasse B gemäß Abschnitt 15 der FCC-Bestimmungen. Diese Anforderungen ermöglichen einen angemessenen Schutz gegen elektromagnetische Störungen im häuslichen Bereich. Dieses Gerät erzeugt und verwendet Hochfrequenzsignale und kann diese abstrahlen. Wenn dieses Gerät nicht gemäß den Anweisungen installiert und betrieben wird, kann es Funkstörungen verursachen. Es kann jedoch nicht in jedem Fall garantiert werden, dass bei ordnungsgemäßer Installation keine Störungen auftreten. Wenn das Gerät Störungen beim Rundfunk- oder Fernsehempfang verursacht, was sich durch Aus- und Wiedereinschalten des Gerätes überprüfen lässt, versuchen Sie, die Störung durch eine der folgenden Maßnahmen zu beheben:

- Verändern Sie die Ausrichtung oder den Standort der Empfangsantenne.
- Erhöhen Sie den Abstand zwischen dem Gerät und dem Empfänger.
- Schließen Sie das Gerät an einen anderen Hausstromkreis an als den Empfänger.
- Wenden Sie sich an den Händler oder einen erfahrenen Radio-/Fernsehtechniker.

Anpassungen und Veränderungen an diesem Produkt, die nicht durch Cisco autorisiert wurden, können die FCC-Genehmigung außer Kraft setzen und zum Verlust der Erlaubnis führen, dieses Produkt zu betreiben.

Die Cisco Implementierung der TCP-Headerkomprimierung ist eine Adaption eines Programms, das an der University of California, Berkeley (UCB) als Teil der Public-Domain-Version der UCB für das UNIX-Betriebssystem entwickelt wurde. Alle Rechte vorbehalten. Copyright © 1981, Regents of the University of California, USA.

UNGEACHTET SONSTIGER GEWÄHRLEISTUNGEN WERDEN ALLE DOKUMENT- UND SOFTWAREDATEIEN DIESER ANBIETER WIE VORLIEGEND OHNE MÄNGELGEWÄHRBEREITGESTELLT. CISCO UND ALLE ZUVOR GENANNTE LIEFERANTEN ÜBERNEHMEN KEINERLEI, AUSDRÜCKLICHE ODER STILLSCHWEIGENDE, GARANTIE, EINSCHLIEBLICH UND OHNE EINSCHRÄNKUNG, DIEJENIGEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG ODER DIEJENIGEN, DIE AUS DEM VERLAUF DES HANDELNS, DER VERWENDUNG ODER DES HANDELSBRAUCHS ENTSTEHEN.

UNTER KEINEN UMSTÄNDEN HAFTEN CISCO ODER SEINE ZULIEFERER FÜR JEDLICHE INDIREKTEN, KONKRETE, ZUFÄLLIGEN ODER FOLGESCHÄDEN, DARUNTER BEISPIELSGEWISSE ENTGANGENE GEWINNE ODER DATENVERLUSTE, DIE AUS DER VERWENDUNG ODER NICHTVERWENDBARKEIT DIESES HANDBUCHS ERWACHSEN, SELBST FÜR DEN FALL, DASS CISCO ODER SEINE ZULIEFERER AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDEN.

Alle in diesem Dokument verwendeten IP-Adressen (Internet Protocol) und Telefonnummern sind als Beispiele zu verstehen und beziehen sich nicht auf tatsächlich existierende Adressen und Telefonnummern. Die in diesem Dokument enthaltenen Beispiele, Befehlsausgaben, Netzwerktopologie-Diagramme und andere Abbildungen dienen lediglich zur Veranschaulichung. Die Verwendung tatsächlicher IP-Adressen oder Telefonnummern in diesem Zusammenhang ist zufällig und nicht beabsichtigt.

Für gedruckte und kopierte digitale Versionen dieses Dokuments besteht keine Gewährleistung. Die aktuelle Online-Version enthält die neueste Version.

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen und Telefonnummern finden Sie auf der Cisco Website unter [www.cisco.com/go/offices](http://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 Rechte vorbehalten.



## INHALTSVERZEICHNIS

---

### KAPITEL 1

#### Neue und geänderte Informationen 1

Neue und geänderte Informationen zur Firmware-Version 14.2(1)	1
Neue und geänderte Informationen zur Firmware-Version 14.1(1)	1
Neue und geänderte Informationen zur Firmware-Version 14.0(1)	2
Neue und geänderte Informationen zur Firmware-Version 12.8(1)	2
Neue und geänderte Informationen zur Firmware-Version 12.7(1)	2
Neue und geänderte Informationen zur Firmware-Version 12.6(1)	2
Neue und geänderte Informationen zur Firmware-Version 12.5(1)SR3	3
Neue und geänderte Informationen zur Firmware-Version 12.5(1)SR2	3
Neue und geänderte Informationen zur Firmware-Version 12.5(1)SR1	3
Neue und geänderte Informationen zur Firmware-Version 12.5(1)	4
Neue und geänderte Informationen zur Firmware-Version 12.1(1)	4

---

### TEIL I:

#### Allgemeines zum Cisco IP-Konferenztelefon 7

---

### KAPITEL 2

#### Cisco IP-Konferenztelefon – Hardware 9

Cisco IP-Konferenztelefon 8832	9
Cisco IP-Konferenztelefon 8832 – Tasten und Hardware	11
Kabelgebundenes externes Mikrofon (nur 8832)	12
Kabelloses externes Mikrofon (nur 8832)	13
Zugehöriges Dokumentationsmaterial	14
Dokumentation für das Cisco IP-Konferenztelefon 8832	14
Dokumentation Cisco Unified Communications Manager	14
Dokumentation Cisco Unified Communications Manager Express	15
Cisco Hosted Collaboration Service – Dokumentation	15
Dokumentation für Cisco Business Edition 4000	15

Dokumentation, Support und Sicherheitsrichtlinien 15

Übersicht über die Cisco Produktsicherheit 15

Begriffsunterschiede 16

---

**KAPITEL 3**

**Technische Details 17**

Physische und Umgebungsspezifikationen 17

Stromversorgung des Telefons 18

Stromausfall 19

Senkung des Stromverbrauchs 19

Netzwerkprotokolle 20

Cisco Unified Communications Manager-Interaktion 22

Cisco Unified Communications Manager Express-Interaktion 23

Interaktion mit dem Sprachnachrichtensystem 23

Konfigurationsdateien für Telefone 24

Verhalten des Telefons bei Netzwerküberlastung 24

Application Programming Interface 24

---

**TEIL II:**

**Cisco IP-Konferenztelefon – Installation 25**

---

**KAPITEL 4**

**Installation des Telefons 27**

Netzwerkconfiguration überprüfen 27

Aktivierungscode-Integration für lokale Telefone 28

Aktivierungscode-Integration mit mobilem und Remotezugriff 29

Aktivieren der automatischen Registrierung für Telefone 29

Daisy-Chain-Modus 31

Installation des Konferenztelefons 31

Ihr Konferenztelefon mit Energie versorgen 33

Kabelgebundene externe Mikrofone installieren 35

Kabellose externe Mikrofone installieren 36

Die Ladeschale des kabellosen Mikrofons installieren 37

Konferenztelefon im Daisy-Chain-Modus installieren 38

Ihr Konferenztelefon über das Backup-Image neu starten 39

Telefone über Menüs konfigurieren 40

Anwenden eines Telefonkennworts 41

Text und Menüeintrag auf dem Telefon	41
Netzwerkeinstellungen konfigurieren	42
Felder für das Netzwerk-Setup	42
Das Feld Domännennamen	47
Wireless-LAN über das Telefon aktivieren	47
Wireless LAN über Cisco Unified Communications Manager einrichten	48
Konfigurieren des Wireless LAN über das Telefon	49
Anzahl der WLAN-Authentifizierungsversuche festlegen	50
Aktivieren des WLAN-Aufforderungsmodus	51
Wi-Fi-Profil mit Cisco Unified Communications Manager festlegen	51
Wi-Fi-Gruppe mit Cisco Unified Communications Manager festlegen	53
Telefonstart überprüfen	54
Telefonmodell eines Benutzers ändern	54

**KAPITEL 5****Cisco Unified Communications Manager – Telefoninstallation 57**

Cisco IP-Konferenztelefon einrichten	57
Die MAC-Adresse des Telefons bestimmen	62
Methoden zum Hinzufügen von Telefonen	62
Einzelne Telefone hinzufügen	62
Telefone über eine BAT-Telefonvorlage hinzufügen	63
Benutzer zu Cisco Unified Communications Manager hinzufügen	63
Benutzer aus einem externen LDAP-Verzeichnis hinzufügen	64
Einen Benutzer direkt Cisco Unified Communications Manager hinzufügen	65
Einer Endbenutzergruppe einen Benutzer hinzufügen	65
Telefone zu Benutzern zuordnen	66
SRST (Survivable Remote Site Telephony)	67

**KAPITEL 6****Verwaltung des Selbstservice-Portals 71**

Übersicht des Selbstservice-Portals	71
Den Benutzerzugriff auf das Selbstservice-Portal konfigurieren	71
Die Ansicht des Selbstservice-Portals anpassen	72

**TEIL III:****Cisco IP-Konferenztelefon – Administration 73**

---

**KAPITEL 7**

**Cisco IP-Konferenztelefon – Sicherheit 75**

- Übersicht der Sicherheit des Cisco IP Phone 75
- Sicherheitsverbesserungen für Ihr Telefonnetzwerk 76
- Unterstützte Sicherheitsfunktionen 77
  - Einrichten eines LSC (Locally Significant Certificate) 79
  - Aktivieren des FIPS-Modus 81
  - Anrufsicherheit 81
    - Sichere Konferenzanruf-ID 82
    - Sichere Anruf-ID 83
    - Verschlüsselung für Aufschaltung bereitstellen 84
    - WLAN-Sicherheit 84
  - Wireless LAN-Sicherheit 87
    - Verwaltungsseite für das Cisco IP-Telefon 87
    - SCEP-Konfiguration 91
    - 802.1x-Authentifizierung 91

---

**KAPITEL 8**

**Cisco IP-Konferenztelefon – Anpassung 93**

- Individuelle Ruftöne 93
  - Einen benutzerdefinierten Rufton konfigurieren 93
  - Dateiformate für benutzerdefinierte Ruftöne 94
- Den Wählton anpassen 95

---

**KAPITEL 9**

**Cisco IP-Konferenztelefon – Funktionen und Einrichtung 97**

- Benutzersupport für Cisco IP-Telefon 97
- Direkte Migration Ihres Telefons zu einem Multiplattform-Telefon 98
- Softkey-Vorlagen konfigurieren 98
- Telefonservices für Benutzer konfigurieren 99
- Telefonfunktion – Konfiguration 100
  - Einrichten von Telefonfunktionen für alle Telefone 100
  - Einrichten von Telefonfunktionen für eine Telefongruppe 101
  - Einrichten von Telefonfunktionen für ein einzelnes Telefon 101
  - Produktspezifische Konfiguration 102
  - Transport Layer Security-Schlüssel deaktivieren 115

Energiesparmodus für Cisco IP-Telefon planen	116
EnergyWise für das Cisco IP-Telefon planen	117
DND konfigurieren	121
Benachrichtigung für Rufumleitung einrichten	121
UCR 2008-Konfiguration	122
UCR 2008 in der allgemeinen Gerätekonfiguration konfigurieren	123
UCR 2008 im allgemeinen Telefonprofil konfigurieren	123
UCR 2008 in der Firmentelefonkonfiguration konfigurieren	124
UCR 2008 auf dem Telefon konfigurieren	124
Mobil- und Remote Access über Expressway	124
Bereitstellungsszenarien	126
Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren	126
Tool zur Problemmeldung	127
Eine Upload-URL für den Kundensupport konfigurieren	127
Bezeichnung einer Leitung festlegen	128

---

<b>KAPITEL 10</b>	<b>Unternehmensverzeichnis und persönliches Verzeichnis</b>	<b>131</b>
	Konfiguration des Firmenverzeichnisses	131
	Konfiguration des persönlichen Verzeichnisses	131

---

<b>TEIL IV:</b>	<b>Cisco IP-Konferenztelefon – Fehlerbehebung</b>	<b>133</b>
-----------------	---	------------

---

<b>KAPITEL 11</b>	<b>Telefonsysteme überwachen</b>	<b>135</b>
	Übersicht der Telefonsystemüberwachung	135
	Cisco IP-Telefon-Status	135
	Fenster „Telefoninformationen anzeigen“	136
	Statusmenü anzeigen	136
	Das Fenster „Statusmeldungen“ anzeigen	136
	Das Fenster „Netzwerkstatistik“ anzeigen	141
	Das Fenster „Anrufstatistik“ anzeigen	144
	Webseite für Cisco IP-Telefon	146
	Auf die Webseite des Telefons zugreifen	146
	Webseite mit Geräteinformationen	147
	Webseite „Netzwerk-Setup“	148

Webseite mit Ethernet-Informationen	153
Netzwerk-Webseiten	153
Webseiten für Konsolenprotokolle, Speicherauszüge, Statusmeldungen und Fehlersuchanzeige	155
Webseite „Streaming-Statistik“	155
Informationen im XML-Format vom Telefon anfordern	158
Beispielausgabe für „CallInfo“	158
Beispielausgabe für „LineInfo“	159
Beispielausgabe für „ModeInfo“	160

**KAPITEL 12**

**Telefonfehlerbehebung 161**

Allgemeine Informationen zur Problembehandlung	161
Startprobleme	162
Cisco IP-Telefon wird nicht normal gestartet	163
Cisco IP-Telefon wird nicht mit Cisco Unified Communications Manager registriert	164
Fehlermeldungen auf dem Telefon	164
Das Telefon kann keine Verbindung mit dem TFTP-Server oder Cisco Unified Communications Manager herstellen	164
Telefon kann keine Verbindung mit dem TFTP-Server herstellen	164
Das Telefon kann sich nicht mit dem Server verbinden	165
Das Telefon kann sich nicht über DNS verbinden	165
Der Cisco Unified Communications Manager- und TFTP-Service werden nicht ausgeführt	165
Die Konfigurationsdatei ist beschädigt	166
Cisco Unified Communications Manager – Telefonregistrierung	166
Cisco IP-Telefon kann keine IP-Adresse abrufen	166
Probleme mit dem Zurücksetzen des Telefons	167
Das Telefon wird aufgrund sporadischer Netzwerkausfälle zurückgesetzt	167
Das Telefon wird aufgrund von DHCP-Einstellungsfehlern zurückgesetzt	167
Das Telefon wird aufgrund einer falschen statischen IP-Adresse zurückgesetzt	167
Das Telefon wird bei hoher Netzwerkauslastung zurückgesetzt	168
Das Telefon wird absichtlich zurückgesetzt	168
Das Telefon wird aufgrund von DNS-Problemen oder anderen Verbindungsproblemen zurückgesetzt	168
Das Telefon schaltet sich nicht ein	169
Das Telefon kann sich nicht mit dem LAN verbinden	169



Sicherheitsprobleme auf Cisco IP-Telefon	169
CTL-Dateiprobleme	169
Authentifizierungsfehler, das Telefon kann die CTL-Datei nicht authentifizieren	169
Das Telefon kann die CTL-Datei nicht authentifizieren	170
Die CTL-Datei wird authentifiziert, aber andere Konfigurationsdateien werden nicht authentifiziert	170
Die ITL-Datei wird authentifiziert, aber andere Konfigurationsdateien werden nicht authentifiziert	170
TFTP-Autorisierung fehlgeschlagen	170
Das Telefon wird nicht registriert	171
Signierte Konfigurationsdateien werden nicht angefordert	171
Audioprobleme	171
Kein Sprachpfad	171
Abgehackte Sprache	172
Ein Telefon im Daisy-Chain-Modus funktioniert nicht	172
Allgemeine Anrufprobleme	172
Anruf kann nicht hergestellt werden	172
Das Telefon erkennt DTMF-Ziffern nicht oder Ziffern werden verzögert	173
Fehlerbehebungsverfahren	173
Telefonproblembenachrichtigungen im Cisco Unified Communications Manager erstellen	173
TFTP-Einstellungen überprüfen	174
DNS-Probleme oder Verbindungsprobleme identifizieren	174
DHCP-Einstellungen überprüfen	175
Erstellen einer neuen Konfigurationsdatei für das Telefon	175
Die DNS-Einstellungen überprüfen	176
Service starten	176
Debuginformationen von Cisco Unified Communications Manager	177
Zusätzliche Informationen zur Problembehandlung	178

---

**KAPITEL 13**
**Wartung 179**

Konferenztelefon neu starten oder zurücksetzen	179
Konferenztelefon neu starten	179
Die Einstellungen des Konferenztelefons über das Telefonmenü zurücksetzen	179
Konferenztelefon über das Tastenfeld auf die Werkseinstellungen zurücksetzen	180

Überwachung der Sprachqualität 180  
    Tipps zur Fehlerbehebung bei der Sprachqualität 181  
Reinigung des Cisco IP-Telefon 182

---

KAPITEL 14

**Unterstützung von Benutzern in anderen Ländern 183**  
    Unified Communications Manager Installationsprogramm für Endpunktsprache 183  
    Internationaler Support für Anrufprotokollierung 183  
    Sprachbeschränkung 184



# KAPITEL 1

## Neue und geänderte Informationen

- [Neue und geänderte Informationen zur Firmware-Version 14.2\(1\), auf Seite 1](#)
- [Neue und geänderte Informationen zur Firmware-Version 14.1\(1\), auf Seite 1](#)
- [Neue und geänderte Informationen zur Firmware-Version 14.0\(1\), auf Seite 2](#)
- [Neue und geänderte Informationen zur Firmware-Version 12.8\(1\), auf Seite 2](#)
- [Neue und geänderte Informationen zur Firmware-Version 12.7\(1\), auf Seite 2](#)
- [Neue und geänderte Informationen zur Firmware-Version 12.6\(1\), auf Seite 2](#)
- [Neue und geänderte Informationen zur Firmware-Version 12.5\(1\)SR3, auf Seite 3](#)
- [Neue und geänderte Informationen zur Firmware-Version 12.5\(1\)SR2, auf Seite 3](#)
- [Neue und geänderte Informationen zur Firmware-Version 12.5\(1\)SR1, auf Seite 3](#)
- [Neue und geänderte Informationen zur Firmware-Version 12.5\(1\), auf Seite 4](#)
- [Neue und geänderte Informationen zur Firmware-Version 12.1\(1\), auf Seite 4](#)

## Neue und geänderte Informationen zur Firmware-Version 14.2(1)

Die folgenden Informationen sind für Firmware-Version 14.2(1) neu oder wurden geändert.

Funktion	Neu oder geändert
Unterstützung für SIP-OAuth für SRST	<a href="#">Sicherheitsverbesserungen für Ihr Telefonnetzwerk, auf Seite 76</a>

## Neue und geänderte Informationen zur Firmware-Version 14.1(1)

Die folgenden Informationen sind für Firmware-Version 14.1(1) neu oder wurden geändert.

Funktion	Neu oder geändert
Unterstützung von SIP-OAuth für Proxy-TFTP	<a href="#">Sicherheitsverbesserungen für Ihr Telefonnetzwerk, auf Seite 76</a>
Telefonmigration ohne Übergangs-Firmware	<a href="#">Direkte Migration Ihres Telefons zu einem Multiplattform-Telefon, auf Seite 98</a>

## Neue und geänderte Informationen zur Firmware-Version 14.0(1)

**Tabelle 1: Neue und geänderte Informationen**

Funktion	Neu oder geändert
Verbesserung der Überwachung von geparkten Anrufen	Produktspezifische Konfiguration, auf Seite 102
SIP-OAuth-Verbesserungen	Sicherheitsverbesserungen für Ihr Telefonnetzwerk, auf Seite 76
OAuth-Verbesserungen für MRA	Mobil- und Remote Access über Expressway, auf Seite 124
Verbesserungen der Benutzeroberfläche	SRST (Survivable Remote Site Telephony), auf Seite 67

Ab Firmware Version 14.0 unterstützen die Telefone DTLS 1.2. DTLS 1.2 erfordert Cisco Adaptive Security Appliance (ASA) Version 9.10 oder höher. Sie konfigurieren die minimale DTLS-Version für eine VPN-Verbindung in ASA. Weitere Informationen finden Sie im *ASDM Buch 3: VPN ASDM-Konfigurationshandbuch der Cisco ASA-Serie* unter <https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html>.

## Neue und geänderte Informationen zur Firmware-Version 12.8(1)

Die folgenden Informationen sind für Firmware-Version 12.8(1) neu oder wurden geändert.

Funktion	Neuer oder geänderter Inhalt
Telefondatenmigration	Telefonmodell eines Benutzers ändern, auf Seite 54
Weitere Informationen zum Feld „Webzugriff“ hinzugefügt	Produktspezifische Konfiguration, auf Seite 102

## Neue und geänderte Informationen zur Firmware-Version 12.7(1)

Für die Firmware-Version 12.7(1) wurden keine Aktualisierungen des Administratorhandbuchs benötigt.

## Neue und geänderte Informationen zur Firmware-Version 12.6(1)

Für die Firmware-Version 12.6(1) wurden keine Aktualisierungen des Administratorhandbuchs benötigt.

## Neue und geänderte Informationen zur Firmware-Version 12.5(1)SR3

Die Referenzen zur Cisco Unified Communications Manager-Dokumentation wurden aktualisiert, um alle Versionen von Cisco Unified Communications Manager zu unterstützen.

**Table 2: Überarbeitung des Cisco IP-Telefon 8832-Administratorhandbuchs für Firmware-Version 12.5(1)SR3**

Überarbeitung	Aktualisierter Abschnitt
Unterstützung für die Integration über Aktivierungscode mit mobilem und Remotezugriff	<a href="#">Aktivierungscode-Integration mit mobilem und Remotezugriff, auf Seite 29</a>
Unterstützung für die Verwendung des Problemberichtstools über Cisco Unified Communications Manager	<a href="#">Telefonproblembereichte im Cisco Unified Communications Manager erstellen, auf Seite 173</a>

## Neue und geänderte Informationen zur Firmware-Version 12.5(1)SR2

Für die Firmware-Version 12.5(1)SR2 wurden keine Administrationshandbuchaktualisierungen benötigt.

Firmware-Version 12.5(1)SR2 ersetzt die Firmware-Version 12.5(1) und die Firmware-Version 12.5(1)SR1. Firmware-Version 12.5(1) und Firmware-Version 12.5(1)SR1 wurden zugunsten von Firmware-Version 12.5(1)SR2 zurückgestellt.

## Neue und geänderte Informationen zur Firmware-Version 12.5(1)SR1

In der folgenden Tabelle werden die Änderungen für das *Cisco IP-Konferenztelefon 8832-Administratorhandbuch für Cisco Unified Communications Manager* zur Unterstützung von Firmware-Version 12.5(1)SR1 aufgeführt.

**Table 3: Überarbeitung des Cisco IP-Konferenztelefon 8832-Administratorhandbuchs zur Firmware-Version 12.5(1)SR1**

Überarbeitung	Neuer oder aktualisierter Abschnitt
Unterstützung für elliptische Kurven	<a href="#">Unterstützte Sicherheitsfunktionen, auf Seite 77</a>

## Neue und geänderte Informationen zur Firmware-Version 12.5(1)

In der folgenden Tabelle werden die Änderungen für das *Cisco IP-Konferenztelefon 8832-Administratorhandbuch für Cisco Unified Communications Manager* zur Unterstützung von Firmware-Version 12.5(1) aufgeführt.

**Tabelle 4: Überarbeitung des Cisco IP-Konferenztelefon 8832-Administratorhandbuchs für Firmware-Version 12.5(1)**

Überarbeitung	Neuer oder aktualisierter Abschnitt
Unterstützung für Whisper Paging auf Cisco Unified Communications Manager Express	<a href="#">Cisco Unified Communications Manager Express-Interaktion, auf Seite 23</a>
Unterstützung für das Deaktivieren des TLS-Schlüssels	<a href="#">Produktspezifische Konfiguration, auf Seite 102</a>
Unterstützung für Blockwahl für T.302-Erweiterung des Interdigit-Timers.	<a href="#">Produktspezifische Konfiguration, auf Seite 102</a>

## Neue und geänderte Informationen zur Firmware-Version 12.1(1)

In der folgenden Tabelle werden die Änderungen für das *Cisco IP-Konferenztelefon 8832-Administratorhandbuch für Cisco Unified Communications Manager* zur Unterstützung von Firmware-Version 12.1(1) beschrieben.

Überarbeitung	Neuer oder aktualisierter Abschnitt
Mit Unterstützung für PoE-Injektor für Cisco IP-Konferenztelefon 8832	<ul style="list-style-type: none"> <li>• <a href="#">Stromversorgung des Telefons, auf Seite 18</a></li> <li>• <a href="#">Ihr Konferenztelefon mit Energie versorgen, auf Seite 33</a></li> <li>• <a href="#">Installation des Konferenztelefons, auf Seite 31</a></li> </ul>
Unterstützung für kabellose Mikrofone	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IP-Konferenztelefon 8832, auf Seite 9</a></li> <li>• <a href="#">Kabelloses externes Mikrofon (nur 8832), auf Seite 13</a></li> <li>• <a href="#">Kabellose externe Mikrofone installieren, auf Seite 36</a></li> <li>• <a href="#">Die Ladeschale des kabellosen Mikrofons installieren, auf Seite 37</a></li> </ul>

Überarbeitung	Neuer oder aktualisierter Abschnitt
Unterstützung für Daisy Chain	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IP-Konferenztelefon 8832</a>, auf Seite 9</li> <li>• <a href="#">Daisy-Chain-Modus</a>, auf Seite 31</li> <li>• <a href="#">Konferenztelefon im Daisy-Chain-Modus installieren</a>, auf Seite 38</li> <li>• <a href="#">Ein Telefon im Daisy-Chain-Modus funktioniert nicht</a>, auf Seite 172</li> </ul>
Mit Unterstützung für Nicht-PoE-fähiger Ethernet-Injektor für Cisco IP-Konferenztelefon 8832	<ul style="list-style-type: none"> <li>• <a href="#">Installation des Konferenztelefons</a>, auf Seite 31</li> <li>• <a href="#">Ihr Konferenztelefon mit Energie versorgen</a>, auf Seite 33</li> </ul>
Unterstützung von Wi-Fi	<ul style="list-style-type: none"> <li>• <a href="#">Installation des Konferenztelefons</a>, auf Seite 31</li> <li>• <a href="#">Ihr Konferenztelefon mit Energie versorgen</a>, auf Seite 33</li> <li>• <a href="#">Das Feld Domännennamen</a>, auf Seite 47</li> <li>• <a href="#">Wireless-LAN über das Telefon aktivieren</a>, auf Seite 47</li> <li>• <a href="#">Wireless LAN über Cisco Unified Communications Manager einrichten</a>, auf Seite 48</li> <li>• <a href="#">Konfigurieren des Wireless LAN über das Telefon</a>, auf Seite 49</li> <li>• <a href="#">Anzahl der WLAN-Authentifizierungsversuche festlegen</a>, auf Seite 50</li> <li>• <a href="#">Aktivieren des WLAN-Aufforderungsmodus</a>, auf Seite 51</li> <li>• <a href="#">Wi-Fi-Profil mit Cisco Unified Communications Manager festlegen</a>, auf Seite 51</li> <li>• <a href="#">Wi-Fi-Gruppe mit Cisco Unified Communications Manager festlegen</a>, auf Seite 53</li> </ul>
Unterstützung für Mobilzugriff und Remote Access über Expressway	<ul style="list-style-type: none"> <li>• <a href="#">Mobil- und Remote Access über Expressway</a>, auf Seite 124</li> <li>• <a href="#">Bereitstellungsszenarien</a>, auf Seite 126</li> <li>• <a href="#">Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren</a>, auf Seite 126</li> </ul>
Unterstützung für das Aktivieren oder Deaktivieren von TLS 1.2 für den Webserverzugriff.	<p><a href="#">Produktspezifische Konfiguration</a>, auf Seite 102</p>
Unterstützung für G722.2 AMR-WB-Audio-Codec	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IP-Konferenztelefon 8832</a>, auf Seite 9</li> <li>• <a href="#">Anrufstatistikfelder</a>, auf Seite 144</li> </ul>







TEIL **I**

## **Allgemeines zum Cisco IP-Konferenztelefon**

- [Cisco IP-Konferenztelefon – Hardware, auf Seite 9](#)
- [Technische Details, auf Seite 17](#)





## KAPITEL 2

# Cisco IP-Konferenztelefon – Hardware

- [Cisco IP-Konferenztelefon 8832, auf Seite 9](#)
- [Cisco IP-Konferenztelefon 8832 – Tasten und Hardware, auf Seite 11](#)
- [Zugehöriges Dokumentationsmaterial, auf Seite 14](#)
- [Dokumentation, Support und Sicherheitsrichtlinien, auf Seite 15](#)
- [Begriffsunterschiede, auf Seite 16](#)

## Cisco IP-Konferenztelefon 8832

Cisco IP-Konferenztelefon 8832 und 8832NR fördern die Kommunikation zwischen Menschen. Es bietet erstklassige HD- (High-Definition)-Audio-Leistung und 360-Grad-Abdeckung in mittleren bis großen Konferenzräumen und Büros. Es bietet ein audiophiles Sound-Erlebnis mit einem Zwei-Wege-Lautsprecher mit Wideband-Audio (G.722) für Freisprechen im Vollduplex-Betrieb. Dieses Telefon ist eine einfache Lösung, die die Anforderungen der unterschiedlichsten Räume erfüllt.

**Abbildung 1: Cisco IP-Konferenztelefon 8832**



Das Telefon hat empfindliche Mikrofone, die 360 Grad abdecken. Die Benutzer können normal sprechen und werden in einer Entfernung von bis zu 3 Metern klar gehört. Die Technologie des Telefons ist auch unempfindlich gegenüber Störungen von Mobiltelefonen und anderen drahtlosen Geräten, um eine klare Kommunikation ohne Ablenkungen sicherzustellen. Das Telefon verfügt über ein Farbdisplay und

Softkey-Tasten zum Zugriff auf Benutzerfunktionen. Bei Verwendung der Basiseinheit ohne Zusatzmikrofone deckt das Telefon einen Raum der Größe 6,1 x 6,1 m und bis zu 10 Personen ab.

Zwei kabelgebundene externe Mikrofone sind für das Telefon erhältlich. Sie können die Reichweite in größeren Konferenzräumen vergrößern, indem Sie die externen Mikrofone ininigem Abstand von der Basiseinheit aufstellen. Bei Verwendung der Basiseinheit mit externen Mikrofonen deckt das Telefon einen Konferenzraum der Größe 6,1 x 10 m und bis zu 22 Personen ab.

Zudem unterstützt das Telefon ein optionales Set von zwei kabellosen externen Mikrofonen. Bei Verwendung der Basiseinheit mit kabellosen externen Mikrofonen deckt das Telefon einen Konferenzraum der Größe 6,1 x 12,2 m und bis zu 26 Personen ab. Um einen Chat-Raum in der Größe von 6,1 x 12,2 m abzudecken, empfehlen wir Ihnen, jedes Mikrofon mit einem maximalen Abstand von 3 Metern von der Basis zu platzieren.

Sie können zwei Basiseinheiten verbinden, um die Abdeckung für einen Raum zu erhöhen. Für diese Konfiguration ist das optionale Daisy-Chain-Kit erforderlich. Sie kann zwei externe Mikrofone unterstützen (entweder kabellos oder kabelgebunden, jedoch keine Kombination aus beiden). Bei Verwendung kabelgebundener Mikrofone mit dem Daisy-Chain-Kit deckt die Konfiguration einen Raum der Größe 6,1 x 15,2 m und bis zu 38 Personen ab. Bei Verwendung kabelloser Mikrofone mit dem Daisy-Chain-Kit deckt die Konfiguration einen Raum der Größe 6,1 x 17,4 m und bis zu 42 Personen ab.

Die (funklose) Cisco IP-Konferenztelefon 8832NR-Version unterstützt kein Wi-Fi, keine kabellosen Mikrofone oder Bluetooth.

Wie andere Geräte muss Cisco IP-Telefon konfiguriert und verwaltet werden. Diese Telefone codieren und decodieren die folgenden Codecs:

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




---

**Vorsicht** Das Verwenden eines Mobiltelefons, Handys oder GSM-Telefons oder eines Funksprechgeräts in unmittelbarer Nähe eines Cisco IP-Telefon kann Störungen verursachen. Weitere Informationen finden Sie in der Herstellerdokumentation zu dem Produkt, das die Störung verursacht.

---

Cisco IP-Telefons bieten klassische Telefoniefunktionen wie Rufumleitung und -übergabe, Wahlwiederholung, Kurzwahl, Konferenzgespräche und Zugriff auf Sprachnachrichtensysteme. Cisco IP-Telefons stellen auch verschiedene andere Funktionen bereit.

Wie andere Netzwerkgeräte müssen Cisco IP-Telefone für den Zugriff auf Cisco Unified Communications Manager und das restliche IP-Netzwerk konfiguriert werden. Wenn Sie DHCP verwenden, müssen Sie weniger Einstellungen auf einem Telefon konfigurieren. Sie können Informationen jedoch manuell konfigurieren, beispielsweise eine IP-Adresse, den TFTP-Server und Subnetzinformationen, wenn dies für Ihr Netzwerk erforderlich ist.

Cisco IP-Telefons können mit anderen Geräten und Services im IP-Netzwerk interagieren, um erweiterte Funktionen bereitzustellen. Sie können beispielsweise das unternehmenseigene LDAP3-Standardverzeichnis (Lightweight Directory Access Protocol 3) in Cisco Unified Communications Manager einbinden, um Benutzern die direkte Suche von Mitarbeiter-Kontaktinformationen mit ihren Cisco IP-Telefonen zu ermöglichen. Sie können auch mithilfe von XML Benutzern den Zugriff auf Informationen wie Wetter, tagesaktuelle Aktienkurse und sonstige webbasierte Informationen ermöglichen.

Da Cisco IP-Telefon ein Netzwerkgerät ist, können Sie detaillierte Statusinformationen direkt abrufen. Diese Informationen können bei der Behebung von Problemen helfen, die mit den IP-Telefonen der Benutzer auftreten. Sie können auch die Statistik eines aktiven Anrufs oder einer Firmware-Version auf dem Telefon anzeigen.

Damit Cisco IP-Telefon im IP-Telefonienetzwerk funktioniert, muss es mit einem Netzwerkgerät verbunden sein, z. B. mit einem Cisco Catalyst-Switch. Zudem müssen Sie Cisco IP-Telefon bei einem Cisco Unified Communications Manager-System registrieren, bevor Anrufe getätigt und angenommen werden können.

## Cisco IP-Konferenztelefon 8832 – Tasten und Hardware





Die folgende Abbildung zeigt das Cisco IP-Konferenztelefon 8832.

**Abbildung 2: Tasten und Funktionen des Cisco IP-Konferenztelefon 8832**



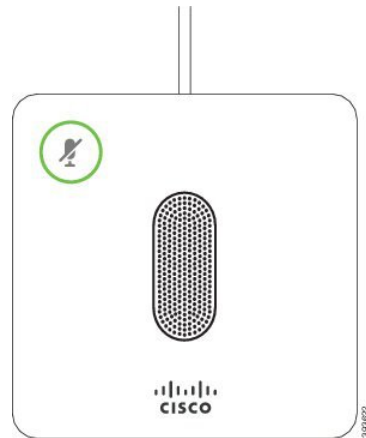
In der folgenden Tabelle werden die Tasten auf dem Cisco IP-Konferenztelefon 8832 beschrieben.

Tabelle 5: Tasten des Cisco IP-Konferenztelefon 8832


1	LED-Leiste	<p>Zeigt den Anrufstatus an:</p> <ul style="list-style-type: none"> <li>• Grün, leuchtend: Aktiver Anruf</li> <li>• Grün, blinkend: Eingehender Anruf</li> <li>• Grün, blinkend: Gehaltener Anruf</li> <li>• Rot, leuchtend: Stummgeschalteter Anruf</li> </ul>
2	Anschluss für externes Mikrofon	Das Kabel des kabelgebundenen externen Mikrofons wird in diesen Anschluss eingesteckt.
3	<b>Stummschaltleiste</b>	 Schaltet das Mikrofon ein bzw. aus. Wenn das Mikrofon stummgeschaltet ist, leuchtet die LED-Leiste rot.
4	Softkeys	 Zugriff auf Funktionen und Dienste.
5	Navigationsleiste und <b>Auswahltaste</b>	 Ermöglicht Ihnen das Navigieren durch Menüs, das Markieren von Elementen sowie das Auswählen der markierten Elemente.
6	<b>Lautstärke-Taste</b>	 Passt die Lautstärke des Lautsprechers (abgenommen) und des Ruftons (aufgelegt) an. Wenn Sie die Lautstärke ändern, leuchtet die LED-Leiste weiß.

## Kabelgebundenes externes Mikrofon (nur 8832)

Das Cisco IP-Konferenztelefon 8832 unterstützt zwei kabelgebundene externe Mikrofone, die in einem optionalen Kit erhältlich sind. Verwenden Sie die externen Mikrofone in größeren Räumen oder in einem überfüllten Raum. Idealerweise sollten die Mikrofone zwischen 0,91 m (3 Fuß) und 2,1 m (7 Fuß) weit vom Telefon entfernt sein.

**Abbildung 3: Kabelgebundenes externes Mikrofon**

Wenn Sie gerade einen Anruf tätigen, leuchtet die LED für das externe Mikrofon neben der Taste

**Stummschalten**  grün.

Wenn das Mikrofon stummgeschaltet ist, leuchtet die LED rot. Wenn Sie die Taste **Stummschalten** drücken, werden Telefon und externe Mikrofone stummgeschaltet.

#### Verwandte Themen

[Kabelgebundene externe Mikrofone installieren](#), auf Seite 35

## Kabelloses externes Mikrofon (nur 8832)

Cisco IP-Konferenztelefon 8832 unterstützt zwei kabellose externe Mikrofone, die in einem optionalen Kit mit Ladeschale verfügbar sind. Wenn das kabellose Mikrofon zum Laden in die Ladeschale gestellt wird, leuchtet die LED an der Ladeschale weiß.

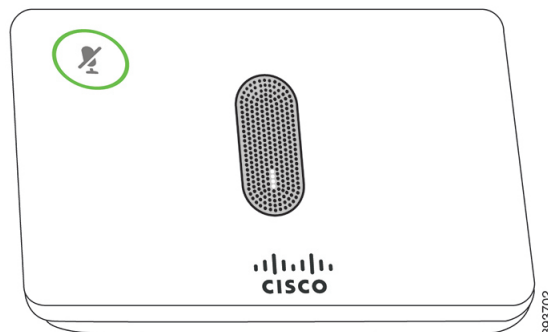
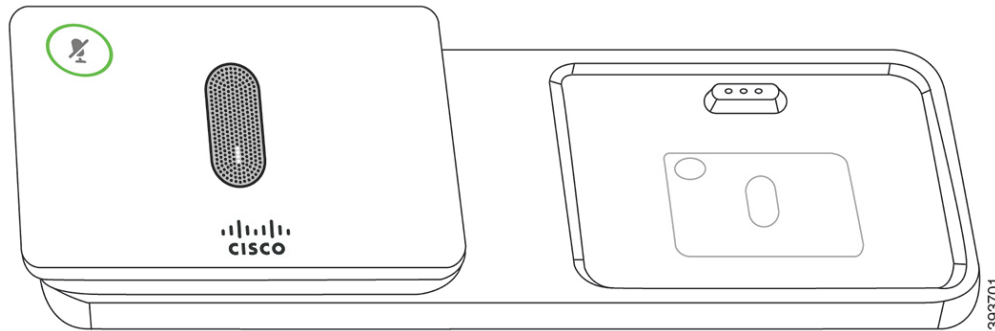

**Abbildung 4: Kabelloses Mikrofon**

Abbildung 5: Kabelloses Mikrofon in der Ladeschale



Wenn vom Konferenztelefon aus gerade ein Anruf getätigt wird, leuchtet das LED für das externe Mikrofon neben der Taste **Stummschalten**  grün.

Wenn das Mikrofon stummgeschaltet ist, leuchtet das LED rot. Wenn Sie die Taste **Stummschalten** drücken, werden Telefon und externe Mikrofone stummgeschaltet.

Wenn das Telefon mit einem kabellosen Mikrofon (z. B. mit dem kabellosen Mikrofon 1) gekoppelt wird und Sie das kabellose Mikrofon mit einem Aufladegerät verbinden, wird durch Drücken des Softkeys **Details anzeigen** der Ladezustand für dieses Mikrofon angezeigt.

Wenn das Telefon mit einem kabellosen Mikrofon gekoppelt wird und Sie ein kabelgebundenes Mikrofon anschließen, wird das kabellose Mikrofon entkoppelt und das Telefon wird mit dem kabelgebundenen Mikrofon gekoppelt. Eine Benachrichtigung wird auf dem Telefonbildschirm mit dem Hinweis angezeigt, dass das kabelgebundene Mikrofon verbunden ist.

#### Verwandte Themen

[Kabellose externe Mikrofone installieren](#), auf Seite 36

[Die Ladeschale des kabellosen Mikrofons installieren](#), auf Seite 37

## Zugehöriges Dokumentationsmaterial

In den folgenden Abschnitten finden Sie zugehörige Informationen.

### Dokumentation für das Cisco IP-Konferenztelefon 8832

Auf der Seite mit [Produkt-Support](#) für die Cisco IP Phone 7800 Series finden Sie Dokumentation für Ihre Sprache, Ihr Telefonmodell und Ihr Anrufsteuerungssystem.

### Dokumentation Cisco Unified Communications Manager

Lesen Sie den *Cisco Unified Communications Manager Dokumentationsleitfaden* und andere Veröffentlichungen für Ihre Cisco Unified Communications Manager-Version. Navigieren Sie zum folgenden Dokumentations-URL:

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



## Dokumentation Cisco Unified Communications Manager Express

Einschlägige Publikationen in Ihrer Sprache, Telefonmodell und Cisco Unified Communications Manager Express-Version festlegen. Navigieren Sie zum folgenden Dokumentations-URL:

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

## Cisco Hosted Collaboration Service – Dokumentation

Lesen Sie den *Cisco Hosted Collaboration Solution Dokumentationsleitfaden* und andere Veröffentlichungen für Ihre Cisco Hosted Collaboration Solution-Version. Navigieren Sie zur folgenden URL:

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

## Dokumentation für Cisco Business Edition 4000

Lesen Sie den *Cisco Business Edition 4000 Dokumentationsleitfaden* und andere Veröffentlichungen für Ihre Cisco Business Edition 4000-Version. Navigieren Sie zur folgenden URL:

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

## Dokumentation, Support und Sicherheitsrichtlinien

Informationen zum Anfordern von Dokumentationsmaterial und Support, zur Erteilung von Feedback zur Dokumentation sowie zu den Sicherheitsrichtlinien und empfohlenen Aliasnamen und allgemeinen Dokumenten von Cisco finden Sie in der monatlichen Veröffentlichung *Neues in der Cisco Produktdokumentation*, in der alle neuen und überarbeiteten technischen Dokumentationen von Cisco aufgeführt sind:

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

Abonnieren Sie *Neuigkeiten bei Cisco Produktdokumentationen* als RSS-Feed (Really Simple Syndication), um alle Neuigkeiten direkt über ein RSS-Programm zu erhalten. Die RSS-Feeds sind ein kostenloser Service. Cisco unterstützt derzeit RSS, Version 2.0.

## Übersicht über die Cisco Produktsicherheit

Dieses Produkt enthält Verschlüsselungsfunktionen und unterliegt den geltenden Gesetzen in den USA oder des jeweiligen Landes bezüglich Import, Export, Weitergabe und Nutzung des Produkts. Die Bereitstellung von Verschlüsselungsprodukten durch Cisco gewährt Dritten nicht das Recht, die Verschlüsselungsfunktionen zu importieren, zu exportieren, weiterzugeben oder zu nutzen. Importeure, Exporteure, Vertriebshändler und Benutzer sind für die Einhaltung aller jeweils geltenden Gesetze verantwortlich. Durch die Verwendung dieses Produkts erklären Sie, alle geltenden Gesetze und Vorschriften einzuhalten. Wenn Sie die geltenden Gesetze nicht einhalten können, müssen Sie das Produkt umgehend zurückgeben.

Weitere Angaben zu den Exportvorschriften der USA finden Sie unter <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>.

# Begriffsunterschiede

In diesem Dokument umfasst der Begriff *Cisco IP-Telefon* das Cisco IP-Konferenztelefon 8832.

Die folgende Tabelle enthält einige der Begriffsunterschiede im *Benutzerhandbuch für das Cisco IP-Konferenztelefon 8832*, im *Administratorhandbuch für das Cisco IP-Konferenztelefon 8832 für Cisco Unified Communications Manager* und in der Dokumentation zu Cisco Unified Communications Manager.

**Tabelle 6: Begriffsunterschiede**

<b>Benutzerhandbuch</b>	<b>Administratorhandbuch</b>
Nachrichtenanzeigen	Briefkastenlampe (MWI)
Voicemail-System	Voicemail-System



# KAPITEL 3

## Technische Details

- [Physische und Umgebungsspezifikationen, auf Seite 17](#)
- [Stromversorgung des Telefons, auf Seite 18](#)
- [Netzwerkprotokolle, auf Seite 20](#)
- [Cisco Unified Communications Manager-Interaktion, auf Seite 22](#)
- [Cisco Unified Communications Manager Express-Interaktion, auf Seite 23](#)
- [Interaktion mit dem Sprachnachrichtensystem, auf Seite 23](#)
- [Konfigurationsdateien für Telefone, auf Seite 24](#)
- [Verhalten des Telefons bei Netzwerküberlastung, auf Seite 24](#)
- [Application Programming Interface, auf Seite 24](#)

## Physische und Umgebungsspezifikationen

Die folgende Tabelle zeigt die physischen Spezifikationen und Umgebungsspezifikationen für das Konferenztelefon.

**Tabelle 7: Physische und Umgebungsspezifikationen**

Spezifikation	Wert oder Bereich
Betriebstemperatur	0 °C bis 40 °C (32 °F bis 104 °F)
Relative Luftfeuchtigkeit beim Betrieb	10 % bis 90 % (nicht kondensierend)
Lagertemperatur	-10 °C bis 60 °C (14 °F bis 140 °F)
Höhe	278 mm (10,9 Zoll)
Breite	278 mm (10,9 Zoll)
Tiefe	61,3 mm (2,4 Zoll)
Gewicht	1852 g (4,07 lb.)
Netzanschluss	IEEE PoE Klasse 3 über einen PoE-Injektor. Das Telefon ist kompatibel mit CDP (Cisco Discovery Protocol) sowie LLDP-PoE (Link Layer Discovery Protocol). Weitere Optionen umfassen einen Nicht-PoE-Injektor, falls die Verbindung über ein LAN erfolgt. Ist ein Cisco IP-Konferenztelefon 8832-Netzteil erforderlich.

Spezifikation	Wert oder Bereich
Sicherheitsfunktionen	Secure Boot
Kabel	USB-C
Abstandsanforderungen	Die Ethernet-Spezifikation setzt voraus, dass die maximale Kabellänge beträgt.

Weitere Informationen finden Sie im *Datenblatt für das Cisco IP-Konferenztelefon 8832*:  
<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html>

## Stromversorgung des Telefons

Das Cisco IP-Konferenztelefon 8832 kann die folgenden Stromquellen nutzen:

- Power-over-Ethernet-(PoE-)Bereitstellung mit PoE-Injektor für Cisco IP-Konferenztelefon 8832
- Nicht-PoE-Ethernet-Bereitstellung mit Nicht-PoE-fähiger Ethernet-Injektor für Cisco IP-Konferenztelefon 8832
- Wi-Fi-Bereitstellung mit einem Cisco IP-Konferenztelefon 8832-Netzteil

**Tabelle 8: Richtlinien zur Stromversorgung des Cisco IP-Konferenztelefon**

Energietyp	Richtlinien
Stromversorgung über PoE: Erfolgt über das am Telefon angeschlossene USB-C-Kabel entweder über PoE-Injektor für Cisco IP-Konferenztelefon 8832 oder Ethernet-Injektor für Cisco IP-Konferenztelefon 8832.	<p>Wenn Sie PoE-Injektor für Cisco IP-Konferenztelefon 8832 oder Ethernet-Injektor für Cisco IP-Konferenztelefon 8832 verwenden, achten Sie darauf, dass der Switch mit einer Notstromversorgung ausgestattet ist, um einen unterbrechungsfreien Betrieb des Telefons sicherzustellen.</p> <p>Stellen Sie sicher, dass die CatOS- oder IOS-Version, die auf dem Switch ausgeführt wird, Ihre geplante Telefonbereitstellung unterstützt. Informationen zur Betriebssystemversion finden Sie in der Dokumentation für den Switch.</p> <p>Wenn Sie ein Telefon installieren, das über PoE betrieben wird, verbinden Sie den Injektor mit dem LAN, bevor Sie das USB-C-Kabel mit dem Telefon verbinden. Wenn Sie ein Telefon entfernen, das PoE verwendet, trennen Sie das USB-C-Kabel vom Telefon, bevor Sie das Netzteil von der Stromversorgung trennen.</p>

Energietyp	Richtlinien
<p>Externe Stromversorgung</p> <ul style="list-style-type: none"> <li>• Nicht-PoE-Ethernet-Bereitstellung mit Nicht-PoE-fähiger Ethernet-Injektor für Cisco IP-Konferenztelefon 8832</li> <li>• Wi-Fi-Bereitstellung mit einem Cisco IP-Konferenztelefon 8832-Netzteil</li> <li>• Nicht-PoE Ethernet-Bereitstellung mit Ethernet-Injektor für Cisco IP-Konferenztelefon 8832 und einem Cisco IP-Konferenztelefon 8832-Netzteil</li> </ul>	<p>Wenn Sie ein Telefon installieren, das über eine externe Stromversorgung betrieben wird, verbinden Sie den Injektor mit der Stromquelle und dem Ethernet, bevor Sie das USB-C-Kabel mit dem Telefon verbinden. Wenn Sie ein Telefon entfernen, das eine externe Stromquelle verwendet, trennen Sie das USB-C-Kabel vom Telefon, bevor Sie das Netzteil von der Stromversorgung trennen.</p>

## Stromausfall

Die Verfügbarkeit der Notfalldienste auf dem Telefon ist nur dann gewährleistet, wenn das Telefon mit Strom versorgt ist. Bei einem Stromausfall können Notrufnummern erst nach Wiederherstellung der Stromzufuhr gewählt werden. Bei einer Unterbrechung der Stromversorgung oder bei einem Stromausfall müssen Sie das Gerät möglicherweise zurücksetzen oder neu konfigurieren, um Notrufnummern wählen zu können.

## Senkung des Stromverbrauchs

Mit dem Energiesparmodus oder EnergyWise-Modus (Power Save Plus) können Sie die Menge der Energie reduzieren, die Cisco IP-Telefon verbraucht.

### Energiesparmodus

Im Energiesparmodus ist die Hintergrundbeleuchtung deaktiviert, wenn das Telefon nicht verwendet wird. Das Telefon verbleibt über die geplante Zeitspanne im Energiesparmodus, oder bis der Benutzer eine beliebige Taste drückt.

### Power Save Plus (EnergyWise)

Cisco IP-Telefon unterstützt den Cisco EnergyWise-Modus (Power Save Plus). Wenn Ihr Netzwerk einen EnergyWise-Controller umfasst (beispielsweise einen Cisco Switch mit aktivierter EnergyWise-Funktion), können Sie diese Telefone so konfigurieren, dass sie basierend auf einem Zeitplan in und aus dem Energiesparmodus wechseln, um den Energieverbrauch weiter zu reduzieren.

Richten Sie die einzelnen Telefone so ein, dass die EnergyWise-Einstellungen aktiviert bzw. deaktiviert werden können. Wenn EnergyWise aktiviert ist, können Sie eine Aus- und Einschaltzeit und auch weitere Parameter konfigurieren. Diese Parameter werden als Teil der XML-Datei für die Telefonkonfiguration an das Telefon gesendet.

**Verwandte Themen**

[Energiesparmodus für Cisco IP-Telefon planen](#), auf Seite 116

[EnergyWise für das Cisco IP-Telefon planen](#), auf Seite 117

# Netzwerkprotokolle

Das Cisco IP-Konferenztelefon 8832 unterstützt mehrere Industriestandard- und Cisco Netzwerkprotokolle, die für die Sprachkommunikation erforderlich sind. Die folgende Tabelle enthält eine Übersicht der Netzwerkprotokolle, die von den Telefonen unterstützt werden.

**Tabelle 9: Auf dem Cisco IP-Konferenztelefon unterstützte Netzwerkprotokolle**

Netzwerkprotokoll	Zweck	Hinweis zur Verwendung
Bootstrap Protocol (BootP)	BootP ermöglicht einem Netzwerkgerät, wie dem Telefon, bestimmte Startinformationen zu erkennen, wie z. B. die IP-Adresse.	—
Cisco Discovery Protocol (CDP)	CDP ist ein Protokoll für die Geräteerkennung, das auf allen Geräten von Cisco ausgeführt wird.  Ein Gerät kann CDP verwenden, um sich für andere Geräte anzukündigen und Informationen über diese Geräte im Netzwerk zu empfangen.	Das Telefon verwendet CDP, um Informationen, beispielsweise Port und QoS-Konfigurationsinformationen, mit dem
Dynamic Host Configuration Protocol (DHCP)	DHCP reserviert und weist IP-Adressen zu Netzwerkgeräten zu.  DHCP ermöglicht, ein IP-Telefon im Netzwerk zu verbinden und zu aktivieren, ohne manuell eine IP-Adresse zuzuordnen oder zusätzliche Netzwerkparameter konfigurieren zu müssen.	DHCP ist standardmäßig aktiviert. Wenn DHCP deaktiviert ist, konfigurieren Sie einen TFTP-Server auf jedem Telefon manuell.  Wir empfehlen, die angepasste DHCP-Option 150 zu konfigurieren, um als Optionswert konfiguriert zu werden. Weitere Informationen finden Sie in den Konfigurationsanweisungen von Cisco Unified Communications Manager.  <b>Hinweis</b> Wenn Sie die Option 150 nicht verwenden, konfigurieren Sie die Option 150 nicht.
Hypertext Transfer Protocol (HTTP)	HTTP ist das Standardprotokoll zum Übertragen von Informationen und Dokumenten im Internet.	Die Telefone nutzen HTTP für XML-Dienste, Berechtigungen und
Hypertext Transfer Protocol Secure (HTTPS)	HTTPS ist eine Kombination der Übertragungsprotokolle HTTP und SSL/TLS, die eine Verschlüsselung und sichere Identifizierung von Servern ermöglicht.	Für Webanwendungen, die HTTP und HTTPS unterstützen, wählen Sie die HTTPS-URL.  Ein Schloss-Symbol zeigt an, ob die Verbindung mit dem Server
IEEE 802.1X	Der IEEE 802.1X-Standard definiert ein Client-/Server-basiertes Zugriffssteuerungs- und Authentifizierungsprotokoll, das verhindert, dass sich nicht autorisierte Clients über öffentliche Ports mit einem LAN verbinden.  Bis der Client authentifiziert ist, erlaubt die 802.1X-Zugriffssteuerung nur den EAPOL-Verkehr (Extensible Authentication Protocol over LAN) über den Port, mit dem der Client verbunden ist. Nach der erfolgreichen Authentifizierung kann der normale Verkehr über den Port weitergeleitet werden.	Das Telefon implementiert den IEEE 802.1X-Standard für die Authentifizierung und EAP-TLS.  Wenn die 802.1X-Authentifizierung auf dem Telefon aktiviert ist, zeigt ein Schloss-Symbol an, ob die Verbindung mit dem Server

Netzwerkprotokoll	Zweck	Hinweis zur Verwendung
Internet Protocol (IP)	IP ist ein Messaging-Protokoll, das Pakete im Netzwerk verarbeitet und sendet.	Um mit IP zu kommunizieren, muss Geräten ein IP-Adressen-, Subnetz- und Gateway-IDs werden (DHCP Configuration Protocol) nutzen. Wenn Sie DHCP zuweisen.  Die Telefone unterstützen IPv6-Adressen. Weitere Informationen zum Unified Communications Manager.
Link Layer Discovery Protocol (LLDP)	LLDP ist ein standardisiertes Netzwerkerkennungsprotokoll (ähnlich wie CDP), das auf einigen Geräten von Cisco und Drittanbietern unterstützt wird.	Das Telefon unterstützt LLDP auf dem PC-Port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED ist eine Erweiterung des LLDP-Standard, der für Sprachprodukte entwickelt wurde.	Das Telefon unterstützt LLDP-MED auf dem SV-Port.  <ul style="list-style-type: none"> <li>• Sprach-VLAN-Konfiguration</li> <li>• Geräteerkennung</li> <li>• Energieverwaltung</li> <li>• Bestandsverwaltung</li> </ul> Weitere Informationen zur Unterstützung von LLDP-MED (LLDP-MED und das Cisco Discovery Protocol) finden Sie unter <a href="https://www.cisco.com/en/US/tech/tk652/tk701/">https://www.cisco.com/en/US/tech/tk652/tk701/</a>
Real-Time Transport Protocol (RTP)	RTP ist ein Standardprotokoll für die Übermittlung von Echtzeit-Daten, beispielsweise interaktive Sprache und Videos, über Datennetze.	Die Telefone verwenden das RTP-Protokoll zum Transport von Medienpaketen zwischen Telefonen und Gateways.
Real-Time Control Protocol (RTCP)	RTCP wird gemeinsam mit RTP genutzt und liefert QoS-Daten (z. B. Jitter-Werte, Latenz, Round-Trip-Verzögerung) von RTP-Datenströmen.	RTCP ist standardmäßig aktiviert.
Session Description Protocol (SDP)	Bei SDP handelt es sich um den Teil des SIP-Protokolls, der festlegt, welche Parameter während einer Verbindung zwischen zwei Endgeräten verfügbar sind. Beim Erstellen von Konferenzen werden nur die SDP-Funktionen verwendet, die von allen an der Konferenz teilnehmenden Endgeräten unterstützt werden.	Normalerweise werden SDP-Funktionen wie Conference-Name, Conference-URL, Conference-Password oder dem Medien-Gateway über den Unified Communications Manager oder dem Medien-Gateway über den Unified Communications Manager können diese Parameter jedoch direkt auf dem Endgerät konfiguriert werden.
Session Initiation Protocol (SIP)	SIP ist der IETF-Standard (Internet Engineering Task Force) für Multimedia-Konferenzen über IP. SIP ist ein ASCII-basiertes Steuerungsprotokoll auf Anwendungsebene (definiert in RFC 3261), das verwendet werden kann, um Anrufe zwischen zwei oder mehr Endpunkten zu initiieren, aufrechtzuerhalten und abzubrechen.	Wie andere VoIP-Protokolle ist SIP ausgelegt, um über IP zu verarbeiten. Die Signalisierung ermöglicht, die Sitzungsverwaltung ermöglicht das Steuern der Sitzungen.
Secure Real-Time Transfer Protocol (SRTP)	SRTP ist eine Erweiterung des RTP Audio-/Videoprofils und stellt die Integrität von RTP- und RTCP-Paketen über Authentifizierung, Integrität und Verschlüsselung der Medienpakete zwischen zwei Endpunkten sicher.	Die Telefone verwenden SRTP zur Medienverschlüsselung.

Netzwerkprotokoll	Zweck	Hinweis zur Verwendung
Transmission Control Protocol (TCP)	TCP ist ein verbindungsorientiertes Transportprotokoll.	Die Telefone nutzen TCP für die Verbindung mit den XML-Diensten.
Transport Layer Security (TLS)	TLS ist ein Standardprotokoll zum Schützen und Authentifizieren der Kommunikation.	Bei implementierter Sicherheit verwenden die Telefone Cisco Unified Communications Manager. Weitere Informationen finden Sie in der Dokumentation für Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP ermöglicht die Dateiübertragung über das Netzwerk. Auf dem Telefon ermöglicht TFTP das Abrufen einer für den Telefontyp spezifischen Konfigurationsdatei.	TFTP erfordert einen TFTP-Server im Netzwerk, oder einen anderen TFTP-Server, als den vom DHCP-Server über das Menü Netzwerkconfiguration auf dem Telefon angegeben. Weitere Informationen finden Sie in der Dokumentation für Cisco Unified Communications Manager.
User Datagram Protocol (UDP)	UDP ist ein verbindungsloses Protokoll für die Übertragung von Datenpaketen.	Dieses Protokoll wird ausschließlich für RTP-Datenpakete verwendet und wird nicht unterstützt.

**Verwandte Themen**

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Cisco Unified Communications Manager-Interaktion

Cisco Unified Communications Manager ist ein offenes Anrufverarbeitungssystem, das dem Industriestandard entspricht. Die Cisco Unified Communications Manager-Software startet und bricht Anrufe zwischen Telefonen ab, indem herkömmliche PBX-Funktionen im IP-Firmennetzwerk integriert werden. Cisco Unified Communications Manager verwaltet die Komponenten des Telefonie-Systems, beispielsweise die Telefone, die Gateways für den Zugriff und die für Funktionen erforderlichen Ressourcen, beispielsweise Konferenzanrufe und Routenplanung. Cisco Unified Communications Manager stellt auch Folgendes bereit:

- Firmware für Telefone
- Certificate Trust List-(CTL-) und Identity Trust List-(ITL-)Dateien, die TFTP- und HTTP-Dienste verwenden
- Telefonregistrierung
- Der Anruf wird beibehalten, damit eine Mediensitzung fortgesetzt wird, wenn das Signal zwischen Cisco Unified Communications Manager und einem Telefon unterbrochen wird.

Weitere Informationen zum Konfigurieren von Cisco Unified Communications Manager für Telefone, die in diesem Kapitel beschrieben werden, finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.



**Hinweis** Wenn das Telefonmodell, das Sie konfigurieren möchten, nicht in der Dropdown-Liste Telefontyp in der Cisco Unified Communications Manager-Verwaltung angezeigt wird, laden Sie das neueste Gerätepaket für Ihre Version von Cisco Unified Communications Manager von Cisco.com herunter.

**Verwandte Themen**

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14



# Cisco Unified Communications Manager Express-Interaktion

Wenn Ihr Telefon mit Cisco Unified Communications Manager Express (Unified CME) verwendet wird, muss es in den CME-Modus wechseln.

Wenn ein Benutzer die Konferenzfunktion aufruft, ermöglicht das Tag dem Telefon, entweder eine lokale oder eine Netzwerk-Hardware-Konferenzbrücke zu verwenden.

Die Telefone bieten keine Unterstützung für folgende Aktionen:

- Übergabe: Wird nur im Übergabeszenario für verbundene Anrufe unterstützt.
- Konferenz: Wird nur im Übergabeszenario für verbundene Anrufe unterstützt.
- Zusammenführen: Wird bei Verwendung der Konferenztaste oder bei Hookflash-Zugriff unterstützt.
- Halten: Wird bei Verwendung der Halten-Taste unterstützt.
- Aufschalten und Zusammenführen: Wird nicht unterstützt.
- Direkte Übergabe: Wird nicht unterstützt.
- Auswählen – wird nicht unterstützt.

Die Benutzer können nicht über verschiedene Leitungen hinweg Konferenzen erstellen und Anrufe übergeben.

Unified CME unterstützt Intercom-Anrufe, was auch als Whisper-Paging bezeichnet wird. Jedoch wird die Seite vom Telefon bei Anrufen abgelehnt.

## Interaktion mit dem Sprachnachrichtensystem

In Cisco Unified Communications Manager können Sie verschiedene Sprachnachrichtensysteme integrieren, u. a. das Sprachnachrichtensystem Cisco Unity Connection. Weil die Integration mit vielen verschiedenen Systemen möglich ist, müssen Sie die Benutzer über den Umgang mit dem bei Ihnen vorhandenen System informieren.

Damit ein Benutzer an Voicemail übergeben kann, richten Sie ein \*xxxxx Wählmuster ein und konfigurieren Sie es als "Alle Anrufe an Voicemail umleiten". Weitere Informationen finden Sie in der Dokumentation zu Cisco Unified Communications Manager.

Sie müssen jedem Benutzer folgende Informationen zur Verfügung stellen:

- Wie der Zugriff auf das Konto des Sprachnachrichtensystems erfolgt.  
Stellen Sie sicher, dass die Taste „Nachrichten“ auf dem Cisco IP-Telefon in Cisco Unified Communications Manager konfiguriert wurde.
- Wie das Initialkennwort für den Zugriff auf das Sprachnachrichtensystem lautet.  
Konfigurieren Sie für das Sprachnachrichtensystem ein Standardkennwort für alle Benutzer.
- Wie das Telefon anzeigt, dass Sprachnachrichten vorhanden sind.  
Verwenden Sie Cisco Unified Communications Manager, um eine Nachrichtenanzeigemethode (MWI) einzurichten.

# Konfigurationsdateien für Telefone

Die Konfigurationsdateien für Telefone sind auf dem TFTP-Server gespeichert und definieren die für die Verbindung mit dem Cisco Unified Communications Manager benötigten Parameter. Generell wird die Konfigurationsdatei eines Telefons immer dann automatisch geändert, wenn Sie im Cisco Unified Communications Manager eine Änderung vornehmen, die ein Zurücksetzen des Telefons erforderlich macht.

Außerdem enthalten Konfigurationsdateien auch Informationen zum geladenen Image, das auf dem Telefon ausgeführt werden sollte. Wenn diese Abbildinformationen nicht mit dem tatsächlich auf dem Telefon geladenen Image übereinstimmen, wird vom Telefon eine Anfrage an den TFTP-Server zur Bereitstellung der erforderlichen Softwaredateien gesendet.

Wenn Sie in Cisco Unified Communications Manager-Verwaltung sicherheitsrelevante Einstellungen konfigurieren, sind in der Telefonkonfigurationsdatei auch vertrauliche Informationen enthalten. Damit die Konfigurationsdatei entsprechend ihrer Vertraulichkeit geschützt ist, müssen Sie die Datei so konfigurieren, dass eine Verschlüsselung erfolgt. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager. Bei jedem Neustart und anschließender Registrierung bei Cisco Unified Communications Manager rufen die Telefone eine Konfigurationsdatei ab.

Wenn die folgenden drei Bedingungen gegeben sind, greift ein Telefon bei diesem Vorgang auf die auf dem TFTP-Server befindliche Standardkonfigurationsdatei `XmlDefault.cnf.xml` zu:

- Sie haben die automatische Registrierung aktiviert in Cisco Unified Communications Manager
- Das Telefon wurde nicht zur Cisco Unified Communications Manager-Datenbank hinzugefügt.
- Das Telefon registriert sich zum ersten Mal.

# Verhalten des Telefons bei Netzwerküberlastung

Alles, was zu einer Verschlechterung der Netzwerkleistung führt, kann auch die Audioqualität des Telefons beeinträchtigen. In manchen Fällen kann es sogar zu einem Abbruch des Telefonats kommen. Eine Netzwerküberlastung kann unter anderem von folgenden Aktivitäten verursacht werden:

- Administrative Aufgaben, beispielsweise einen internen Port- oder Sicherheits-Scan.
- Netzwerkangriffe, beispielsweise ein Denial-of-Service-Angriff.

# Application Programming Interface

Cisco unterstützt die Nutzung der Telefon-API durch Drittanbieter-Anwendungen, die vom Entwickler der Drittanbieter-Anwendung über Cisco getestet und zertifiziert wurden. Alle Telefonprobleme im Zusammenhang mit einer Interaktion einer nicht zertifizierten Anwendung müssen vom Drittanbieter behoben werden und werden nicht von Cisco bearbeitet.

Einzelheiten zum Support-Modell für von Cisco zertifizierte Drittanbieter-Anwendungen/-Lösungen finden Sie auf der Website des [Cisco Solution Partner-Programm](#).



## TEIL II

# Cisco IP-Konferenztelefon – Installation

- [Installation des Telefons, auf Seite 27](#)
- [Cisco Unified Communications Manager – Telefoninstallation, auf Seite 57](#)
- [Verwaltung des Selbstservice-Portals, auf Seite 71](#)





## KAPITEL 4

# Installation des Telefons

---

- Netzwerkkonfiguration überprüfen, auf Seite 27
- Aktivierungscode-Integration für lokale Telefone, auf Seite 28
- Aktivierungscode-Integration mit mobilem und Remotezugriff, auf Seite 29
- Aktivieren der automatischen Registrierung für Telefone, auf Seite 29
- Daisy-Chain-Modus, auf Seite 31
- Installation des Konferenztelefons, auf Seite 31
- Telefone über Menüs konfigurieren, auf Seite 40
- Wireless-LAN über das Telefon aktivieren, auf Seite 47
- Telefonstart überprüfen, auf Seite 54
- Telefonmodell eines Benutzers ändern, auf Seite 54

## Netzwerkkonfiguration überprüfen

Wenn ein neues IP-Telefonsystem bereitgestellt wird, müssen die System- und Netzwerkadministratoren mehrere Konfigurationsaufgaben ausführen, um das Netzwerk für den IP-Telefonservice vorzubereiten. Weitere Informationen und eine Prüfliste für die Konfiguration eines Cisco IP-Telefon-Telefonienetzwerks finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Damit das Telefon als Endpunkt im Netzwerk funktioniert, muss das Netzwerk bestimmte Anforderungen erfüllen. Zu den Anforderungen gehört eine angemessene Bandbreite. Die Telefone benötigen mehr Bandbreite als die empfohlenen 32 Kbit/s, wenn sie sich beim Cisco Unified Communications Manager registrieren. Berücksichtigen Sie diese höhere Bandbreitenanforderung, wenn Sie Ihre QoS-Bandbreite konfigurieren. Weitere Informationen finden Sie in *Cisco Collaboration System 12.x Solution Reference Network Designs (SRND)* oder höher ([https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/srnd/collab12/collab12.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html)).



---

**Hinweis** Das Telefon zeigt das Datum und die Uhrzeit von Cisco Unified Communications Manager an. Die auf dem Telefon angezeigte Uhrzeit kann von der Zeit von Cisco Unified Communications Manager um bis zu 10 Sekunden abweichen.

---

### Prozedur

#### Schritt 1

Konfigurieren Sie ein VoIP-Netzwerk, um die folgenden Anforderungen zu erfüllen:

- VoIP ist auf Routern und Gateways konfiguriert.
- Cisco Unified Communications Manager ist im Netzwerk installiert und konfiguriert, um die Anrufverarbeitung vorzunehmen.

**Schritt 2**

Konfigurieren Sie das Netzwerk, um eine der folgenden Komponenten zu unterstützen:

- DHCP-Unterstützung
- Manuelle Zuordnung der IP-Adresse, des Gateways und der Subnetzmaske

---

**Verwandte Themen**

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Aktivierungscode-Integration für lokale Telefone

Sie können die Integration des Aktivierungscodes verwenden, um schnell neue Telefone ohne automatische Registrierung einzurichten. Bei diesem Ansatz steuern Sie den Integrationsprozess des Telefons mit einem der folgenden Tools:

- Cisco Unified Communications Bulk Administration Tool (BAT)
- Cisco Unified Communications Manager-Administratoroberfläche
- Administrative XML Web Service (AXL)

Aktivieren Sie dieses Feature im Abschnitt **Geräteinformationen** der Telefonkonfigurationsseite. Wählen Sie **Aktivierungscode für Onboarding erfordern**, wenn Sie dieses Feature für ein einzelnes, lokales Telefon übernehmen möchten.

Benutzer müssen einen Aktivierungscode eingeben, bevor ihre Telefone registriert werden können. Die Integration des Aktivierungscodes kann auf einzelne Telefone, eine Gruppe von Telefonen oder in einem gesamten Netzwerk angewendet werden.

Dies stellt eine einfache Möglichkeit für Benutzer dar, ihre Telefone zu integrieren, da sie nur einen aus 16 Ziffern bestehenden Aktivierungscode eingeben müssen. Codes werden manuell oder mit einem QR-Code eingegeben, falls das Telefon eine Videokamera besitzt. Wir empfehlen Ihnen, eine sichere Methode zu verwenden, um Benutzern diese Informationen zur Verfügung zu stellen. Wenn ein Benutzer jedoch einem Telefon zugewiesen ist, sind diese Informationen im Selbsthilfe-Portal verfügbar. Das Auditprotokoll erstellt einen Eintrag, wenn ein Benutzer über das Portal auf den Code zugreift.

Aktivierungscodes können nur einmal verwendet werden, und sie laufen nach einer Woche standardmäßig ab. Wenn ein Code abgelaufen ist, müssen Sie dem Benutzer einen neuen bereitstellen.

Sie werden feststellen, dass dieser Ansatz eine einfache Möglichkeit bietet, um Ihr Netzwerk zu sichern, da ein Telefon erst registriert werden kann, wenn das Manufacturing Installed Certificate (MIC) und der Aktivierungscode verifiziert wurden. Mit dieser Methode können Sie ganz praktisch eine Massen-Integration der Telefone durchführen, da das Tool nicht für die automatisch registrierte Telefonunterstützung oder die automatische Registrierung verwendet wird. Die Rate für die Integration beträgt ein Telefon pro Sekunde oder ungefähr 3600 Telefone pro Stunde. Telefone können mit der Cisco Unified Communications Manager-Verwaltung mit Administrative XML Web Service (AXL) oder BAT hinzugefügt werden.

Vorhandene Telefone zurücksetzen, nachdem Sie für die Integration des Aktivierungscodes konfiguriert wurden. Sie werden erst registriert, wenn der Aktivierungscode eingegeben und der MIC des Telefons verifiziert wurde. Informieren Sie die aktuellen Benutzer darüber, dass Sie zur Integration des Aktivierungscodes wechseln, bevor Sie diese Methode implementieren.

Weitere Informationen hierzu finden Sie im *Administratorhandbuch für Cisco Unified Communications Manager und IM sowie Präsenzservice Version 12.0(1)* oder höher.

## Aktivierungscode-Integration mit mobilem und Remotezugriff

Sie können die Aktivierungscode-Integration mit mobilem und Remotezugriff bei der Bereitstellung von Cisco IP-Telefonen für Remote-Benutzer verwenden. Diese Funktion ist eine sichere Methode, um nicht lokale Telefone bereitzustellen, wenn keine automatische Registrierung erforderlich ist. Sie können ein Telefon jedoch so konfigurieren, dass bei der Verwendung im Büro die automatische Registrierung erfolgt und bei der Verwendung außerhalb der Räumlichkeiten die Aktivierungscode-Integration verwendet wird. Diese Funktion ähnelt der Aktivierungscode-Integration für lokale Telefone, stellt aber auch für nicht lokale Telefone einen Aktivierungscode bereit.

Die Aktivierungscode-Integration für mobilen und Remotezugriff erfordert Cisco Unified Communications Manager 12.5(1)SU1 oder höher und Cisco Expressway X12.5 oder höher. Smart Licensing sollte ebenfalls aktiviert sein.

Sie können diese Funktion in der Cisco Unified Communications Manager Administration aktivieren, beachten Sie jedoch Folgendes:

- Aktivieren Sie dieses Feature im Abschnitt **Geräteinformationen** der Telefonkonfigurationsseite.
- Wählen Sie **Aktivierungscode für Onboarding erfordern**, wenn Sie dieses Feature nur für ein einzelnes, lokales Telefon übernehmen möchten.
- Wählen Sie **Aktivierungscode über MRA zulassen** und **Aktivierungscode für Onboarding erfordern** aus, wenn Sie die Aktivierungscode-Integration für ein einzelnes nicht lokales Telefon verwenden möchten. Wenn es sich um ein lokales Telefon handelt, wechselt es in den Modus für mobilen und Remotezugriff und verwendet das Expressway. Wenn das Telefon das Expressway nicht erreichen kann, wird es erst registriert, wenn es sich außerhalb der Räumlichkeiten befindet.

Weitere Informationen finden Sie in den folgenden Dokumenten:

- *Administratorhandbuch für Cisco Unified Communications Manager und IM sowie Präsenzservice Version 12.0(1)*
- *Mobiler und Remotezugriff über Cisco Expressway* für Cisco Expressway X12.5 oder höher

## Aktivieren der automatischen Registrierung für Telefone

Cisco IP-Telefon erfordert, dass Anrufe von Cisco Unified Communications Manager verarbeitet werden. Lesen Sie die Dokumentation für Ihre Version von Cisco Unified Communications Manager oder die kontextbezogene Hilfe in der Cisco Unified Communications Manager-Verwaltung, um sicherzustellen, dass Cisco Unified Communications Manager ordnungsgemäß konfiguriert ist, um das Telefon zu verwalten und Anrufe richtig weiterzuleiten und zu verarbeiten.

Bevor Sie Cisco IP-Telefone installieren, müssen Sie die Methode auswählen, mit der Telefone zur Cisco Unified Communications Manager-Datenbank hinzugefügt werden.

Wenn Sie die automatische Registrierung aktivieren, bevor Sie die Telefone installieren, können Sie:

- Telefone hinzufügen, ohne zuerst die MAC-Adressen von den Telefonen ermitteln zu müssen.
- Cisco IP-Telefone automatisch zur Cisco Unified Communications Manager-Datenbank hinzufügen, wenn Sie das Telefon physisch mit dem IP-Telefonnetzwerk verbinden. Während der automatischen Registrierung weist Cisco Unified Communications Manager dem Telefon die nächste verfügbare Verzeichnisnummer zu.
- Telefone schnell in der Cisco Unified Communications Manager-Datenbank eingeben und die Einstellungen in Cisco Unified Communications Manager ändern, beispielsweise die Verzeichnisnummern.
- automatisch registrierte Telefone an neue Standorte verlegen und verschiedenen Gerätepools zuweisen, ohne die Verzeichnisnummern zu beeinflussen.

Die automatische Registrierung ist standardmäßig deaktiviert. Möglicherweise möchten Sie die automatische Registrierung nicht verwenden, wenn Sie dem Telefon eine bestimmte Verzeichnisnummer zuweisen oder eine sichere Verbindung mit Cisco Unified Communications Manager nutzen. Weitere Informationen zur automatischen Registrierung finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager. Wenn Sie das Cluster über den Cisco CTL-Client für den gemischten Modus konfigurieren, wird die Autoregistrierung automatisch deaktiviert. Sie können Sie jedoch aktivieren. Wenn Sie den Cluster über den Cisco CTL-Client für den nicht sicheren Modus konfigurieren, wird die automatische Registrierung nicht aktiviert.

Mit der automatischen Registrierung und TAPS (Tool for AutoRegistered Phones Support) können Sie Telefone hinzufügen, ohne die MAC-Adressen der Telefone zu benötigen.

TAPS funktioniert mit BAT (Bulk Administration Tool), um mehrere Telefone zu aktualisieren, die bereits mit Dummy-MAC-Adressen zur Cisco Unified Communications Manager-Datenbank hinzugefügt wurden. Verwenden Sie TAPS, um die MAC-Adressen zu aktualisieren und vordefinierte Konfigurationen für Telefone herunterzuladen.

Cisco empfiehlt, mit der automatischen Registrierung und TAPS weniger als 100 Telefone zu einem Netzwerk hinzuzufügen. Um mehr als 100 Telefone zum Netzwerk hinzuzufügen, verwenden Sie BAT.

Um TAPS zu implementieren, wählen Sie eine TAPS-Verzeichnisnummer und folgen Sie den Anweisungen. Nachdem der Prozess abgeschlossen wurde, enthält das Telefon die Verzeichnisnummer und andere Einstellungen und wird in der Cisco Unified Communications Manager-Verwaltung mit der korrekten MAC-Adresse aktualisiert.

Stellen Sie sicher, dass die automatische Registrierung aktiviert und in der Cisco Unified Communications Manager-Verwaltung richtig konfiguriert ist, bevor Sie ein Cisco IP-Telefon mit dem Netzwerk verbinden. Weitere Informationen zum Konfigurieren der automatischen Registrierung finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Die automatische Registrierung muss in der Cisco Unified Communications Manager-Verwaltung aktiviert werden, damit TAPS funktioniert.

## Prozedur

### Schritt 1

Klicken Sie in der Cisco Unified Communications Manager-Verwaltung auf **System > Cisco Unified CM**.

### Schritt 2

Klicken Sie auf **Suchen**, und wählen Sie den erforderlichen Server aus.



- Schritt 3** Konfigurieren Sie diese Felder unter **Automatische Registrierungsinformationen**.
- **Universal-Gerätevorlage**
  - **Universal-Leitungsvorlage**
  - **Startverzeichnisnummer**
  - **Endverzeichnisnummer**
- Schritt 4** Deaktivieren Sie das Kontrollkästchen **Automatische Registrierung in diesem Cisco Unified Communications Manager deaktiviert**.
- Schritt 5** Klicken Sie auf **Speichern**.
- Schritt 6** Klicken Sie auf **Konfiguration übernehmen**.
- 

## Daisy-Chain-Modus

Sie können zwei Konferenztelefone mit Smart-Adapter und die USB-C-Kabel, die im Daisy-Chain-Kit bereitgestellt werden, anschließen, um die Audioabdeckung in einem Raum zu erweitern.

Im Daisy-Chain-Modus werden beide Einheiten durch den Smart-Adapter mit Strom versorgt, der an ein Netzteil angeschlossen ist. Sie können nur ein externes Mikrofon pro Einheit verwenden. Sie können entweder zwei kabelgebundene Mikrofone für die Geräte oder zwei kabellose Mikrofone für die Geräte verwenden, aber keine Kombination aus beiden Mikrofonen. Wenn ein kabelgebundenes Mikrofon mit einem der Geräte verbunden ist, werden alle drahtlosen Mikrofone, die am selben Gerät angeschlossen sind, entkoppelt. Bei einem aktiven Anruf werden die LEDs und die Menüoptionen auf dem Telefonbildschirm beider Geräte synchronisiert.

### Verwandte Themen

[Konferenztelefon im Daisy-Chain-Modus installieren](#), auf Seite 38

[Ein Telefon im Daisy-Chain-Modus funktioniert nicht](#), auf Seite 172

## Installation des Konferenztelefons

Nach dem Verbinden des Telefons mit dem Netzwerk wird das Telefon gestartet, und das Gerät wird bei Cisco Unified Communications Manager registriert. Wenn Sie den DHCP-Dienst deaktivieren, müssen Sie die Netzwerkeinstellungen auf dem Telefon konfigurieren.

Wenn Sie die automatische Registrierung verwendet haben, müssen Sie bestimmte Konfigurationsinformationen für das Telefon aktualisieren, um beispielsweise einem Benutzer ein Telefon zuzuweisen und die Tastentabelle oder die Verzeichnisnummer zu ändern.

Wenn das Telefon verbunden ist, bestimmt es, ob eine neue Firmware-Version auf dem Telefon installiert werden soll.

Lesen Sie sich [Konferenztelefon im Daisy-Chain-Modus installieren, auf Seite 38](#) durch, falls Sie das Konferenztelefon im Daisy-Chain-Modus verwenden.

## Vorbereitungen

Stellen Sie sicher, dass Sie die neueste Firmware-Version auf Ihrem Cisco Unified Communications Manager installiert haben. Suchen Sie hier nach aktualisierten Gerätepaketen:

[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](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)

## Prozedur

---

### Schritt 1

Wählen Sie die Stromquelle für das Telefon aus:

- Power-over-Ethernet-(PoE-)Bereitstellung mit PoE-Injektor für Cisco IP-Konferenztelefon 8832
- Nicht-PoE-Ethernet-Bereitstellung mit Nicht-PoE-fähiger Ethernet-Injektor für Cisco IP-Konferenztelefon 8832
- Wi-Fi-Bereitstellung mit einem Cisco IP-Konferenztelefon 8832-Netzteil

Weitere Informationen finden Sie unter [Ihr Konferenztelefon mit Energie versorgen, auf Seite 33](#).

### Schritt 2

Schließen Sie das Telefon am Switch an.

- Wenn Sie PoE verwenden:
  1. Verbinden Sie das Ethernet-Kabel mit dem LAN-Port.
  2. Schließen Sie das andere Ende des Ethernet-Kabels entweder an PoE-Injektor für Cisco IP-Konferenztelefon 8832 oder Ethernet-Injektor für Cisco IP-Konferenztelefon 8832 an.
  3. Verbinden Sie den Injektor mit einem USB-C-Kabel mit dem Konferenztelefon.
- Wenn Sie PoE nicht verwenden:
  1. Wenn Sie Ethernet-Injektor für Cisco IP-Konferenztelefon 8832 verwenden, stecken Sie das Netzteil in die Steckdose.
  2. Verbinden Sie das Netzteil mit einem USB-C-Kabel mit dem Ethernet-Injektor.  
ODER  
Wenn Sie Nicht-PoE-fähiger Ethernet-Injektor für Cisco IP-Konferenztelefon 8832 verwenden, stecken Sie es in die Steckdose.
  3. Schließen Sie das Ethernet-Kabel am Nicht-PoE-Ethernet-Injektor oder am Ethernet-Injektor an.
  4. Verbinden Sie das Ethernet-Kabel mit dem LAN-Port.
  5. Verbinden Sie den Nicht-PoE-Ethernet-Injektor oder den Ethernet-Injektor mit einem USB-C-Kabel mit dem Konferenztelefon.
- Bei Verwendung von Wi-Fi:
  1. Stecken Sie das Cisco IP-Konferenztelefon 8832-Netzteil in die Steckdose.
  2. Verbinden Sie das Netzteil mit einem USB-C-Kabel mit dem Konferenztelefon.

**Hinweis** Anstelle des Netzteils können Sie den Nicht-PoE-Ethernet-Injektor für die Stromversorgung des Telefons verwenden. Sie müssen jedoch das LAN-Kabel abziehen. Das Telefon wird nur über Wi-Fi verbunden, wenn die Ethernet-Verbindung nicht verfügbar ist.

- Schritt 3** Überwachen Sie den Startprozess des Telefons. Dieser Schritt stellt sicher, dass das Telefon richtig konfiguriert ist.
- Schritt 4** Wenn Sie die automatische Registrierung nicht verwenden, konfigurieren Sie die Sicherheitseinstellungen auf dem Telefon manuell.
- Schritt 5** Lassen Sie zu, dass das Telefon auf das aktuelle Firmware-Image aktualisiert wird, das auf Ihrem Cisco Unified Communications Manager gespeichert ist.
- Schritt 6** Tätigen Sie mit dem Telefon Anrufe, um sicherzustellen, dass das Telefon richtig funktioniert.
- Schritt 7** Informieren Sie die Benutzer über die Verwendung der Telefone und die Konfiguration der Telefonoptionen. Dieser Schritt stellt sicher, dass die Benutzer hinreichend informiert sind, um ihr Cisco IP-Telefon richtig zu nutzen.

---

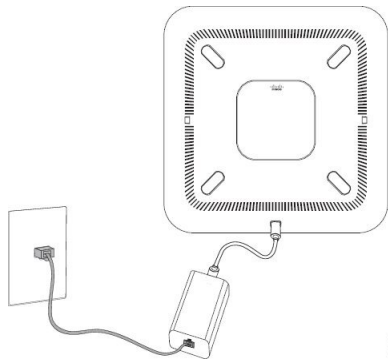
## Ihr Konferenztelefon mit Energie versorgen

Ihr Konferenztelefon muss über eine der folgenden Quellen mit Energie versorgt werden:

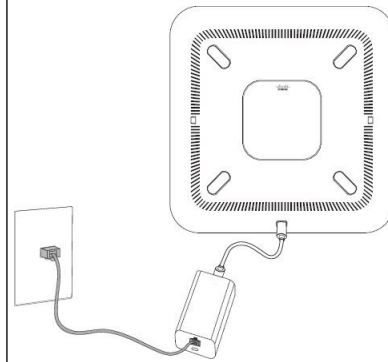
- Power over Ethernet (PoE)
  - Nordamerika
    - PoE-Injektor für Cisco IP-Konferenztelefon 8832
    - Ethernet-Injektor für Cisco IP-Konferenztelefon 8832
  - Außerhalb von Nordamerika: PoE-Injektor für Cisco IP-Konferenztelefon 8832
- Nicht-PoE-Ethernet
  - Nordamerika
    - Nicht-PoE-fähiger Ethernet-Injektor für Cisco IP-Konferenztelefon 8832
    - Ethernet-Injektor für Cisco IP-Konferenztelefon 8832 mit einem Cisco IP-Konferenztelefon 8832-Netzteil, das an eine Steckdose angeschlossen ist.
  - Außerhalb von Nordamerika: Nicht-PoE-fähiger Ethernet-Injektor für Cisco IP-Konferenztelefon 8832
- Wi-Fi: Verwenden Sie das Cisco IP-Konferenztelefon 8832-Netzteil, das an eine Steckdose angeschlossen ist.

### *Abbildung 6: PoE-Stromversorgungsoptionen für Konferenztelefone*

Die folgende Abbildung zeigt die zwei Optionen für die PoE-Stromversorgung.



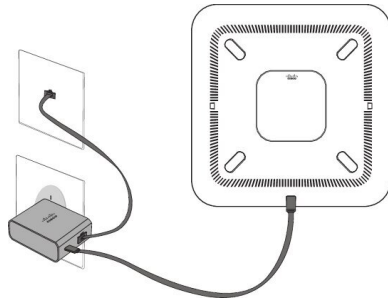
PoE-Injektor für Cisco IP-Konferenztelefon 8832 mit Option zur PoE-Stromversorgung



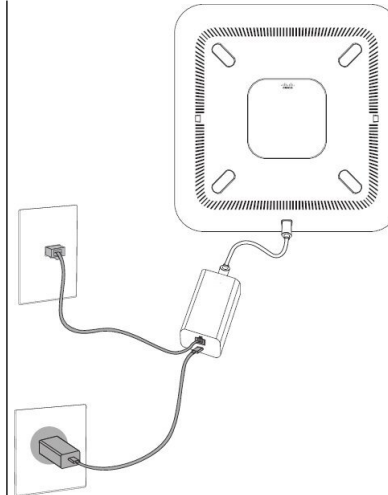
Ethernet-Injektor für Cisco IP-Konferenztelefon 8832 mit Option zur PoE-Stromversorgung

**Abbildung 7: Ethernet-Stromversorgungsoptionen für Konferenztelefone**

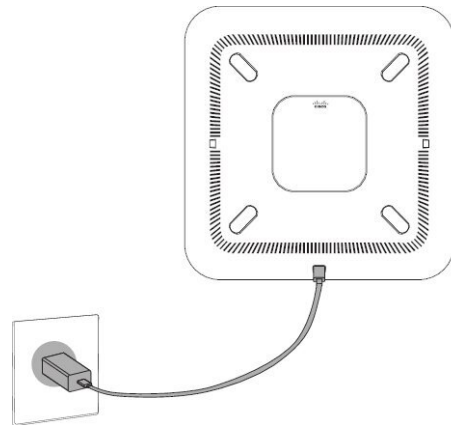
Die folgende Abbildung zeigt die Stromversorgungsoptionen für Ethernet an.



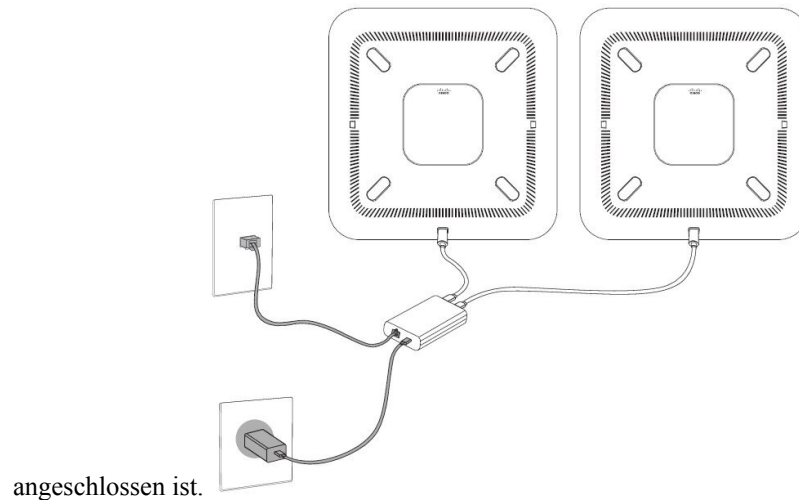
Nicht-PoE-fähiger Ethernet-Injektor für Cisco IP-Konferenztelefon 8832 mit Ethernet-Stromversorgungsoption



Ethernet-Injektor für Cisco IP-Konferenztelefon 8832 mit Ethernet-Stromversorgungsoption

**Abbildung 8: Stromversorgungsoption für Konferenztelefone bei Verbindung mit einem Wi-Fi-Netzwerk****Abbildung 9: Stromversorgungsoption im Daisy-Chain-Modus für Konferenztelefone**

Die folgende Abbildung zeigt die Stromversorgungsoption an, wenn das Telefon im Daisy-Chain-Modus



angeschlossen ist.

## Kabelgebundene externe Mikrofone installieren

Das Telefon unterstützt ein optionales Kit mit zwei kabelgebundenen externen Mikrofonen. Sie können die Mikrofone in einer Entfernung von bis zu 2,13 m (7 Fuß) vom Telefon aufstellen. Idealerweise sollten die Mikrofone zwischen 0,91 m (3 Fuß) und 2,1 m (7 Fuß) weit vom Telefon entfernt sein.

### Prozedur

#### Schritt 1

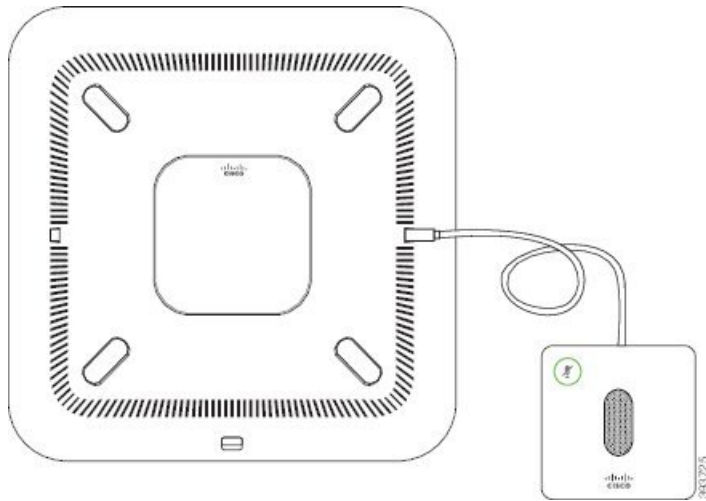
Stecken Sie das Mikrofonkabel in den seitlichen Anschluss des Telefons ein.

#### Schritt 2

Verlegen Sie das Mikrofonkabel bis zur gewünschten Position.

Die folgende Abbildung zeigt die Installation eines kabelgebundenen externen Mikrofons.

Abbildung 10: Installation eines kabelgebundenen externen Mikrofons



## Kabellose externe Mikrofone installieren

Das Konferenztelefon bietet die Möglichkeit zum Anschluss von zwei kabellosen externen Mikrofonen.



**Hinweis** Sie müssen entweder zwei kabelgebundene oder zwei kabellose Mikrofone bei dem Telefon verwenden, jedoch keine Kombination aus beiden.

Wenn vom Telefon aus gerade ein Anruf getätigt wird, leuchtet die LED am externen Mikrofon grün. Zum Stummschalten des externen Mikrofons drücken Sie die Taste **Stumm**. Wenn das Mikrofon stummgeschaltet ist, leuchtet das LED rot. Wenn der Akku im Mikrofon einen niedrigen Ladestand hat, blinkt die LED für den Akkustand schnell.

### Vorbereitungen

Entfernen Sie die kabelgebundenen externen Mikrofone, bevor Sie kabellose externe Mikrofone installieren. Sie können nicht gleichzeitig kabellose und kabelgebundene externe Mikrofone verwenden.

### Prozedur

- Schritt 1** Stellen Sie die Tischmontageplatte an der Position auf die Tischoberfläche, an der Sie das Mikrofon aufstellen möchten.
- Schritt 2** Entfernen Sie die Schutzfolie des doppelseitigen Klebebands auf der Unterseite der Tischmontageplatte. Kleben Sie die Tischmontageplatte auf die Tischoberfläche.
- Schritt 3** Bringen Sie das Mikrofon auf der Tischmontageplatte an. Im Mikrofon sind Magneten eingebettet, um das Gerät in der Halterung zu befestigen.

Sie können das Mikrofon bewegen und die Tischhalterung bei Bedarf an einer anderen Stelle der Tischoberfläche anbringen. Gehen Sie beim Verschieben vorsichtig vor, um das Gerät nicht zu beschädigen.

---

**Verwandte Themen**

[Kabelloses externes Mikrofon \(nur 8832\)](#), auf Seite 13

[Die Ladeschale des kabellosen Mikrofons installieren](#), auf Seite 37

## Die Ladeschale des kabellosen Mikrofons installieren

Sie verwenden die Ladeschale, um den Akku des kabellosen Mikrofons aufzuladen.

**Prozedur****Schritt 1**

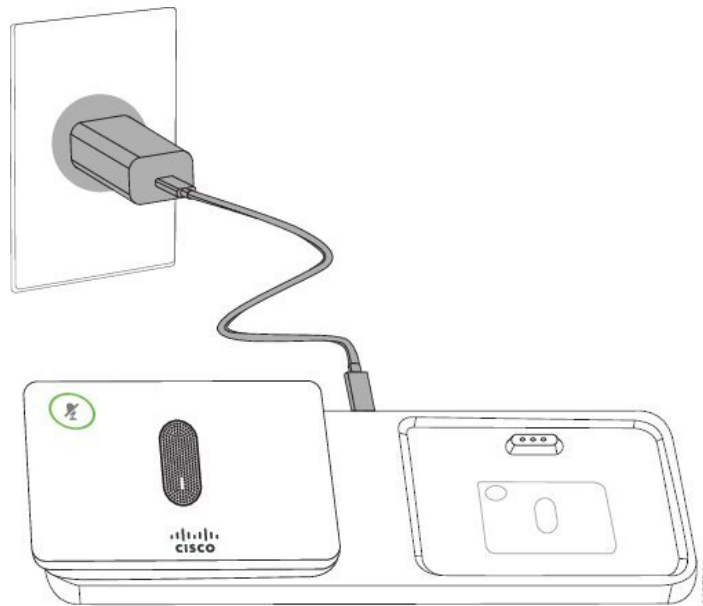
Stecken Sie das Netzteil der Ladeschale in die Steckdose.

**Schritt 2**

Stecken Sie ein Ende des USB-C-Kabels in die Ladeschale und das andere Ende in das Netzteil.

Die folgende Abbildung zeigt die Installation der Ladeschale eines kabellosen Mikrofons.

**Abbildung 11: Installation der Ladeschale eines kabellosen Mikrofons**



---

**Verwandte Themen**

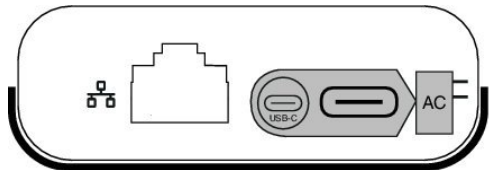
[Kabelloses externes Mikrofon \(nur 8832\)](#), auf Seite 13

[Kabellose externe Mikrofone installieren](#), auf Seite 36

## Konferenztelefon im Daisy-Chain-Modus installieren

Das Daisy-Chain-Kit enthält Smart-Adapter, ein kurzes LAN-Kabel, zwei lange, dickere USB-C-Kabel und ein kürzeres, dickeres USB-C-Kabel. Im Daisy-Chain-Modus benötigen die Konferenztelefone externen Strom aus einer Steckdose. Sie müssen Smart-Adapter verwenden, um die Telefone miteinander zu verbinden. Das lange USB-C-Kabel ist für das Telefon und das kürzere für das Netzteil. Schauen Sie sich die folgende Abbildung an, wenn Sie das Netzteil und den LAN-Port mit Smart-Adapter verbinden.

**Abbildung 12: Netz-Port und LAN-Port für den Smart-Adapter**



Sie können nur ein Mikrofon pro Gerät verwenden.



**Hinweis** Sie müssen entweder zwei kabelgebundene oder zwei kabellose Mikrofone bei dem Telefon verwenden, jedoch keine Kombination aus beiden.

Das USB-C-Kabel für das Netzteil ist schmäler als die USB-C-Kabel, die an das Telefon angeschlossen werden.

### Prozedur

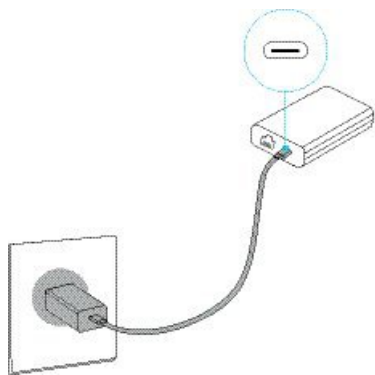
#### Schritt 1

Stecken Sie das Netzteil in die Steckdose.

#### Schritt 2

Verbinden Sie das kurze, schmalere USB-C-Kabel vom Netzteil mit Smart-Adapter.

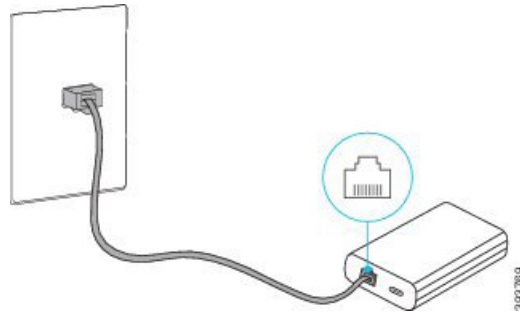
**Abbildung 13: An der Steckdose angeschlossener USB-Port des Smart-Adapters**



#### Schritt 3

Erforderlich: Verbinden Sie das Ethernet-Kabel mit Smart-Adapter und dem LAN-Port.



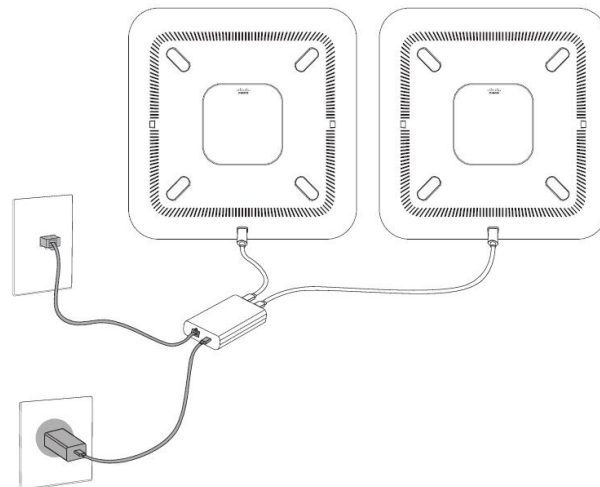
**Abbildung 14:** Mit dem LAN-Port an der Wandsteckdose verbundener LAN-Port des Smart-Adapters**Schritt 4**

Verbinden Sie das erste Telefon über das längere, dickere USB-C-Kabel mit Smart-Adapter.

**Schritt 5**

Verbinden Sie das zweite Telefon über ein USB-Kabel mit Smart-Adapter.

In der folgenden Abbildung wird die Installation des Konferenztelefons im Daisy-Chain-Modus angezeigt.

**Abbildung 15:** Installation des Konferenztelefons im Daisy-Chain-Modus**Verwandte Themen**

[Daisy-Chain-Modus](#), auf Seite 31

[Ein Telefon im Daisy-Chain-Modus funktioniert nicht](#), auf Seite 172

## Ihr Konferenztelefon über das Backup-Image neu starten

Ihr Cisco IP-Konferenztelefon 8832 besitzt ein zweites Backup-Image, mit dem Sie das Telefon wiederherstellen können, wenn das Standard-Image beschädigt wurde.

Gehen Sie wie folgt vor, um Ihr Telefon über das Backup-Image neu zu starten.

**Prozedur****Schritt 1**

Halten Sie die \*-Taste gedrückt, während die Stromversorgung mit dem Konferenztelefon verbunden wird.

- Schritt 2** Nachdem die LED-Leiste grün für "Ein" und anschließend "Aus" leuchtet, können Sie die \*-Taste loslassen.
- Schritt 3** Das Konferenztelefon wird über das Backup-Image neu gestartet.

## Telefone über Menüs konfigurieren

Das Telefon umfasst viele konfigurierbare Netzwerkeinstellungen, die Sie möglicherweise ändern müssen, damit das Telefon von den Benutzern verwendet werden kann. Sie können über die Menüs auf dem Telefon auf diese Einstellungen zugreifen und einige der Einstellungen ändern.

Das Telefon umfasst die folgenden Konfigurationsmenüs:

- **Netzwerkkonfiguration:** Enthält Optionen zum Anzeigen und Konfigurieren verschiedener Netzwerkeinstellungen.
  - **IPv4-Konfiguration:** Dieses Untermenü enthält weitere Netzwerkoptionen.
  - **IPv6-Konfiguration:** Dieses Untermenü enthält weitere Netzwerkoptionen.
- **Sicherheitsoptionen:** Enthält Optionen zum Anzeigen und Konfigurieren verschiedener Sicherheitseinstellungen.



**Hinweis** Sie können steuern, ob ein Telefon Zugriff auf das Menü „Einstellungen“ oder die Optionen in diesem Menü hat. Verwenden Sie das Feld **Zugriff auf Einstellungen** im Cisco Unified Communications Manager-Verwaltung Telefonkonfigurationsfenster, um den Zugriff zu steuern. Das Feld **Zugriff auf Einstellungen** akzeptiert folgende Werte:

- **Aktiviert:** Erlaubt den Zugriff auf das Menü Einstellungen.
- **Deaktiviert:** Verhindert den Zugriff auf die meisten Einträge im Menü „Einstellungen“. Der Benutzer kann weiterhin auf **Einstellungen > Status** zugreifen.
- **Eingeschränkt:** Erlaubt den Zugriff auf die Benutzervoreinstellungen sowie Elemente des Menüs „Status“ und das Speichern von Lautstärkeänderungen. Verhindert den Zugriff auf andere Optionen im Menü Einstellungen.

Wenn Sie auf eine Option im Menü „Administratoreinstellungen“ nicht zugreifen können, überprüfen Sie das Feld **Zugriff auf Einstellungen**.


Die Einstellungen, die nur auf dem Telefon angezeigt werden, werden in Cisco Unified Communications Manager-Verwaltung konfiguriert.

### Prozedur

- Schritt 1** Drücken Sie **Einstellungen**.
- Schritt 2** Wählen Sie **Administratoreinstellungen** aus.
- Schritt 3** Geben Sie gegebenenfalls das Kennwort ein und klicken Sie auf **Anmelden**.
- Schritt 4** Wählen Sie **Netzwerk-Setup** oder **Sicherheits-Setup** aus.

- Schritt 5** Führen Sie einen dieser Schritte aus, um das gewünschte Menü anzuzeigen:
- Verwenden Sie die Navigationspfeile, um das gewünschte Menü auszuwählen, und drücken Sie **Auswählen**.
  - Geben Sie die dem Menü entsprechende Nummer auf dem Tastenfeld ein.

**Schritt 6** Um ein Untermenü anzuzeigen, wiederholen Sie Schritt 5.

**Schritt 7** Um das Menü zu schließen, drücken Sie **Zurück** .

---

#### Verwandte Themen

[Konferenztelefon neu starten oder zurücksetzen](#), auf Seite 179

[Netzwerkeinstellungen konfigurieren](#), auf Seite 42

[Konfigurieren der Sicherheitseinstellungen](#)


## Anwenden eines Telefonkennworts

### Prozedur

- 
- Schritt 1** Navigieren Sie in Cisco Unified Communications Manager Administration zum Fenster „Allgemeine Telefonprofilkonfiguration“ (**Gerät > Geräteeinstellungen > Allgemeines Telefonprofil**).
- Schritt 2** Geben Sie unter Kennwort zum Entsperren des lokalen Telefons ein Kennwort ein.
- Schritt 3** Übernehmen Sie das Kennwort für das allgemeine Telefonprofil, das vom Telefon verwendet wird.
- 

## Text und Menüeintrag auf dem Telefon

Wenn Sie den Wert einer Einstellung bearbeiten, halten Sie die folgenden Richtlinien ein:

- Verwenden Sie die Pfeile in der Navigationsleiste, um das Feld zu markieren, das Sie bearbeiten möchten. Drücken Sie in der Navigationsleiste auf **Auswahl**, um das Feld zu aktivieren. Nachdem ein Feld aktiviert wurde, können Sie die Werte eingeben.
- Verwenden Sie die Tasten auf dem Tastenfeld, um Zahlen und Buchstaben einzugeben.
- Um Buchstaben über das Tastenfeld einzugeben, verwenden Sie die entsprechende Zifferntaste. Drücken Sie die Taste einmal bzw. mehrmals, um einen bestimmten Buchstaben einzugeben. Drücken Sie beispielsweise die **2**-Taste einmal für „a“, zweimal schnell hintereinander für „b“ oder dreimal schnell hintereinander für „c“. Nach kurzer Pause springt der Cursor eine Stelle weiter, sodass der nächste Buchstabe eingegeben werden kann.
- Drücken Sie den Softkey , wenn Sie einen Fehler gemacht haben. Dieser Softkey löscht die Zeichen links vom Cursor.
- Drücken Sie **Zurücksetzen**, bevor Sie **Übernehmen** drücken, um alle vorgenommenen Änderungen zu verwerfen.
- Um eine Zeitdauer (beispielsweise in einer IP-Adresse) einzugeben, drücken Sie \* auf dem Tastenfeld.
- Um einen Doppelpunkt für eine IPv6-Adresse einzugeben, drücken Sie \* auf dem Tastenfeld.



**Hinweis** Cisco IP-Telefon bietet mehrere Methoden, um Einstellungen zurückzusetzen oder wiederherzustellen.

## Netzwerkeinstellungen konfigurieren

### Prozedur

- Schritt 1** Drücken Sie **Einstellungen**.
- Schritt 2** Wählen Sie **Administratoreinstellungen** > **Netzwerk-Setup** > **Ethernet-Setup** aus.
- Schritt 3** Legen Sie die Felder fest, wie in [Felder für das Netzwerk-Setup, auf Seite 42](#) beschrieben. Nachdem Sie die Felder festgelegt haben, müssen Sie das Telefon möglicherweise neu starten.

### Felder für das Netzwerk-Setup

Das Menü „Netzwerk-Setup“ enthält Felder und Untermenüs für IPv4 und IPv6.

Sie müssen DHCP deaktivieren, um einige diese Felder ändern zu können.

**Tabelle 10: Menü „Netzwerk-Setup“**

Eintrag	Typ	Standard	Beschreibung
IPv4-Setup	Menü		Weitere Informationen finden Sie in der Tabelle „IPv4-Setup (Untermenü)“. Diese Option wird nur im Dual-Stack-Modus angezeigt.
IPv6-Setup	Menü		Weitere Informationen finden Sie in der Tabelle „IPv6-Setup (Untermenü)“.
Host-Name	Zeichenfolge		Host-Name des Telefons. Bei Verwendung von DHCP wird dieser Name automatisch zugewiesen.
Domänenname	Zeichenfolge		Name der DNS-Domäne (Domain Name System), in der sich das Telefon befindet. Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
VLAN-ID (Betrieb)			Das VLAN (Virtual Local Area Network), das auf einem Cisco Catalyst-Switch konfiguriert ist, in dem das Telefon ein Mitglied ist.
VLAN-ID (Verwaltung)			Zusätzliches VLAN, in dem das Telefon ein Mitglied ist.

Eintrag	Typ	Standard	Beschreibung
SW-Portkonfiguration	Autom. aushandeln 10 Halb 10 Voll 100 Halb 100 Voll	Autom. aushandeln	Geschwindigkeit und Duplex-Status des Switch-Ports: <ul style="list-style-type: none"> <li>• 10 Halb = 10-BaseT/Halbduplex</li> <li>• 10 Voll = 10-BaseT/Vollduplex</li> <li>• 100 Halb = 100-BaseT/Halbduplex</li> <li>• 100 Voll = 100-BaseT/Vollduplex</li> </ul>
LLDP-MED: SW-Port	Deaktiviert Aktiviert	Aktiviert	Gibt an, ob LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) auf dem Switch-Port aktiviert ist.

Tabelle 11: IPv4-Setup (Untermenü)

Eintrag	Typ	Standard	Beschreibung
DHCP	Deaktiviert Aktiviert	Aktiviert	Aktiviert oder deaktiviert die Verwendung von DHCP.
IP-Adresse			IP-Adresse (IPv4) des Telefons Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
Subnetzmaske			Die vom Telefon verwendete Subnetzmaske. Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
Standardrouter 1			Der vom Telefon verwendete Standardrouter. Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
DNS-Server 1			Vom Telefon verwendeter primärer DNS-Server (Domain Name System) (DNS-Server 1) Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
DNS-Server 2			Vom Telefon verwendeter primärer DNS-Server (Domain Name System) (DNS-Server 2).

Eintrag	Typ	Standard	Beschreibung
DNS-Server 3			Vom Telefon verwendeter primärer DNS-Server (Domain Name System) (DNS-Server 3).
Alternativer TFTP-Server	Nein Ja	Nein	Gibt an, ob das Telefon einen alternativen TFTP-Server verwendet.
TFTP-Server 1			<p>Der vom Telefon verwendete primäre TFTP-Server (Trivial File Transfer Protocol).</p> <p>Wenn die Option „Alternativer TFTP-Server“ auf „Ein“ gesetzt ist, müssen Sie für die Option „TFTP-Server 1“ einen Wert ungleich null eingeben. Wenn weder der primäre TFTP-Server noch der Backup-TFTP-Server in der CTL- oder ITL-Datei auf dem Telefon aufgeführt ist, müssen Sie die Datei entsperren, bevor Sie Änderungen an der Option „TFTP-Server 1“ speichern können. In diesem Fall löscht das Telefon die Datei, wenn Sie Änderungen an der Option „TFTP-Server 1“ speichern. Von der Adresse des neuen TFTP-Servers 1 wird eine neue CTL- oder ITL-Datei heruntergeladen.</p> <p>Weitere Informationen finden Sie in den Hinweisen zu TFTP nach der letzten Tabelle.</p>

Eintrag	Typ	Standard	Beschreibung
TFTP Server 2			<p>Vom Telefon verwendeter sekundärer TFTP-Server.</p> <p>Wenn weder der primäre TFTP-Server noch der Backup-TFTP-Server in der CTL- oder ITL-Datei auf dem Telefon aufgeführt ist, müssen Sie die Datei entsperren, bevor Sie Änderungen an der Option „TFTP-Server 2“ speichern können. In diesem Fall löscht das Telefon die Datei, wenn Sie Änderungen an der Option „TFTP-Server 2“ speichern. Von der Adresse des neuen TFTP-Servers 2 wird eine neue CTL- oder ITL-Datei heruntergeladen.</p> <p>Weitere Informationen finden Sie im Abschnitt mit Hinweisen zu TFTP nach der letzten Tabelle.</p>
DHCP-Adressfreigabe	Nein Ja	Nein	

Tabelle 12: IPv6-Setup (Untermenü)

Eintrag	Typ	Standard	Beschreibung
DHCPv6 aktiviert	Deaktiviert Aktiviert	Aktiviert	Aktiviert oder deaktiviert die Verwendung von IPv6 DHCP.
IPv6-Adresse			<p>Die IPv6-Adresse des Telefons.</p> <p>Deaktivieren Sie DHCP, um dieses Feld ändern zu können.</p>
Länge des IPv6-Präfixes			<p>Länge der IPv6-Adresse.</p> <p>Deaktivieren Sie DHCP, um dieses Feld ändern zu können.</p>
IPv6 - Standardrouter 1			<p>Standard-IPv6-Router.</p> <p>Deaktivieren Sie DHCP, um dieses Feld ändern zu können.</p>
IPv6 – DNS-Server 1			<p>Primärer IPv6-DNS-Server</p> <p>Deaktivieren Sie DHCP, um dieses Feld ändern zu können.</p>

Eintrag	Typ	Standard	Beschreibung
IPv6 – Alternativer TFTP-Server	Nein Ja	Nein	Gibt an, ob das Telefon einen alternativen IPv6-TFTP-Server verwendet.
IPv6 – TFTP-Server 1			Der vom Telefon verwendete primäre IPv6-TFTP-Server.  Weitere Informationen finden Sie im Abschnitt mit Hinweisen zu TFTP nach dieser Tabelle.
IPv6 – TFTP-Server 2			Der vom Telefon verwendete sekundäre IPv6-TFTP-Server.  Weitere Informationen finden Sie im Abschnitt mit Hinweisen zu TFTP nach dieser Tabelle.
IPv6-Adresse freigegeben	Nein Ja	Nein	

Sie können erst IPv6-Setup-Optionen auf Ihrem Gerät konfigurieren, nachdem Sie IPv6 aktiviert und in Cisco Unified Communication Administration konfiguriert haben. Für die IPv6-Konfiguration sind die folgenden Gerätekonfigurationsfelder von Bedeutung:

- IP-Adressierungsmodus
- IP-Adressierungsmodus – Signalisierungsvoreinstellung

Wenn IPv6 im Unified-Cluster aktiviert ist, lautet die Standardeinstellung für den IP-Adressierungsmodus „IPv4 und IPv6“. In diesem Adressierungsmodus verwendet das Telefon eine IPv4-Adresse und eine IPv6-Adresse. Diese Adressen können je nach Bedarf verwendet werden. Das Telefon verwendet entweder die IPv4- oder die IPv6-Adresse zur Anrufsteuerung.

Weitere Informationen zu IPv6 finden Sie unter:

- „Abschnitt zur allgemeinen Gerätekonfiguration“ im *Funktions- und Services-Handbuch für Cisco Unified Communications Manager*, Kapitel „IPv6-Unterstützung in Cisco Unified Communications-Geräten“.
- *IPv6-Bereitstellungshandbuch für Cisco Collaboration Systems Version 12.0* unter: <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html>

### Hinweise zu TFTP

Wenn das Telefon nach dem TFTP-Server sucht, haben unabhängig vom Protokoll manuell zugewiesene TFTP-Server Vorrang. Wenn Ihre Konfiguration sowohl IPv6- als auch IPv4-TFTP-Server umfasst, priorisiert das Telefon die Suchreihenfolge, indem es manuell zugewiesene IPv6-TFTP-Server und IPv4-TFTP-Server vorrangig behandelt. Das Telefon sucht in folgender Reihenfolge nach dem TFTP-Server:

1. Manuell zugewiesene IPv4-TFTP-Server
2. Manuell zugewiesene IPv6-TFTP-Server



3. Durch DHCP zugewiesene TFTP-Server
4. Durch DHCPv6 zugewiesene TFTP-Server

Weitere Informationen zur CTL- und ITL-Datei finden Sie im *Cisco Unified Communications Manager Security Guide* (Sicherheitshandbuch zu Cisco Unified Communications Manager).

## Das Feld Domännennamen

### Prozedur

---

- Schritt 1** Setzen Sie die Option „DHCP aktiviert“ auf **Nein**.
- Schritt 2** Führen Sie einen Bildlauf zur Option „Domänenname“ durch, drücken Sie **Auswahl**, und geben Sie einen neuen Domännennamen ein.
- Schritt 3** Drücken Sie **Übernehmen**.
- 

## Wireless-LAN über das Telefon aktivieren

Vergewissern Sie sich, dass die WLAN-Abdeckung an dem Ort, wo das Wireless LAN zum Einsatz kommen soll, zur Übertragung von Audiopaketen geeignet ist.

Für Wi-Fi-Benutzer wird eine Fast-Secure-Roaming-Methode empfohlen. Wir empfehlen Ihnen die Verwendung von 802.11r (FT).

Ausführliche Informationen zur Konfiguration finden Sie im *Cisco IP-Telefon 8832 Wireless LAN Deployment Guide* (WLAN-Bereitstellungshandbuch für das Cisco IP-Telefon 8832) unter:

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

Das *Cisco IP-Telefon 8832 Wireless LAN Deployment Guide* (WLAN-Bereitstellungshandbuch für das Cisco IP-Telefon 8832) enthält die folgenden Konfigurationsinformationen:

- Wireless-Netzwerkkonfiguration
- Wireless-Netzwerkkonfiguration in der Cisco Unified Communications Manager-Verwaltung
- Wireless-Netzwerkkonfiguration auf dem Cisco IP-Telefon

### Vorbereitungen

Stellen Sie sicher, dass Wi-Fi auf dem Telefon aktiviert und das Ethernet-Kabel getrennt ist.

### Prozedur

---

- Schritt 1** Drücken Sie zum Aktivieren der Anwendung **Einstellungen**.
- Schritt 2** Navigieren Sie zu **Administratoreinstellungen** > **Netzwerk-Setup** > **Wi-Fi-Client-Einrichtung** > **Drahtlos**.

**Schritt 3** Drücken Sie **Ein**.

---

## Wireless LAN über Cisco Unified Communications Manager einrichten

Für das Konferenztelefon müssen Sie in der Cisco Unified Communications Manager Administration den Parameter „Wi-Fi“ aktivieren.



**Hinweis** Verwenden Sie für die Konfiguration der MAC-Adresse im Fenster „Telefonkonfiguration“ in der Cisco Unified Communications Manager-Verwaltung (**Gerät > Telefon**) die MAC-Adresse der Kabelverbindung. Für die Cisco Unified Communications Manager-Registrierung wird die Wireless-MAC-Adresse nicht verwendet.

---

Führen Sie die folgenden Schritte in der Cisco Unified Communications Manager-Verwaltung aus.

### Prozedur

---

**Schritt 1** Führen Sie zum Aktivieren von Wireless LAN auf einem bestimmten Telefon die folgenden Schritte aus:

- a) Wählen Sie **Gerät > Telefon**.
- b) Suchen Sie das erforderliche Telefon.
- c) Wählen Sie die Einstellung **Aktiviert** für den Wi-Fi-Parameter im Abschnitt „Produktspezifische Konfiguration – Layout“ aus.
- d) Aktivieren Sie das Kontrollkästchen **Allgemeine Einstellungen überschreiben**.

**Schritt 2** Führen Sie zum Aktivieren von Wireless LAN für eine Gruppe von Telefonen die folgenden Schritte aus:

- a) Wählen Sie **Gerät > Geräteeinstellungen > Allgemeines Telefonprofil**.
- b) Wählen Sie die Einstellung **Aktiviert** für den Parameter „Wi-Fi“ aus.

**Hinweis** Um sicherzustellen, dass die Konfiguration in diesem Schritt funktioniert, deaktivieren Sie das in Schritt 1d erwähnte Kontrollkästchen **Allgemeine Einstellungen überschreiben**.

- c) Aktivieren Sie das Kontrollkästchen **Allgemeine Einstellungen überschreiben**.
- d) Ordnen Sie die Telefone dem allgemeinen Telefonprofil über **Gerät > Telefon** zu.

**Schritt 3** Führen Sie zum Aktivieren von Wireless LAN für alle WLAN-fähigen Telefone in Ihrem Netzwerk die folgenden Schritte aus:

- a) Wählen Sie **System > Konfiguration des Bürotelefons**.
- b) Wählen Sie die Einstellung **Aktiviert** für den Parameter „Wi-Fi“ aus.

**Hinweis** Um sicherzustellen, dass die Konfiguration in diesem Schritt funktioniert, deaktivieren Sie das in den Schritten 1d und 2c erwähnte Kontrollkästchen **Allgemeine Einstellungen überschreiben**.

- c) Aktivieren Sie das Kontrollkästchen **Allgemeine Einstellungen überschreiben**.
-

## Konfigurieren des Wireless LAN über das Telefon

Bevor sich Cisco IP-Telefon mit dem WLAN (Wireless LAN) verbinden kann, müssen Sie für das Netzwerkprofil des Telefons die entsprechenden WLAN-Einstellungen konfigurieren. Über das Menü **Netzwerk-Setup** des Telefons können Sie auf das Untermenü **WLAN-Client-Einrichtung** zugreifen und dort die WLAN-Konfiguration vornehmen.



**Hinweis** Wenn Wi-Fi im Cisco Unified Communications Manager deaktiviert ist, wird die Option **WLAN-Client-Einrichtung** im Menü **Netzwerk-Setup** nicht angezeigt.

Weitere Informationen hierzu finden Sie im *WLAN-Bereitstellungshandbuch für das Cisco IP-Konferenztelefon 8832*, auf das Sie hier zugreifen können: <http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>

### Vorbereitungen

Konfigurieren Sie das Wireless LAN in Cisco Unified Communications Manager.

### Prozedur

#### Schritt 1

Drücken Sie **Einstellungen**.

#### Schritt 2

Wählen Sie **Administratoreinstellungen** > **Netzwerk-Setup** > **WLAN-Client-Einrichtung** aus.

#### Schritt 3

Richten Sie die Wireless-Konfiguration wie in der folgenden Tabelle beschrieben ein.

**Tabelle 13: Menüoptionen für die Wi-Fi-Client-Konfiguration**

Option	Beschreibung	Änderung
Wireless	Schaltet den Funkempfänger des Cisco IP-Telefon ein bzw. aus.	Führen Sie einen Bildlauf zur Option durch, und aktivieren bzw. deaktivieren mit dem Umschalter.
Netzwerkname	Ermöglicht Ihnen die Verbindung mit einem Drahtlosnetzwerk über das Fenster <b>Netzwerk auswählen</b> . Dieses Fenster enthält zwei Softkeys – <b>Zurück</b> und <b>Sonstige</b> .	Wählen Sie im Fenster <b>Netzwerk auswählen</b> ein Netzwerk aus, mit dem Sie eine Verbindung herstellen möchten.
Zugriff auf WLAN-Anmeldung	Ermöglicht die Anzeige der Wi-Fi-Anmeldung im Fenster.	Führen Sie einen Bildlauf zur Option <b>WLAN-Anmeldung</b> durch, und schalten die Einstellung mit dem Umschalter auf „Aus“.

Option	Beschreibung	Änderung
IPv4-Setup	<p>Im Konfigurations-Untermenü „IPv4-Setup“ können Sie folgende Aktionen ausführen:</p> <ul style="list-style-type: none"> <li>• Nutzung der vom DHCP-Server zugewiesenen IP-Adresse auf dem Telefon aktivieren oder deaktivieren.</li> <li>• IP-Adresse, Subnetzmaske, Standardrouter, DNS-Server und alternative TFTP-Server manuell festlegen.</li> </ul> <p>Weitere Informationen zu den IPv4-Adressfeldern finden Sie in der Tabelle "Untermenü IPv4-Setup".</p>	Führen Sie einen Bildlauf zu <b>IPv4-Setup</b> und drücken Sie dann <b>Auswählen</b> .
IPv6-Setup	<p>Im Konfigurations-Untermenü „IPv6-Setup“ können Sie folgende Aktionen ausführen:</p> <ul style="list-style-type: none"> <li>• Das Telefon aktivieren bzw. deaktivieren, um die IPv6-Adresse zu nutzen, die entweder vom DHCPv6-Server zugewiesen oder von der SLAAC über einen IPv6-fähigen Router abgerufen wird.</li> <li>• IPv6-Adresse, Präfixlänge, Standardrouter, DNS-Server und alternative TFTP-Server manuell festlegen.</li> </ul> <p>Weitere Informationen zu den IPv6-Adressfeldern finden Sie in der Tabelle "Untermenü IPv6-Setup".</p>	Führen Sie einen Bildlauf zu <b>IPv6-Setup</b> und drücken Sie dann <b>Auswählen</b> .
MAC-Adresse	Eindeutige MAC-Adresse (Media Access Control) des Telefons.	Wird nur angezeigt. Der Wert kann nicht konfiguriert werden.
Domänenname	Name der DNS-Domäne (Domain Name System), in der sich das Telefon befindet.	Siehe <a href="#">Das Feld Domännennamen, auf S. 10</a>

**Schritt 4**

Drücken Sie auf **Speichern**, um Änderungen vorzunehmen, oder auf **Zurücks.**, um die Verbindung zu verwerfen.

## Anzahl der WLAN-Authentifizierungsversuche festlegen

Eine Authentifizierungsanforderung ist eine Bestätigung der Anmeldeinformationen des Benutzers. Sie wird durchgeführt, wenn ein Telefon, das bereits Teil eines Wi-Fi-Netzwerkes ist, versucht, erneut eine Verbindung mit dem Wi-Fi-Server herzustellen. Beispiele dafür sind, wenn eine Wi-Fi-Sitzung das Zeitlimit überschreitet oder eine Wi-Fi-Verbindung getrennt und anschließend wieder hergestellt wird.

Sie können konfigurieren, wie oft ein Wi-Fi-Telefon eine Authentifizierungsanforderung an den Wi-Fi-Server sendet. Die Standardanzahl der Versuche ist zwei, aber Sie können diesen Parameter zwischen eins und drei festlegen. Wenn die Authentifizierung bei einem Telefon fehlschlägt, wird der Benutzer aufgefordert, sich erneut anzumelden.

Sie können WLAN-Authentifizierungsversuche auf einzelne Telefone, einen Pool von Telefonen oder alle Wi-Fi-Telefone in Ihrem Netzwerk anwenden.

### Prozedur

---

- Schritt 1** Wählen Sie in Cisco Unified Communications Manager Administration **Gerät > Telefon** aus, und navigieren Sie zum Telefon.
  - Schritt 2** Navigieren Sie zum produktspezifischen Konfigurationsbereich, und konfigurieren Sie das Feld **WLAN-Authentifizierungsversuche**.
  - Schritt 3** Wählen Sie **Speichern** aus.
  - Schritt 4** Wählen Sie **Konfiguration übernehmen**.
  - Schritt 5** Starten Sie das Telefon neu.
- 

## Aktivieren des WLAN-Aufforderungsmodus

Aktivieren Sie den Aufforderungsmodus für WLAN-Profil 1, wenn Sie möchten, dass sich ein Benutzer beim Wi-Fi-Netzwerk anmeldet, wenn dessen Telefon gestartet oder zurückgesetzt wird.

### Prozedur

---

- Schritt 1** Wählen Sie **Gerät > Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.
  - Schritt 2** Suchen Sie das Telefon, das Sie konfigurieren müssen.
  - Schritt 3** Navigieren Sie zum produktspezifischen Konfigurationsbereich, und legen Sie das Feld **Aufforderungsmodus für WLAN-Profil 1** auf **Aktiv**. fest.
  - Schritt 4** Wählen Sie **Speichern** aus.
  - Schritt 5** Wählen Sie **Konfiguration übernehmen**.
  - Schritt 6** Starten Sie das Telefon neu.
- 

## Wi-Fi-Profil mit Cisco Unified Communications Manager festlegen

Sie können ein Wi-Fi-Profil konfigurieren und dieses anschließend den Telefonen zuweisen, die Wi-Fi unterstützen. Das Profil enthält die Parameter, die für Telefone erforderlich sind, um über Wi-Fi eine Verbindung zum Cisco Unified Communications Manager herzustellen. Wenn Sie ein Wi-Fi-Profil erstellen und verwenden, müssen Sie oder Ihre Benutzer das drahtlose Netzwerk für einzelne Telefone nicht konfigurieren.

Wi-Fi-Profile werden unter Cisco Unified Communications Manager, Version 10.5(2) oder höher, unterstützt. EAP-FAST, PEAP-GTC und PEAP-MSCHAPv2 werden in Cisco Unified Communications Manager Version 10.0 und höher unterstützt. EAP-TLS wird in Cisco Unified Communications Manager Release 11.0 und höher unterstützt.

Mit Wi-Fi-Profilen können Sie Änderungen an der Wi-Fi-Konfiguration auf dem Telefon durch den Benutzer verhindern bzw. beschränken.

Wir empfehlen, bei Nutzung eines Wi-Fi-Profiles ein sicheres Profil mit aktivierter TFTP-Verschlüsselung zu verwenden, um Schlüssel und Kennwörter zu schützen.

Wenn Sie die Telefone für die Verwendung der EAP-FAST-, PEAP-MSCHAPv2- oder PEAP-GTC-Authentifizierung konfigurieren, benötigen die Benutzer eigene Benutzer-IDs und Kennwörter zur Anmeldung am Telefon.

Die Telefone unterstützen nur ein Serverzertifikat, das entweder über SCEP oder die manuelle Installationsmethode, jedoch nicht über beide, installiert werden kann. Die Telefone unterstützen nicht die TFTP-Methode zur Zertifikatsinstallation.

## Prozedur

- 
- Schritt 1** Wählen Sie in der Cisco Unified Communications-Verwaltung **Gerät > Geräteeinstellungen > Wireless LAN-Profil** aus.
- Schritt 2** Klicken Sie auf **Neu hinzufügen**.
- Schritt 3** Legen Sie im Abschnitt **Wireless LAN-Profilinformationen** die folgenden Parameter fest:
- **Name** – Geben Sie einen eindeutigen Namen für das Wi-Fi-Profil ein. Dieser Name wird auf dem Telefon angezeigt.
  - **Beschreibung** – Geben Sie eine Beschreibung für das Wi-Fi-Profil ein, anhand derer Sie dieses Profil von anderen Wi-Fi-Profilen unterscheiden können.
  - **Vom Benutzer änderbar** – Wählen Sie eine Option aus:
    - **Zulässig** – Zeigt an, dass der Benutzer auf seinem Telefon Änderungen an den Wi-Fi-Einstellungen vornehmen kann. Diese Option ist standardmäßig aktiviert.
    - **Unzulässig** – Zeigt an, dass der Benutzer auf seinem Telefon keine Änderungen an den Wi-Fi-Einstellungen vornehmen kann.
    - **Eingeschränkt** – Zeigt an, dass der Benutzer auf seinem Telefon Wi-Fi-Benutzernamen und -Kennwort ändern kann. Benutzer können auf dem Telefon jedoch keine Änderungen an anderen Wi-Fi-Einstellungen vornehmen.
- Schritt 4** Legen Sie im Abschnitt **Wireless-Einstellungen** die folgenden Parameter fest:
- **SSID (Netzwerkname)** – Geben Sie den in der Benutzerumgebung verfügbaren Namen des Netzwerks ein, mit dem das Telefon verbunden werden kann. Dieser Name wird in der Liste der verfügbaren Netzwerke auf dem Telefon angezeigt, und das Telefon kann mit diesem drahtlosen Netzwerk verbunden werden.
  - **Frequenzband** – Verfügbare Optionen sind „Auto“, „2,4 GHz“ und „5 GHz“. Mit diesem Feld wird das Frequenzband bestimmt, das von der drahtlosen Verbindung verwendet wird. Wenn Sie Auto auswählen, versucht das Telefon zuerst, das 5-GHz-Frequenzband zu verwenden, und verwendet das 2,4-GHz-Frequenzband nur, wenn 5 GHz nicht verfügbar ist.
- Schritt 5** Legen Sie im Abschnitt **Authentifizierungseinstellungen** die **Authentifizierungsmethode** auf eine der folgenden Authentifizierungsmethoden fest: EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP und „Keine“.

Nachdem Sie dieses Feld festgelegt haben, werden möglicherweise zusätzliche Felder angezeigt, die Sie konfigurieren müssen.

- **Benutzerzertifikat** – Für die EAP-TLS-Authentifizierung erforderlich. Wählen Sie **Vom Hersteller installiert** oder **Vom Benutzer installiert** aus. Es ist erforderlich, dass auf dem Telefon ein Zertifikat installiert wird, entweder automatisch über das SCEP oder manuell über die Verwaltungsseite auf dem Telefon.
  - **PSK-Passphrase** – Für die PSK-Authentifizierung erforderlich. Geben Sie eine ASCII-Passphrase mit 8 – 63 Zeichen oder eine 64 HEX-Zeichen-Passphrase ein.
  - **WEP-Schlüssel** – Für die WEP-Authentifizierung erforderlich. Geben Sie den 40/102, 64/128-ASCII oder HEX-WEP-Schlüssel ein.
    - 40/104 ASCII umfasst 5 Zeichen.
    - 64/128 ASCII umfasst 13 Zeichen.
    - 40/104 HEX umfasst 10 Zeichen.
    - 64/128 HEX umfasst 26 Zeichen.
  - **Gemeinsam genutzte Anmeldeinformationen angeben:** Für die EAP-FAST-, PEAP-MSCHAPv2- und PEAP-GTC-Authentifizierung erforderlich.
    - Wenn der Benutzer den Benutzernamen und das Kennwort verwaltet, lassen Sie die Felder **Benutzername** und **Kennwort** leer.
    - Wenn alle Benutzer denselben Benutzernamen und dasselbe Kennwort verwenden, können Sie die Informationen in die Felder **Benutzername** und **Kennwort** eingeben.
    - Geben Sie eine Beschreibung in das Feld **Kennwortbeschreibung** ein.
- Hinweis** Wenn Sie jedem Benutzer einen eindeutigen Benutzernamen und ein eindeutiges Kennwort zuweisen möchten, müssen Sie für jeden Benutzer ein Profil erstellen.

## Schritt 6

Klicken Sie auf **Speichern**.

---

### Nächste Maßnahme

Wenden Sie die WLAN-Profilgruppe auf einen Geräte-Pool (**System** > **Geräte-Pool**) oder direkt auf das Telefon (**Gerät** > **Telefon**) an.

## Wi-Fi-Gruppe mit Cisco Unified Communications Manager festlegen

Sie können eine Wireless LAN-Profilgruppe erstellen und Wireless LAN-Profile zu dieser Gruppe hinzufügen. Die Profilgruppe kann dann während der Telefoneinrichtung dem Telefon zugewiesen werden.

**Prozedur**

- 
- Schritt 1** Wählen Sie in Cisco Unified Communications Administration **Gerät > Geräteeinstellungen > Wireless LAN-Profilgruppe** aus.  
Sie können eine Wireless LAN-Profilgruppe auch über **System > Geräte-Pool** definieren.
- Schritt 2** Klicken Sie auf **Neu hinzufügen**.
- Schritt 3** Geben Sie im Abschnitt **Wireless LAN-Profil-Gruppeninformationen** einen Gruppennamen und eine Beschreibung ein.
- Schritt 4** Wählen Sie im Abschnitt **Profile für diese Wireless LAN-Profilgruppe** ein Profil aus der Liste **Verfügbare Profile** aus, und verschieben Sie das ausgewählte Profil in die Liste **Ausgewählte Profile**.  
Wenn mehrere Wireless LAN-Profile ausgewählt werden, wird vom Telefon nur das erste Wireless LAN-Profil verwendet.
- Schritt 5** Klicken Sie auf **Speichern**.
- 

## Telefonstart überprüfen

Nachdem das Telefon an eine Stromquelle angeschlossen wurde, durchläuft es automatisch den Startdiagnoseprozess.

**Prozedur**


---

Schließen Sie das Telefon an eine Stromquelle an.  
Wenn der Hauptbildschirm angezeigt wird, wurde es ordnungsgemäß gestartet.

---

## Telefonmodell eines Benutzers ändern

Sie oder Ihr Benutzer können das Telefonmodell eines Benutzers ändern. Die Änderung kann aus mehreren Gründen erforderlich sein, z. B.:

- Sie haben Ihr Cisco Unified Communications Manager (Unified CM) auf eine Softwareversion aktualisiert, die das Telefonmodell nicht unterstützt.
- Der Benutzer möchte ein anderes Telefonmodell als das aktuelle Modell verwenden.
- Das Telefon erfordert eine Reparatur oder einen Austausch.

Unified CM kennzeichnet das alte Telefon und verwendet die MAC-Adresse des alten Telefons zur Identifikation der alten Telefonkonfiguration. Unified CM kopiert die alte Telefonkonfiguration in den Eintrag für das neue Telefon. Das neue Telefon hat dann die gleiche Konfiguration wie das alte Telefon.



**Einschränkung:** Wenn das alte Telefon mehr Leitungen oder Leitungstasten als das neue Telefon umfasst, sind die zusätzlichen Leitungen bzw. Leitungstasten für das neue Telefon nicht konfiguriert.

Das Telefon wird nach der Konfiguration neu gestartet.

### Vorbereitungen

Richten Sie Ihr Cisco Unified Communications Manager nach den Anweisungen im *Funktionskonfigurationshandbuch für Cisco Unified Communications Manager* ein.

Sie benötigen ein neues, nicht verwendetes Telefon, auf dem die Firmware-Version 12.8(1) oder höher vorinstalliert ist.

### Prozedur

---

- Schritt 1** Schalten Sie das alte Telefon aus.
  - Schritt 2** Schalten Sie das neue Telefon ein.
  - Schritt 3** Wählen Sie auf dem neuen Telefon **Vorhandenes Telefon ersetzen** aus.
  - Schritt 4** Geben Sie den Hauptanschluss des alten Telefons ein.
  - Schritt 5** Wenn dem alten Telefon eine PIN zugewiesen wurde, geben Sie diese PIN ein.
  - Schritt 6** Drücken Sie **Senden**.
  - Schritt 7** Wenn für den Benutzer mehrere Geräte vorhanden sind, wählen Sie das zu ersetzende Gerät aus, und drücken Sie **Weiter**.
-





## KAPITEL 5

# Cisco Unified Communications Manager – Telefoninstallation

---

- [Cisco IP-Konferenztelefon einrichten, auf Seite 57](#)
- [Die MAC-Adresse des Telefons bestimmen, auf Seite 62](#)
- [Methoden zum Hinzufügen von Telefonen, auf Seite 62](#)
- [Benutzer zu Cisco Unified Communications Manager hinzufügen, auf Seite 63](#)
- [Einer Endbenutzergruppe einen Benutzer hinzufügen, auf Seite 65](#)
- [Telefone zu Benutzern zuordnen, auf Seite 66](#)
- [SRST \(Survivable Remote Site Telephony\), auf Seite 67](#)

## Cisco IP-Konferenztelefon einrichten

Wenn die automatische Registrierung nicht aktiviert und das Telefon nicht in der Cisco Unified Communications Manager-Datenbank vorhanden ist, müssen Sie das Cisco IP Phone manuell in Cisco Unified Communications Manager Administration konfigurieren. Abhängig von Ihrem System und den Benutzeranforderungen sind einige Aufgaben in diesem Verfahren optional.

Weitere Informationen zu diesen Schritten finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Führen Sie die Konfigurationsschritte im folgenden Verfahren in der Cisco Unified Communications Manager-Verwaltung aus.

### Prozedur

---

#### Schritt 1

Stellen Sie die folgenden Telefoninformationen zusammen:

- Telefonmodell
- MAC-Adresse: Siehe [Die MAC-Adresse des Telefons bestimmen, auf Seite 62](#)
- Physischer Standort des Telefons
- Name oder Benutzer-ID des Telefonbenutzers
- Gerätepool

- Partition, Anrufsuchraum und Standortinformationen
- Verzeichnisnummer (DN, Directory number), die dem Telefon zugewiesen werden soll
- Cisco Unified Communications Manager-Benutzer, der dem Telefon zugeordnet werden soll
- Informationen zur Telefonnutzung in Bezug auf die Softkey-Vorlage, die Telefonfunktionen, die IP-Telefonservices oder die Telefonanwendungen

Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager und unter den zugehörigen Links.

**Schritt 2**

Stellen Sie sicher, dass genügend Einheitenlizenzen für Ihr Telefon vorhanden sind.

Weitere Informationen finden Sie im Lizenzierungsdokument für Ihre Version von Cisco Unified Communications Manager.

**Schritt 3**

Definieren Sie die Gerätepools. Wählen Sie **System > Gerätepool** aus.

Gerätepools definieren allgemeine Eigenschaften für Geräte, beispielsweise die Region, die Datums-/Uhrzeitgruppe und die Softkey-Vorlage.

**Schritt 4**

Definieren Sie das allgemeine Telefonprofil. Wählen Sie **Gerät > Geräteeinstellungen > Allgemeines Telefonprofil** aus.

Allgemeine Telefonprofile enthalten Daten für den Cisco TFTP-Server und allgemeine Telefoneinstellungen, wie z. B. „Bitte nicht stören“ (Ruhefunktion) und Funktionssteuerungsoptionen.

**Schritt 5**

Definieren Sie einen Anrufsuchraum. Klicken Sie in der Cisco Unified Communications Manager-Verwaltung auf **Anrufumleitung > Steuerungsklasse > Anrufsuchraum**.

Ein Anrufsuchraum (engl. Calling Search Space, CSS) besteht aus mehreren Partitionen, die durchsucht werden, um das Routing einer gewählten Nummer zu ermitteln. Die Anrufschräume für das Gerät und die Verzeichnisnummer werden zusammen verwendet. Die Verzeichnisnummern-CSS hat Vorrang vor der Geräte-CSS.

**Schritt 6**

Konfigurieren Sie ein Sicherheitsprofil für den Gerätetyp und das Protokoll. Wählen Sie **System > Sicherheit > Telefonsicherheitsprofil** aus.

**Schritt 7**

Konfigurieren Sie das Telefon. Wählen Sie **Gerät > Telefon**.

- Suchen Sie das Telefon, das Sie ändern möchten, oder fügen Sie ein neues Telefon hinzu.
- Konfigurieren Sie das Telefon, indem Sie die erforderlichen Felder unter „Geräteinformationen“ im Fenster „Telefonkonfiguration“ ausfüllen.
  - MAC-Adresse (erforderlich): Stellen Sie sicher, dass der Wert aus 12 Hexadezimalzeichen besteht.
  - Beschreibung: Geben Sie eine Beschreibung ein, die hilfreich ist, wenn Sie Benutzerinformationen suchen müssen.
  - Gerätepool (erforderlich)
  - Allgemeines Telefonprofil
  - Anrufsuchraum
  - Standort
  - Besitzer („Benutzer“ oder „Anonym“), und bei Auswahl von „Benutzer“ die Benutzer-ID des Besitzers

Das Gerät wird mit den Standardeinstellungen zur Cisco Unified Communications Manager-Datenbank hinzugefügt.

Weitere Informationen zu den produktspezifischen Konfigurationsfeldern finden Sie unter „?“ Tastenhilfe im Fenster „Telefonkonfiguration“ und der zugehörige Link.

**Hinweis** Wenn Sie das Telefon und den Benutzer zur Cisco Unified Communications Manager-Datenbank hinzufügen möchten, lesen Sie die Dokumentation für Ihre Version von Cisco Unified Communications Manager.

- c) Wählen Sie im protokollspezifischen Bereich des Fensters ein Gerätesicherheitsprofil aus und legen Sie den Sicherheitsmodus fest.

**Hinweis** Wählen Sie ein Sicherheitsprofil basierend auf der Sicherheitsstrategie Ihres Unternehmens aus. Wenn das Telefon die Sicherheit nicht unterstützt, wählen Sie ein nicht sicheres Profil aus.

- d) Aktivieren Sie im Bereich Anschlussinformationen das Kontrollkästchen Anschlussmobilität aktivieren, wenn das Telefon die Cisco Anschlussmobilität unterstützt.  
e) Klicken Sie auf **Speichern**.

### Schritt 8

Wählen Sie **Gerät > Geräteeinstellungen > SIP-Profil** aus, um SIP-Parameter zu konfigurieren.

### Schritt 9

Wählen Sie **Gerät > Telefon** aus, um Verzeichnisnummern (Leitungen) auf dem Telefon zu konfigurieren, indem Sie die erforderlichen Felder im Fenster Verzeichnisnummernkonfiguration ausfüllen.

- a) Suchen Sie das Telefon.  
b) Klicken Sie im Fenster „Telefonkonfiguration“ auf „Leitung 1“ im linken Fensterbereich.

Konferenztelefone haben nur eine Leitung.

- c) Geben Sie im Feld Verzeichnisnummer eine gültige Nummer ein, die gewählt werden kann.

**Hinweis** Dieses Feld sollte die gleiche Nummer enthalten, die im Feld Telefonnummer im Fenster Benutzerkonfiguration angezeigt wird.

- d) Wählen Sie in der Dropdown-Liste „Routenpartition“ die Partition aus, zu der die Verzeichnisnummer gehört. Wenn Sie den Zugriff auf die Verzeichnisnummer einschränken möchten, wählen Sie <None> für die Partition aus.  
e) Wählen Sie in der Dropdown-Liste „Anrufsuchraum“ den geeigneten Anrufsuchraum aus. Der ausgewählte Wert wird für alle Geräte übernommen, die diese Verzeichnisnummer verwenden.  
f) Wählen Sie in den Einstellungen für die Anrufweiterleitung und Anrufübernahme die Elemente (beispielsweise Alle weiterleiten oder Bei besetzt intern weiterleiten) und die Ziele aus, an die Anrufe gesendet werden.

#### Beispiel:

Wenn Sie eingehende interne und externe Anrufe, die ein Besetztsymbol erhalten, an die Voicemail für diese Leitung weiterleiten möchten, aktivieren Sie das Kontrollkästchen Voicemail neben Bei besetzt intern weiterleiten und Bei besetzt extern weiterleiten in der linken Spalte im Bereich Anrufübernahme und Anrufweiterleitung.

- g) Konfigurieren Sie unter Leitung 1 des Geräts die folgenden Felder:

- Anzeige (Interne Anrufer-ID: Sie können den Vornamen und Nachnamen des Benutzers des Geräts eingeben, um diesen Namen für alle internen Anrufe anzuzeigen. Lassen Sie dieses Feld leer, damit das System den Anschluss anzeigt.

- Externe Nummernmaske: Zeigt die Telefonnummer (oder Maske) an, die verwendet wird, um die Anrufer-ID zu senden, wenn ein Anruf auf dieser Leitung getätigt wird. Sie können maximal 24 numerische und „X“ Zeichen eingeben. Das X steht für die Verzeichnisnummer und muss am Ende des Musters angezeigt werden.

**Beispiel:**

Wenn Sie die Maske 408902XXXX angeben, wird für einen externen Anruf von Anschluss 6640 die Anrufer-ID 4089026640 angezeigt.

Diese Einstellung betrifft nur das aktuelle Gerät, außer Sie aktivieren das Kontrollkästchen rechts (Einstellungen für gemeinsam genutztes Gerät aktualisieren) und klicken auf **Auswahl verteilen**. Das Kontrollkästchen rechts wird nur angezeigt, wenn andere Geräte diese Verzeichnisnummer verwenden.

- h) Wählen Sie **Speichern** aus.

Weitere Informationen zu Verzeichnisnummern finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager und unter den zugehörigen Links.

**Schritt 10**

(optional) Weisen Sie dem Benutzer ein Telefon zu. Klicken Sie auf **Benutzer zuweisen** unten im Fenster „Telefonkonfiguration“, um einen Benutzer zur Leitung zuzuweisen, die konfiguriert wird.

- Verwenden Sie **Suchen** zusammen mit den Suchfeldern, um den Benutzer zu suchen.
- Aktivieren Sie das Kontrollkästchen neben dem Benutzernamen und klicken Sie auf **Auswahl hinzufügen**.

Der Benutzername und die Benutzer-ID werden im Fenster Verzeichnisnummernkonfiguration unter Der Leitung zugewiesene Benutzer angezeigt.

- c) Wählen Sie **Speichern** aus.

Der Benutzer ist nun der Leitung 1 auf dem Telefon zugewiesen.

**Schritt 11**

(optional) Weisen Sie dem Benutzer ein Gerät zu:

- Wählen Sie **Benutzerverwaltung > Benutzer** aus.
- Verwenden Sie die Suchfelder und **Suchen**, um den Benutzer zu suchen, den Sie hinzugefügt haben.
- Klicken Sie auf die Benutzer-ID.
- Wählen Sie in der Dropdown-Liste unter „Verzeichnisnummernzuordnungen“ den Hauptanschluss aus.
- (optional) Aktivieren Sie das Kontrollkästchen Mobilität aktivieren unter Mobilitätsinformationen.
- Verwenden Sie die Schaltflächen unter **Zugriffssteuerungsgruppe hinzufügen** im Bereich Berechtigungsinformationen, um den Benutzer zu Benutzergruppen hinzuzufügen.

Beispielsweise können Sie den Benutzer zu einer Gruppen hinzufügen, die als eine CCM-Standardbenutzergruppe definiert ist.

- Um die Informationen einer Gruppe anzuzeigen, wählen Sie die Gruppe aus und klicken Sie auf **Details anzeigen**.
- Aktivieren Sie unter Anschlussmobilität das Kontrollkästchen Anschlussmobilität im Cluster aktivieren, damit der Benutzer diesen Service verwenden kann.
- Klicken Sie in den Geräteinformationen auf **Gerätezuordnungen**.
- Verwenden Sie die Suchfelder und **Suchen**, um das Gerät zu suchen, das Sie dem Benutzer zuweisen möchten.
- Wählen Sie das Gerät aus und klicken Sie auf **Auswahl/Änderungen speichern**.
- Klicken Sie auf **Los** neben dem Link „Zurück zu Benutzer“ in der oberen rechten Bildschirmcke.
- Wählen Sie **Speichern** aus.

**Schritt 12**

Passen Sie die Softkey-Vorlagen an. Wählen Sie **Gerät > Geräteeinstellungen > Softkey-Vorlage** aus.

Auf dieser Seite können Sie die Softkey-Funktionen, die auf dem Telefon des Benutzer angezeigt werden, hinzufügen, löschen oder sortieren.

Für das Konferenztelefon gelten spezielle Softkey-Anforderungen. Weitere Informationen finden Sie unter den zugehörigen Links.

**Schritt 13**

Konfigurieren Sie die Cisco IP Phone-Services und weisen Sie Services zu. Wählen Sie **Gerät > Geräteeinstellungen > Telefonservices** aus.

Stellt IP-Telefonservices für das Telefon bereit.

**Hinweis** Im Cisco Unified Communications Selbstservice-Portal können die Benutzer Services auf ihren Telefonen hinzufügen oder ändern.

**Schritt 14**

(optional) Fügen Sie Benutzerinformationen zum globalen Verzeichnis für Cisco Unified Communications Manager hinzu. Wählen Sie **Benutzerverwaltung > Benutzer** aus, klicken Sie auf **Neu hinzufügen** und konfigurieren Sie die erforderlichen Felder. Erforderliche Felder sind mit einem Sternchen (\*) markiert.

**Hinweis** Wenn Ihr Unternehmen ein LDAP-Verzeichnis (Lightweight Directory Access Protocol) zum Speichern der Benutzerinformationen verwendet, können Sie Cisco Unified Communications für die Verwendung des vorhandenen LDAP-Verzeichnisses konfigurieren (siehe [Konfiguration des Firmenverzeichnisses, auf Seite 131](#)). Nachdem die Option Synchronisierung vom LDAP-Server aktivieren ausgewählt wurde, können Sie keine weiteren Benutzer über die Cisco Unified Communications Manager-Verwaltung hinzufügen.

- a) Füllen Sie die Felder Benutzer-ID und Nachname aus.
- b) Weisen Sie ein Kennwort (für das Selbstservice-Portal) zu.
- c) Weisen Sie eine PIN (für Cisco Extension Mobility und das persönliche Verzeichnis) zu.
- d) Weisen Sie dem Benutzer ein Telefon zu.

Verleiht den Benutzern Kontrolle über ihr Telefon, z. B. zum Weiterleiten von Anrufen oder Hinzufügen von Kurzwahlnummern oder Diensten.

**Hinweis** Einigen Telefone, beispielsweise Telefonen in Konferenzräumen, sind keine Benutzer zugewiesen.

**Schritt 15**

(optional) Weisen Sie einen Benutzer einer Benutzergruppe zu. Wählen Sie **Benutzerverwaltung > Benutzereinstellungen > Zugriffssteuerungsgruppe** aus.

Weist Benutzern allgemeine Rollen und Berechtigungen zu, die für alle Benutzer in einer Benutzergruppe übernommen werden. Administratoren können Benutzergruppen, Rollen und Berechtigungen verwalten, um die Zugriffsstufe (und damit die Sicherheitsstufe) für Systembenutzer zu steuern.

Damit die Benutzer auf das Cisco Unified Communications Selbstservice-Portal zugreifen können, müssen Sie die Benutzer zur Cisco Communications Manager-Standardbenutzergruppe hinzufügen.

**Verwandte Themen**

[Produktspezifische Konfiguration](#), auf Seite 102

[Cisco IP-Konferenztelefon – Funktionen und Einrichtung](#), auf Seite 97

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

[Softkey-Vorlagen konfigurieren](#), auf Seite 98

## Die MAC-Adresse des Telefons bestimmen

Um Telefone zu Cisco Unified Communications Manager hinzuzufügen, müssen Sie die MAC-Adresse eines Telefons bestimmen.

### Prozedur

---

Führen Sie einen der folgenden Schritte aus:

- Wählen Sie auf dem Telefon **Einstellungen** > **Telefoninformationen** aus, und sehen Sie sich das Feld „MAC-Adresse“ an.
  - Das MAC-Label befindet sich an der Rückseite des Telefons.
  - Öffnen Sie die Webseite für das Telefon und klicken Sie auf **Geräteinformationen**.
- 

## Methoden zum Hinzufügen von Telefonen

Nachdem Sie Cisco IP-Telefon installiert haben, können Sie eine der folgenden Optionen auswählen, um Telefone zur Cisco Unified Communications Manager-Datenbank hinzuzufügen.

- Hinzufügen einzelner Telefone mit der Cisco Unified Communications Manager Administration
- Hinzufügen mehrerer Telefone mit dem Massen-Verwaltung-Tool (BAT)
- Automatische Registrierung
- BAT und TAPS (Tool for Auto-Registered Phones Support)

Bevor Sie Telefone einzeln oder mit dem BAT hinzufügen, benötigen Sie die MAC-Adresse des Telefons. Weitere Informationen hierzu finden Sie unter [Die MAC-Adresse des Telefons bestimmen, auf Seite 62](#).

Weitere Informationen zu BAT finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Einzelne Telefone hinzufügen

Notieren Sie die MAC-Adresse und Telefoninformationen, die Sie zu Cisco Unified Communications Manager hinzufügen müssen.

### Prozedur

---

#### Schritt 1

Wählen Sie **Gerät** > **Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.



- Schritt 2** Klicken Sie auf **Neu hinzufügen**.
- Schritt 3** Wählen Sie den Telefontyp aus.
- Schritt 4** Wählen Sie **Weiter** aus.
- Schritt 5** Vervollständigen Sie die Informationen über das Telefon, einschließlich die MAC-Adresse.  
Die vollständigen Anweisungen und weitere Informationen zu Cisco Unified Communications Manager finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.
- Schritt 6** Wählen Sie **Speichern** aus.

---

**Verwandte Themen**

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Telefone über eine BAT-Telefonvorlage hinzufügen

Das Cisco Unified Communications BAT (Bulk Administration Tool) ermöglicht das Ausführen von Batchvorgängen, einschließlich die Registrierung von mehreren Telefonen.

Um Telefone nur mit BAT (nicht zusammen mit TAPS) hinzuzufügen, benötigen Sie die MAC-Adressen der Telefone.

Weitere Informationen zu BAT finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

**Prozedur**

- 
- Schritt 1** Wählen Sie **Massenverwaltung > Telefone > Telefonvorlage** in der Cisco Unified Communications-Verwaltung aus.
- Schritt 2** Klicken Sie auf **Neu hinzufügen**.
- Schritt 3** Wählen Sie einen Telefontyp aus und klicken Sie auf **Weiter**.
- Schritt 4** Geben Sie die Informationen der telefonspezifischen Parameter ein, beispielsweise Geräte-Pool, Telefontastenvorlage und Gerätesicherheitsprofil.
- Schritt 5** Klicken Sie auf **Speichern**.
- Schritt 6** Wählen Sie **Gerät > Telefon > Neu hinzufügen** aus, um eine Telefon mit der BAT-Telefonvorlage hinzuzufügen.

---

**Verwandte Themen**

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Benutzer zu Cisco Unified Communications Manager hinzufügen

Sie können die Informationen über Benutzer, die in Cisco Unified Communications Manager registriert sind, anzeigen und verwalten. Mit Cisco Unified Communications Manager können die Benutzer folgende Aufgaben ausführen:

- Auf das Firmenverzeichnis und andere Verzeichnisse auf einem Cisco IP-Telefon zugreifen.

- Ein persönliches Verzeichnis erstellen.
- Kurzwahlnummern und Nummern für die Anrufweiterleitung konfigurieren.
- Services abonnieren, die über Cisco IP-Telefon verfügbar sind.

### Prozedur

---

- Schritt 1** Um einzelne Benutzer hinzuzufügen, siehe [Einen Benutzer direkt Cisco Unified Communications Manager hinzufügen, auf Seite 65](#).
- Schritt 2** Um mehrere Benutzer hinzuzufügen, verwenden Sie das entsprechende Verwaltungstool. Diese Methode ermöglicht das Festlegen eines Standardkennworts für alle Benutzer.
- Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.
- 

### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Benutzer aus einem externen LDAP-Verzeichnis hinzufügen

Wenn Sie einen Benutzer zu einem LDAP-Verzeichnis (kein Cisco Unified Communications Server-Verzeichnis) hinzugefügt haben, können Sie das LDAP-Verzeichnis sofort mit dem Cisco Unified Communications Manager synchronisieren, auf dem Sie den Benutzer und das Benutzertelefon hinzufügen.



- Hinweis** Wenn Sie das LDAP-Verzeichnis nicht sofort mit Cisco Unified Communications Manager synchronisieren, legt der Zeitplan für die LDAP-Verzeichnissynchronisierung im Fenster LDAP-Verzeichnis fest, wann die nächste automatische Synchronisierung ausgeführt wird. Die Synchronisierung muss ausgeführt werden, bevor Sie einem neuen Benutzer ein Gerät zuweisen.
- 

### Prozedur

---

- Schritt 1** Melden Sie sich an der Cisco Unified Communications Manager-Verwaltung an.
- Schritt 2** Wählen Sie **System > LDAP > LDAP-Verzeichnis** aus.
- Schritt 3** Wählen Sie **Suchen** aus, um das LDAP-Verzeichnis zu suchen.
- Schritt 4** Klicken Sie auf den Namen des LDAP-Verzeichnisses.
- Schritt 5** Klicken Sie auf **Vollständige Synchronisierung jetzt ausführen**.
-

## Einen Benutzer direkt Cisco Unified Communications Manager hinzufügen

Wenn Sie kein LDAP-Verzeichnis (Lightweight Directory Access Protocol) verwenden, können Sie Benutzer direkt mit der Cisco Unified Communications Manager-Verwaltung hinzufügen, indem Sie folgende Schritte ausführen.



**Hinweis** Wenn LDAP synchronisiert ist, können Sie mit der Cisco Unified Communications Manager-Verwaltung keine Benutzer hinzufügen.

### Prozedur

- Schritt 1** Wählen Sie **Benutzerverwaltung** > **Endbenutzer** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Klicken Sie auf **Neu hinzufügen**.
- Schritt 3** Geben Sie die folgenden Benutzerinformationen ein:
- **Benutzer-ID:** Geben Sie die ID des Benutzers ein. Cisco Unified Communications Manager erlaubt es nicht, dass die Benutzer-ID nach ihrer Erstellung geändert werden kann. Sie können die folgenden Sonderzeichen verwenden: =, +, <, >, #, ;, \, , , „, und Leerzeichen. **Beispiel:** johndoe
  - **Kennwort und Kennwort bestätigen:** Geben Sie mindestens fünf alphanumerische Zeichen oder Sonderzeichen für das Kennwort des Benutzers ein. Sie können die folgenden Sonderzeichen verwenden: =, +, <, >, #, ;, \, , , „, und Leerzeichen.
  - **Nachname:** Geben Sie den Nachnamen des Benutzers ein. Sie können die folgenden Sonderzeichen verwenden: =, +, <, >, #, ;, \, , , „, und Leerzeichen. **Beispiel:** doe
  - **Telefonnummer:** Geben Sie die primäre Verzeichnisnummer für den Benutzer ein. Ein Benutzer kann mehrere Leitungen auf seinem Telefon haben. **Beispiel:** 26640 (John Does interne Firmenummer)
- Schritt 4** Klicken Sie auf **Speichern**.

## Einer Endbenutzergruppe einen Benutzer hinzufügen

Um einen Benutzer zu einer Standardbenutzergruppe in Cisco Unified Communications Manager hinzuzufügen, führen Sie die folgenden Schritte aus:

### Prozedur

- Schritt 1** Wählen Sie **Benutzerverwaltung** > **Benutzereinstellungen** > **Zugriffssteuerungsgruppe** in der Cisco Unified Communications Manager-Verwaltung aus.
- Das Fenster Benutzer suchen und auflisten wird angezeigt.
- Schritt 2** Geben Sie die Suchkriterien ein und klicken Sie auf **Suchen**.

- Schritt 3** Wählen Sie den Link **CCM-Standardbenutzer** aus. Das Fenster Benutzergruppenkonfiguration für die CCM-Standardbenutzer wird geöffnet.
- Schritt 4** Wählen Sie **Benutzer zu einer Gruppe hinzufügen** aus. Das Fenster Benutzer suchen und auflisten wird angezeigt.
- Schritt 5** Verwenden Sie die Dropdown-Liste Benutzer suchen, um die Benutzer zu suchen, die Sie hinzufügen möchten, und klicken Sie auf **Suchen**.  
Die Benutzer, die mit Ihren Suchkriterien übereinstimmen, werden aufgelistet.
- Schritt 6** Aktivieren Sie in der angezeigten Eintragsliste die Kontrollkästchen neben den Benutzern, die Sie zu dieser Benutzergruppe hinzufügen möchten. Wenn die Liste lang ist, verwenden Sie die Links unten, um mehr Ergebnisse anzuzeigen.  
**Hinweis** Benutzer, die bereits zu der Benutzergruppe gehören, werden nicht in den Suchergebnissen angezeigt.
- Schritt 7** Wählen Sie **Auswahl hinzufügen** aus.
- 

## Telefone zu Benutzern zuordnen

Benutzern werden Telefone im Fenster Benutzer in Cisco Unified Communications Manager zugewiesen.

### Prozedur

---

- Schritt 1** Wählen Sie **Benutzerverwaltung > Endbenutzer** in der Cisco Unified Communications Manager-Verwaltung aus.  
Das Fenster Benutzer suchen und auflisten wird angezeigt.
- Schritt 2** Geben Sie die Suchkriterien ein und klicken Sie auf **Suchen**.
- Schritt 3** Wählen Sie in der angezeigten Eintragsliste den Link für den Benutzer aus.
- Schritt 4** Wählen Sie **Gerätezuordnung** aus.  
Das Fenster Benutzergerätezuordnung wird geöffnet.
- Schritt 5** Geben Sie die Suchkriterien ein und klicken Sie auf **Suchen**.
- Schritt 6** Wählen Sie das Gerät aus, das Sie dem Benutzer zuweisen möchten, indem Sie das Kontrollkästchen links neben dem Gerät aktivieren.
- Schritt 7** Wählen Sie **Auswahl/Änderungen speichern** aus, um dem Benutzer das Gerät zuzuweisen.
- Schritt 8** Wählen Sie in der Dropdown-Liste Ähnliche Links in der oberen rechten Fensterecke die Option **Zurück zum Benutzer** aus und klicken Sie auf **Los**.  
Das Fenster Benutzerkonfiguration wird angezeigt und die zugewiesenen Geräte, die Sie ausgewählt haben, werden unter Gesteuerte Geräte aufgelistet.
- Schritt 9** Wählen Sie **Auswahl/Änderungen speichern** aus.
-

## SRST (Survivable Remote Site Telephony)

SRST (Survivable Remote Site Telephony) stellt sicher, dass die Standardtelefonfunktionen weiterhin verfügbar sind, wenn die Kommunikation mit dem steuernden Cisco Unified Communications Manager unterbrochen wird. In diesem Szenario bleibt ein aktueller Anruf aktiv und der Benutzer kann auf eine Untergruppe der verfügbaren Funktionen zugreifen. Bei einem Failover wird auf dem Telefon eine Warnung angezeigt.

Weitere Informationen zu SRST finden Sie in <https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html>

In der folgenden Tabelle ist die Verfügbarkeit der Funktionen während eines Failovers angegeben.

**Tabelle 14: Unterstützte SRST-Funktionen**

Funktion	Unterstützt	Hinweise
Neuer Anruf	Ja	
Anruf beenden	Ja	
Wahlwiederholung	Ja	
Anrufannahme	Ja	
Halten	Ja	
Fortsetzen	Ja	
Konferenz	Ja	Nur Dreiweg und lokales Mischen.
Konferenzliste	Nein	
Übergabe	Ja	Nur mit Ansage.
Übergabe an aktive Anrufe (direkte Übergabe)	Nein	
Automatische Anrufannahme	Ja	
Anklopfen	Ja	
Anrufer-ID	Ja	
Unified-Sitzungspräsentation	Ja	Konferenz ist aufgrund anderen Funktionseinschränkungen die einzige unterstützte Funktion.
Voicemail	Ja	Die Voicemail wird nicht mit anderen Benutzern im Cisco Unified Communications Manager-Cluster synchronisiert.

Funktion	Unterstützt	Hinweise
Alle Anrufe umleiten	Ja	Der Weiterleitungsstatus ist nur auf dem Telefon verfügbar, das die Weiterleitung festlegt, da im SRST-Modus keine gemeinsam genutzte Leitung angezeigt wird. Die Einstellungen für Alle Anrufe weiterleiten werden beim Failover zu SRST von Cisco Unified Communications Manager oder bei einem SRST-Failback zu Communications Manager nicht beibehalten. Alle ursprünglichen Einstellungen für Alle Anrufe weiterleiten, die auf Communications Manager aktiv sind, sollten angezeigt werden, wenn das Gerät nach dem Failover wieder mit Communications Manager verbunden wird.
Kurzwahl	Ja	
An Voicemail (Sofortumleitung)	Nein	Der Softkey SofUml. wird nicht angezeigt.
Leitungsfiler	Teilweise	Leitungen werden unterstützt, können jedoch nicht gemeinsam genutzt werden.
Überwachung geparkter Anrufe	Nein	Der Softkey Parken wird nicht angezeigt.
Erweiterte Nachrichtenanzeige	Ja	Auf dem Telefonbildschirm werden Felder für die Anzahl von Nachrichten angezeigt.
Gezieltes Parken	Nein	Der Softkey wird nicht angezeigt.
Halten zurücksetzen	Ja	
Extern gehaltener Anruf	Nein	Anrufe werden als lokal gehaltene Anrufe angezeigt.
MeetMe	Nein	Der Softkey MeetMe wird nicht angezeigt.
Übernahme	Ja	
Gruppenübernahme	Nein	Der Softkey wird nicht angezeigt.
Andere Übernahme	Nein	Der Softkey wird nicht angezeigt.
Fangschaltung	Ja	
QRT	Ja	
Sammelanschlussgruppe	Nein	Der Softkey wird nicht angezeigt.
Mobilität	Nein	Der Softkey wird nicht angezeigt.
Privatfunktion	Nein	Der Softkey wird nicht angezeigt.

<b>Funktion</b>	<b>Unterstützt</b>	<b>Hinweise</b>
Rückruf	Nein	Der Softkey Rückruf wird nicht angezeigt.
Service-URL	Ja	Die programmierbare Leitungstaste mit der zugewiesenen Dienst-URL wird nicht angezeigt.







## KAPITEL 6

# Verwaltung des Selbstservice-Portals

- [Übersicht des Selbstservice-Portals, auf Seite 71](#)
- [Den Benutzerzugriff auf das Selbstservice-Portal konfigurieren, auf Seite 71](#)
- [Die Ansicht des Selbstservice-Portals anpassen, auf Seite 72](#)

## Übersicht des Selbstservice-Portals

Im Cisco Unified Communications Selbstservice-Portal können Benutzer die Funktionen und Einstellungen des Telefons anpassen und steuern.

Als Administrator steuern Sie den Zugriff auf das Selbstservice-Portal. Sie müssen Informationen an die Benutzer weitergeben, damit diese auf das Selbstservice-Portal zugreifen können.

Bevor ein Benutzer auf das Cisco Unified Communications Benutzerportal zugreifen kann, müssen Sie den Benutzer über Cisco Unified Communications Manager-Administration zu einer Cisco Unified Communications Manager-Standardbenutzergruppe hinzufügen.

Sie müssen den Benutzern die folgenden Informationen über das Selbstservice-Portal geben:

- Die URL, um auf die Anwendung zuzugreifen. Die URL lautet:  
`https://<server_name:portnumber>/ucmuser/`, wobei `server_name` der Host ist, auf dem der Webserver installiert ist, und `portnumber` für die Portnummer des Hosts steht.
- Eine Benutzer-ID und ein Standardkennwort, um auf die Anwendung zuzugreifen.
- Eine Übersicht der Aufgaben, die der Benutzer im Portal ausführen kann.

Diese Einstellungen entsprechen den Werten, die Sie eingegeben haben, als Sie den Benutzer zu Cisco Unified Communications Manager hinzugefügt haben.

Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Den Benutzerzugriff auf das Selbstservice-Portal konfigurieren

Bevor ein Benutzer auf das Selbstservice-Portal zugreifen kann, müssen Sie den Zugriff autorisieren.

**Prozedur**

- 
- Schritt 1** Wählen Sie unter Cisco Unified Communications Manager-Administration **Benutzerverwaltung > Endbenutzer** aus.
- Schritt 2** Suchen Sie den Benutzer.
- Schritt 3** Klicken Sie auf den Link Benutzer-ID.
- Schritt 4** Stellen Sie sicher, dass für den Benutzer ein Kennwort und eine PIN konfiguriert sind.
- Schritt 5** Stellen Sie Bereich „Berechtigungsinformationen“ sicher, dass die Gruppenliste **CCM-Standardbenutzer** enthält.
- Schritt 6** Wählen Sie **Speichern** aus.
- 

## Die Ansicht des Selbstservice-Portals anpassen

Die meisten Optionen werden im Selbstservice-Portal angezeigt. Die folgenden Optionen müssen jedoch mit den Einstellungen für die Enterprise-Parameterkonfiguration in der Cisco Unified Communications Manager-Verwaltung festgelegt werden:

- Ruftoneinstellungen anzeigen
- Einstellungen für Leitungsbezeichnung anzeigen




---

**Hinweis** Die Einstellungen gelten für alle Seiten des Selbstservice-Portals an Ihrem Standort.

---

**Prozedur**

- 
- Schritt 1** Wählen Sie **Gerät > Enterprise-Parameter** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Legen Sie im Selbstservice-Portal das Feld **Selbstservice-Portal-Standardserver** fest.
- Schritt 3** Aktivieren oder deaktivieren Sie die Parameter, auf die die Benutzer im Portal zugreifen können.
- Schritt 4** Wählen Sie **Speichern** aus.
-



## TEIL **III**

# Cisco IP-Konferenztelefon – Administration

- [Cisco IP-Konferenztelefon – Sicherheit, auf Seite 75](#)
- [Cisco IP-Konferenztelefon – Anpassung, auf Seite 93](#)
- [Cisco IP-Konferenztelefon – Funktionen und Einrichtung, auf Seite 97](#)
- [Unternehmensverzeichnis und persönliches Verzeichnis, auf Seite 131](#)





## KAPITEL 7

# Cisco IP-Konferenztelefon – Sicherheit

- [Übersicht der Sicherheit des Cisco IP Phone, auf Seite 75](#)
- [Sicherheitsverbesserungen für Ihr Telefonnetzwerk, auf Seite 76](#)
- [Unterstützte Sicherheitsfunktionen, auf Seite 77](#)

## Übersicht der Sicherheit des Cisco IP Phone

Die Sicherheitsfunktionen schützen vor mehreren Gefahren, beispielsweise der Gefährdung der Identität des Telefons und der Daten. Diese Funktionen erstellen und halten authentifizierte Kommunikationsstreams zwischen dem Telefon und dem Cisco Unified Communications Manager-Server aufrecht, und stellen sicher, dass das Telefon nur digital signierte Dateien verwendet.

In Cisco Unified Communications Manager Version 8.5(1) und höheren Versionen ist Security by Default implementiert. Diese Komponente stellt die folgenden Sicherheitsfunktionen für Cisco IP-Telefons ohne CTL-Client bereit:

- Signierung der Konfigurationsdateien für das Telefon
- Verschlüsselung der Telefonkonfigurationsdatei
- HTTPS mit Tomcat und andere Webservices



**Hinweis** Für sichere Signalübertragungs- und Medienfunktionen muss der CTL-Client jedoch weiterhin ausgeführt werden, und es ist weiterhin die Verwendung von Hardware-eToken erforderlich.

Weitere Informationen zu den Sicherheitsfunktionen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Nachdem Sie die für die CAPF (Certificate Authority Proxy Function) erforderlichen Aufgaben ausgeführt haben, wird auf den Telefonen ein LSC (Locally Significant Certificate) installiert. Sie können ein LSC in der Cisco Unified Communications Manager Administration-Verwaltung konfigurieren. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Ein LSC kann für EAP-TLS mit WLAN-Authentifizierung nicht als Benutzerzertifikat verwendet werden.

Alternativ dazu können Sie die Installation eines LSC auch im Menü „Sicherheits-Setup“ des Telefons veranlassen. In diesem Menü können Sie ein LSC auch aktualisieren und entfernen.

Das Cisco IP-Konferenztelefon 8832 entspricht dem FIPS (Federal Information Processing Standard). Um ordnungsgemäß zu funktionieren, ist für den FIPS-Modus eine RSA-Schlüssellänge von mindestens 2048 Bit erforderlich. Wenn das RSA-Serverzertifikat nicht 2048 Bit oder mehr umfasst, wird das Telefon nicht beim Cisco Unified Communications Manager registriert und die Meldung `Telefon konnte nicht registriert werden` erscheint. Die Größe des Zertifikatsschlüssels ist nicht FIPS-konform. wird in den Statusmeldungen des Telefons angezeigt.

Sie können im FIPS-Modus keine privaten Schlüssel (LSC oder MIC) verwenden.

Wenn das Telefon über ein vorhandenen LSC mit weniger als 2.048 Bits verfügt, müssen Sie die LSC-Schlüssellänge auf 2048 Bit oder mehr aktualisieren, bevor Sie FIPS aktivieren.

#### Verwandte Themen

[Einrichten eines LSC \(Locally Significant Certificate\)](#), auf Seite 79

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Sicherheitsverbesserungen für Ihr Telefonnetzwerk

Sie können Cisco Unified Communications Manager 11.5(1) und 12.0(1) ermöglichen, in einer Umgebung mit verbesserter Sicherheit zu arbeiten. Mit diesen Verbesserungen wird Ihr Telefonnetzwerk unter Anwendung einer Reihe von strengen Sicherheits- und Risikomanagementkontrollen betrieben, um Sie und die Benutzer zu schützen.

Cisco Unified Communications Manager 12.5 (1) unterstützt keine Umgebung mit verbesserter Sicherheit. Deaktivieren Sie FIPS, bevor Sie ein Upgrade auf Cisco Unified Communications Manager 12.5(1) vornehmen oder Ihr TFTP-Dienst wird nicht ordnungsgemäß funktionieren.

Die Umgebung mit verbesserter Sicherheit bietet die folgenden Funktionen:

- Kontaktsuchen-Authentifizierung
- TCP als Standardprotokoll für Remote-Audit-Protokolle
- FIPS-Modus
- Verbesserte Richtlinie für Anmeldeinformationen
- Unterstützung für die SHA-2-Hash-Familie für digitale Signaturen
- Unterstützung für eine RSA-Schlüsselgröße von 512 und 4096 Bits.

Mit Cisco Unified Communications Manager Version 14.0 und Cisco IP-Telefon-Firmware Version 14.0 und höher unterstützen die Telefone die SIP-OAuth-Authentifizierung.

OAuth wird für Proxy Trivial File Transfer Protocol (TFTP) mit Cisco Unified Communications Manager Version 14.0 (1) SU1 oder höher und Cisco IP-Telefon-Firmware Version 14.1 (1) unterstützt. Proxy-TFTP und OAuth für Proxy-TFTP werden für Mobile Remote Access (MRA) nicht unterstützt.

Weitere Informationen zur Sicherheit finden Sie unter:

- *Systemkonfigurationshandbuch für Cisco Unified Communications Manager*, Version 14.0(1) oder höher (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>)

- *Sicherheitshandbuch für 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: Funktionskonfigurationshandbuch für 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>)

**Hinweis**

Ihr Cisco IP-Telefon kann nur eine begrenzte Anzahl an Identity Trust List (ITL-)Dateien speichern. ITL-Dateien dürfen die Begrenzung von 64000 nicht überschreiten. Begrenzen Sie daher die Anzahl an Dateien, die Cisco Unified Communications Manager an das Telefon senden kann.

## Unterstützte Sicherheitsfunktionen

Die Sicherheitsfunktionen schützen vor mehreren Gefahren, beispielsweise der Gefährdung der Identität des Telefons und der Daten. Diese Funktionen erstellen und halten authentifizierte Kommunikationsstreams zwischen dem Telefon und dem Cisco Unified Communications Manager-Server aufrecht, und stellen sicher, dass das Telefon nur digital signierte Dateien verwendet.

In Cisco Unified Communications Manager Version 8.5(1) und höheren Versionen ist Security by Default implementiert. Diese Komponente stellt die folgenden Sicherheitsfunktionen für Cisco IP-Telefons ohne CTL-Client bereit:

- Signierung der Konfigurationsdateien für das Telefon
- Verschlüsselung der Telefonkonfigurationsdatei
- HTTPS mit Tomcat und andere Webservices

**Hinweis**

Für sichere Signalübertragungs- und Medienfunktionen muss der CTL-Client jedoch weiterhin ausgeführt werden, und es ist weiterhin die Verwendung von Hardware-eToken erforderlich.

Die Implementierung von Sicherheitsfunktionen in das Cisco Unified Communications Manager-System verhindert den Identitätsdiebstahl hinsichtlich Telefon und Cisco Unified Communications Manager-Server und schützt vor unbefugtem Zugriff auf Daten, Anrufsignale und Medien-Datenströme.

Zur Abwehr von Bedrohungen dieser Art erstellt das Cisco IP-Telefonienetzwerk zwischen Telefon und Server sichere (verschlüsselte) Kommunikationsdatenströme und erhält diese aufrecht, signiert Dateien digital, bevor diese auf ein Telefon übertragen werden, und verschlüsselt alle Mediendatenströme und Signale, die zwischen Cisco IP-Telefons übertragen werden.

Nachdem Sie die für die CAPF (Certificate Authority Proxy Function) erforderlichen Aufgaben ausgeführt haben, wird auf den Telefonen ein LSC (Locally Significant Certificate) installiert. Zum Konfigurieren eines LSC können Sie die Cisco Unified Communications Manager-Verwaltung verwenden. Die Vorgehensweise hierfür ist im Sicherheitshandbuch für Cisco Unified Communications Manager beschrieben. Alternativ dazu können Sie die Installation eines LSC auch im Menü „Sicherheits-Setup“ des Telefons veranlassen. In diesem Menü können Sie ein LSC auch aktualisieren und entfernen.

Ein LSC kann für EAP-TLS mit WLAN-Authentifizierung nicht als Benutzerzertifikat verwendet werden.

Im Telefonsicherheitsprofil ist definiert, ob das Gerät sicher oder nicht sicher ist. Weitere Informationen zum Anwenden des Sicherheitsprofils auf das Telefon finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.

Wenn Sie in der Cisco Unified Communications Manager-Verwaltung sicherheitsrelevante Einstellungen konfigurieren, sind in der Telefonkonfigurationsdatei auch vertrauliche Informationen enthalten. Damit die Konfigurationsdatei entsprechend ihrer Vertraulichkeit geschützt ist, müssen Sie die Datei so konfigurieren, dass eine Verschlüsselung erfolgt. Ausführliche Informationen hierzu finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.

Die Implementierung von Sicherheitsfunktionen in das Cisco Unified Communications Manager-System verhindert den Identitätsdiebstahl hinsichtlich Telefon und Cisco Unified Communications Manager-Server und schützt vor unbefugtem Zugriff auf Daten, Anrufsignale und Medien-Datenströme.

Die folgende Tabelle enthält eine Übersicht der Sicherheitsfunktionen, die von Cisco IP-Konferenztelefon 8832 unterstützt werden. Weitere Informationen zu diesen Funktionen und zur Sicherheit von Cisco Unified Communications Manager und Cisco IP-Telefon finden Sie in der Dokumentation zu Ihrer Version von Cisco Unified Communications Manager.

**Tabelle 15: Überblick der Sicherheitsfunktionen**

<b>Funktion</b>	<b>Beschreibung</b>
Imageauthentifizierung	Signierte Binärdateien (mit der Erweiterung SBN) verhindern. Wenn das Image manipuliert wurde, kann das Telefon nicht au
Installation des Zertifikats am Kundenstandort	Für jedes Telefon ist zur Geräteauthentifizierung ein eindeutiges Installed Certificate), aber für zusätzliche Sicherheit können Sie ein Zertifikat über die CAPF (Certificate Authority Proxy Function) auch über das Menü Sicherheitskonfiguration auf dem Telefon
Geräteauthentifizierung	Die Geräteauthentifizierung erfolgt zwischen dem Cisco Unified Certificate der anderen Entität akzeptiert. Bestimmt, ob eine sichere Verbindung hergestellt wird, und erstellt, falls erforderlich, mit dem Cisco Unified Communications Manager registriert Telefone nur, wenn sie
Dateiauthentifizierung	Überprüft digital signierte Dateien, die das Telefon heruntergeladen wurden, nachdem sie erstellt wurde, nicht manipuliert wurde. Dateien, die auf dem Telefon geschrieben. Das Telefon weist diese Dateien ohne
Signalisierungsauthentifizierung	Verwendet das TLS-Protokoll, um sicherzustellen, dass die Sign
MIC (Manufacturing Installed Certificate)	Auf jedem Telefon ist ein eindeutiges, vom Hersteller installiertes MIC, die Geräteauthentifizierung verwendet wird. Das MIC ist ein eindeutiges Certificate, das Cisco Unified Communications Manager, das Telefon zu authentifizieren.
Sichere SRST-Referenz	Nachdem Sie eine SRST-Referenz für die Sicherheit konfiguriert haben, Cisco Unified Communications Manager-Verwaltung zurückgesetzt haben, fügt der TFTP-Server die Referenz dem Telefon. Ein sicheres Telefon verwendet eine TLS-Verbindung



Funktion	Beschreibung
Medienverschlüsselung	Verwendet SRTP, um sicherzustellen, dass die Medienstreams an vorgesehenen Geräten empfangen und gelesen werden können. SRTP schützt den Datenstrom an die Geräte und schützt die Schlüssel, während diese über den Stream übertragen werden.
CAPF (Certificate Authority Proxy Function)	Implementiert Teile des Prozesses für die Zertifikatsgenerierung. Ein Telefon bei der Schlüsselgenerierung und Zertifikatsinstallation kann von kundenspezifischen Zertifizierungsstellen anzufragen oder von einem CAPF zu erhalten.
Sicherheitsprofile	Definiert, ob das Telefon nicht sicher, authentifiziert oder verschlüsselt sein soll.
Verschlüsselte Konfigurationsdateien	Ermöglicht Ihnen, den Datenschutz für Telefonkonfigurationen zu aktivieren.
Die Webserverfunktionalität für ein Telefon deaktivieren	Sie können den Zugriff auf eine Telefon-Webseite verhindern.
Telefonhärtung	Weitere Sicherheitsoptionen, die in der Cisco Unified Communications Manager Konfiguration für ein Telefon verfügbar sind. <ul style="list-style-type: none"> <li>• Zugriff auf die Webseiten für ein Telefon deaktivieren</li> </ul> <p><b>Hinweis</b> Sie können die aktuellen Einstellungen für die Telefonkonfigurationsmenü anzeigen.</p>
802.1X-Authentifizierung	Das Telefon kann die 802.1X-Authentifizierung verwenden.
AES 256-Verschlüsselung	Telefone, die mit Cisco Unified Communications Manager Version 8.5 oder höher konfiguriert sind, unterstützen TLS für TLS und SIP für die Signalisierung und Medienverschlüsselung. Diese Telefone unterstützen auch AES 256-Bit-Schlüsseln, die mit SHA-2 (Secure Hash Algorithm) und FIPS 140-2 (Federal Information Processing Standards) unterstützen. Die neuen Schlüssel: <ul style="list-style-type: none"> <li>• Für TLS-Verbindungen: <ul style="list-style-type: none"> <li>• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</li> <li>• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</li> </ul> </li> <li>• Für sRTP: <ul style="list-style-type: none"> <li>• AEAD_AES_256_GCM</li> <li>• AEAD_AES_128_GCM</li> </ul> </li> </ul> <p>Weitere Informationen finden Sie in der Dokumentation zu <a href="#">AES 256-Bit-Schlüssel</a>.</p>
Elliptic Curve Digital Signature Algorithm (ECDSA)-Zertifikate	Als Teil der Common Criteria(CC-)Zertifizierung hat Cisco ECDSA-Zertifikate für die Authentifizierung implementiert. Dies betrifft alle VOS-Produkte (Voice Operating System).

**Verwandte Themen**

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Einrichten eines LSC (Locally Significant Certificate)

Diese Aufgabe bezieht sich auf das Einrichten eines LSC mit der Methode der Authentifizierungszeichenfolge.

## Vorbereitungen

Stellen Sie sicher, dass die Sicherheitskonfiguration von Cisco Unified Communications Manager und CAPF (Certificate Authority Proxy Function) vollständig ist:

- Die CTL- oder ITL-Datei hat ein CAPF-Zertifikat.
- Überprüfen Sie in der Cisco Unified Communications Operating System-Verwaltung, ob das CAPF-Zertifikat installiert ist.
- CAPF wird ausgeführt und ist konfiguriert.

Weitere Informationen zu diesen Einstellungen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

## Prozedur

- 
- Schritt 1** Sie benötigen den CAPF-Authentifizierungscode, der während der Konfiguration von CAPF festgelegt wurde.
- Schritt 2** Wählen Sie auf dem Telefon **Einstellungen** aus.
- Schritt 3** Wählen Sie **Administratoreinstellungen > Sicherheits-Setup** aus.

**Hinweis** Sie können den Zugriff auf das Menü „Einstellungen“ mit dem Feld „Zugriff auf Einstellungen“ im Fenster „Telefonkonfiguration“ in der Cisco Unified Communications Manager-Verwaltung steuern.

- Schritt 4** Wählen Sie **LSC** aus und drücken Sie **Auswählen** oder **Aktualisieren**.  
Das Telefon fordert eine Authentifizierungszeichenfolge an.

- Schritt 5** Geben Sie die Authentifizierungscode ein und drücken Sie **Senden**.

Das Telefon installiert, aktualisiert oder entfernt das LSC, abhängig davon, wie CAPF konfiguriert ist. Während des Verfahrens werden mehrere Meldungen im LSC-Optionsfeld im Menü Sicherheitskonfiguration angezeigt, damit Sie den Status überwachen können. Wenn das Verfahren abgeschlossen ist, wird **Installiert** oder **Nicht installiert** auf dem Telefon angezeigt.

Der Prozess zum Installieren, Aktualisieren oder Entfernen des LSC kann längere Zeit dauern.

Wenn das Telefon erfolgreich installiert wurde, wird die Meldung **Installiert** angezeigt. Wenn das Telefon **Nicht installiert** anzeigt, ist möglicherweise die Autorisierungszeichenfolge ungültig oder das Telefon ist nicht für Updates aktiviert. Wenn der CAPF-Vorgang die LSC löscht, zeigt das Telefon **Nicht installiert** an. Der CAPF-Server protokolliert die Fehlermeldungen. Der Pfad zu den Protokollen und die Bedeutung der Fehlermeldungen werden in der CAPF-Serverdokumentation beschrieben.

---

## Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Aktivieren des FIPS-Modus


### Prozedur

- 
- |                  |  |
|------------------|--|
| <b>Schritt 1</b> | Wählen Sie in Cisco Unified Communications Manager Administration <b>Gerät &gt; Telefon</b> aus, und navigieren Sie zum Telefon. |
| <b>Schritt 2</b> | Navigieren Sie zum produktspezifischen Konfigurationsbereich.  |
| <b>Schritt 3</b> | Legen Sie das Feld <b>FIPS-Modus</b> auf „Aktiviert“ fest.   |
| <b>Schritt 4</b> | Wählen Sie <b>Konfiguration übernehmen</b> .   |
| <b>Schritt 5</b> | Wählen Sie <b>Speichern</b> aus.   |
| <b>Schritt 6</b> | Starten Sie das Telefon neu.   |
- 

## Anrufssicherheit

Wenn die Sicherheit für ein Telefon implementiert wird, können sichere Anrufe auf dem Telefondisplay mit Symbolen gekennzeichnet werden. Sie können auch bestimmen, ob das verbundene Telefon sicher und geschützt ist, wenn zu Beginn des Anrufs ein Sicherheitssignal ausgegeben wird.

In einem sicheren Anruf sind alle Anrufsignale und Medienstreams verschlüsselt. Ein sicherer Anruf bietet eine hohe Sicherheitsstufe und stellt die Integrität und den Datenschutz des Anrufs sicher. Wenn ein aktiver Anruf verschlüsselt wird, ändert sich das Anrufstatus-Symbol rechts neben der Anrufdauer in das folgende

Symbol:  .




---

**Hinweis** Wenn der Anruf über nicht-IP-Anrufabschnitte, beispielsweise ein Festnetz, geleitet wird, ist der Anruf möglicherweise nicht sicher, auch wenn er im IP-Netzwerk verschlüsselt wurde und ein Schloss-Symbol angezeigt wird.

---

Zu Beginn eines sicheren Anrufs wird ein Sicherheitssignal ausgegeben, das angibt, dass das andere verbundene Telefon ebenfalls sicheres Audio empfangen und senden kann. Wenn Sie mit einem nicht sicheren Telefon verbunden sind, wird kein Sicherheitssignal ausgegeben.




---

**Hinweis** Sichere Anrufe werden zwischen zwei Telefonen unterstützt. Sichere Konferenzen, Cisco Extension Mobility und gemeinsam genutzte Leitungen können über eine sichere Konferenzbrücke konfiguriert werden.

---


Wenn ein Telefon in Cisco Unified Communications Manager als sicher (verschlüsselt und vertrauenswürdig) konfiguriert wird, kann es den Status „Geschützt“ erhalten. Anschließend kann das geschützte Telefon so konfiguriert werden, dass es zu Beginn eines Anrufs einen Signalton ausgibt.

- Geschütztes Gerät: Um den Status eines sicheren Telefons in „Geschützt“ zu ändern, aktivieren Sie das Kontrollkästchen „Geschütztes Gerät“ im Fenster „Telefonkonfiguration“ in Cisco Unified Communications Manager Administration (**Gerät > Telefon**).

- Sicherheitssignal ausgeben: Damit das geschützte Telefon ein Signal ausgibt, das angibt, ob der Anruf sicher oder nicht sicher ist, legen Sie die Einstellung Sicherheitssignal ausgeben auf True fest. Die Einstellung Sicherheitssignal ausgeben ist standardmäßig auf False festgelegt. Sie legen diese Option in der Cisco Unified Communications Manager-Verwaltung fest (**System > Serviceparameter**). Wählen Sie den Server und anschließend den Unified Communications Manager-Service aus. Wählen Sie im Fenster Serviceparameterkonfiguration die Option unter Funktion - Sicherheitssignal aus. Der Standardwert ist False.

## Sichere Konferenzeruf-ID

Sie können einen sicheren Konferenzeruf initiieren und die Sicherheitsstufe der Teilnehmer überwachen. Ein sicherer Konferenzeruf wird mit diesem Prozess initiiert:

1. Ein Benutzer startet die Konferenz auf einem sicheren Telefon.
2. Cisco Unified Communications Manager weist dem Anruf eine sichere Konferenzbrücke zu.
3. Während Teilnehmer hinzugefügt werden, überprüft Cisco Unified Communications Manager den Sicherheitsmodus aller Telefone und hält die Sicherheitsstufe für die Konferenz aufrecht.
4. Das Telefon zeigt die Sicherheitsstufe des Konferenzerufs an. Eine sichere Konferenz zeigt das Sicherheitssymbol  rechts neben **Konferenz** auf dem Telefon an.



### Hinweis

Sichere Anrufe werden zwischen zwei Telefonen unterstützt. Für geschützte Telefone sind einige Funktionen, beispielsweise Konferenzerufe, gemeinsam genutzte Leitungen und die Anschlussmobilität, nicht verfügbar, wenn sichere Anrufe konfiguriert sind.

Die folgende Tabelle enthält Informationen zu den Änderungen der Konferenzsicherheitsstufe, abhängig von der Sicherheitsstufe des Telefons des Initiators und der Verfügbarkeit von sicheren Konferenzbrücken.

**Tabelle 16: Sicherheitseinschränkungen für Konferenzerufe**


Sicherheitsstufe des Telefons des Initiators	Verwendete Funktion	Sicherheitsstufe der Teilnehmer	Ergebnisse der Aktion
Nicht sicher	Konferenz	Sicher	Nicht sichere Konferenzbrücke Nicht sichere Konferenz
Sicher	Konferenz	Mindestens ein Mitglied ist nicht sicher.	Sichere Konferenzbrücke Nicht sichere Konferenz
Sicher	Konferenz	Sicher	Sichere Konferenzbrücke Verschlüsselungsstufe der sicheren Konferenz
Nicht sicher	MeetMe	Die minimale Sicherheitsstufe ist verschlüsselt.	Der Initiator erhält die Meldung Sicherheit nicht erfüllt, Anruf abgelehnt.

Sicherheitsstufe des Telefons des Initiators	Verwendete Funktion	Sicherheitsstufe der Teilnehmer	Ergebnisse der Aktion
Sicher	MeetMe	Die minimale Sicherheitsstufe ist nicht sicher.	Sichere Konferenzbrücke Die Konferenz nimmt alle Anrufe an.

## Sichere Anruf-ID

Ein sicherer Anruf wird initiiert, wenn Ihr Telefon und das Telefon des anderen Teilnehmers für sichere Anrufe konfiguriert ist. Das andere Telefon kann sich im gleichen Cisco IP-Netzwerk oder in einem Netzwerk außerhalb des IP-Netzwerks befinden. Sichere Anrufe sind nur zwischen zwei Telefonen möglich. Konferenzanrufe sollten sichere Anrufe unterstützen, nachdem eine sichere Konferenzbrücke konfiguriert wurde.

Ein sicherer Anruf wird mit diesem Prozess initiiert:

1. Der Benutzer initiiert einen Anruf auf einem geschützten Telefon (Sicherheitsmodus).
2. Das Telefon zeigt das Sicherheitssymbol  auf dem Telefondisplay an. Dieses Symbol zeigt an, dass das Telefon für sichere Anrufe konfiguriert ist. Dies bedeutet jedoch nicht, dass das andere verbundene Telefon ebenfalls geschützt ist.
3. Der Benutzer hört einen Signalton, wenn der Anruf mit einem anderen sicheren Telefon verbunden wird, der angibt, dass beide Enden der Konversation verschlüsselt und geschützt sind. Wenn der Anruf mit einem nicht sicheren Telefon verbunden wird, hört der Benutzer keinen Signalton.



**Hinweis** Sichere Anrufe werden zwischen zwei Telefonen unterstützt. Für geschützte Telefone sind einige Funktionen, beispielsweise Konferenzanrufe, gemeinsam genutzte Leitungen und die Anschlussmobilität, nicht verfügbar, wenn sichere Anrufe konfiguriert sind.

Ein Sicherheitssignal wird nur auf einem geschützten Telefon ausgegeben. Auf einem nicht geschützten Telefon wird kein Signalton ausgegeben. Wenn sich der Gesamtstatus des Anrufs während des Anrufs ändert, gibt das geschützte Telefon den geänderten Signalton wieder.

Geschützte Telefone spielen unter folgenden Umständen einen Signalton ab:

- Wenn die Option Sicherheitssignalton aktiviert ist:
  - Wenn auf beiden Seiten sichere Medien eingerichtet sind und der Anrufstatus „Sicher“ lautet, gibt das Telefon das Signal für eine sichere Verbindung wieder (drei lange Signaltöne mit Pausen).
  - Wenn auf beiden Seiten nicht sichere Medien eingerichtet sind und der Anrufstatus „Nicht sicher“ lautet, wird das Signal für eine nicht sichere Verbindung abgespielt (sechs kurze Signaltöne mit kurzen Pausen).

Wenn die Option Sicherheitssignalton wiedergeben deaktiviert ist, erklingt kein Signalton.

## Verschlüsselung für Aufschaltung bereitstellen

Cisco Unified Communications Manager überprüft den Sicherheitsstatus des Telefons, wenn Konferenzen erstellt werden, und ändert die Sicherheitsanzeige für die Konferenz oder blockiert die Durchführung des Anrufs, um Integrität und Sicherheit im System aufrechtzuerhalten.

Ein Benutzer kann sich nicht auf einen verschlüsselten Anruf aufschalten, wenn das für die Aufschaltung verwendete Telefon nicht für die Verschlüsselung konfiguriert ist. Wenn in einem solchen Fall die Aufschaltung fehlschlägt, wird auf dem Telefon, auf dem die Aufschaltung initiiert wurde, ein „Verbindung nicht möglich“-Ton (schneller Besetztton) ausgegeben.

Wenn das Telefon des Initiators für die Verschlüsselung konfiguriert ist, kann sich der Initiator der Aufschaltung über das verschlüsselte Telefon auf einen nicht sicheren Anruf aufschalten. Nach der Aufschaltung klassifiziert Cisco Unified Communications Manager den Anruf als nicht sicher.

Wenn das Telefon des Initiators für die Verschlüsselung konfiguriert ist, kann der Initiator der Aufschaltung sich auf einen verschlüsselten Anruf aufschalten. Auf dem Telefon wird dann angezeigt, dass der Anruf verschlüsselt ist.

## WLAN-Sicherheit

Da alle WLAN-Geräte, die sich innerhalb der Reichweite befinden, den gesamten anderen WLAN-Datenverkehr empfangen können, ist die Sicherung der Sprachkommunikation in einem WLAN besonders wichtig. Um zu verhindern, dass der Sprachdatenverkehr von Angreifern manipuliert oder abgefangen wird, unterstützt die Cisco SAFE-Sicherheitsarchitektur das Cisco IP-Telefon und Cisco Aironet Access Points. Weitere Informationen zur Sicherheit in Netzwerken finden Sie unter [http://www.cisco.com/en/US/netsol/ns744/networking\\_solutions\\_program\\_home.html](http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html).

Die Cisco Wireless IP-Telefonlösung bietet Sicherheit für Wireless-Netzwerke, die nicht autorisierte Anmeldungen und kompromittierte Kommunikation mithilfe der folgenden, durch das Cisco Wireless IP-Telefon unterstützten Authentifizierungsmethoden verhindert:

- **Offene Authentifizierung:** In einem offenen System kann jedes kabellose Gerät die Authentifizierung anfordern. Der Access Point, der die Anforderung empfängt, kann die Authentifizierung entweder jedem Anforderer oder nur denjenigen Anforderern gewähren, die in einer Benutzerliste aufgeführt sind. Die Kommunikation zwischen dem kabellosen Gerät und dem Access Point kann entweder unverschlüsselt sein, oder die Geräte können zur Gewährleistung der Sicherheit WEP-Schlüssel (Wired Equivalent Privacy) verwenden. Geräte, die WEP verwenden, versuchen sich nur bei einem Access Point zu authentifizieren, der ebenfalls WEP verwendet.
- **EAP-FAST-Authentifizierung (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling):** Diese Client-Server-Sicherheitsarchitektur verschlüsselt EAP-Transaktionen innerhalb eines TLS-Tunnels (Transport Layer Security) zwischen dem Access Point und dem RADIUS-Server, z. B. dem Cisco ACS (Access Control Server).

Der TLS-Tunnel verwendet PACs (Protected Access Credentials) für die Authentifizierung zwischen dem Client (Telefon) und dem RADIUS-Server. Der Server sendet eine Autoritäts-ID (Authority ID, AID) an den Client (Telefon), der wiederum die richtige PAC auswählt. Der Client (Telefon) gibt einen PAC-Opaque-Wert an den RADIUS-Server zurück. Der Server entschlüsselt die PAC mit dem primären Schlüssel. Beide Endpunkte verfügen nun über den PAC-Schlüssel, und ein TLS-Tunnel wird erstellt. EAP-FAST unterstützt die automatische PAC-Bereitstellung, muss jedoch auf dem RADIUS-Server aktiviert werden.



**Hinweis** Auf dem Cisco ACS läuft die PAC standardmäßig nach einer Woche ab. Wenn auf dem Telefon eine abgelaufene PAC vorhanden ist, dauert die Authentifizierung beim RADIUS-Server länger, da das Telefon eine neue PAC abrufen muss. Um Verzögerungen bei der PAC-Bereitstellung zu vermeiden, sollten Sie den Ablaufzeitraum für die PAC auf dem ACS oder RADIUS-Server auf mindestens 90 Tage festlegen.

- Extensible Authentication Protocol-Transport Layer Security-(EAP-TLS-)-Authentifizierung: EAP-TLS erfordert ein Client-Zertifikat für Authentifizierung und Netzwerkzugriff. Bei einem kabelgebundenen EAP-TLS kann es sich beim Client-Zertifikat entweder um das MIC oder das LSC des Telefons handeln. LSC ist das empfohlene Client-Authentifizierungszertifikat für kabelgebundenes EAP-TLS.
- PEAP (Protected Extensible Authentication Protocol): ein von Cisco entwickeltes, kennwortbasiertes Schema zur gegenseitigen Authentifizierung zwischen Client (Telefon) und RADIUS-Server. Das Cisco IP-Telefon kann PEAP für die Authentifizierung beim Wireless-Netzwerk verwenden. Es wird nur PEAP-MSCHAPV2 unterstützt. PEAP-GTC wird nicht unterstützt.

Folgende Authentifizierungsschemata verwenden den RADIUS-Server, um Authentifizierungsschlüssel zu verwalten:

- WPA/WPA2: Verwendet RADIUS-Serverinformationen, um eindeutige Authentifizierungsschlüssel zu generieren. Da diese Schlüssel auf dem zentralen RADIUS-Server generiert werden, bietet WPA/WPA2 eine höhere Sicherheit als die vorinstallierten WPA-Schlüssel, die am Access Point und auf dem Telefon gespeichert sind.
- Fast Secure Roaming: Verwendet RADIUS-Serverinformationen und WDS-Informationen (Wireless Domain Server), um Schlüssel zu verwalten und zu authentifizieren. Der WDS erstellt einen Cache mit Sicherheitsanmeldedaten für CCKM-fähige Client-Geräte, um eine schnelle und sichere erneute Authentifizierung zu gewährleisten. Die Cisco IP-Telefon 8800-Serie unterstützt 802.11r (FT). Sowohl 11r (FT) als auch CCKM werden unterstützt, um ein schnelles, sicheres Roaming zu ermöglichen. Jedoch Cisco empfiehlt dringend die 802.11r (links) über Air Methode nutzen.

Bei WPA/WPA2 und CCKM werden die Verschlüsselungsschlüssel nicht auf dem Telefon eingegeben, sondern zwischen dem Access Point und dem Telefon automatisch abgeleitet. Der EAP-Benutzername und das Kennwort, die zur Authentifizierung verwendet werden, müssen jedoch auf jedem Telefon eingegeben werden.

Um die Sicherheit des Sprachdatenverkehrs zu gewährleisten, unterstützt das Cisco IP-Telefon die Verschlüsselung mit WEP, TKIP und AES (Advanced Encryption Standard). Bei diesen Verschlüsselungsmechanismen werden sowohl die SIP-Signalkpakete als auch die RTP-Pakete (Real-Time Transport Protocol) zwischen dem Access Point und dem Cisco IP-Telefon verschlüsselt.

## WEP

Bei Verwendung von WEP in einem Wireless-Netzwerk erfolgt die Authentifizierung am Access Point mit offener Authentifizierung oder Authentifizierung über einen gemeinsamen Schlüssel. Der auf dem Telefon eingerichtete WEP-Schlüssel muss mit dem am Access Point konfigurierten WEP-Schlüssel übereinstimmen, um erfolgreiche Verbindungen zu ermöglichen. Das Cisco IP-Telefon unterstützt WEP-Schlüssel, die 40- oder 128-Bit-Verschlüsselung verwenden und auf dem Telefon und am Access Point statisch bleiben.

Bei der EAP- und der CCKM-Authentifizierung können zur Verschlüsselung WEP-Schlüssel verwendet werden. Der RADIUS-Server verwaltet den WEP-Schlüssel und übergibt nach der Authentifizierung einen eindeutigen Schlüssel zur Verschlüsselung aller Sprachpakete an den Access Point. Daher können sich diese WEP-Schlüssel mit jeder Authentifizierung ändern.

### TKIP

WPA und CCKM verwenden die TKIP-Verschlüsselung. Dabei handelt es sich um eine Methode, die im Vergleich zu WEP mehrere Verbesserungen aufweist. TKIP ermöglicht die Verschlüsselung einzelner Pakete und bietet längere Initialisierungsvektoren (IVs), um die Sicherheit der Verschlüsselung zu erhöhen. Darüber hinaus gewährleistet eine Nachrichtenintegritätsprüfung, dass die verschlüsselten Pakete nicht geändert werden. TKIP besitzt nicht die Vorhersehbarkeit von WEP, die es Angreifern ermöglicht, den WEP-Schlüssel zu entschlüsseln.

### AES

Eine Verschlüsselungsmethode, die für die WPA2-Authentifizierung verwendet wird. Dieser nationale Verschlüsselungsstandard verwendet einen symmetrischen Algorithmus, bei dem die Schlüssel für Ver- und Entschlüsselung identisch sind. AES verwendet CBC-Verschlüsselung (Cipher Blocking Chain) mit einer Größe von 128 Bit, wodurch Schlüssellängen von mindestens 128 Bit, 192 Bit und 256 Bit unterstützt werden. Das Cisco IP-Telefon unterstützt eine Schlüssellänge von 256 Bit.




---

**Hinweis** Das Cisco IP-Telefon bietet keine Unterstützung für CKIP (Cisco Key Integrity Protocol) mit CMIC.

---

Authentifizierungs- und Verschlüsselungsschemata werden innerhalb des Wireless LAN eingerichtet. VLANs werden im Netzwerk und an den Access Points konfiguriert und geben verschiedene Kombinationen von Authentifizierung und Verschlüsselung an. Eine SSID wird einem VLAN und dem spezifischen Authentifizierungs- und Verschlüsselungsschema zugeordnet. Damit kabellose Client-Geräte erfolgreich authentifiziert werden können, müssen Sie an den Access Points und auf dem Cisco IP-Telefon die gleichen SSIDs mit ihren Authentifizierungs- und Verschlüsselungsschemata konfigurieren.

Einige Authentifizierungsschemata erfordern bestimmte Arten von Verschlüsselung. Mit der offenen Authentifizierung können Sie für zusätzliche Sicherheit die statische WEP-Verschlüsselung verwenden. Wenn Sie jedoch die Authentifizierung über einen gemeinsamen Schlüssel verwenden, müssen Sie statisches WEP als Verschlüsselung festlegen und einen WEP-Schlüssel auf dem Telefon konfigurieren.



- 
- Hinweis**
- Wenn Sie WPA Pre-shared Key oder WPA2 Pre-shared Key verwenden, muss der vorinstallierte Schlüssel auf dem Telefon statisch festgelegt werden. Diese Schlüssel müssen mit den Schlüsseln am Access Point übereinstimmen.
  - Das Cisco IP-Telefon unterstützt die automatische EAP-Aushandlung nicht. Wenn der EAP-FAST-Modus verwendet werden soll, müssen Sie diesen festlegen.
- 

Die folgende Tabelle enthält eine Liste der Authentifizierungs- und Verschlüsselungsschemata, die auf den vom Cisco IP-Telefon unterstützten Cisco Aironet Access Points konfiguriert werden können. Die Tabelle zeigt die Netzwerkkonfigurationsoption für das Telefon, die der Konfiguration des Access Points entspricht.



Tabelle 17: Authentifizierungs- und Verschlüsselungsschemata

Konfiguration des Cisco IP-Telefon	Konfiguration des Access Points			
	Sicherheit	Schlüsselverwaltung	Verschlüsselung	Schnelles Roaming
Keine	Keine	Keine	Keine	–
WEP	Statisches WEP	Statisch	WEP	–
PSK	PSK	WPA	TKIP	Kein
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Weitere Informationen zum Konfigurieren von Authentifizierungs- und Verschlüsselungsschemata auf Access Points finden Sie im *Cisco Aironet Configuration Guide* (Konfigurationshandbuch für Cisco Aironet) zu Ihrem Modell und Ihrer Version unter folgender URL:

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

## Wireless LAN-Sicherheit

Cisco Telefone, die Wi-Fi unterstützen, besitzen mehr Sicherheitsanforderungen und benötigen eine zusätzliche Konfiguration. Diese zusätzlichen Schritte umfassen die Installation von Zertifikaten und die Einrichtung der Sicherheit auf den Telefonen und auf dem Cisco Unified Communications Manager.

Weitere Informationen finden Sie im *Sicherheitshandbuch für Cisco Unified Communications Manager*.

## Verwaltungsseite für das Cisco IP-Telefon

Für Cisco Telefone, die Wi-Fi unterstützen, sind spezielle Webseiten verfügbar, die sich von den Webseiten für andere Telefone unterscheiden. Sie verwenden diese speziellen Webseiten für die Sicherheitskonfiguration der Telefone, wenn SCEP (Simple Certificate Enrollment Protocol) nicht verfügbar ist. Auf diesen Webseiten können Sie Sicherheitszertifikate auf einem Telefon installieren, ein Sicherheitszertifikat herunterladen oder das Datum und die Uhrzeit des Telefons manuell konfigurieren.

Die Webseiten zeigen die gleichen Informationen wie die Webseiten für andere Telefone an, einschließlich die Geräteinformationen, Protokolle und Statistiken.

### Konfigurieren der Verwaltungsseite für das Telefon

Die Verwaltungswebseite ist bei Auslieferung des Telefons aktiviert, und das Kennwort ist auf „Cisco“ festgelegt. Wenn ein Telefon jedoch beim Cisco Unified Communications Manager registriert wird, muss die Verwaltungswebseite aktiviert und ein neues Kennwort konfiguriert werden.

Aktivieren Sie diese Webseite, und legen Sie vor der erstmaligen Verwendung der Webseite, nachdem das Telefon registriert wurde, die Anmeldeinformationen fest.

Nach der Aktivierung können Sie über HTTPS-Port 8443 auf die Verwaltungswebseite zugreifen (**https://x.x.x.x:8443**, wobei x.x.x.x die IP-Adresse eines Telefons ist).

#### Vorbereitungen

Legen Sie vor der Aktivierung der Verwaltungswebseite ein Kennwort fest. Das Kennwort kann eine beliebige Kombination aus Buchstaben oder Ziffern sein, muss aber zwischen 8 und 127 Zeichen umfassen.

Ihr Benutzername ist dauerhaft auf „Admin“ festgelegt.

#### Prozedur

- 
- Schritt 1** Wählen Sie **Gerät > Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.
  - Schritt 2** Navigieren Sie zu Ihrem Telefon.
  - Schritt 3** Legen Sie im Abschnitt **Produktspezifische Konfiguration** den Parameter **Webadministrator** auf **Aktiviert** fest.
  - Schritt 4** Geben Sie im Feld **Administrator-Kennwort** ein Kennwort ein.
  - Schritt 5** Wählen Sie **Speichern** aus, und klicken Sie auf **OK**.
  - Schritt 6** Wählen Sie **Konfiguration übernehmen** aus, und klicken Sie auf **OK**.
  - Schritt 7** Starten Sie das Telefon neu.
- 

### Auf die Administrations-Webseite des Telefons zugreifen

Wenn Sie auf die Verwaltungswebseiten zugreifen möchten, müssen Sie den Verwaltungsport angeben.

#### Prozedur

- 
- Schritt 1** Rufen Sie die IP-Adresse des Telefons ab:
    - Wählen Sie in Cisco Unified Communications Manager Administration **Gerät > Telefon** aus, und navigieren Sie zum Telefon. Für Telefone, die sich beim Cisco Unified Communications Manager registrieren, wird die IP-Adresse im Fenster **Telefone suchen und auflisten** sowie oben im Fenster **Telefonkonfiguration** angezeigt.
  - Schritt 2** Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein, wobei *IP-Adresse* für die jeweilige IP-Adresse des Cisco IP-Telefon steht:
 

```
https://<IP_address>:8443
```

**Schritt 3** Geben Sie im Feld „Kennwort“ das Kennwort ein.

**Schritt 4** Klicken Sie auf **Senden**.

---

### Installieren eines Benutzerzertifikats über die Webseite zur Telefonverwaltung

Sie können ein Benutzerzertifikat manuell auf dem Telefon installieren, wenn das SCEP (Simple Certificate Enrollment Protocol) nicht verfügbar ist.

Das vom Hersteller installierte Zertifikat (MIC) kann als das Benutzerzertifikat für EAP-TLS verwendet werden.

Nachdem das Benutzerzertifikat installiert wurde, müssen Sie es der Vertrauensliste des RADIUS-Servers hinzufügen.

#### Vorbereitungen

Bevor Sie ein Benutzerzertifikat für ein Telefon installieren können, benötigen Sie Folgendes:

- Ein Benutzerzertifikat muss auf Ihrem PC gespeichert sein. Das Zertifikat muss im PKCS #12-Format vorliegen.
- Das genaue Kennwort des Zertifikats.

#### Prozedur

---

**Schritt 1** Wählen Sie auf der Webseite für die Telefonverwaltung **Zertifikate** aus.

**Schritt 2** Navigieren Sie zum Zertifikat auf Ihren PC.

**Schritt 3** Geben Sie im Feld **Kennwort extrahieren** das Extraktionskennwort des Zertifikats an.

**Schritt 4** Klicken Sie auf **Hochladen**.

**Schritt 5** Starten Sie das Telefon neu, nachdem der Upload abgeschlossen ist.

---

### Installieren eines Authentifizierungsserver-Zertifikats über die Webseite zur Telefonverwaltung

Sie können ein Authentifizierungsserver-Zertifikat manuell auf dem Telefon installieren, wenn das SCEP (Simple Certificate Enrollment Protocol) nicht verfügbar ist.

Das CA-Stammzertifikat, über das das RADIUS-Serverzertifikat ausgestellt wurde, muss für EAP-TLS installiert sein.

#### Vorbereitungen

Bevor Sie ein Zertifikat auf einem Telefon installieren können, müssen Sie ein Authentifizierungsserver-Zertifikat auf Ihrem PC gespeichert haben. Das Zertifikat muss in PEM (Base-64) oder DER codiert sein.

#### Prozedur

---

**Schritt 1** Wählen Sie auf der Webseite für die Telefonverwaltung **Zertifikate** aus.

## Manuelles Entfernen eines Sicherheitszertifikats von der Webseite zur Telefonverwaltung

- Schritt 2** Navigieren Sie zum Feld **Authentifizierungsserver-Zertifikat (Administrator-Webseite)** und klicken Sie auf **Installieren**.
- Schritt 3** Navigieren Sie zum Zertifikat auf Ihren PC.
- Schritt 4** Klicken Sie auf **Hochladen**.
- Schritt 5** Starten Sie das Telefon neu, nachdem der Upload abgeschlossen ist.
- Wenn Sie mehr als ein Zertifikat installieren, installieren Sie alle Zertifikate vor dem Neustart des Telefons.
- 

## Manuelles Entfernen eines Sicherheitszertifikats von der Webseite zur Telefonverwaltung

Sie können ein Sicherheitszertifikat manuell von einem Telefon entfernen, wenn das SCEP (Simple Certificate Enrollment Protocol) nicht verfügbar ist.

### Prozedur

---

- Schritt 1** Wählen Sie auf der Webseite für die Telefonverwaltung **Zertifikate** aus.
- Schritt 2** Navigieren Sie auf der Seite **Zertifikate** zum Zertifikat.
- Schritt 3** Klicken Sie auf **Löschen**.
- Schritt 4** Starten Sie das Telefon nach Abschluss des Löschvorgangs neu.
- 

## Manuelles Festlegen des Datums und der Uhrzeit des Telefons

Bei einer auf Zertifikaten basierenden Authentifizierung müssen auf dem Telefon das richtige Datum und die richtige Uhrzeit angezeigt werden. Ein Authentifizierungsserver vergleicht das Datum und die Uhrzeit des Telefons mit dem Ablaufdatum des Zertifikats. Wenn Datum und Uhrzeit auf dem Telefon und dem Server nicht übereinstimmen, funktioniert das Telefon nicht mehr.

Verwenden Sie dieses Verfahren, um das Datum und die Uhrzeit auf dem Telefon manuell einzustellen, wenn das Telefon die richtige Informationen nicht über das Netzwerk abrufen kann.

### Prozedur

---

- Schritt 1** Führen Sie auf der Webseite zu Telefonverwaltung einen Bildlauf zu **Datum und Uhrzeit** durch.
- Schritt 2** Führen Sie einen der folgenden Schritte aus:
- Klicken Sie auf **Telefon auf lokales Datum und lokale Zeit festlegen**, um das Telefon mit einem lokalen Server zu synchronisieren.
  - Wählen Sie im Feld **Datum und Uhrzeit angeben** in den Menüs den Monat, den Tag, das Jahr, die Stunde, die Minute und die Sekunde aus, und klicken Sie auf **Telefon auf bestimmtes Datum und bestimmte Zeit festlegen**.
-

## SCEP-Konfiguration

SCEP (Simple Certificate Enrollment Protocol) ist der Standard für die automatische Bereitstellung und Erneuerung von Zertifikaten. Mit SCEP müssen Zertifikate nicht manuell auf Ihrem Telefon installiert werden.

### Konfigurieren der produktspezifischen SCEP-Konfigurationsparameter

Sie müssen die folgenden SCEP-Parameter auf der Telefon-Webseite konfigurieren.

- RA-IP-Adresse
- SHA-1- oder SHA-256-Fingerabdruck des CA-Stammzertifikats für den SCEP-Server

Die Cisco IOS-Registrierungsstelle (RA) dient als Proxy für den SCEP-Server. Der SCEP-Client auf dem Telefon verwendet die Parameter, die von Cisco Unified Communication Manager heruntergeladen werden. Nachdem Sie die Parameter konfiguriert haben, sendet das Telefon eine SCEP `getcs`-Anforderung an die RA, und das CA-Stammzertifikat wird mithilfe des definierten Fingerabdrucks validiert.

### Prozedur

- 
- |                  |   |
|------------------|---|
| <b>Schritt 1</b> | Wählen Sie <b>Gerät &gt; Telefon</b> in der Cisco Unified Communications Manager-Verwaltung aus.  |
| <b>Schritt 2</b> | Suchen Sie das Telefon.   |
| <b>Schritt 3</b> | Navigieren Sie zum Bereich <b>Produktspezifische Konfiguration – Layout</b> .   |
| <b>Schritt 4</b> | Aktivieren Sie das Kontrollkästchen <b>WLAN SCEP-Server</b> , um den SCEP-Parameter zu aktivieren.  |
| <b>Schritt 5</b> | Aktivieren Sie das Kontrollkästchen <b>WLAN-Stammzertifizierungsstellen-Fingerabdruck (SHA256 oder SHA1)</b> , um den SCEP-QED-Parameter zu aktivieren. |
- 

### SCEP-Serverunterstützung

Wenn Sie einen SCEP-Server (Simple Certificate Enrollment Protocol) verwenden, kann der Server die Benutzer- und Server-Zertifikate automatisch beibehalten. Konfigurieren Sie auf dem SCEP-Server den SCEP-Registrierungs-Agent (RA) so, dass:

- er als vertrauenswürdiger PKI-Punkt fungiert.
- er als PKI-RA fungiert.
- die Geräteauthentifizierung mit einem RADIUS-Server durchgeführt wird.

Weitere Informationen finden Sie in der Dokumentation zum SCEP-Server.

## 802.1x-Authentifizierung

Cisco IP-Telefons unterstützen die 802.1X-Authentifizierung.

Cisco IP-Telefons und Cisco Catalyst-Switches verwenden normalerweise CDP (Cisco Discovery Protocol), um sich gegenseitig zu identifizieren und Parameter zu bestimmen, beispielsweise die VLAN-Zuweisung und Inline-Energieanforderungen.

Für die Unterstützung der 802.1X-Authentifizierung sind mehrere Komponenten erforderlich:

- Cisco IP-Telefon: Das Telefon initiiert die Anforderung, um auf das Netzwerk zuzugreifen. Die Telefone enthalten einen 802.1X-Supplicant. Dieses Supplicant ermöglicht Netzwerkadministratoren die Verbindung von IP-Telefonen mit den LAN-Switch-Ports zu steuern. Die aktuelle Version des 802.1X Supplicant verwendet EAP-FAST und EAP-TLS für die Netzwerkauthentifizierung.
- Cisco Catalyst-Switch (oder Switch eines Drittanbieters): Der Switch muss 802.1X unterstützen, damit er als Authentifikator agieren und Meldungen zwischen dem Telefon und dem Authentifizierungsserver übermitteln kann. Nach dem Meldungsaustausch gewährt oder verweigert der Switch dem Telefon den Zugriff auf das Netzwerk.

Um 802.1X zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

- Konfigurieren Sie die anderen Komponenten, bevor Sie die 802.1X-Authentifizierung auf dem Telefon aktivieren.
- Sprach-VLAN konfigurieren: Da in der 802.1X-Standardkonfiguration keine VLANs vorgesehen sind, sollten Sie diese Einstellung je nach Switch-Unterstützung konfigurieren.
  - Aktiviert: Wenn Sie einen Switch verwenden, der die Authentifizierung in mehreren Domänen unterstützt, können Sie das Sprach-VLAN weiterhin verwenden.
  - Deaktiviert: Wenn der Switch die Authentifizierung in mehreren Domänen nicht unterstützt, deaktivieren Sie das Sprach-VLAN und weisen den Port dem systemeigenen VLAN zu.

#### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14



## KAPITEL 8

# Cisco IP-Konferenztelefon – Anpassung

- [Individuelle Ruftöne, auf Seite 93](#)
- [Den Wählton anpassen, auf Seite 95](#)

## Individuelle Ruftöne

Cisco IP-Telefon wird mit zwei Standardruftontypen geliefert, die in der Hardware implementiert sind: Chirp1 und Chirp2. Cisco Unified Communications Manager stellt auch einen Standardsatz zusätzlicher Ruftöne, die in der Software implementiert sind, als PCM-Dateien (Pulse Code Modulation) bereit. Die PCM-Dateien und eine XML-Datei (Ringlist-wb.xml), welche die an Ihrem Standort verfügbaren Ruftonlistenoptionen beschreiben, befinden sich im TFTP-Verzeichnis auf den Cisco Unified Communications Manager-Servern.



**Achtung** Für alle Dateinamen muss die Groß-/Kleinschreibung beachtet werden. Wenn Sie den Dateinamen in einer anderen Groß-/Kleinschreibung angeben, übernimmt das Telefon Ihre Änderungen nicht.

Weitere Informationen finden Sie im Kapitel „Custom Phone Rings and Backgrounds“ (Benutzerdefinierte Ruftöne und Hintergründe) im [Funktionskonfigurationshandbuch für Cisco Unified Communications Manager](#).

### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Einen benutzerdefinierten Rufton konfigurieren

### Prozedur

- Schritt 1** Erstellen Sie für jeden benutzerdefinierten Rufton eine PCM-Datei (pro Datei nur ein Rufton).  
Stellen Sie sicher, dass die PCM-Dateien die Formatrichtlinien einhalten, die im Abschnitt [Formate benutzerdefinierter Ruftondateien](#) aufgeführt sind.
- Schritt 2** Laden Sie die neuen PCM-Dateien, die Sie erstellt haben, auf den Cisco TFTP-Server für jeden Cisco Unified Communications Manager im Cluster hoch.  
Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

**Schritt 3** Speichern Sie die Änderungen und schließen Sie die Datei Ringlist-wb.

**Schritt 4** So speichern Sie die neue Ringlist.wb-Datei zwischen:

- Stoppen und starten Sie den TFTP-Dienst mit Cisco Unified Serviceability
- Deaktivieren und aktivieren Sie den Parameter „Beim Starten Caching von konstanten und Binärdateien aktivieren“ des TFTP-Dienstes im Bereich „Dienstparameter – Erweitert“.

---

#### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Dateiformate für benutzerdefinierte Ruftöne

Die Datei Ringlist-wb.xml definiert ein XML-Objekt, das eine Liste der Ruftontypen enthält. Diese Datei enthält bis zu 50 Ruftontypen. Jeder Ruftontyp umfasst einen Verweis auf die PCM-Datei, die für diesen Ruftontyp und den Text verwendet wird, der im Menü Ruftontyp für diesen Rufton auf einem Cisco IP-Telefon angezeigt wird. Der Cisco TFTP-Server für Cisco Unified Communications Manager enthält diese Datei.

Das XML-Objekt CiscoIPPhoneRinglist XML verwendet die folgenden Tags, um die Informationen zu beschreiben:

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

Die folgenden Eigenschaften gelten für Definitionsnamen. Sie müssen für jeden Ruftontyp die erforderlichen Angaben zu „DisplayName“ und „FileName“ machen.

- Der Anzeigename gibt den Namen des benutzerdefinierten Ruftons in der zugehörigen PCM-Datei an, der im Menü Ruftontyp des Cisco IP-Telefon angezeigt wird.
- Der Dateiname gibt den Namen der PCM-Datei für den benutzerdefinierten Rufton an, der mit dem Anzeigenamen verknüpft wird.




---

**Hinweis** Die Felder Anzeigename und Dateiname dürfen maximal 25 Zeichen enthalten.

---

Dieses Beispiel zeigt die Datei Ringlist-wb.xml, die zwei Ruftontypen definiert:

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

Die PCM-Dateien für die Ruftöne müssen für die richtige Wiedergabe auf Cisco IP-Telefonen die folgenden Anforderungen erfüllen:



- Raw PCM (kein Header)
- 8000 Samples pro Sekunde
- 8 Bits pro Sample
- Mu-law-Komprimierung
- Maximale Ruftongröße = 16080 Samples
- Minimale Ruftongröße = 240 Samples
- Anzahl der Samples im Rufton = Das Mehrfache von 240.
- Der Rufton startet und endet bei einem Crossing von Null.

Um PCM-Dateien für benutzerdefinierte Ruftöne zu erstellen, verwenden Sie ein Standardpaket für die Audibearbeitung, das diese Dateiformate unterstützt.

## Den Wählton anpassen

Sie können die Telefone so konfigurieren, das die Benutzer für interne und externe Anrufe verschiedene Wählöne hören. Je nach Ihren Anforderungen können Sie aus drei verschiedenen Wählton-Optionen wählen:

- Standard: Unterschiedliche Wählöne für interne und externe Anrufe.
- Intern: Der Wählton für interne Anrufe wird für alle Anrufe verwendet.
- Extern: Der Wählton für externe Anrufe wird für alle Anrufe verwendet.

„Immer Wählton verwenden“ ist ein Pflichtfeld im Cisco Unified Communications Manager.

### Prozedur

- 
- |                  |  |
|------------------|--|
| <b>Schritt 1</b> | Wählen Sie in Cisco Unified Communications Manager Administration <b>System &gt; Dienstparameter</b> aus.  |
| <b>Schritt 2</b> | Wählen Sie den gewünschten Server aus.   |
| <b>Schritt 3</b> | Wählen Sie <b>Cisco CallManager</b> als Dienst aus.  |
| <b>Schritt 4</b> | Navigieren Sie zum Bereich „Clusterweite Parameter“.   |
| <b>Schritt 5</b> | Legen Sie <b>Immer Wählton verwenden</b> auf eine der folgenden Einstellungen fest: <ul style="list-style-type: none"><li>• Extern</li><li>• Intern</li><li>• Standard</li></ul> |
| <b>Schritt 6</b> | Wählen Sie <b>Speichern</b> aus.   |
| <b>Schritt 7</b> | Starten Sie die Telefone neu.  |
-





## KAPITEL 9

# Cisco IP-Konferenztelefon – Funktionen und Einrichtung

---

- [Benutzersupport für Cisco IP-Telefon, auf Seite 97](#)
- [Direkte Migration Ihres Telefons zu einem Multiplattform-Telefon, auf Seite 98](#)
- [Softkey-Vorlagen konfigurieren, auf Seite 98](#)
- [Telefonservices für Benutzer konfigurieren, auf Seite 99](#)
- [Telefonfunktion – Konfiguration, auf Seite 100](#)

## Benutzersupport für Cisco IP-Telefon

Wenn Sie ein Systemadministrator sind, sind Sie wahrscheinlich die primäre Informationsquelle für die Benutzer von Cisco IP-Telefonen in Ihrem Netzwerk bzw. Unternehmen. Es ist wichtig, dass die Benutzer aktuelle und ausführliche Informationen erhalten.

Um einige der Funktionen des Cisco IP-Telefon (einschließlich Optionen für Services und Sprachnachrichtensystem) zu verwenden, benötigen die Benutzer weitere Informationen von Ihnen oder Ihrem Netzwerkteam oder müssen sich an Sie wenden können, um Hilfestellung zu erhalten. Stellen Sie sicher, dass die Benutzer die Namen und Kontaktinformationen der Personen erhalten, an die sie sich für Hilfe wenden können.

Wir empfehlen, eine Webseite auf Ihrer internen Support-Website zu erstellen, die wichtige Informationen über Cisco IP-Telefone für die Benutzer enthält.

Die Webseite sollte die folgenden Informationen enthalten:

- Benutzerhandbücher für alle Cisco IP-Telefon-Modelle, die Sie unterstützen
- Informationen über den Zugriff auf das Cisco Unified Communications Benutzerportal
- Eine Liste der unterstützten Funktionen
- Benutzerhandbuch oder Kurzanleitung für Ihr Sprachspeichersystem

# Direkte Migration Ihres Telefons zu einem Multiplattform-Telefon

Sie können Ihr Unternehmenstelefon problemlos in einem Schritt zu einem Multiplattform-Telefon migrieren, ohne eine Übergangs-Firmware verwenden zu müssen. Sie müssen lediglich die Migrationslizenz vom Server abrufen und autorisieren.

Weitere Informationen hierzu finden Sie unter [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](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)

## Softkey-Vorlagen konfigurieren

Sie müssen einer Softkey-Vorlage Softkeys hinzufügen, um den Benutzer den Zugriff auf einige Funktionen zu ermöglichen. Wenn Sie z. B. möchten, dass die Benutzer „Bitte nicht stören“ verwenden können, müssen Sie den entsprechenden Softkey aktivieren. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Es kann sinnvoll sein, mehrere Vorlagen zu erstellen. Beispielsweise sollten Sie vielleicht eine Vorlage für ein Telefon in einem Konferenzraum und eine andere Vorlage für ein Telefon im Büro der Geschäftsführung erstellen.

In dieser Vorgehensweise werden die einzelnen Schritte beschrieben, die Sie ausführen müssen, um eine neue Softkey-Vorlage zu erstellen und sie einem bestimmten Telefon zuzuweisen. Wie bei anderen Telefonfunktionen können Sie die Vorlage für alle Ihre Konferenztelefone oder eine Gruppe von Telefonen verwenden.

### Prozedur

- 
- Schritt 1** Melden Sie sich als Administrator bei Cisco Unified Communications Manager Administration an.
- Schritt 2** Wählen Sie **Gerät > Geräteeinstellungen > Softkey-Vorlage** aus.
- Schritt 3** Klicken Sie auf **Suchen**.
- Schritt 4** Wählen Sie eine der folgenden Optionen aus:
- Cisco Unified Communications Manager 11.5 und frühere Versionen: **Standardbenutzer**
  - Cisco Unified Communications Manager 12.0 und neuere Versionen: **Personal Conference User (Benutzer persönliche Konferenz)** oder **Public Conference User (Benutzer öffentliche Konferenz)**.
- Schritt 5** Klicken Sie auf **Kopieren**.
- Schritt 6** Ändern Sie den Namen der Vorlage.  
Beispiel: 8832 Konferenzraumvorlage.
- Schritt 7** Klicken Sie auf **Speichern**.
- Schritt 8** Navigieren Sie über das Menü oben rechts zur Seite **Softkey-Layout konfigurieren**.
- Schritt 9** Legen Sie für jeden Anrufstatus fest, welche Funktionen angezeigt werden sollen.
- Schritt 10** Klicken Sie auf **Speichern**.
- Schritt 11** Kehren Sie über das Menü oben rechts zurück zum Bildschirm **Suchen/Liste**.

Die neue Vorlage wird in der Vorlagenliste angezeigt.

- Schritt 12** Wählen Sie **Gerät > Telefon**.
- Schritt 13** Suchen Sie das Telefon, dem Sie die neue Vorlage zuweisen möchten, und wählen Sie es aus.
- Schritt 14** Wählen Sie im Feld **Softkey-Vorlage** die neue Softkey-Vorlage aus.
- Schritt 15** Klicken Sie auf **Speichern** und **Konfiguration übernehmen**.

---

#### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Telefonservices für Benutzer konfigurieren

Sie können den Benutzern den Zugriff auf Cisco IP-Telefon-Services auf dem IP-Telefon gewähren. Außerdem können Sie eine Taste verschiedenen Telefonservices zuordnen. Das IP-Telefon verwaltet jeden Service als eine separate Anwendung.

Bevor ein Benutzer auf einen Service zugreifen kann:

- Verwenden Sie Cisco Unified Communications Manager-Verwaltung, um Dienste zu konfigurieren, die standardmäßig nicht verfügbar sind.
- Der Benutzer muss die Dienste im Self-Service-Portal für Cisco Unified Communications abonnieren. Die Webanwendung stellt eine grafische Benutzeroberfläche für die begrenzte Benutzerkonfiguration der IP-Telefonanwendungen bereit. Ein Benutzer kann einen Service jedoch nicht abonnieren, den Sie als Enterprise-Abonnement konfiguriert haben.

Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Bevor Sie Services konfigurieren, sammeln Sie die URLs für die entsprechenden Websites und stellen Sie sicher, dass die Benutzer über das firmeneigene IP-Telefonnetzwerk auf diese Websites zugreifen können. Dieser Vorgang muss für die von Cisco bereitgestellten Standardservices nicht ausgeführt werden.

#### Prozedur

- 
- Schritt 1** Wählen Sie in Cisco Unified Communications Manager-Verwaltung **Gerät > Geräteeinstellungen > Telefondienste** aus.
- Schritt 2** Stellen Sie sicher, dass die Benutzer auf Self-Service-Portal für Cisco Unified Communications zugreifen können, damit sie die konfigurierten Dienste auswählen und abonnieren können.
- Siehe [Übersicht des Selbstservice-Portals, auf Seite 71](#) für eine Übersicht der Informationen, die Sie an die Benutzer weitergeben müssen.

---

#### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

# Telefonfunktion – Konfiguration

Sie können Telefone so einrichten, dass sie entsprechend den Anforderungen der Benutzer über die benötigten Funktionen verfügen. Sie können Funktionen auf alle Telefone, auf eine Gruppe von Telefonen oder auf einzelne Telefone anwenden.

Wenn Sie Funktionen einrichten, werden im Fenster Cisco Unified Communications Manager-Verwaltung Informationen, die für alle Telefone gelten, sowie Informationen zum Telefonmodell angezeigt. Die Informationen, die speziell für das Telefonmodell gelten, befinden sich im Bereich „Produktspezifische Konfiguration – Layout“ des Fensters.

Informationen zu den Feldern, die für alle Telefonmodelle gelten, finden Sie in der Cisco Unified Communications Manager-Dokumentation.

Wenn Sie ein Feld konfigurieren, ist das Fenster wichtig, in dem Sie das Feld konfigurieren, da für die Fenster eine Rangfolge gilt. Die Rangfolge lautet:

1. Einzelne Telefone (höchste Priorität)
2. Gruppe von Telefonen
3. Alle Telefone (niedrigste Priorität)

Beispiel: Wenn Sie möchten, dass eine bestimmte Benutzergruppe nicht auf die Telefon-Webseiten zugreifen kann, die übrigen Benutzer jedoch schon, können Sie Folgendes tun:

1. Aktivieren Sie den Zugriff auf die Telefon-Webseiten für alle Benutzer.
2. Deaktivieren Sie den Zugriff auf die Telefon-Webseiten für jeden einzelnen Benutzer, oder erstellen Sie eine Benutzergruppe, und deaktivieren Sie den Zugriff auf die Telefon-Webseiten für die Benutzergruppe.
3. Wenn ein bestimmter Benutzer in der Benutzergruppe Zugriff auf die Telefon-Webseiten benötigt, können Sie den Zugriff für diesen speziellen Benutzer aktivieren.

## Verwandte Themen

[Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren](#), auf Seite 126

## Einrichten von Telefonfunktionen für alle Telefone

### Prozedur

- 
- |                  |   |
|------------------|---|
| <b>Schritt 1</b> | Melden Sie sich als Administrator bei der Cisco Unified Communications Manager-Administration an.             |
| <b>Schritt 2</b> | Wählen Sie <b>System &gt; Konfiguration des Bürotelefons</b> .  |
| <b>Schritt 3</b> | Legen Sie die Felder fest, die Sie ändern möchten.  |
| <b>Schritt 4</b> | Aktivieren Sie das Auswahlkästchen <b>Unternehmenseinstellungen überschreiben</b> für alle geänderten Felder. |
| <b>Schritt 5</b> | Klicken Sie auf <b>Speichern</b> .  |
| <b>Schritt 6</b> | Klicken Sie auf <b>Konfiguration übernehmen</b> .   |
| <b>Schritt 7</b> | Starten Sie die Telefone neu.   |

**Hinweis** Dies wirkt sich auf alle Telefone in Ihrem Unternehmen aus.

---

**Verwandte Themen**

[Produktspezifische Konfiguration](#), auf Seite 102

## Einrichten von Telefonfunktionen für eine Telefongruppe

---

**Prozedur**

- Schritt 1** Melden Sie sich als Administrator bei der Cisco Unified Communications Manager-Administration an.
- Schritt 2** Wählen Sie **Gerät > Geräteeinstellungen > Allgemeines Telefonprofil**.
- Schritt 3** Suchen Sie das Profil.
- Schritt 4** Navigieren Sie zum Bereich „Produktspezifische Konfiguration – Layout“, und legen Sie die Felder fest.
- Schritt 5** Aktivieren Sie das Auswahlkästchen **Unternehmenseinstellungen überschreiben** für alle geänderten Felder.
- Schritt 6** Klicken Sie auf **Speichern**.
- Schritt 7** Klicken Sie auf **Konfiguration übernehmen**.
- Schritt 8** Starten Sie die Telefone neu.

---

**Verwandte Themen**

[Produktspezifische Konfiguration](#), auf Seite 102

## Einrichten von Telefonfunktionen für ein einzelnes Telefon

---

**Prozedur**

- Schritt 1** Melden Sie sich als Administrator bei der Cisco Unified Communications Manager-Administration an.
- Schritt 2** Wählen Sie **Gerät > Telefon**.
- Schritt 3** Navigieren Sie zu dem Telefon, das dem Benutzer zugeordnet ist.
- Schritt 4** Navigieren Sie zum Bereich „Produktspezifische Konfiguration – Layout“, und legen Sie die Felder fest.
- Schritt 5** Aktivieren Sie das Kontrollkästchen **Allgemeine Einstellungen überschreiben** für alle geänderten Felder.
- Schritt 6** Klicken Sie auf **Speichern**.
- Schritt 7** Klicken Sie auf **Konfiguration übernehmen**.
- Schritt 8** Starten Sie das Telefon neu.

---

**Verwandte Themen**

[Produktspezifische Konfiguration](#), auf Seite 102

## Produktspezifische Konfiguration

In der folgenden Tabelle werden die Felder im Bereich „Produktspezifische Konfiguration – Layout“ beschrieben. Einige in dieser Tabelle aufgeführten Felder werden nur auf der Seite **Gerät > Telefon** angezeigt.

**Tabelle 18: Felder im Bereich „Produktspezifische Konfiguration“**

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Zugriff auf Einstellungen	Deaktiviert Aktiviert Eingeschränkt	Aktiviert	Aktiviert, deaktiviert oder schränkt den Zugriff auf die lokalen Konfigurationseinstellungen in der App „Einstellungen“ ein.  Mit beschränktem Zugriff kann auf die Menüs „Voreinstellungen“ und „Systeminformation“ zugegriffen werden. Auf einige Einstellungen im Menü „WLAN“ kann ebenfalls zugegriffen werden.  Wenn der Zugriff deaktiviert ist, werden im Menü „Einstellungen“ keine Optionen angezeigt.
ARP unnötig	Deaktiviert Aktiviert	Deaktiviert	Aktiviert oder deaktiviert die Möglichkeit des Telefons, MAC-Adressen von Gratuitous ARP-Paketen zu erkennen. Diese Funktion ist erforderlich, um Sprach-Streams zu überwachen oder aufzuzeichnen.
Webzugriff	Deaktiviert Aktiviert	Deaktiviert	Aktiviert oder deaktiviert den Zugriff auf die Webseiten des Telefons über einen Webbrowser.  <b>Vorsicht</b> Wenn Sie dieses Feld aktivieren, legen Sie möglicherweise vertrauliche Daten über das Telefon offen.
TLS 1.0 und TLS 1.1 für Webzugriff deaktivieren	Deaktiviert Aktiviert	Aktiviert	Steuert die Verwendung von TLS 1.2 für eine Webserververbindung.  <ul style="list-style-type: none"> <li>• Deaktiviert: Ein für TLS 1.0, TLS 1.1 oder TLS 1.2 konfiguriertes Telefon kann als HTTPS-Server fungieren.</li> <li>• Aktiviert: Nur ein für TLS 1.2 konfiguriertes Telefon kann als HTTPS-Server fungieren.</li> </ul>



Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Enbloc-Wählen	Deaktiviert Aktiviert	Deaktiviert	<p>Steuert die Wählmethode.</p> <ul style="list-style-type: none"> <li>• Deaktiviert: Der Cisco Unified Communications Manager wartet, bis der Interdigit-Timer abläuft, wenn eine Überschneidung beim Rufnummernplan oder beim Routenmuster vorliegt.</li> <li>• Aktiviert: Die gesamte gewählte Zeichenfolge wird an den Cisco Unified Communications Manager gesendet, sobald der Wählvorgang abgeschlossen ist. Um das T.302-Timer-Timeout zu vermeiden, wird empfohlen, Blockwahl zu aktivieren, sobald sich ein Wählplan oder ein Routenmuster überschneiden.</li> </ul> <p>Berechtigungscode (Forced Authorization Codes, FAC) oder Projektkennziffern (Client Matter Codes, CMC) unterstützen nicht das Enbloc-Wählen. Wenn Sie FAC oder CMC zum Verwalten des Anrufzugriffs und der Buchhaltung verwenden, können Sie diese Funktion nicht verwenden.</p>
Hintergrundbeleuchtung nicht aktiv – Tage	Tage der Woche		<p>Definiert die Tage, an denen sich die Hintergrundbeleuchtung nicht automatisch zur im Feld „Hintergrundbeleuchtung eingeschaltet - Uhrzeit“ angegebenen Uhrzeit einschaltet.</p> <p>Wählen Sie in der Dropdown-Liste die Tage aus. Halten Sie zur Auswahl mehrerer Tage die <b>Strg-Taste gedrückt, und klicken Sie</b> auf die gewünschten Tage.</p> <p>Siehe <a href="#">Energiesparmodus für Cisco IP-Telefon planen, auf Seite 116</a>.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Hintergrundbeleuchtung eingeschaltet – Uhrzeit	hh:mm		<p>Definiert die Uhrzeit, an der sich die Hintergrundbeleuchtung jeden Tag automatisch einschaltet (außer an den im Feld „Hintergrundbeleuchtung nicht aktiv – Tage“ angegebenen Tagen).</p> <p>Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (0:00 ist Mitternacht).</p> <p>Um die Hintergrundbeleuchtung beispielsweise um 07:00 Uhr (0700) einzuschalten, geben Sie 07:00 ein. Um die Hintergrundbeleuchtung um 14:00 Uhr (1400) einzuschalten, geben Sie 14:00 ein.</p> <p>Wenn in dieses Feld nichts eingegeben wird, schaltet sich die Hintergrundbeleuchtung automatisch um 00:00 Uhr ein.</p> <p>Siehe <a href="#">Energiesparmodus für Cisco IP-Telefon planen, auf Seite 116</a>.</p>
Hintergrundbeleuchtung aktiv – Dauer	hh:mm		<p>Definiert den Zeitraum, über den die Hintergrundbeleuchtung eingeschaltet bleibt, nachdem sie sich zu der im Feld „Hintergrundbeleuchtung eingeschaltet – Uhrzeit“ angegebenen Uhrzeit eingeschaltet hat.</p> <p>Damit die Hintergrundbeleuchtung nach der automatischen Aktivierung beispielsweise vier Stunden und 30 Minuten lang aktiviert bleibt, geben Sie 04:30 ein.</p> <p>Wenn in dieses Feld nichts eingegeben wird, schaltet sich der Bildschirm am Tagesende (00:00 Uhr) ab.</p> <p>Wenn im Feld „Hintergrundbeleuchtung eingeschaltet - Uhrzeit“ der Wert „00:00“ eingetragen und im Feld „Hintergrundbeleuchtung eingeschaltet – Dauer“ kein Wert (oder „24:00“) vorhanden ist, wird die Hintergrundbeleuchtung nicht ausgeschaltet.</p> <p>Siehe <a href="#">Energiesparmodus für Cisco IP-Telefon planen, auf Seite 116</a>.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Hintergrundbeleuchtung – Leerlauf-Zeitlimit	hh:mm		<p>Definiert den Zeitraum, über den das Telefon inaktiv gewesen sein muss, bevor sich die Hintergrundbeleuchtung abschaltet. Trifft nur zu, wenn die Hintergrundbeleuchtung wie geplant ausgeschaltet und vom Benutzer eingeschaltet wurde (durch das Drücken einer Taste oder das Abheben des Hörers).</p> <p>Wenn die Hintergrundbeleuchtung beispielsweise ausgeschaltet werden soll, wenn das Telefon nach dem Einschalten der Hintergrundbeleuchtung durch einen Benutzer 1 Stunde und 30 Minuten lang inaktiv war, geben Sie 01:30 ein.</p> <p>Siehe <a href="#">Energiesparmodus für Cisco IP-Telefon planen, auf Seite 116</a>.</p>
Hintergrundbeleuchtung ein bei eingehendem Anruf	Deaktiviert Aktiviert	Aktiviert	Schaltet die Hintergrundbeleuchtung ein, wenn ein Anruf eingeht.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Power Save Plus aktivieren	Tage der Woche		<p>Definiert die Tage, an denen das Telefon deaktiviert werden soll.</p> <p>Wählen Sie in der Dropdown-Liste die Tage aus. Halten Sie zur Auswahl mehrerer Tage die <b>Strg-Taste gedrückt, und klicken Sie</b> auf die gewünschten Tage.</p> <p>Wenn das Feld „Power Save Plus aktivieren“ aktiv ist, erhalten Sie eine Warnmeldung aufgrund von Sicherheitsbedenken (E911-Meldung).</p> <p><b>Vorsicht</b> Wenn der Power Save Plus-Modus (der Modus) aktiviert ist, werden die Endpunkte, die für den Modus konfiguriert sind, für Notrufe und eingehende Anrufe deaktiviert. Indem Sie diesen Modus auswählen, stimmen Sie Folgendem zu: (i) Sie übernehmen die volle Verantwortung dafür, dass alternative Methoden für Notrufe und eingehende Anrufe bereitgestellt werden, während der Modus aktiviert ist; (ii) Cisco übernimmt keine Haftung in Bezug auf Ihre Auswahl des Modus und die gesamte Haftung in Zusammenhang mit der Aktivierung des Modus liegt in Ihrer Verantwortung; und (iii) Sie informieren die Benutzer über die Auswirkungen des Modus auf Anrufe und andere Funktionen.</p> <p>Um Power Save Plus zu deaktivieren, müssen Sie das Kontrollkästchen „EnergyWise-Überschreibungen zulassen“ deaktivieren. Wenn EnergyWise-Überschreibung zulassen aktiviert ist, aber keine Tage im Feld „Power Save Plus aktivieren“ ausgewählt sind, wird Power Save Plus nicht deaktiviert.</p> <p>Siehe <a href="#">EnergyWise für das Cisco IP-Telefon planen, auf Seite 117</a>.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Telefon einschalten – Uhrzeit	hh:mm		<p>Legt fest, wann das Telefon an den Tagen, die im Feld Power Save Plus aktivieren ausgewählt sind, automatisch eingeschaltet wird.</p> <p>Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (00:00 ist Mitternacht).</p> <p>Um das Telefon beispielsweise um 07:00 Uhr (0700) automatisch einzuschalten, geben Sie 07:00 ein. Um das Telefon um 14:00 Uhr (1400) einzuschalten, geben Sie 14:00 ein.</p> <p>Der Standardwert ist leer, das heißt 00:00.</p> <p>Die Einschaltzeit des Telefons muss mindestens 20 Minuten später als die Ausschaltzeit sein. Wenn die Ausschaltzeit beispielsweise auf 07:00 festgelegt ist, darf die Einschaltzeit nicht früher als 07:20 sein.</p> <p>Siehe <a href="#">EnergyWise für das Cisco IP-Telefon planen, auf Seite 117</a>.</p>
Telefon ausschalten – Uhrzeit	hh:mm		<p>Definiert die Tageszeit, zu der das Telefon an den im Feld „Power Save Plus aktivieren“ ausgewählten Tagen deaktiviert wird. Wenn die Felder den gleichen Wert enthalten, wird das Telefon nicht ausgeschaltet.</p> <p>Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (00:00 ist Mitternacht).</p> <p>Um das Telefon beispielsweise um 7:00 Uhr (0700) automatisch auszuschalten, geben Sie 7:00 ein. Um das Telefon um 14:00 Uhr (1400) auszuschalten, geben Sie 14:00 ein.</p> <p>Der Standardwert ist leer, das heißt 00:00.</p> <p>Die Einschaltzeit des Telefons muss mindestens 20 Minuten später als die Ausschaltzeit sein. Wenn die Ausschaltzeit beispielsweise auf 07:00 festgelegt ist, darf die Einschaltzeit nicht früher als 07:20 sein.</p> <p>Siehe <a href="#">EnergyWise für das Cisco IP-Telefon planen, auf Seite 117</a>.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Telefon ausschalten - Leerlauf-Timeout	hh:mm		<p>Gibt den Zeitraum an, für den das Telefon inaktiv gewesen sein muss, bevor es sich deaktiviert.</p> <p>Der Timeout tritt unter folgenden Bedingungen auf:</p> <ul style="list-style-type: none"> <li>• Wenn das Telefon, wie geplant, in den Power Save Plus-Modus gewechselt ist und eingeschaltet wurde, da der Benutzer die Taste „Auswahl“ gedrückt hat.</li> <li>• Wenn das Telefon vom angeschlossenen Switch wieder eingeschaltet wurde.</li> <li>• Wenn die Ausschaltzeit des Telefons erreicht wird, aber das Telefon verwendet wird.</li> </ul> <p>Siehe <a href="#">EnergyWise für das Cisco IP-Telefon planen, auf Seite 117</a>.</p>
Signalton aktivieren	Kontrollkästchen	Deaktiviert	<p>Wenn diese Option aktiviert ist, gibt das Telefon 10 Minuten vor der angegebenen Ausschaltzeit einen Signalton aus.</p> <p>Dieses Kontrollkästchen ist nur relevant, wenn im Listenfeld Power Save Plus aktivieren mindestens ein Tag ausgewählt ist.</p> <p>Siehe <a href="#">EnergyWise für das Cisco IP-Telefon planen, auf Seite 117</a>.</p>
EnergyWise-Domäne	Bis zu 127 Zeichen		<p>Ermittelt die EnergyWise-Domäne, in der sich das Telefon befindet.</p> <p>Siehe <a href="#">EnergyWise für das Cisco IP-Telefon planen, auf Seite 117</a>.</p>
EnergyWise-Secret	Bis zu 127 Zeichen		<p>Ermittelt das Kennwort der Sicherheitsabfrage, das in der Kommunikation mit den Endgeräten in der EnergyWise-Domäne verwendet wird.</p> <p>Siehe <a href="#">EnergyWise für das Cisco IP-Telefon planen, auf Seite 117</a>.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
EnergyWise-Überschreibung zulassen	Kontrollkästchen	Deaktiviert	<p>Bestimmt, ob die Controller-Richtlinie der EnergyWise-Domäne aktualisierte Energiepegeldaten an die Telefone senden darf. Es gelten die folgenden Bedingungen:</p> <ul style="list-style-type: none"> <li>• Im Feld Power Save Plus aktivieren muss mindestens ein Tag ausgewählt werden.</li> <li>• Die Einstellungen in der Cisco Unified Communications Manager-Verwaltung werden planmäßig übernommen, auch wenn EnergyWise eine Überschreibung sendet.</li> </ul> <p>Beispielsweise kann die Ausschaltzeit auf 22:00 Uhr, der Wert für die Einschaltzeit auf 06:00 Uhr und für Power Save Plus ist mindestens ein Tag festgelegt sein.</p> <ul style="list-style-type: none"> <li>• Wenn EnergyWise das Telefon anweist, sich um 20:00 Uhr auszuschalten, bleibt diese Anweisung bis zur festgelegten Einschaltzeit um 6:00 Uhr in Kraft.</li> <li>• Um 6 Uhr schaltet sich das Telefon ein und empfängt wieder die Energiepegeländerungen aus den Einstellungen in Cisco Unified Communications Manager Administration.</li> <li>• Um den Energiepegel auf dem Telefon erneut zu ändern, muss EnergyWise einen neuen Befehl ausgeben.</li> </ul> <p>Um Power Save Plus zu deaktivieren, müssen Sie das Kontrollkästchen „EnergyWise-Überschreibungen zulassen“ deaktivieren. Wenn EnergyWise-Überschreibung zulassen aktiviert ist, aber keine Tage im Feld „Power Save Plus aktivieren“ ausgewählt sind, wird Power Save Plus nicht deaktiviert.</p> <p>Siehe <a href="#">EnergyWise für das Cisco IP-Telefon planen, auf Seite 117</a>.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Richtlinie für Zusammenführung und direkte Übergabe	Nur gleiche Leitung aktivieren Nur gleiche Leitung deaktivieren	Gleiche Leitung, mehrere Leitungen aktivieren	Steuert die Möglichkeit eines Benutzers, Anrufen beitreten und diese zu übergeben. <ul style="list-style-type: none"> <li>Nur gleiche Leitung aktivieren: Benutzer können einen Anruf auf der aktuellen Leitung an einen Anruf auf derselben Leitung übergeben oder diesem beitreten.</li> <li>Nur gleiche Leitung deaktivieren: Benutzer können keine Anrufe auf derselben Leitung übergeben oder diesen beitreten. Die Beitritts- und Übergabefunktionen sind deaktiviert, und der Benutzer kann diese Funktionen nicht verwenden.</li> </ul>
Aufzeichnungston	Deaktiviert Aktiviert	Deaktiviert	Steuert die Wiedergabe des Tons, wenn ein Benutzer einen Anruf aufzeichnet.
Aufzeichnungston-Lautstärke lokal	Ganzzahl 0 bis 100	100	Regelt die Lautstärke des Aufzeichnungstons für den lokalen Benutzer.
Aufzeichnungston-Lautstärke – Gesprächspartner	Ganzzahl 0 bis 100	50	Regelt die Lautstärke des Aufzeichnungstons für den Remote-Benutzer.
Aufzeichnungsdauer	Ganzzahl 1 bis 3000 Millisekunden		Steuert die Dauer des Aufzeichnungstons.
Protokollserver	Zeichenfolge mit bis zu 256 Zeichen		Identifiziert den IPv4-Syslog-Server für die Debug-Ausgabe des Telefons. Das Format für die Adresse lautet: <b>address : &lt;port&gt;@&lt;base=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b>
Remote-Protokoll	Deaktiviert Aktiviert	Deaktiviert	Steuert die Möglichkeit, Protokolle an den Syslog-Server zu senden.



Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Protokollprofil	Standard Voreinstellung Telefonie SIP UI Netzwerk Medien Upgrade Zubehörteil Sicherheit EnergyWise MobileRemoteAccess	Voreinstellung	Gibt das vordefinierte Protokollierungsprofil an. <ul style="list-style-type: none"> <li>• Standard – Standard-Protokollierungsebene bei der Fehlersuche</li> <li>• Voreinstellung – Überschreibt nicht die lokale Einstellung für die Fehlersuchprotokollierung des Telefons.</li> <li>• Telefonie – Protokolliert Informationen zu den Funktionen für Telefonie oder Anrufe.</li> <li>• SIP – Protokolliert Informationen zu den SIP-Signalen.</li> <li>• UI – Protokolliert Informationen zur Benutzeroberfläche des Telefons.</li> <li>• Netzwerk – Protokolliert Informationen zum Netzwerk.</li> <li>• Medien – Protokolliert Mediendaten.</li> <li>• Upgrade – Protokolliert Upgrade-Informationen.</li> <li>• Zubehör – Protokolliert Zubehör-Informationen.</li> <li>• Sicherheit – Protokolliert Sicherheitsinformationen.</li> <li>• EnergyWise – Protokolliert Energiesparinformationen.</li> <li>• MobileRemoteAccess: Protokolliert Informationen zum Mobil- und Remotezugriff über Expressway.</li> </ul>
IPv6 – Protokollserver	Zeichenfolge mit bis zu 256 Zeichen		Identifiziert den IPv6-Syslog-Server für die Debug-Ausgabe des Telefons.
Cisco Discovery Protocol (CDP): Switchport	Deaktiviert Aktiviert	Aktiviert	Steuert das CDP (Cisco Discovery Protocol) auf dem Telefon.
Link Layer Discovery Protocol – Media Endpoint Discover (LLDP-MED): Switchport	Deaktiviert Aktiviert	Aktiviert	Aktiviert LLDP-MED für den SW-Port.
LLDP Asset-ID	Zeichenfolge mit bis zu 32 Zeichen		Identifiziert die Asset-ID, die dem Telefon für die Bestandsverwaltung zugewiesen wird.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Energy Efficient Ethernet(EEE): Switch-Port	Deaktiviert Aktiviert	Deaktiviert	Steuert EEE für den Switch-Port.
LLDP-Leistungspriorität	Unbekannt Niedrig Hoch Kritisch	Unbekannt	Weist dem Switch eine Energiepriorität des Telefons zu, damit der Switch die entsprechende Leistung für die Telefone bereitstellen kann.
802.1x-Authentifizierung	Vom Benutzer gesteuert Deaktiviert Aktiviert	Vom Benutzer gesteuert	Gibt den Status der 802.1x-Authentifizierungsfunktion an. <ul style="list-style-type: none"> <li>• Vom Benutzer gesteuert – Der Benutzer kann die 802.1x-Authentifizierung auf dem Telefon konfigurieren.</li> <li>• Deaktiviert: 802.1x-Authentifizierung wird nicht verwendet.</li> <li>• Aktiviert – 802.1x-Authentifizierung wird verwendet, und Sie konfigurieren die Authentifizierung für die Telefone.</li> </ul>
Remotekonfiguration für Switchport	Deaktiviert Autom. aushandeln 10 Halb 10 Voll 100 Halb 100 Voll	Deaktiviert	Ermöglicht es Ihnen, die Geschwindigkeit und Duplex-Funktion für den SW-Port des Telefons remote zu konfigurieren. Dies verbessert die Leistung für große Bereitstellungen mit bestimmten Porteeinstellungen.  Wenn die SW-Ports in Cisco Unified Communications Manager für die Remote-Portkonfiguration konfiguriert sind, können die Daten auf dem Telefon nicht geändert werden.
SSH-Zugriff	Deaktiviert Aktiviert	Deaktiviert	Steuert den Zugriff auf den SSH-Daemon über Port 22. Wenn Port 22 geöffnet bleibt, ist das Telefon anfällig für DOS-Angriffe (Denial of Service).
Ruftonbereich	Standard Japan	Standard	Steuert das Ruftonmuster.
TLS-Fortsetzungs-Timer	Ganzzahl 0 bis 3600 Sekunden	3600	Legt fest, ob eine TLS-Sitzung fortgesetzt werden kann, ohne den gesamten TLS-Authentifizierungsvorgang zu wiederholen. Wenn das Feld auf 0 gesetzt wird, ist die Fortsetzung der TLS-Sitzung deaktiviert.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
FIPS-Modus	Deaktiviert Aktiviert	Deaktiviert	Aktiviert oder deaktiviert den FIPS-Modus (Federal Information Processing Standards) auf dem Telefon.
Anrufverlauf für gemeinsam genutzte Leitung aufzeichnen	Deaktiviert Aktiviert	Deaktiviert	Legt fest, ob das Anrufprotokoll von einer gemeinsam genutzten Leitung aufgezeichnet wird.
Minimale Ruftonlautstärke	0 – Stumm 1–15	0 – Stumm	Steuert die minimale Ruftonlautstärke für das Telefon.
Peer-Firmware-Freigabe	Deaktiviert Aktiviert	Aktiviert	<p>Ermöglicht es dem Telefon, andere Telefone desselben Modells im Subnetz zu finden und aktualisierte Firmware-Dateien gemeinsam zu nutzen. Wenn das Telefon über eine neue Firmware-Software verfügt, kann es diese Software für die anderen Telefone freigeben. Wenn eines der anderen Telefone eine neue Firmware-Version besitzt, kann die Firmware von diesem anderen Telefon, anstatt vom TFTP-Server, auf das Telefon heruntergeladen werden.</p> <p>Peer-Firmware-Freigabe:</p> <ul style="list-style-type: none"> <li>• Beschränkt Überlastungen bei TFTP-Übertragungen an zentrale Remote-TFTP-Server.</li> <li>• Firmware-Updates müssen nicht mehr manuell gesteuert werden.</li> <li>• Reduziert die Ausfallzeiten der Telefone während Updates, wenn zahlreiche Telefone gleichzeitig zurückgesetzt werden.</li> <li>• Unterstützt Firmware-Updates bei Bereitstellungen in Niederlassungen oder an Remotestandorten, die über WAN-Links mit beschränkter Bandbreite laufen.</li> </ul>
Software-Server	Zeichenfolge mit bis zu 256 Zeichen		Identifiziert den alternativen IPv4-Server, den das Telefon verwendet, um Firmware und Updates abzurufen.
IPv6 – Lastserver	Zeichenfolge mit bis zu 256 Zeichen		Identifiziert den alternativen IPv6-Server, den das Telefon verwendet, um Firmware und Updates abzurufen.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Unified CM-Verbindungsfehler erkennen	Normal Verzögert	Normal	<p>Legt die Empfindlichkeit des Telefons für die Erkennung eines Verbindungsfehlers mit Cisco Unified Communications Manager (Unified CM) fest. Dies ist der erste Schritt vor dem Gerätefailover auf einen Sicherungs-Unified CM/SRST.</p> <p>Zulässig sind die Werte „Normal“ (Unified CM-Verbindungsfehler werden in der Standardsystemgeschwindigkeit erkannt) und „Verzögert“ (Unified CM-Verbindungsfehler werden etwa viermal langsamer erkannt als bei der Einstellung „Normal“)</p> <p>Für eine schnellere Erkennung eines Unified CM-Verbindungsfehlers wählen Sie „Normal“ aus. Wenn Sie den Failover etwas verzögern möchten, um zu versuchen, die Verbindung wiederherzustellen, wählen Sie „Verzögert“ aus.</p> <p>Der genaue Zeitunterschied zwischen Normal und Verzögert hängt von mehreren Faktoren ab, die sich ständig ändern.</p>
ID für spezielle Anforderung	Zeichenfolge		Steuert benutzerdefinierte Funktionen von ES-Lasten (Engineering Special).
HTTPS-Server	HTTP und HTTPS aktiviert Nur HTTPS	HTTP und HTTPS aktiviert	Steuert die Art der Kommunikation mit dem Telefon. Wenn Sie „Nur HTTPS“ auswählen, ist die Telefonkommunikation besser geschützt.
Dauerhafte Benutzeranmeldedaten für die Expressway-Anmeldung	Deaktiviert Aktiviert	Deaktiviert	<p>Legt fest, ob das Telefon die Anmeldeinformationen des Benutzers speichert. Wenn diese Option deaktiviert ist, sieht der Benutzer immer die Aufforderung zum Anmelden beim Expressway-Server für Mobil- und Remote-Zugriff (MRA).</p> <p>Wenn Sie die Benutzeranmeldung vereinfachen möchten, können Sie dieses Feld aktivieren, damit die Expressway-Anmeldedaten beibehalten werden. Der Benutzer muss dann die Anmeldeinformationen nur beim ersten Mal eingeben. Im Anschluss (wenn das Telefon an einem externen Standort eingeschaltet wird) werden die Anmeldeinformationen auf dem Anmeldebildschirm vorab ausgefüllt.</p> <p>Weitere Informationen finden Sie im Abschnitt <a href="#">Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren</a>, auf Seite 126.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Upload-URL für Kundensupport	Zeichenfolge mit bis zu 256 Zeichen		Stellt die URL für das Tool für Problemlberichte (PRT) bereit.  Wenn Sie Geräte mit Mobil- und Remote-Zugriff über Expressway bereitstellen, müssen Sie zudem die PRT-Serveradresse der Liste der zulässigen HTTP-Server auf dem Expressway-Server hinzufügen.  Weitere Informationen finden Sie im Abschnitt <a href="#">Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren</a> , auf Seite 126.
TLS-Schlüssel deaktivieren	Siehe <a href="#">Transport Layer Security-Schlüssel deaktivieren</a> , auf Seite 115.	Keine	Deaktiviert den ausgewählten TLS-Schlüssel.  Deaktivieren Sie mehr als eine Verschlüsselungs-Suite, indem Sie die <b>Strg</b> -Taste auf Ihrer Computertastatur auswählen und gedrückt halten.
Eine Zeile für das Parken von Anrufen reservieren	Deaktiviert Aktiviert	Aktiviert	Steuert, ob ein geparkter Anruf eine Leitung belegt.  Weitere Informationen finden Sie in der Dokumentation zu Cisco Unified Communications Manager.

**Verwandte Themen**

[Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren](#), auf Seite 126

## Transport Layer Security-Schlüssel deaktivieren

Sie können die Transport Layer Security-(TLS-)Schlüssel mit dem Parameter **TLS-Schlüssel deaktivieren** deaktivieren. So können Sie Ihre Sicherheit für bekannte Schwachstellen anpassen und Ihr Netzwerk an die Unternehmensrichtlinien für Verschlüsselungen ausrichten.

"Keine" ist die Standardeinstellung.

Deaktivieren Sie mehr als eine Verschlüsselungs-Suite, indem Sie die **Strg**-Taste auf Ihrer Computertastatur auswählen und gedrückt halten. Die Auswahl aller Telefonschlüssel wirkt sich auf den TLS-Dienst des Telefons aus. Ihre Auswahlmöglichkeiten sind:

- Kein
- 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

Weitere Informationen zur Telefonsicherheit finden Sie im *Whitepaper zum Sicherheitsüberblick über die Cisco IP-Telefon 7800- und 8800-Serie* (<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html>).

## Energiesparmodus für Cisco IP-Telefon planen

Um Energie zu sparen und die Langlebigkeit des Telefondisplays sicherzustellen, können Sie das Display deaktivieren, wenn es nicht benötigt wird.

Sie können die Einstellungen in der Cisco Unified Communications Manager-Verwaltung konfigurieren, um das Display an einigen Tagen zu einem festgelegten Zeitpunkt oder den ganzen Tag zu deaktivieren. Beispielsweise können Sie das Display an Wochentagen nach Geschäftsschluss und an Samstagen und Sonntagen ausschalten.

Mit den folgenden Aktionen können Sie das Display jederzeit einschalten:

- Drücken Sie die eine beliebige Taste auf dem Telefon.  
Das Telefon schaltet das Display ein und führt die der Taste zugeordnete Aktion aus.
- Nehmen Sie den Hörer ab.

Wenn Sie das Display einschalten, bleibt es aktiviert, bis das Telefon für eine festgelegte Zeitdauer inaktiv ist.

### Prozedur

#### Schritt 1

Wählen Sie **Gerät > Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.

#### Schritt 2

Suchen Sie das Telefon, das Sie konfigurieren müssen.

#### Schritt 3

Navigieren Sie zum produktspezifischen Konfigurationsbereich, und legen Sie die folgenden Felder fest:

- Display nicht aktiv – Tage
- Display eingeschaltet – Uhrzeit
- Display eingeschaltet – Dauer
- Display-Leerlaufzeitüberschreitung

**Tabelle 19: Konfigurationsfelder für den Energiesparmodus**

Feld	Beschreibung
Display nicht aktiv – Tage	Die Tage, an denen das Display nicht automatisch zum angegebenen Zeitpunkt eingeschaltet wird. Wählen Sie in der Dropdown-Liste die Tage aus. Halten Sie zur Auswahl mehrerer Tage die Strg-Taste gedrückt, und klicken Sie auf die gewünschten Tage.

Feld	Beschreibung
Display eingeschaltet – Uhrzeit	<p>Die Uhrzeit, zu der das Display jeden Tag automatisch eingeschaltet wird (außer an den festgelegten Tagen).</p> <p>Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (00:00 ist Mitternacht).</p> <p>Um das Display beispielsweise um 07:00 Uhr einzuschalten, geben Sie <b>07:00</b> ein. Um das Display um 14.00 Uhr (1400) einzuschalten, geben Sie <b>14:00 ein</b>.</p> <p>Wenn das Feld leer ist, wird das Display automatisch um 0:00 aktiviert.</p>
Display eingeschaltet – Dauer	<p>Die Zeitdauer, die das Display eingeschaltet bleibt, nachdem es zum festgelegten Zeitpunkt eingeschaltet wurde.</p> <p>Geben Sie den Wert in diesem Feld im Format <i>Stunden:Minuten</i> ein.</p> <p>Um das Display beispielsweise für vier Stunden und 30 Minuten zu aktivieren, nachdem es automatisch aktiviert wurde, geben Sie <b>04:30</b> ein.</p> <p>Wenn das Feld leer ist, wird das Telefon am Ende des Tages (0:00) ausgeschaltet.</p> <p><b>Hinweis</b> Wenn der Zeitpunkt zum Einschalten des Displays auf 0:00 festgelegt ist und die Zeitdauer leer (oder 24:00) ist, bleibt das Display eingeschaltet.</p>
Display-Leerlaufzeitüberschreitung	<p>Die Zeitdauer, die das Telefon inaktiv ist, bevor das Display ausgeschaltet wird. Trifft nur zu, wenn das Display wie geplant ausgeschaltet und vom Benutzer eingeschaltet wurde (durch das Drücken einer Taste oder das Abheben des Hörers).</p> <p>Geben Sie den Wert in diesem Feld im Format <i>Stunden:Minuten</i> ein.</p> <p>Um das Display beispielsweise zu deaktivieren, wenn das Telefon eine Stunde und 30 Minuten inaktiv ist, nachdem der Benutzer die Anzeige aktiviert hat, geben Sie <b>01:30</b> ein.</p> <p>Der Standardwert ist 01:00.</p>

- Schritt 4** Wählen Sie **Speichern** aus.
- Schritt 5** Wählen Sie **Konfiguration übernehmen**.
- Schritt 6** Starten Sie das Telefon neu.

## EnergyWise für das Cisco IP-Telefon planen

Um den Stromverbrauch zu reduzieren, konfigurieren Sie das Telefon so, dass es ausgeschaltet und eingeschaltet wird, wenn das System einen EnergyWise-Controller umfasst.

Konfigurieren Sie die Einstellungen in der Cisco Unified Communications Manager-Verwaltung, um EnergyWise zu aktivieren und das Aus- und Einschalten des Telefons festzulegen. Diese Parameter sind eng mit den Parametern für die Konfiguration des Telefondisplays verknüpft.

Wenn EnergyWise aktiviert und der Zeitpunkt für das Ausschalten festgelegt ist, sendet das Telefon eine Anforderung an den Switch, damit es zum konfigurierten Zeitpunkt aktiviert wird. Der Switch akzeptiert oder lehnt die Anforderung ab. Wenn der Switch die Anforderung ablehnt oder nicht antwortet, wird das Telefon nicht ausgeschaltet. Wenn der Switch die Anforderung akzeptiert, wird das inaktive Telefon ausgeschaltet.

und der Stromverbrauch wird auf einen angegebenen Pegel reduziert. Ein aktives Telefon legt einen Leerlauf-Timer fest und schaltet sich aus, nachdem der Timer abgelaufen ist.

Um das Telefon zu aktivieren, drücken Sie Auswählen. Zum Zeitpunkt der geplanten Aktivierung stellt das System die Stromzufuhr an das Telefon wieder her, um es zu aktivieren.

## Prozedur

- Schritt 1** Wählen Sie **Gerät > Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Suchen Sie das Telefon, das Sie konfigurieren müssen.
- Schritt 3** Navigieren Sie zum produktspezifischen Konfigurationsbereich und legen Sie die folgenden Felder fest.
- Power Save Plus aktivieren
  - Telefon einschalten – Uhrzeit
  - Telefon ausschalten – Uhrzeit
  - Telefon ausschalten - Leerlauf-Timeout
  - Signalton aktivieren
  - EnergyWise-Domäne
  - EnergyWise-Secret
  - EnergyWise-Überschreibung zulassen

**Tabelle 20: EnergyWise-Konfigurationsfelder**

Feld	Beschreibung
Power Save Plus aktivieren	<p>Wählen Sie die Tage für den Zeitplan aus, an denen das Telefon ausgeschaltet wird. Wählen Sie mehrere Tage aus, indem Sie die Strg-Taste gedrückt halten, während Sie auf die Tage für den Zeitplan klicken.</p> <p>Standardmäßig sind keine Tage ausgewählt.</p> <p>Wenn „Power Save Plus aktivieren“ ausgewählt ist, wird eine Warnung bezüglich Notfällen angezeigt.</p> <p><b>Vorsicht</b> Wenn der Power Save Plus-Modus (der „Modus“) aktiviert ist, werden die Endpunkte, die für den Modus konfiguriert sind, für Notrufe und eingehende Anrufe deaktiviert. Indem Sie diesen Modus auswählen, stimmen Sie Folgendem zu: (i) Sie übernehmen die volle Verantwortung dafür, dass alternative Methoden für Notrufe und eingehende Anrufe bereitgestellt werden, während der Modus aktiviert ist; (ii) Cisco übernimmt keine Haftung in Bezug auf Ihre Auswahl des Modus und die gesamte Haftung in Zusammenhang mit der Aktivierung des Modus liegt in Ihrer Verantwortung; und (iii) Sie informieren die Benutzer über die Auswirkungen des Modus auf Anrufe und andere Funktionen.</p> <p><b>Hinweis</b> Um Power Save Plus zu deaktivieren, müssen Sie das Kontrollkästchen „EnergyWise-Überschreibungen zulassen“ deaktivieren. Wenn EnergyWise-Überschreibung zulassen aktiviert ist, aber keine Tage im Feld „Power Save Plus aktivieren“ ausgewählt sind, wird Power Save Plus nicht deaktiviert.</p>



Feld	Beschreibung
Telefon einschalten – Uhrzeit	<p>Legt fest, wann das Telefon an den Tagen, die im Feld Power Save Plus aktivieren ausgewählt sind, automatisch eingeschaltet wird.</p> <p>Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (00:00 ist Mitternacht).</p> <p>Um das Telefon beispielsweise um 07:00 Uhr (0700) automatisch einzuschalten, geben Sie 07:00 ein. Um das Telefon um 14:00 Uhr (1400) einzuschalten, geben Sie 14:00 ein.</p> <p>Der Standardwert ist leer, das heißt 00:00.</p> <p><b>Hinweis</b> Die Einschaltzeit des Telefons muss mindestens 20 Minuten später als die Ausschaltzeit sein. Wenn die Ausschaltzeit beispielsweise auf 07:00 festgelegt ist, darf die Einschaltzeit nicht früher als 07:20 sein.</p>
Telefon ausschalten – Uhrzeit	<p>Die Tageszeit, zu der das Telefon ausgeschaltet wird, die im Feld Power Save Plus aktivieren festgelegt sind. Wenn die Felder den gleichen Wert enthalten, wird das Telefon nicht ausgeschaltet.</p> <p>Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (00:00 ist Mitternacht).</p> <p>Um das Telefon beispielsweise um 7:00 Uhr (0700) automatisch auszuschalten, geben Sie 7:00 ein. Um das Telefon um 14:00 Uhr (1400) auszuschalten, geben Sie 14:00 ein.</p> <p>Der Standardwert ist leer, das heißt 00:00.</p> <p><b>Hinweis</b> Die Einschaltzeit des Telefons muss mindestens 20 Minuten später als die Ausschaltzeit sein. Wenn die Ausschaltzeit beispielsweise auf 07:00 festgelegt ist, darf die Einschaltzeit nicht früher als 07:20 sein.</p>
Telefon ausschalten - Leerlauf-Timeout	<p>Die Länge der Zeitdauer, die das Telefon inaktiv sein muss, bevor es ausgeschaltet wird.</p> <p>Der Timeout tritt unter folgenden Bedingungen auf:</p> <ul style="list-style-type: none"> <li>• Wenn das Telefon, wie geplant, in den Power Save Plus-Modus gewechselt ist und eingeschaltet wurde, da der Benutzer die Taste <b>Auswahl</b> gedrückt hat.</li> <li>• Wenn das Telefon vom angeschlossenen Switch wieder eingeschaltet wurde.</li> <li>• Wenn die Ausschaltzeit des Telefons erreicht wird, aber das Telefon verwendet wird.</li> </ul> <p>Das Feld hat einen Bereich von 20 und 1440 Minuten.</p> <p>Der Standardwert ist 60 Minuten.</p>

Feld	Beschreibung
Signalton aktivieren	<p>Wenn diese Option aktiviert ist, gibt das Telefon 10 Minuten vor der angegebenen Ausschaltzeit einen Signalton aus.</p> <p>Der Signalton ist der Rufton des Telefons, der während der 10-minütigen Warnperiode zu bestimmten Zeitpunkten wiedergegeben wird. Der Signalton wird in der vom Benutzer festgelegten Lautstärke wiedergegeben. Zeitplan für den Signalton:</p> <ul style="list-style-type: none"> <li>• Zehn Minuten vor dem Ausschalten wird der Rufton viermal wiedergegeben.</li> <li>• Sieben Minuten vor dem Ausschalten wird der Rufton viermal wiedergegeben.</li> <li>• Vier Minuten vor dem Ausschalten wird der Rufton viermal wiedergegeben.</li> <li>• 30 Sekunden vor dem Ausschalten wird der Rufton 15 Mal wiedergegeben oder so lange, bis sich das Telefon ausschaltet.</li> </ul> <p>Dieses Kontrollkästchen ist nur relevant, wenn im Listenfeld Power Save Plus aktivieren mindestens ein Tag ausgewählt ist.</p>
EnergyWise-Domäne	<p>Die EnergyWise-Domäne, in der sich das Telefon befindet.</p> <p>Dieses Feld darf maximal 127 Zeichen enthalten.</p>
EnergyWise-Secret	<p>Das Sicherheitskennwort, das verwendet wird, um mit den Endpunkten in der EnergyWise-Domäne zu kommunizieren.</p> <p>Dieses Feld darf maximal 127 Zeichen enthalten.</p>
EnergyWise-Überschreibung zulassen	<p>Dieses Kontrollkästchen legt fest, ob die EnergyWise-Domänencontrollerrichtlinie Energiepegelaktualisierungen an die Telefone senden kann. Es gelten die folgenden Bedingungen:</p> <ul style="list-style-type: none"> <li>• Im Feld Power Save Plus aktivieren muss mindestens ein Tag ausgewählt werden.</li> <li>• Die Einstellungen in der Cisco Unified Communications Manager-Verwaltung werden planmäßig übernommen, auch wenn EnergyWise eine Überschreibung sendet.</li> </ul> <p>Beispielsweise kann die Ausschaltzeit auf 22:00 Uhr, der Wert für die Einschaltzeit auf 06:00 Uhr und für Power Save Plus ist mindestens ein Tag festgelegt sein.</p> <ul style="list-style-type: none"> <li>• Wenn EnergyWise das Telefon anweist, sich um 20:00 Uhr auszuschalten, bleibt diese Anweisung bis zur festgelegten Einschaltzeit um 6:00 Uhr in Kraft.</li> <li>• Um 6:00 Uhr schaltet sich das Telefon ein und empfängt die Energiepegelaktualisierungen basierend auf den Einstellungen in der Unified Communications Manager-Verwaltung.</li> <li>• Um den Energiepegel auf dem Telefon erneut zu ändern, muss EnergyWise einen neuen Befehl ausgeben.</li> </ul> <p><b>Hinweis</b> Um Power Save Plus zu deaktivieren, müssen Sie das Kontrollkästchen „EnergyWise-Überschreibungen zulassen“ deaktivieren. Wenn EnergyWise-Überschreibung zulassen aktiviert ist, aber keine Tage im Feld „Power Save Plus aktivieren“ ausgewählt sind, wird Power Save Plus nicht deaktiviert.</p>

**Schritt 4** Wählen Sie **Speichern** aus.

- Schritt 5** Wählen Sie **Konfiguration übernehmen**.
- Schritt 6** Starten Sie das Telefon neu.

## DND konfigurieren

Wenn „Nicht stören“ aktiviert ist, leuchtet die Kopfzeile auf dem Bildschirm des Konferenztelefons rot.

Weitere Informationen zu DND finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

### Prozedur

- Schritt 1** Wählen Sie **Gerät > Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Suchen Sie das gewünschte Telefon.
- Schritt 3** Legen Sie die folgenden Parameter fest:
- DND: Mit diesem Kontrollkästchen können Sie DND auf dem Telefon aktivieren.
  - DND-Option: Rufton aus, Anruf ablehnen oder Allgemeine Telefonprofileinstellungen verwenden.
  - DND-Benachrichtigung für eingehenden Anruf: Wählen Sie den Typ der Benachrichtigung für eingehende Anrufe aus, wenn DND aktiviert ist.
- Hinweis** Dieser Parameter befindet sich in den Fenstern „Allgemeines Telefonprofil“ und „Telefonkonfiguration“. Der Wert im Fenster „Telefonkonfiguration“ hat Vorrang.
- Schritt 4** Wählen Sie **Speichern** aus.

### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Benachrichtigung für Rufumleitung einrichten

Sie können die Einstellungen für die Anrufweiterleitung steuern.

### Prozedur

- Schritt 1** Wählen Sie **Gerät > Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Suchen Sie das Telefon, das konfiguriert werden soll.
- Schritt 3** Konfigurieren Sie die Felder Benachrichtigung für Anrufweiterleitung.

Feld	Beschreibung
Name des Anrufers	Wenn dieses Kontrollkästchen aktiviert ist, wird der Name des Anrufers im Benachrichtigungsfenster angezeigt. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Feld	Beschreibung
Nummer des Anrufers	Wenn dieses Kontrollkästchen aktiviert ist, wird die Nummer des Anrufers im Benachrichtigungsfenster angezeigt.  Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Umgeleitete Nummer	Wenn dieses Kontrollkästchen aktiviert ist, werden die Informationen des Anrufers, der den Anruf zuletzt weitergeleitet hat, im Benachrichtigungsfenster angezeigt.  Beispiel: Wenn Teilnehmer A Teilnehmer B anruft, aber B alle Anrufe an C weitergeleitet hat und C alle Anrufe an D weitergeleitet hat, enthält das Benachrichtigungsfenster, das D sieht, die Telefoninformationen für Teilnehmer C.  Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gewählte Nummer	Wenn dieses Kontrollkästchen aktiviert ist, werden die Informationen des ursprünglichen Empfängers des Anrufs im Benachrichtigungsfenster angezeigt.  Beispiel: Wenn Teilnehmer A Teilnehmer B anruft, aber B alle Anrufe an C weitergeleitet hat und C alle Anrufe an D weitergeleitet hat, enthält das Benachrichtigungsfenster, das D sieht, die Telefoninformationen für Teilnehmer B.  Dieses Kontrollkästchen ist standardmäßig aktiviert.

**Schritt 4**

Wählen Sie **Speichern** aus.

## UCR 2008-Konfiguration

Die Parameter, die UCR 2008 unterstützen, befinden sich in der Cisco Unified Communications Manager-Verwaltung. In der folgenden Tabelle werden die Parameter und das Ändern der Einstellungen beschrieben.

**Tabelle 21: UCR 2008-Parameterpfad**

Parameter	Verwaltungspfad
FIPS-Modus	<b>Gerät &gt; Geräteeinstellungen &gt; Allgemeines Telefonprofil</b>
	<b>System &gt; Firmentelefonkonfiguration</b>
	<b>Gerät &gt; Telefone</b>
SSH-Zugriff	<b>Gerät &gt; Telefon</b>
	<b>Gerät &gt; Geräteeinstellungen &gt; Allgemeines Telefonprofil</b>

Parameter	Verwaltungspfad
Webzugriff	<b>Gerät &gt; Telefon</b>
	<b>System &gt; Firmentelefonkonfiguration</b>
	<b>Gerät &gt; Geräteeinstellungen &gt; Allgemeines Telefonprofil</b>
<b>System &gt; Firmentelefonkonfiguration</b>	
IP-Adressierungsmodus	<b>Gerät &gt; Geräteeinstellungen &gt; Allgemeine Gerätekonfiguration</b>
Bevorzugter IP-Adressierungsmodus für die Signalisierung	<b>Gerät &gt; Geräteeinstellungen &gt; Allgemeine Gerätekonfiguration</b>

## UCR 2008 in der allgemeinen Gerätekonfiguration konfigurieren

Verwenden Sie dieses Verfahren, um die folgenden UCR 2008-Parameter festzulegen:

- IP-Adressierungsmodus
- Bevorzugter IP-Adressierungsmodus für die Signalisierung

### Prozedur

- 
- Schritt 1** Wählen Sie **Gerät > Geräteeinstellungen > Allgemeine Gerätekonfiguration** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Legen Sie den Parameter für den IP-Adressierungsmodus fest.
- Schritt 3** Legen Sie den bevorzugten IP-Adressierungsmodus für den Signalisierungsparameter fest.
- Schritt 4** Wählen Sie **Speichern** aus.
- 

## UCR 2008 im allgemeinen Telefonprofil konfigurieren

Verwenden Sie dieses Verfahren, um die folgenden UCR 2008-Parameter festzulegen:

- FIPS-Modus
- SSH-Zugriff
- Webzugriff

### Prozedur

- 
- Schritt 1** Wählen Sie **Gerät > Geräteeinstellungen > Allgemeines Telefonprofil** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Legen Sie den FIPS-Modusparameter auf **Aktiviert** fest.
- Schritt 3** Legen Sie den SSH-Zugriffparameter auf **Deaktiviert** fest.

- Schritt 4** Legen Sie den Webzugriffsparameter auf **Deaktiviert** fest.
- Schritt 5** Legen Sie den 80-Bit SRTCP-Parameter auf **Aktiviert** fest.
- Schritt 6** Wählen Sie **Speichern** aus.
- 

## UCR 2008 in der Firmentelefonkonfiguration konfigurieren

Verwenden Sie dieses Verfahren, um die folgenden UCR 2008-Parameter festzulegen:

- FIPS-Modus
- Webzugriff

### Prozedur

---

- Schritt 1** Wählen Sie **System** > **Firmentelefonkonfiguration** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Legen Sie den FIPS-Modusparameter auf **Aktiviert** fest.
- Schritt 3** Legen Sie den Webzugriffsparameter auf **Deaktiviert** fest.
- Schritt 4** Wählen Sie **Speichern** aus.
- 

## UCR 2008 auf dem Telefon konfigurieren

Verwenden Sie dieses Verfahren, um die folgenden UCR 2008-Parameter festzulegen:

- FIPS-Modus
- SSH-Zugriff
- Webzugriff

### Prozedur

---

- Schritt 1** Wählen Sie **Gerät** > **Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Legen Sie den SSH-Zugriffsparameter auf **Deaktiviert** fest.
- Schritt 3** Legen Sie den FIPS-Modusparameter auf **Aktiviert** fest.
- Schritt 4** Legen Sie den Webzugriffsparameter auf **Deaktiviert** fest.
- Schritt 5** Wählen Sie **Speichern** aus.
- 

## Mobil- und Remote Access über Expressway

Mobil- und Remote Access über Expressway(MRA) ermöglicht Remotebenutzern, sich einfach und sicher mit dem Firmennetzwerk zu verbinden, ohne einen VPN-Clienttunnel verwenden zu müssen. Expressway verwendet TLS (Transport Layer Security), um den Netzwerkverkehr zu schützen. Damit ein Telefon ein Expressway-Zertifikat authentifizieren und eine TLS-Sitzung einrichten kann, muss das Expressway-Zertifikat

von einer öffentlichen Zertifizierungsstelle, der die Telefon-Firmware vertraut, signiert sein. Es ist nicht möglich, andere CA-Zertifikate auf Telefonen für die Authentifizierung eines Expressway-Zertifikats zu installieren oder anderen Zertifikaten zu vertrauen.

Die Liste der CA-Zertifikate, die in der Telefon-Firmware eingebettet sind, ist unter <http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html> verfügbar.

Mobil- und Remote Access über Expressway (MRA) funktioniert mit Cisco Expressway. Sie sollten mit der Cisco Expressway-Dokumentation vertraut sein, einschließlich dem *Cisco Expressway Administratorhandbuch* und dem *Cisco Expressway Standardkonfiguration, Bereitstellungshandbuch*. Sie erhalten die Cisco Expressway-Dokumentation unter <http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html>.

Für Mobil- und Remote Access über Expressway-Benutzer wird nur das IPv4-Protokoll unterstützt.

Weitere Informationen zur Verwendung von Mobil- und Remote Access über Expressway finden Sie unter:

- *Cisco Preferred Architecture für Enterprise Collaboration, Design-Übersicht*
- *Cisco Preferred Architecture für Enterprise Collaboration, CVD*
- *Unified Communications Mobil- und Remotezugriff über Cisco VCS, Bereitstellungshandbuch*
- *Cisco TelePresence Video Communication Server (VCS), Konfigurationshandbücher*
- *Mobil- und Remote-Zugriff über Cisco Expressway – Bereitstellungshandbuch*

Während der Telefonregistrierung synchronisiert das Telefon das angezeigte Datum und die Uhrzeit mit dem NTP-Server (Network Time Protocol). Mit MRA wird das DHCP-Optionstag 42 verwendet, um die IP-Adressen der NTP-Server zu ermitteln, die für die Datum- und Zeitsynchronisierung vorgesehen sind. Wenn das DHCP-Optionstag 42 nicht in den Konfigurationsinformationen gefunden wird, sucht das Telefon nach dem Tag 0.tandberg.pool.ntp.org, um die NTP-Server zu identifizieren.

Nach der Registrierung verwendet das Telefon die Informationen in der SIP-Nachricht, um das Datum und die Uhrzeit, die angezeigt werden, zu synchronisieren, außer wenn ein NTP-Server in der Cisco Unified Communications Manager-Telefonkonfiguration konfiguriert ist.



---

**Hinweis** Wenn für das Telefonsicherheitsprofil die Einstellung Verschlüsselte TFTP-Konfiguration aktiviert ist, können Sie das Telefon nicht mit Mobil- und Remotezugriff verwenden. Die MRA-Lösung unterstützt keine Geräteinteraktion mit CAPF (Certificate Authority Proxy Function).

---

Der SIP-OAuth-Modus wird für MRA unterstützt. In diesem Modus können Sie OAuth-Zugriffstoken für die Authentifizierung in sicheren Umgebungen verwenden.



---

**Hinweis** Für SIP-OAuth im MRA-Modus (Mobile and Remote Access) verwenden Sie bei der Bereitstellung des Telefons nur Onboarding des Aktivierungscode mit mobilem und Remote-Zugriff. Die Aktivierung mit einem Benutzernamen und einem Kennwort wird nicht unterstützt.

---

Der SIP-OAuth-Modus erfordert Expressway x 14.0(1) und höher oder Cisco Unified Communications Manager 14.0(1) und höher.

Weitere Informationen zum SIP-OAuth-Modus finden Sie im *Funktionskonfigurationshandbuch für Cisco Unified Communications Manager*, Version 14.0(1) oder höher.

## Bereitstellungsszenarien

In der folgenden Tabelle sind verschiedene Bereitstellungsszenarien für Mobil- und Remote Access über Expressway aufgeführt.

Szenario	Aktionen
Vor Ort meldet sich der Benutzer am Unternehmensnetzwerk an, nachdem Mobil- und Remote Access über Expressway bereitgestellt wurde.	Das Firmennetzwerk wird erkannt und das Telefon wird wie üblich mit Cisco Unified Communications Manager registriert.
Außerhalb des Unternehmens meldet sich der Benutzer mit Mobil- und Remote Access über Expressway am Unternehmensnetzwerk an.	<p>Wenn das Telefon erkennt, dass es sich nicht im Büro befindet, wird das Mobil- und Remote Access über Expressway Anmeldefenster angezeigt und der Benutzer kann die Verbindung mit dem Unternehmensnetzwerk herstellen.</p> <p>Der Benutzer benötigt einen gültigen Servicenamen, einen Benutzernamen und ein Kennwort, um die Verbindung mit dem Netzwerk herzustellen.</p> <p>Zudem müssen Benutzer den Servicemodus zurücksetzen, um die Einstellung für „Alternativer TFTP-Server“ zu löschen, ehe sie auf das Unternehmensnetzwerk zugreifen können. Dadurch werden die Werte der Einstellung „Alternativer TFTP-Server“ gelöscht, sodass das Telefon das externe Netzwerk erkennt.</p> <p>Wenn ein neues Telefon direkt bereitgestellt wird, kann der Benutzer das Zurücksetzen der Netzwerkeinstellungen überspringen.</p> <p>Wenn für Benutzer die DHCP-Option 150 oder 66 auf dem Netzwerkrouter aktiviert ist, können sie sich unter Umständen nicht beim Unternehmensnetzwerk anmelden. Die Benutzer sollten diese DHCP-Einstellungen deaktivieren oder die statische IP-Adresse direkt konfigurieren.</p>

## Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren

Bei der Anmeldung eines Benutzers am Netzwerk mit Mobil- und Remote Access über Expressway wird der Benutzer aufgefordert, eine Servicedomäne, einen Benutzernamen und ein Kennwort anzugeben. Wenn Sie den Parameter „Dauerhafte Anmeldeinformationen für Expressway-Anmeldung“ aktivieren, werden die Anmeldeinformationen für Benutzer gespeichert, sodass die Benutzer diese Informationen nicht erneut eingeben müssen. Dieser Parameter ist standardmäßig deaktiviert.

Sie können Anmeldeinformationen so konfigurieren, dass sie für ein einzelnes Telefon, eine Gruppe von Telefonen oder alle Telefone beibehalten werden.



**Verwandte Themen**

[Telefonfunktion – Konfiguration](#), auf Seite 100

[Produktspezifische Konfiguration](#), auf Seite 102

## Tool zur Problemmeldung

Die Benutzer senden Problembenachrichtungen mit dem Tool für Problembenachrichtungen (PRT).



**Hinweis** Die PRT-Protokolle werden vom Cisco TAC für die Problembehandlung benötigt. Die Protokolle werden gelöscht, wenn Sie das Telefon neu starten. Erfassen Sie die Protokolle, bevor Sie die Telefone neu starten.

Um einen Problembenachrichtung zu erstellen, greifen die Benutzer auf das Tool für Problembenachrichtungen zu und geben das Datum und die Uhrzeit sowie eine Beschreibung des Problems ein.

Wenn der PRT-Upload fehlschlägt, können Sie über die URL

**http://<phone-ip-address>/FS/<prt-file-name>** auf die PRT-Datei für das Telefon zugreifen.

Die URL wird in folgenden Fällen auf dem Telefon angezeigt:

- Wenn sich das Telefon im Standardwerksstatus befindet. Die URL ist eine Stunde lang aktiv. Nach einer Stunde sollte der Benutzer versuchen, die Telefonprotokolle erneut zu senden.
- Wenn eine Konfigurationsdatei auf das Telefon heruntergeladen wurde und das Anrufsteuerungssystem den Webzugriff auf das Telefon zulässt.

Sie müssen eine Serveradresse zum Feld **Upload-URL für Kundensupport** in Cisco Unified Communications Manager hinzufügen.

Wenn Sie Geräte mit Mobil- und Remote Access über Expressway bereitstellen, müssen Sie die PRT-Serveradresse zur Zulassungsliste des HTTP-Servers auf dem Expressway-Server hinzufügen.

### Eine Upload-URL für den Kundensupport konfigurieren

Um PRT-Dateien zu empfangen, benötigen Sie einen Server mit einem Upload-Skript. PRT verwendet eine HTTP POST-Methode mit den folgenden Parametern im Upload (mehnteilige MIME-Codierung):

- devicename (Beispiel: „SEP001122334455“)
- serialno (Beispiel: „FCH12345ABC“)
- username (der in Cisco Unified Communications Manager konfigurierte Benutzername, der Gerätebesitzer)
- prt\_file (Beispiel: „probrep-20141021-162840.tar.gz“)

Im Folgenden finden Sie ein Beispielskript. Dieses Skript dient nur zu Referenzzwecken. Cisco bietet keinen Support für ein Upload-Skript, das auf dem Server eines Kunden installiert ist.

```
<?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.");
}

?>

```




---

**Hinweis** Die Telefone unterstützen nur HTTP-URLs.

---

### Prozedur

---

- Schritt 1** Konfigurieren Sie einen Server, auf dem das PRT-Upload-Skript ausgeführt werden kann.
- Schritt 2** Schreiben Sie ein Skript, das die oben angegebenen Parameter verarbeiten kann, oder bearbeiten Sie das Beispielskript entsprechend Ihrer Anforderungen.
- Schritt 3** Laden Sie das Skript auf den Server hoch.
- Schritt 4** Navigieren Sie in Cisco Unified Communications Manager zum produktspezifischen Konfigurationsbereich im Fenster Gerätekonfiguration, Allgemeines Telefonprofil oder Firmentelefonkonfiguration.
- Schritt 5** Aktivieren Sie **Upload-URL für Kundensupport** und geben Sie die Upload-URL ein.

#### Beispiel:

`http://example.com/prtscript.php`

- Schritt 6** Speichern Sie Ihre Änderungen.
- 

## Bezeichnung einer Leitung festlegen

Sie können ein Telefon so konfigurieren, dass eine Textbezeichnung anstatt der Verzeichnisnummer angezeigt wird. Mit dieser Bezeichnung kann die Leitung anhand des Namens oder der Funktion identifiziert werden. Wenn der Benutzer die Leitungen auf dem Telefon für andere Benutzer freigibt, können Sie die Leitung anhand des Namens dieses Benutzers identifizieren.

Wenn Sie einem Schlüsselerweiterungsmodul eine Bezeichnung hinzufügen, werden nur die ersten 25 Zeichen auf einer Leitung angezeigt.

## Prozedur

---

- Schritt 1** Wählen Sie **Gerät > Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Suchen Sie das gewünschte Telefon.
- Schritt 3** Suchen Sie die Leitungsinstanz und legen Sie das Feld Textbezeichnung für Leitung fest.
- Schritt 4** (optional) Wenn die Bezeichnung für andere Geräte, die die Leitung verwenden, übernommen werden muss, aktivieren Sie das Kontrollkästchen „Einstellungen für gemeinsam genutztes Gerät aktualisieren“ und klicken Sie auf **Auswahl verbreiten**.
- Schritt 5** Wählen Sie **Speichern** aus.
-

■ Bezeichnung einer Leitung festlegen



## KAPITEL 10

# Unternehmensverzeichnis und persönliches Verzeichnis

---

- [Konfiguration des Firmenverzeichnisses, auf Seite 131](#)
- [Konfiguration des persönlichen Verzeichnisses, auf Seite 131](#)

## Konfiguration des Firmenverzeichnisses

Im Firmenverzeichnis kann ein Benutzer die Telefonnummern von Kollegen suchen. Damit diese Funktion unterstützt wird, müssen Sie Firmenverzeichnisse konfigurieren.

Cisco Unified Communications Manager verwendet ein Lightweight Directory Access Protocol(LDAP)-Verzeichnis, um Authentifizierungs- und Autorisierungsinformationen über Benutzer von Cisco Unified Communications Manager-Anwendungen zu speichern, die mit Cisco Unified Communications Manager interagieren. Die Authentifizierung legt die Benutzerrechte für den Zugriff auf das System fest. Die Autorisierung identifiziert die Telefonressourcen, die ein Benutzer verwenden kann, beispielsweise einen bestimmten Telefonanschluss.

Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Nachdem Sie das LDAP-Verzeichnis konfiguriert haben, können die Benutzer das Firmenverzeichnis auf ihren Telefonen verwenden, um Firmenbenutzer zu suchen.

### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Konfiguration des persönlichen Verzeichnisses

Das persönliche Verzeichnis ermöglicht dem Benutzer, persönliche Nummern zu speichern.

Das persönliche Verzeichnis umfasst folgende Features:

- Persönliches Adressbuch (PAB)
- Kurzwahl

Die Benutzer können mit folgenden Methoden auf die Funktionen des persönlichen Verzeichnisses zugreifen:

- Über einen Webbrowser: Die Benutzer können auf PAB und Kurzwahlfunktionen im Cisco Unified Communications Benutzerportal zugreifen.
- Über Cisco IP-Telefon: Die Benutzer können **Kontakte** auswählen, um das Unternehmensverzeichnis oder ihr persönliches Adressbuch zu durchsuchen.

Um das persönliche Verzeichnis über einen Webbrowser zu konfigurieren, müssen die Benutzer auf ihr Selbstservice-Portal zugreifen. Sie müssen eine URL und die Anmeldeinformationen an die Benutzer weitergeben.



## TEIL **IV**

# Cisco IP-Konferenztelefon – Fehlerbehebung

- [Telefonsysteme überwachen, auf Seite 135](#)
- [Telefonfehlerbehebung, auf Seite 161](#)
- [Wartung, auf Seite 179](#)
- [Unterstützung von Benutzern in anderen Ländern, auf Seite 183](#)







# KAPITEL 11

## Telefonsysteme überwachen

---

- [Übersicht der Telefonsystemüberwachung, auf Seite 135](#)
- [Cisco IP-Telefon-Status, auf Seite 135](#)
- [Webseite für Cisco IP-Telefon, auf Seite 146](#)
- [Informationen im XML-Format vom Telefon anfordern, auf Seite 158](#)

### Übersicht der Telefonsystemüberwachung

Unter Verwendung des Menüs Telefonstatus auf dem Telefon und den Telefon-Webseiten können Sie verschiedene Informationen anzeigen. Diese Informationen umfassen:

- Geräteinformationen
- Informationen zur Netzwerkkonfiguration
- Netzwerkstatistik
- Geräteprotokolle
- Streaming-Statistik

Dieses Kapitel beschreibt die Informationen, die auf der Telefon-Webseite verfügbar sind. Sie können diese Informationen verwenden, um den Betrieb eines Telefons remote zu überwachen und bei der Fehlerbehebung zu helfen.

#### Verwandte Themen

[Telefonfehlerbehebung](#), auf Seite 161

### Cisco IP-Telefon-Status

In den folgenden Abschnitten wird beschrieben, wie die Modellinformationen, Statusmeldungen und die Netzwerkstatistik auf Cisco IP-Telefon angezeigt werden.

- **Modellinformationen:** Zeigt Hardware- und Softwareinformationen zum Telefon an.
- **Statusmenü:** Ermöglicht den Zugriff auf Bildschirme, die Statusmeldungen, die Netzwerkstatistik und die Statistik für den aktuellen Anruf anzeigen.

Sie können die Informationen auf diesen Bildschirmen verwenden, um den Betrieb eines Telefons zu überwachen und bei der Fehlerbehebung zu helfen.

Sie können diese und andere Informationen auch remote über die Webseite für das Telefon abrufen.

## Fenster „Telefoninformationen anzeigen“

### Prozedur

- 
- Schritt 1** Drücken Sie **Einstellungen** > **Systeminformationen**.
- Schritt 2** Um das Menü zu verlassen, drücken Sie **Beenden**.
- 

## Statusmenü anzeigen

### Prozedur

- 
- Schritt 1** Drücken Sie **Einstellungen** > **Status**.
- Schritt 2** Um das Menü zu verlassen, drücken Sie **Beenden**.
- 

## Das Fenster „Statusmeldungen“ anzeigen

### Prozedur

- 
- Schritt 1** Drücken Sie **Einstellungen** > **Status** > **Statusmeldungen**.
- Schritt 2** Um das Menü zu verlassen, drücken Sie **Beenden**.
- 

### Statusmeldungen

In der folgenden Tabelle werden die Statusmeldungen beschrieben, die auf dem Bildschirm Statusmeldungen auf dem Telefon angezeigt werden.

*Tabelle 22: Statusmeldungen auf Cisco IP-Telefon*

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
IP-Adresse konnte nicht von DHCP abgerufen werden	Das Telefon hat zuvor noch keine IP-Adresse von einem DHCP-Server abgerufen. Dies kann auftreten, wenn Sie das Telefon auf die Werkseinstellungen zurücksetzen.	Stellen Sie sicher, dass der DHCP-Server für das Telefon verfügbar sind.

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
TFTP-Größenfehler	Die Konfigurationsdatei ist zu groß für das Dateisystem auf dem Telefon.	Schalten Sie das Telefon aus und w
ROM-Prüfsummenfehler	Die heruntergeladene Softwaredatei ist beschädigt.	Beziehen Sie eine neue Kopie der T speichern Sie diese im TFTPPath-V Dateien nur in dieses Verzeichnis k TFTP-Serversoftware deaktiviert is beschädigt werden können.
Doppelte IP	Ein anderes Gerät verwendet die IP-Adresse, die dem Telefon zugewiesen ist.	Wenn das Telefon eine statische IP- sicher, dass keine doppelte IP-Adre  Wenn Sie DHCP verwenden, überp DHCP-Serverkonfiguration.
CTL- und ITL-Dateien löschen	Löschen Sie die CTL- oder ITL-Datei.	Keine. Diese Meldung ist nur für Inf
Fehler beim Aktualisieren des Gebietsschemas	Mindestens eine Lokalisierungsdatei konnte nicht im TFTP-Pfadverzeichnis gefunden werden oder ist ungültig. Das Gebietsschema wurde geändert.	Überprüfen Sie von der Administra Unified-Betriebssystems aus, ob in TFTP-Dateiverwaltung folgende D  <ul style="list-style-type: none"> <li>• Im Unterverzeichnis, das den g Netzwerkgebietsschema hat: <ul style="list-style-type: none"> <li>• tones.xml</li> </ul> </li> <li>• Mit dem gleichen Namen wie im Unterverzeichnis gespeiche <ul style="list-style-type: none"> <li>• glyphs.xml</li> <li>• dictionary.xml</li> <li>• kate.xml</li> </ul> </li> </ul>
Datei nicht gefunden <Cfg File>	Die auf dem Namen basierende und Standardkonfigurationsdatei wurde nicht auf dem TFTP-Server gefunden.	Die Konfigurationsdatei für ein Tel Telefon zur Cisco Unified Communi hinzugefügt wird. Wenn das Telefo Communications Manager-Datenba der TFTP-Server eine <b>CFG-Datei</b> <b>gefunden</b> -Antwort.  <ul style="list-style-type: none"> <li>• Das Telefon ist nicht mit Cisco Manager registriert.  Sie müssen das Telefon manue Communications Manager hin automatische Registrierung vo</li> <li>• Wenn Sie DHCP verwenden, s DHCP-Server auf den richtige</li> <li>• Wenn Sie statische IP-Adresser die Konfiguration des TFTP-S</li> </ul>

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
Datei nicht gefunden <CTLFile.tlv>	Diese Meldung wird auf dem Telefon angezeigt, wenn sich der Cisco Unified Communications Manager-Cluster nicht im sicheren Modus befindet.	Keine Auswirkung. Das Telefon kann sich nicht mit dem Cisco Unified Communications Manager registrieren.
IP-Adresse freigegeben	Das Telefon ist konfiguriert, um die IP-Adresse freizugeben.	Das Telefon bleibt inaktiv, bis es aus- oder die DHCP-Adresse zurückgesetzt wird.
IPv4 DHCP-Zeitüberschreitung	Der IPv4 DHCP-Server reagiert nicht.	<p>Netzwerk ist ausgelastet: Die Fehler sollten verschwinden, wenn die Netzwerklast reduziert wird.</p> <p>Keine Netzwerkverbindung zwischen dem Netzwerk und dem Telefon: Überprüfen Sie die Netzwerkkonfiguration.</p> <p>IPv4 DHCP-Server ist ausgefallen: Überprüfen Sie die Konfiguration des IPv4 DHCP-Servers.</p> <p>Fehler treten erneut auf: Weisen Sie ein anderes IP-Adressenpaar zu.</p>
IPv6 DHCP-Zeitüberschreitung	Der IPv6 DHCP-Server reagiert nicht.	<p>Netzwerk ist ausgelastet: Die Fehler sollten verschwinden, wenn die Netzwerklast reduziert wird.</p> <p>Keine Netzwerkverbindung zwischen dem Netzwerk und dem Telefon: Überprüfen Sie die Netzwerkkonfiguration.</p> <p>IPv6 DHCP-Server ist ausgefallen: Überprüfen Sie die Konfiguration des IPv6 DHCP-Servers.</p> <p>Fehler treten erneut auf: Weisen Sie ein anderes IP-Adressenpaar zu.</p>
IPv4 DNS-Zeitüberschreitung	Der IPv4 DNS-Server reagiert nicht.	<p>Netzwerk ist ausgelastet: Die Fehler sollten verschwinden, wenn die Netzwerklast reduziert wird.</p> <p>Keine Netzwerkverbindung zwischen dem Netzwerk und dem Telefon: Überprüfen Sie die Netzwerkkonfiguration.</p> <p>IPv4 DNS-Server ist ausgefallen: Überprüfen Sie die Konfiguration des IPv4 DNS-Servers.</p>
IPv6 DNS-Zeitüberschreitung	Der IPv6 DNS-Server reagiert nicht.	<p>Netzwerk ist ausgelastet: Die Fehler sollten verschwinden, wenn die Netzwerklast reduziert wird.</p> <p>Keine Netzwerkverbindung zwischen dem Netzwerk und dem Telefon: Überprüfen Sie die Netzwerkkonfiguration.</p> <p>IPv6 DNS-Server ist ausgefallen: Überprüfen Sie die Konfiguration des IPv6 DNS-Servers.</p>
Unbekannter DNS IPv4-Host	IPv4 DNS konnte den Namen des TFTP-Servers oder von Cisco Unified Communications Manager nicht auflösen.	<p>Überprüfen Sie, ob die Hostnamen des TFTP-Servers von Cisco Unified Communications Manager konfiguriert sind.</p> <p>Verwenden Sie IPv4-Adressen anstatt Hostnamen.</p>

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
Unbekannter DNS IPv6-Host	IPv6 DNS konnte den Namen des TFTP-Servers oder von Cisco Unified Communications Manager nicht auflösen.	Überprüfen Sie, ob die Hostnamen in Cisco Unified Communications Manager korrekt konfiguriert sind. Verwenden Sie IPv6-Adressen anstelle von Hostnamen.
Last zurückgewiesen – HC	Die heruntergeladene Anwendung ist nicht mit der Telefonhardware kompatibel.	Dieses Problem kann auftreten, wenn Sie dem Telefon eine Softwareversion installieren, die nicht mit den Hardware-Veränderungen der Hardware des Telefons kompatibel ist. Überprüfen Sie die Last-ID, die dem Telefon zugeordnet ist (wählen Sie <b>Gerät</b> > <b>Telefon</b> in Cisco Unified Communications Manager aus). Geben Sie die auf dem Telefon angegebene Last-ID erneut ein.
Kein Standardrouter	DHCP oder die statische Konfiguration geben keinen Standardrouter an.	Wenn das Telefon eine statische IP-Konfiguration verwendet, ob der Standardrouter konfiguriert ist. Wenn Sie DHCP verwenden, hat der Standardrouter bereitgestellt. Überprüfen Sie die DHCP-Serverkonfiguration.
Kein IPv4 DNS-Server	Ein Name wurde angegeben, aber DHCP oder die statische IP-Konfiguration geben keine IPv4 DNS-Serveradresse an.	Wenn das Telefon eine statische IP-Konfiguration verwendet, ob der IPv4 DNS-Server konfiguriert ist. Wenn Sie DHCP verwenden, hat der DNS-Server bereitgestellt. Überprüfen Sie die DHCP-Serverkonfiguration.
Kein IPv6 DNS-Server	Ein Name wurde angegeben, aber DHCP oder die statische IP-Konfiguration geben keine IPv6 DNS-Serveradresse an.	Wenn das Telefon eine statische IP-Konfiguration verwendet, ob der IPv6 DNS-Server konfiguriert ist. Wenn Sie DHCP verwenden, hat der DNS-Server bereitgestellt. Überprüfen Sie die DHCP-Serverkonfiguration.
Keine Vertrauensliste installiert	Die CTL- oder ITL-Datei ist nicht auf dem Telefon installiert.	Die Vertrauensliste ist nicht in Cisco Unified Communications Manager konfiguriert und die Sicherheit ist nicht standardmäßig unterstützt. Die Vertrauensliste ist nicht konfiguriert. Weitere Informationen zu Vertrauenslisten finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.
Telefon konnte nicht registriert werden. Die Größe des Zertifikatsschlüssels ist nicht FIPS-konform.	FIPS erfordert, dass das RSA-Serverzertifikat 2048 Bit oder mehr umfasst.	Aktualisieren Sie das Zertifikat.
Neustart von Cisco Unified Communications Manager angefordert	Das Telefon wird aufgrund einer Anforderung von Cisco Unified Communications Manager neu gestartet.	In Cisco Unified Communications Manager sind möglicherweise Konfigurationsänderungen vorgenommen und <b>Konfiguration</b> um die Änderungen zu übernehmen.

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
TFTP-Zugriffsfehler	Der TFTP-Server verweist auf ein Verzeichnis, das nicht vorhanden ist.	Wenn Sie DHCP verwenden, stellen Sie den DHCP-Server auf den richtigen TFTP-Server. Wenn Sie statische IP-Adressen verwenden, überprüfen Sie die Konfiguration des TFTP-Servers.
TFTP-Fehler	Das Telefon erkennt einen Fehlercode vom TFTP-Server nicht.	Kontaktieren Sie das Cisco TAC.
TFTP-Zeitüberschreitung	Der TFTP-Server reagiert nicht.	Netzwerk ist ausgelastet: Die Fehler sollten verschwinden, wenn die Netzwerklast reduziert wird. Keine Netzwerkverbindung zwischen dem Telefon und dem TFTP-Server: Überprüfen Sie die Netzwerkverbindung. TFTP-Server ist ausgefallen: Überprüfen Sie den Status des TFTP-Servers.
Zeitüberschreitung	Supplicant versuchte eine 802.1X-Transaktion, aber die Zeit wurde überschritten, da kein Authentifikator vorhanden ist.	Bei der Authentifizierung tritt normalerweise keine Zeitüberschreitung auf, wenn 802.1X normal konfiguriert ist.
Aktualisierung der Vertrauensliste fehlgeschlagen	Die Aktualisierung der CTL- und ITL-Datei ist fehlgeschlagen.	Auf dem Telefon sind CTL- und ITL-Dateien vorhanden, aber die neuen CTL- und ITL-Dateien konnten nicht geladen werden. Mögliche Fehlerursachen: <ul style="list-style-type: none"> <li>• Ein Netzwerkfehler ist aufgetreten.</li> <li>• Der TFTP-Server ist ausgefallen.</li> <li>• Der neue Sicherheitstoken, der zur Aktualisierung der CTL-Datei verwendet wurde, und der alte Token, der zum Signieren der ITL-Datei verwendet wurde, sind nicht verfügbar.</li> <li>• Ein interner Telefonfehler ist aufgetreten.</li> </ul> Mögliche Lösungen: <ul style="list-style-type: none"> <li>• Überprüfen Sie die Netzwerkverbindung.</li> <li>• Überprüfen Sie, ob der TFTP-Server normal funktioniert.</li> <li>• Wenn der TVS-Server (Transactional Voice Signaling) des Cisco Unified Communications Managers nicht normal funktioniert, überprüfen Sie, ob der TVS-Server normal funktioniert.</li> <li>• Überprüfen Sie, ob der Sicherheitstoken des TFTP-Servers gültig sind.</li> </ul> Löschen Sie die CTL- und ITL-Dateien auf dem Telefon. Die Lösungen fehlschlagen. Setzen Sie das Telefon zurück. Weitere Informationen zu Vertrauenslisten finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
Vertrauensliste aktualisiert	Die CTL-Datei, die ITL-Datei oder beide Dateien werden aktualisiert.	Keine. Diese Meldung ist nur für Inf... Weitere Informationen zu Vertraue... Dokumentation für Ihre Version vo... Communications Manager.
Versionsfehler	Der Name der Telefonlastdatei ist ungültig.	Stellen Sie sicher, dass die Telefonla... hat.
XmlDefault.cnf.xml oder .cnf.xml übereinstimmend mit dem Gerätenamen des Telefons.	Name der Konfigurationsdatei.	Keine. Die Meldung zeigt den Nam... für das Telefon an.

**Verwandte Themen**

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

**Das Fenster „Netzwerkstatistik“ anzeigen****Prozedur**

- Schritt 1** Drücken Sie **Einstellungen > Status > Netzwerkstatistik**.
- Schritt 2** Um das Menü zu verlassen, drücken Sie **Beenden**.

**Netzwerkstatistikfelder**

In der folgenden Tabelle werden die Elemente auf dem Bildschirm Netzwerkstatistik beschrieben.

**Tabelle 23: Netzwerkstatistikfelder**

Element	Beschreibung
Übertr. – Frames	Anzahl der Pakete, die das Telefon gesendet hat
Tx Broadcast	Anzahl der Broadcast-Pakete, die das Telefon gesendet hat
Tx Unicast	Gesamtanzahl der Unicast-Pakete, die das Telefon gesendet hat
Rx Frames	Anzahl der Pakete, die das Telefon empfangen hat
Rx Broadcast	Anzahl der Broadcast-Pakete, die das Telefon empfangen hat
Rx Unicast	Gesamtanzahl der Unicast-Pakete, die das Telefon empfangen hat
CDP Nachbargeräte-ID	ID eines Geräts, das mit diesem Port verbunden ist und vom CDP-Protokoll erkannt wird.
CDP Nachbar-IP-Adresse	ID eines Geräts, das mit diesem Port verbunden ist und vom CDP-Protokoll mit IP erkannt wird.

Element	Beschreibung
CDP Nachbar-Port	ID eines Geräts, das mit diesem Port verbunden ist und vom CDP-Protokoll erkannt wird.
Ursache des Neustarts: Einer dieser Werte: <ul style="list-style-type: none"> <li>• Zurücksetzen der Hardware (Power-On-Reset)</li> <li>• Zurücksetzen der Software (Speichercontroller wird ebenfalls zurückgesetzt)</li> <li>• Zurücksetzen der Software (Speichercontroller wird nicht zurückgesetzt)</li> <li>• Watchdog zurücksetzen</li> <li>• Initialisiert</li> <li>• Unbekannt</li> </ul>	Ursache des letzten Zurücksetzens des Telefons
Port 1	Linkstatus und Verbindung des Netzwerk-Ports (z. B. bedeutet <b>100 Full</b> , dass der PC-Port verbunden ist und automatisch eine Vollduplex-100-Mbit/s-Verbindung ausgehandelt hat)
IPv4	Informationen zum DHCP-Status. Dies schließt die folgenden Statusangaben ein: <ul style="list-style-type: none"> <li>• CDP BOUND</li> <li>• CDP INIT</li> <li>• DHCP BOUND</li> <li>• DHCP DISABLED</li> <li>• DHCP INIT</li> <li>• DHCP INVALID</li> <li>• DHCP REBINDING</li> <li>• DHCP REBOOT</li> <li>• DHCP RENEWING</li> <li>• DHCP REQUESTING</li> <li>• DHCP RESYNC</li> <li>• DHCP UNRECOGNIZED</li> <li>• DHCP WAITING COLDBOOT TIMEOUT</li> <li>• DISABLED DUPLICATE IP</li> <li>• SET DHCP COLDBOOT</li> <li>• SET DHCP DISABLED</li> <li>• SET DHCP FAST</li> </ul>



Element	Beschreibung
IPv6	<p>Informationen zum DHCP-Status. Dies schließt die folgenden Statusangaben ein:</p> <ul style="list-style-type: none"> <li>• CDP INIT</li> <li>• DHCP6 BOUND</li> <li>• DHCP6 DISABLED</li> <li>• DHCP6 RENEW</li> <li>• DHCP6 REBIND</li> <li>• DHCP6 INIT</li> <li>• DHCP6 SOLICIT</li> <li>• DHCP6 REQUEST</li> <li>• DHCP6 RELEASING</li> <li>• DHCP6 RELEASED</li> <li>• DHCP6 DISABLING</li> <li>• DHCP6 DECLINING</li> <li>• DHCP6 DECLINED</li> <li>• DHCP6 INFOREQ</li> <li>• DHCP6 INFOREQ DONE</li> <li>• DHCP6 INVALID</li> <li>• DISABLED DUPLICATE IPV6</li> <li>• DHCP6 DECLINED DUPLICATE IP</li> <li>• ROUTER ADVERTISE</li> <li>• DHCP6 WAITING COLDBOOT TIMEOUT</li> <li>• DHCP6 TIMEOUT USING RESTORED VAL</li> <li>• DHCP6 TIMEOUT CANNOT RESTORE</li> <li>• IPV6 STACK TURNED OFF</li> <li>• ROUTER ADVERTISE</li> <li>• ROUTER ADVERTISE</li> <li>• UNRECOGNIZED MANAGED BY</li> <li>• ILLEGAL IPV6 STATE</li> </ul>

## Das Fenster „Anrufstatistik“ anzeigen

### Prozedur

**Schritt 1** Drücken Sie **Einstellungen** > **Status** > **Anrufstatistiken**.

**Schritt 2** Um das Menü zu verlassen, drücken Sie **Beenden**.

### Anrufstatistikfelder

In der folgenden Tabelle werden die Elemente auf dem Bildschirm Anrufstatistik beschrieben.

**Tabelle 24: Anrufstatistikelemente**

Element	Beschreibung
Empfänger – Codec	Typ des empfangenen Sprachstreams (RTP-Audiostreaming vom Codec): <ul style="list-style-type: none"> <li>• G.729</li> <li>• G.722</li> <li>• G. 722 AMR WB</li> <li>• G.711 mu-law</li> <li>• G.711 A-law</li> <li>• iLBC</li> <li>• OPUS</li> </ul>
Sender – Codec	Typ des übertragenen Sprachstreams (RTP-Audiostreaming vom Codec): <ul style="list-style-type: none"> <li>• G.729</li> <li>• G.722</li> <li>• G. 722 AMR WB</li> <li>• G.711 mu-law</li> <li>• G.711 A-law</li> <li>• iLBC</li> <li>• OPUS</li> </ul>
Empfänger – Größe	Größe der Sprachpakete (in Millisekunden) im empfangenem Voicestream (RTP-Streaming-Audio).
Sender – Größe	Größe der Sprachpakete (in Millisekunden) im gesendeten Voicestream.

Element	Beschreibung
Empfänger – Pakete	Anzahl der RTP-Sprachpakete, die empfangen wurden, seit der Voicestream geöffnet wurde.  <b>Hinweis</b> Diese Anzahl ist nicht unbedingt mit der Anzahl der RTP-Sprachpakete identisch, die seit Beginn des Anrufs empfangen wurden, da der Anruf möglicherweise gehalten wurde.
Sender – Pakete	Anzahl der RTP-Sprachpakete, die gesendet wurden, seit der Voicestream geöffnet wurde.  <b>Hinweis</b> Diese Anzahl ist nicht unbedingt mit der Anzahl der RTP-Sprachpakete identisch, die seit Beginn des Anrufs gesendet wurden, da der Anruf möglicherweise gehalten wurde.
Avg Jitter (Durchschnittlicher Jitter)	Geschätzter, durchschnittlicher RTP-Paket-Jitter (dynamische Verzögerung eines Pakets bei der Übertragung im Netzwerk), in Millisekunden, der bemerkt wurde, seit der empfangene Voicestream geöffnet wurde.
Max Jitter (Maximaler Jitter)	Maximaler Jitter, in Millisekunden, der bemerkt wurde, seit der empfangene Voicestream geöffnet wurde.
Empfänger – Verworfen	Anzahl der RTP-Pakete im eingehenden Voicestream, die verworfen wurden (ungültige Pakete, zu spät usw.).  <b>Hinweis</b> Das Telefon verwirft Comfort Noise-Pakete des Nutzlasttyps 19, die von den Cisco Gateways generiert werden, da diese den Zähler erhöhen.
Rcvr Lost Packets (Empfänger – Verlorene Pakete)	Fehlende RTP-Pakete (während Übertragung verloren).
<b>Sprachqualitätsmetrik</b>	
Cumulative Conceal Ratio (Verdeckung – kumulierte Rate)	Gesamtanzahl der Verdeckungsrahmen dividiert durch die Gesamtanzahl der Sprachrahmen, die ab Beginn des Voicestreams empfangen wurden.
Verdeckung (Intervallrate)	Verhältnis der Verdeckungsrahmen zu den Sprachrahmen im vorherigen 3-Sekundenintervall aktiver Sprache. Wenn VAD (Voice Activity Detection) verwendet wird, ist möglicherweise ein längeres Intervall erforderlich, um drei Sekunden der aktiven Sprache zu sammeln.
Max Conceal Ratio (Verdeckung – Maximalrate)	Die höchste Intervallrate der Verdeckung seit Beginn des Audio-Streams.
Verdeckung Sekunden	Anzahl der Sekunden mit Verdeckungsereignissen (verlorene Rahmen) ab Beginn des Voicestreams (einschließlich schwerwiegende Verdeckung).

Element	Beschreibung
Severely Conceal Seconds (Verdeckung (schwerwiegend) Sekunden)	Anzahl der Sekunden mit mehr als fünf Prozent Verdeckungsereignissen (verlorene Rahmen) ab Beginn des Voicestreams.
Latenz	Geschätzte Netzwerklatenz in Millisekunden. Mittelwert der Round-Trip-Verzögerung, der gemessen wird, wenn RTCP-Empfängerberichtsblöcke empfangen werden.

## Webseite für Cisco IP-Telefon

Jedes Cisco IP-Telefon hat eine Webseite, auf der verschiedene Informationen über das Telefon angezeigt werden, einschließlich:

- Geräteinformationen: Zeigt die Geräteeinstellungen und zugehörige Informationen für das Telefon an.
- Netzwerkkonfiguration: Zeigt Informationen über die Netzwerkkonfiguration und andere Telefoneinstellungen an.
- Netzwerkstatistik: Zeigt Links zu Informationen über den Netzwerkverkehr an.
- Geräteprotokolle: Zeigt Links zu Informationen für die Problembehandlung an.
- Streaming-Statistik: Zeigt Links zu verschiedenen Streaming-Statistiken an.

Dieses Kapitel beschreibt die Informationen, die auf der Telefon-Webseite verfügbar sind. Sie können diese Informationen verwenden, um den Betrieb eines Telefons remote zu überwachen und bei der Fehlerbehebung zu helfen.

Sie können viele dieser Informationen auch direkt vom Telefon abrufen.

## Auf die Webseite des Telefons zugreifen



**Hinweis** Wenn Sie nicht auf die Webseite zugreifen können, ist diese möglicherweise standardmäßig deaktiviert.

### Prozedur

#### Schritt 1

Ermitteln Sie die IP-Adresse des Cisco IP-Telefon mit einer dieser Methoden:

- Suchen Sie das Telefon in der Cisco Unified Communications Manager-Verwaltung, indem Sie **Gerät > Telefon** auswählen. Für Telefone, die bei Cisco Unified Communications Manager registriert sind, wird die IP-Adresse im Fenster „Telefone suchen und auflisten“ sowie oben im Fenster „Telefonkonfiguration“ angezeigt.
- Drücken Sie auf dem Telefon **Einstellungen > Systeminformationen**, und blättern Sie zum IPv4-Adressfeld.

**Schritt 2**

Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein, wobei *IP-Adresse* für die jeweilige IP-Adresse des Cisco IP-Telefon steht:

**http://<IP\_address>**

## Webseite mit Geräteinformationen

Unter Geräteinformationen auf der Telefon-Webseite werden die Geräteeinstellungen und zugehörige Informationen für das Telefon angezeigt. Diese Elemente werden in der folgenden Tabelle beschrieben.

Um die Geräteinformationen anzuzeigen, öffnen Sie die Webseite für das Telefon und klicken Sie auf den Link **Geräteinformationen**.

**Tabelle 25: Felder der Webseite mit Geräteinformationen**

Feld	Beschreibung
Servicemodus	Der Servicemodus für das Telefon.
Servicedomäne	Die Domäne für den Service.
Servicestatus	Der aktuelle Status des Service.
MAC-Adresse	Die MAC-Adresse (Media Access Control) des Telefons.
Host-Name	Eindeutiger, unveränderlicher Name, der dem Telefon gemäß der MAC-Adresse automatisch zugewiesen wird.
Telefon-DN	Verzeichnisnummer, die dem Telefon zugewiesen ist.
Anwendungs-ID	Identifiziert die Anwendungsversion.
Boot-Software-ID	Gibt die Version der Boot-Software an.
Version	ID der Firmware, die auf dem Telefon ausgeführt wird.
Hardwarerevision	Nebenversionswert der Telefonhardware.
Seriennummer	Die Seriennummer des Telefons.
Modellnummer	Die Modellnummer des Telefons.
Wartende Nachricht vorhanden	Zeigt an, ob eine Voicemail auf der primären Leitung des Telefons wartet.

Feld	Beschreibung
UDI	Zeigt die folgenden Cisco UDI-Informationen (Unique Device Identifier) über das Telefon an: <ul style="list-style-type: none"> <li>• Hardwaretyp</li> <li>• Name des Telefonmodells</li> <li>• Produktbezeichner</li> <li>• Versions-ID (VID): Gibt die Hauptversionsnummer der Hardware an.</li> <li>• Seriennummer</li> </ul>
Zeit	Zeit für die Datum/Zeit-Gruppe, zu der das Telefon gehört. Diese Informationen kommen vom Cisco Unified Communications Manager.
Zeitzone	Zeitzone für die Datum/Zeit-Gruppe, zu der das Telefon gehört. Diese Informationen kommen vom Cisco Unified Communications Manager.
Datum	Datum für die Datum/Zeit-Gruppe, zu der das Telefon gehört. Diese Informationen kommen vom Cisco Unified Communications Manager.
System – Freier Speicherplatz	Menge des verfügbaren Systemspeichers.
Java-Heap – Freier Speicher	Der für den Java-Heap verfügbare Speicher.
Java-Pool – Freier Speicher	Der für den Java-Pool verfügbare Speicher.
FIPS-Modus aktiviert	Zeigt an, ob der FIPS-Modus (Federal Information Processing Standard) aktiviert ist.

## Webseite „Netzwerk-Setup“

Im entsprechenden Bereich auf einer Telefon-Webseite werden Informationen zur Netzwerkkonfiguration und zu anderen Telefoneinstellungen angezeigt. Diese Elemente werden in der folgenden Tabelle beschrieben.

Sie können viele dieser Elemente im Menü Netzwerkkonfiguration auf dem Cisco IP-Telefon anzeigen und festlegen.

Um die Netzwerkkonfiguration anzuzeigen, öffnen Sie die Webseite für das Telefon und klicken Sie auf den Link **Netzwerkkonfiguration**.

**Tabelle 26: Elemente der Netzwerkkonfiguration**

Element	Beschreibung
MAC-Adresse	Die MAC-Adresse (Media Access Control) des Telefons.
Host-Name	Der Host-Name, der dem Telefon durch den DHCP-Server zugewiesen wurde.

Element	Beschreibung
Domänenname	Name der DNS-Domäne (Domain Name System), in der sich das Telefon befindet.
DHCP-Server	Die IP-Adresse des DHCP-Servers (Dynamic Host Configuration Protocol), von dem das Telefon die IP-Adresse erhält.
BOOTP-Server	Gibt an, ob das Telefon die Konfiguration von einem BootP-Server (Bootstrap Protocol) verwendet.
DHCP	Gibt an, ob das Telefon DHCP verwendet.
IP-Adresse	Die IP-Adresse (Internet Protocol) des Telefons.
Subnetzmaske	Die vom Telefon verwendete Subnetzmaske.
Standardrouter 1	Der vom Telefon verwendete Standardrouter.
DNS-Server 1–3	Der primäre DNS-Server (DNS Server 1) und optionale DNS-Backupserver (DNS-Server 2 und 3), die das Telefon verwendet.
Alternativer TFTP-Server	Gibt an, ob das Telefon einen alternativen TFTP-Server verwendet.
TFTP-Server 1	Der vom Telefon verwendete primäre TFTP-Server (Trivial File Transfer Protocol).
TFTP Server 2	Der TFTP-Backupserver (Trivial File Transfer Protocol), den das Telefon verwendet.
DHCP-Adressfreigabe	Gibt die Einstellung der Option DHCP-Adressfreigabe an.
VLAN-ID (Betrieb)	Das VLAN (Virtual Local Area Network), das auf einem Cisco Catalyst-Switch konfiguriert ist, dem das Telefon ein Mitglied ist.
VLAN-ID (Verwaltung)	Zusätzliches VLAN, in dem das Telefon ein Mitglied ist.
Unified CM 1-5	<p>Hostnamen oder IP-Adressen der Cisco Unified Communications Manager-Server, mit denen das Telefon registrieren kann, in der Reihenfolge ihrer Priorität. Ein Element kann auch die IP-Adresse eines verfügbaren SRST-Routers anzeigen, der eingeschränkte Funktionen von Cisco Unified Communications Manager bereitstellt.</p> <p>Für einen verfügbaren Server zeigt ein Element die IP-Adresse des Cisco Unified Communications Manager-Servers und eine der folgenden Statusangaben an:</p> <ul style="list-style-type: none"> <li>• Aktiv: Der Cisco Unified Communications Manager-Server, der derzeit die Anrufverarbeitungsservices für das Telefon bereitstellt.</li> <li>• Standby: Der Cisco Unified Communications Manager-Server, zu dem das Telefon vorgeht, wenn der aktuelle Server nicht mehr verfügbar ist.</li> <li>• Leer: Keine aktuelle Verbindung mit diesem Cisco Unified Communications Manager-Server.</li> </ul> <p>Ein Eintrag kann auch die SRST-Bezeichnung (Survivable Remote Site Telephony) enthalten, die den SRST-Router angibt, der Cisco Unified Communications Manager-Funktionen in eingeschränktem Umfang bereitstellt. Dieser Router übernimmt die Steuerung der Anrufverarbeitung, wenn alle Cisco Unified Communications Manager-Server nicht mehr erreichbar sind. Der SRST-Router in der Cisco Unified Communications Manager-Serverliste wird immer zuletzt angezeigt, auch wenn er nicht aktiv ist. Sie können die SRST-Routeradresse unter Gerätepool im Cisco Unified Communications Manager-Konfigurationsfenster konfigurieren.</p>
Informations-URL	Die URL des Hilfetextes, der auf dem Telefon angezeigt wird.

Element	Beschreibung
Verzeichnis-URL	URL des Servers, von dem das Telefon Verzeichnisinformationen abrufen.
Nachrichten-URL	URL des Servers, von dem das Telefon Nachrichtenservices erhält.
Service-URL	URL des Servers, von dem das Telefon Cisco IP-Telefon-Services erhält.
Leerlauf-URL	URL, die das Telefon anzeigt, wenn es für die im Feld URL-Leerlaufzeit angegebene Zeitdauer inaktiv ist und kein Menü geöffnet ist.
URL-Leerlaufzeit	Anzahl der Sekunden, die das Telefon inaktiv und kein Menü geöffnet ist, bevor der XML-Service in der URL angegeben ist, aktiviert wird.
Proxy-Server-URL	URL des Proxy-Servers, der HTTP-Anforderungen für HTTP-Telefonclients an nicht lokale Hosts sendet und Antworten vom nicht lokalen Host an den HTTP-Telefonclient weitergibt.
Authentifizierungs-URL	Die URL, die das Telefon verwendet, um Anforderungen an den Telefonwebserver zu überprüfen.
SW-Portkonfiguration	Geschwindigkeit und Duplex-Status des Switch-Ports: <ul style="list-style-type: none"> <li>• A = Automatisch aushandeln</li> <li>• 10H = 10-BaseT/Halbduplex</li> <li>• 10F = 10-BaseT/Vollduplex</li> <li>• 100H = 100-BaseT/Halbduplex</li> <li>• 100F = 100-BaseT/Vollduplex</li> <li>• 1000F = 1000-BaseT/Vollduplex</li> <li>• Kein Link= Keine Verbindung zum Switch-Port</li> </ul>
Benutzergebietsschema	Das dem Telefonbenutzer zugeordnete Gebietsschema. Detaillierte Informationen, um den Benutzer zu unterstützen, einschließlich Sprache, Schriftart, Datum- und Uhrzeitformat sowie Textinformatoren zur alphanumerischen Tastatur.
Netzwerkgebietsschema	Das dem Telefonbenutzer zugeordnete Netzwerkgebietsschema. Detaillierte Informationen, um das Telefon an einem bestimmten Standort zu unterstützen, einschließlich Definitionen der vom Standort verwendeten Töne und Kadenzen.
Version des Benutzergebietsschemas	Version des Benutzergebietsschemas, das auf dem Telefon geladen ist.
Version des Netzwerkgebietsschemas	Version des Netzwerkgebietsschemas, das auf dem Telefon geladen ist.
Lautsprecher aktiviert	Gibt an, ob der Lautsprecher des Telefons aktiviert ist.
Mithören	Gibt an, ob die Funktion zum Mithören auf dem Telefon aktiviert ist. Mithören ermöglicht es dem Benutzer, über den Hörer sprechen und den Ton über den Lautsprecher ausgeben.
GARP aktiviert	Gibt an, ob das Telefon MAC-Adressen von Gratuitous ARP-Antworten lernt.
Automatische Leitungsauswahl aktiviert	Gibt an, ob das Telefon den Anruf-Fokus auf die eingehenden Anrufe aller Leitungen wechselt.
DSCP für Anrufsteuerung	DSCP IP-Klassifizierung für Anrufsteuerungssignale.



Element	Beschreibung
DSCP für Konfiguration	DSCP IP-Klassifizierung zur Weitergabe von Telefonkonfigurationen.
DSCP für Services	DSCP IP-Klassifizierung für telefonbasierte Services.
Sicherheitsmodus	Der für das Telefon festgelegte Sicherheitsmodus.
Webzugriff aktiviert	Gibt an, ob der Webzugriff für das Telefon aktiviert (Ja) oder deaktiviert (Nein) ist.
SSH-Zugriff aktiviert	Gibt an, ob das Telefon die SSH-Verbindungen akzeptiert oder blockiert.
CDP: SW-Port	<p>Gibt an, ob die CDP-Unterstützung auf dem Switch-Port verfügbar ist (standardmäßig aktiviert).</p> <p>Aktivieren Sie CDP auf dem Switch-Port für die VLAN-Zuweisung für das Telefon, Stromverbrauch, QoS-Verwaltung und 802.1x-Sicherheit.</p> <p>Aktivieren Sie CDP, wenn das Telefon mit einem Cisco Switch verbunden ist.</p> <p>Wenn CDP in Cisco Unified Communications Manager deaktiviert ist, wird eine Warnung angezeigt, dass CDP auf dem Switch-Port nur deaktiviert werden sollte, wenn das Telefon mit einem Cisco Switch verbunden ist.</p> <p>Die aktuellen CDP-Werte für den PC- und Switch-Port werden im Menü „Einstellungen“ angezeigt.</p>
LLDP-MED: SW-Port	Gibt an, ob LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) auf dem Switch-Port aktiviert ist.
LLDP-Leistungspriorität	<p>Kündigt die Energiepriorität des Telefons auf dem Switch an, damit der Switch die entsprechende Leistung für die Telefone bereitstellen kann. Die Einstellungen umfassen folgende Optionen:</p> <ul style="list-style-type: none"> <li>• Unbekannt: Dies ist der Standardwert.</li> <li>• Niedrig</li> <li>• Hoch</li> <li>• Kritisch</li> </ul>
LLDP Asset-ID	Identifiziert die Asset-ID, die dem Telefon für die Bestandsverwaltung zugewiesen wird.
CTL-Datei	Identifiziert die CTL-Datei.
ITL-Datei	Die ITL-Datei enthält die Initial Trust List.
ITL-Signatur	Verbessert die Sicherheit mit einem sicheren Hash-Algorithmus (SHA-1) in der CTL-Datei.
CAPF-Server	Der Name des CAPF-Servers, der vom Telefon verwendet wird.
TVS	Die Hauptkomponente von Security by Default. Mit TVS (Trust Verification Services) können Unified IP-Telefone Anwendungsserver, beispielsweise EM-Services, Verzeichnis und Mailbox, bei der Herstellung einer HTTPS-Verbindung authentifizieren.
TFTP-Server	Der Name des TFTP-Servers, der vom Telefon verwendet wird.
Automatische Portsynchronisierung	Synchronisiert die Ports in einer langsameren Geschwindigkeit, um Paketverlust zu verhindern.

Element	Beschreibung
Remotekonfiguration für Switchport	Ermöglicht dem Administrator, die Geschwindigkeit und Funktionalität des Cisco Desktop Collaboration Experience-Ports unter Verwendung der Cisco Unified Communications Manager-Verwaltung konfigurieren.
Remotekonfiguration für PC-Port	Gibt an, ob die Remotekonfiguration der Geschwindigkeit und des Duplexmodus für den PC aktiviert oder deaktiviert ist.
IP-Adressierungsmodus	Zeigt den IP-Adressierungsmodus an, der auf dem Telefon verfügbar ist.
Bevorzugter IP-Modus	Gibt die IP-Adressenversion an, die das Telefon bei der Signalisierung mit Cisco Unified Communications Manager verwendet, wenn sowohl IPv4 als auch IPv6 auf dem Telefon verfügbar sind.
Bevorzugter IP-Modus für Medien	Gibt an, dass für das Gerät für das Medium eine IPv4-Adresse verwendet, um die Verbindung mit Cisco Unified Communications Manager herzustellen.
Automatisch IPv6-Konfiguration	Zeigt an, ob die automatisch Konfiguration auf dem Telefon aktiviert oder deaktiviert ist.
IPv6 – DAD (Erkennung doppelter Adressen)	Überprüft die Eindeutigkeit neuer IPv6-Unicastadressen, bevor die Adressen den Schnittstellen zugewiesen werden.
IPv6 – Nachrichtenumleitung akzeptieren	Gibt an, ob das Telefon umgeleitete Nachrichten vom Router akzeptiert, der für die Zielnummer verwendet wird.
IPv6 – Antwort auf Multicast-Echo-Anforderung	Gibt an, ob das Telefon eine Echo-Antwort auf eine Echo-Anforderung an eine IPv6-Adresse sendet.
IPv6 – Lastserver	Wird verwendet, um die Installationsdauer für Updates der Telefon-Firmware zu optimieren und den WAN zu entlasten, indem Bilder lokal gespeichert werden, sodass es nicht erforderlich ist, bei jedem Telefon-Upgrade den WAN-Link zu verwenden.
IPv6 – Protokollserver	Gibt die IP-Adresse und den Port des Remotecomputers für die Protokollierung an, an den das Telefon die Protokollnachrichten sendet.
IPv6 - CAPF-Server	Allgemeiner Name (im Cisco Unified Communications Manager-Zertifikat) des CAPF-Servers, der vom Telefon verwendet wird.
DHCPv6	DHCP (Dynamic Host Configuration Protocol) weist einem Gerät automatisch eine IPv6-Adresse zu, wenn es mit dem Netzwerk verbunden wird. Cisco Unified IP-Telefone aktivieren DHCP standardmäßig.
IPv6-Adresse	Zeigt die aktuelle IPv6-Adresse des Telefons an oder ermöglicht dem Benutzer, eine neue IPv6-Adresse einzugeben.
Länge des IPv6-Präfixes	Zeigt die aktuelle Länge des Präfixes für das Subnetz an oder ermöglicht dem Benutzer, eine neue Länge einzugeben.
IPv6 - Standardrouter 1	Zeigt den Standardrouter an, der vom Telefon verwendet wird, oder ermöglicht dem Benutzer, einen neuen IPv6-Standardrouter einzugeben.
IPv6 – DNS-Server 1	Zeigt den primären DNSv6-Server an, der vom Telefon verwendet wird, oder ermöglicht dem Benutzer, einen neuen Server festzulegen.

Element	Beschreibung
IPv6 – DNS-Server 2	Zeigt den sekundären DNSv6-Server an, der vom Telefon verwendet wird, oder ermöglicht dem Benutzer, einen neuen Server festzulegen.
IPv6 – Alternativer TFTP-Server	Ermöglicht dem Benutzer einen alternativen (sekundären) IPv6 TFTP-Server zu verwenden.
IPv6 – TFTP-Server 1	Zeigt den primären IPv6 TFTP-Server an, der vom Telefon verwendet wird, oder ermöglicht dem Benutzer, einen neuen Server festzulegen.
IPv6 – TFTP-Server 2	Zeigt den sekundären IPv6 TFTP-Server an, der vom Telefon verwendet wird, wenn der primäre nicht verfügbar ist, oder ermöglicht dem Benutzer, einen neuen Server festzulegen.
IPv6-Adresse freigegeben	Ermöglicht dem Benutzer IPv6-bezogene Informationen freizugeben.
Energywise-Energiepegel	Eine Messung der von den Geräten in einem EnergyWise-Netzwerk verbrauchten Energie.
EnergyWise-Domäne	Eine administrative Gerätegruppe für die Energieüberwachung und Steuerung.

## Webseite mit Ethernet-Informationen

In der folgenden Tabelle wird der Inhalt der Webseite mit den Ethernet-Informationen beschrieben.

**Tabelle 27: Ethernet-Informationselemente**

Element	Beschreibung
Übertr. – Frames	Gesamtanzahl der Pakete, die das Telefon gesendet hat.
Tx Broadcast	Gesamtanzahl der Broadcast-Pakete, die das Telefon gesendet hat.
Tx multicast	Gesamtanzahl der Multicast-Pakete, die das Telefon gesendet hat.
Tx Unicast	Gesamtanzahl der Unicast-Pakete, die das Telefon gesendet hat.
Rx Frames	Gesamtanzahl der Pakete, die das Telefon empfangen hat.
Rx Broadcast	Gesamtanzahl der Broadcast-Pakete, die das Telefon empfangen hat.
Rx multicast	Gesamtanzahl der Multicast-Pakete, die das Telefon empfangen hat.
Rx Unicast	Gesamtanzahl der Unicast-Pakete, die das Telefon empfangen hat.
Rx PacketNoDes	Gesamtanzahl der Shed-Pakete, die vom DMA-Deskriptor (Direct Memory Access) verursacht werden.

## Netzwerk-Webseiten

In der folgenden Tabelle werden die Informationen auf den Netzwerkbereich-Webseiten erläutert.



**Hinweis** Wenn Sie unter „Netzwerkstatistik“ auf den Link **Netzwerk** klicken, wird eine Seite mit dem Titel „Port-Informationen“ angezeigt.

**Tabelle 28: Elemente des Netzwerkbereichs**

Element	Beschreibung
Rx totalPkt	Gesamtanzahl der Pakete, die das Telefon empfangen hat.
Rx multicast	Gesamtanzahl der Multicast-Pakete, die das Telefon empfangen hat.
Rx Broadcast	Gesamtanzahl der Broadcast-Pakete, die das Telefon empfangen hat.
Rx Unicast	Gesamtanzahl der Unicast-Pakete, die das Telefon empfangen hat.
Rx tokenDrop	Gesamtanzahl der Pakete, die aufgrund unzureichender Ressourcen verworfen wurden (beispielsweise FIFO-Überlauf).
Tx totalGoodPkt	Gesamtanzahl der gültigen Pakete (Multicast, Broadcast und Unicast), die das Telefon empfangen hat.
Tx Broadcast	Gesamtanzahl der Broad-Pakete, die das Telefon gesendet hat.
Tx multicast	Gesamtanzahl der Multicast-Pakete, die das Telefon gesendet hat.
LLDP FramesOutTotal	Gesamtanzahl der LLDP-Rahmen, die das Telefon gesendet hat.
LLDP AgeoutsTotal	Gesamtanzahl der LLDP-Rahmen, die die Zeit um Cache überschritten haben.
LLDP FramesDiscardedTotal	Gesamtanzahl der LLDP-Rahmen, die verworfen wurden, da die erforderlichen TLVs fehlen, unzulässig sind oder zu lange Zeichenfolgen enthalten.
LLDP FramesInErrorsTotal	Gesamtanzahl der LLDP-Rahmen, die mit mindestens einem erkennbaren Fehler empfangen wurden.
LLDP FramesInTotal	Gesamtanzahl der LLDP-Rahmen, die das Telefon empfangen hat.
LLDP TLVDiscardedTotal	Gesamtanzahl der LLDP TLVs, die verworfen werden.
LLDP TLVUnrecognizedTotal	Gesamtanzahl der LLDP TLVs, die auf dem Telefon nicht erkannt werden.
CDP Nachbargeräte-ID	ID eines Geräts, das mit diesem Port verbunden ist, der von CDP erkannt wurde.
CDP Nachbar-IP-Adresse	IP-Adresse des Nachbargeräts, das von CDP erkannt wurde.
CDP Nachbar-IPv6-Adresse	IPv6-Adresse des Nachbargeräts, das von CDP erkannt wurde.
CDP Nachbar-Port	Nachbargeräteport, mit dem das Telefon verbunden ist, der von CDP erkannt wurde.

Element	Beschreibung
LLDP Nachbargeräte-ID	ID eines mit diesem Port verbundenen Geräts, das von LLDP erkannt wurde.
LLDP Nachbar-IP-Adresse	IP-Adresse des Nachbargeräts, das von LLDP erkannt wurde.
LLDP Nachbar-IPv6-Adresse	IPv6-Adresse des Nachbargeräts, das von CDP erkannt wurde.
LLDP Nachbar-Port	Nachbargeräteport, mit dem das Telefon verbunden ist, der von LLDP erkannt wurde.
Port-Informationen	Geschwindigkeits- und Duplex-Informationen.

## Webseiten für Konsolenprotokolle, Speicherauszüge, Statusmeldungen und Fehlersuchanzeige

Über die Hyperlinks „Konsolenprotokolle“, „Speicherauszüge“, „Statusmeldungen“ und „Fehlersuchanzeige“ unter der Überschrift „Geräteprotokolle“ können Sie auf Informationen zugreifen, die Sie beim Überwachen des Telefons und bei der Fehlerbehebung unterstützen.

- **Konsolenprotokolle:** Hier finden sich Hyperlinks zu den einzelnen Protokolldateien. Konsolenprotokolldateien enthalten Debug- und Fehlermeldungen, die das Telefon empfangen hat.
- **Speicherauszüge:** Hier finden sich Hyperlinks zu einzelnen Dumpdateien. Die Speicherauszugdateien enthalten Daten von einem Telefonabsturz.
- **Statusmeldungen:** Zeigt die 10 letzten Statusmeldungen an, die das Telefon seit dem letzten Start generiert hat. Sie können diese Informationen auch dem Fenster „Statusmeldungen“ auf dem Telefon entnehmen.
- **Fehlersuchanzeige:** Hier werden Debug-Meldungen angezeigt, die für Cisco TAC hilfreich sein können, wenn Sie Unterstützung bei der Fehlerbehebung anfordern.

## Webseite „Streaming-Statistik“

Ein Cisco IP-Telefon kann Informationen gleichzeitig zu oder von drei Geräten streamen. Ein Telefon streamt Informationen, wenn ein Anruf aktiv ist oder ein Service ausgeführt wird, der Audio oder Daten sendet bzw. empfängt.

Die Streaming-Statistikbereiche auf einer Telefon-Webseite enthalten Informationen über die Streams.

Um die Streaming-Statistik anzuzeigen, öffnen Sie die Webseite für das Telefon und klicken Sie auf den Hyperlink **Stream**.

In der folgenden Tabelle werden die Elemente im Bereich Streaming-Statistik beschrieben.

**Tabelle 29: Streaming-Statistikfelder**

Element	Beschreibung
Remoteadresse	IP-Adresse und UDP-Port des Ziel des Streams.
Lokale Adresse	IP-Adresse und UPD-Port des Telefons.

Element	Beschreibung
Startzeit	Der interne Zeitstempel zeigt an, wann Cisco Unified Communications Manager angefordert hat, dass das Telefon die Paketübermittlung startet.
Stream-Status	Zeigt an, ob der Stream aktiv ist.
Host-Name	Eindeutiger, unveränderlicher Name, der dem Telefon gemäß der MAC-Adresse automatisch zugewiesen wird.
Sender – Pakete	Gesamtanzahl der RTP-Datenpakete, die das Telefon gesendet hat, seit die Verbindung hergestellt wurde. Der Wert ist 0, wenn die Verbindung auf den Empfangsmodus festgelegt ist.
Sender - Oktette	Gesamtanzahl der Nutzlast-Oktette, die das Telefon in RTP-Datenpaketen gesendet hat, seit die Verbindung hergestellt wurde. Der Wert ist 0, wenn die Verbindung auf den Empfangsmodus festgelegt ist.
Sender – Codec	Typ der Audiocodierung für den gesendeten Stream.
Sender – Gesendete Berichte (siehe Hinweis)	Wie oft der RTCP-Senderbericht gesendet wurde.
Sender – Sendezeit Bericht (siehe Hinweis)	Interner Zeitstempel, der angibt, wann der letzte RTCP-Senderbericht gesendet wurde.
Rcvr Lost Packets (Empfänger – Verlorene Pakete)	Gesamtanzahl der RTP-Datenpakete, die verloren wurden, seit der Datenempfang auf der Verbindung gestartet wurde. Wird als die Anzahl der erwarteten Pakete abzüglich der Anzahl der tatsächlich empfangenen Pakete definiert, wobei die Anzahl der empfangenen Pakete verzögerten und doppelten Pakete umfasst. Der Wert ist 0, wenn die Verbindung auf den Sendemodus festgelegt ist.
Avg Jitter (Durchschnittlicher Jitter)	Schätzung der mittleren Abweichung der Zwischenankunftszeit der RTP-Datenpakete in Millisekunden. Der Wert ist 0, wenn die Verbindung auf den Sendemodus festgelegt ist.
Empfänger – Codec	Typ der für den Streaming-Empfang verwendeten Audiocodierung.
Empfänger – Gesendete Berichte (siehe Hinweis)	Wie oft die RTCP-Empfängerberichte gesendet wurden.
Empfänger – Sendezeit Bericht (siehe Hinweis)	Interner Zeitstempel, der angibt, wann der RTCP-Empfängerbericht gesendet wurde.
Empfänger – Pakete	Gesamtanzahl der RTP-Datenpakete, die das Telefon empfangen hat, seit die Verbindung hergestellt wurde. Umfasst Pakete, die von verschiedenen Quellen empfangen wurden, wenn der Anruf ein Multicast-Anruf ist. Der Wert ist 0, wenn die Verbindung auf den Sendemodus festgelegt ist.
Empfänger – Oktette	Gesamtanzahl der Nutzlast-Oktette, die das Telefon in RTP-Datenpaketen empfangen hat, seit die Verbindung hergestellt wurde. Umfasst Pakete, die von verschiedenen Quellen empfangen wurden, wenn der Anruf ein Multicast-Anruf ist. Der Wert ist 0, wenn die Verbindung auf den Sendemodus festgelegt ist.

Element	Beschreibung
Cumulative Conceal Ratio (Verdeckung – kumulierte Rate)	Gesamtanzahl der Verdeckungsrahmen dividiert durch die Gesamtanzahl der Sprachrahmen, die ab Beginn des Voicestreams empfangen wurden.
Verdeckung (Intervallrate)	Verhältnis der Verdeckungsrahmen zu den Sprachrahmen im vorherigen 3-Sekunden-Intervall aktiver Sprache. Wenn VAD (Voice Activity Detection) verwendet wird, ist möglicherweise ein längeres Intervall erforderlich, um drei Sekunden der aktiven Sprache zu sammeln.
Max Conceal Ratio (Verdeckung – Maximalrate)	Höchstes Intervall der Verdeckungsrate ab Beginn des Voicestreams.
Verdeckung Sekunden	Anzahl der Sekunden mit Verdeckungsereignissen (verlorene Rahmen) ab Beginn des Voicestreams (einschließlich schwerwiegende Verdeckung).
Severely Conceal Seconds (Verdeckung (schwerwiegend) Sekunden)	Anzahl der Sekunden mit mehr als fünf Prozent Verdeckungsereignissen (verlorene Rahmen) ab Beginn des Voicestreams.
Latenz (siehe Hinweis)	Geschätzte Netzwerklatenz in Millisekunden. Mittelwert der Round-Trip-Verzögerung gemessen wird, wenn RTCP-Empfängerberichtsblöcke empfangen werden.
Max Jitter (Maximaler Jitter)	Maximaler Wert des unmittelbaren Jitters in Millisekunden.
Sender – Größe	RTP-Paketgröße in Millisekunden für den übermittelten Stream.
Sender - Empfangene Berichte (siehe Hinweis)	Wie oft die RTCP-Senderberichte empfangen wurden.
Sender - Empfangszeit Bericht (siehe Hinweis)	Letzter Zeitpunkt, zu dem ein RTCP-Senderbericht empfangen wurde.
Empfänger – Größe	RTP-Paketgröße in Millisekunden für den empfangenen Stream.
Empfänger – Verworfen	RTP-Pakete, die vom Netzwerk empfangen, aber von den Jitter-Puffern verworfen wurden.
Empfänger - Empfangene Berichte (siehe Hinweis)	Wie oft die RTCP-Empfängerberichte empfangen wurden.
Empfänger - Empfangszeit Bericht (siehe Hinweis)	Zeitpunkt, an dem zuletzt ein RTCP-Empfängerbericht empfangen wurde.



**Hinweis** Wenn das RTP-Steuerungsprotokoll deaktiviert ist, werden für dieses Feld keine Daten erzeugt. In diesem Fall wird der Wert 0 angezeigt.

# Informationen im XML-Format vom Telefon anfordern

Für die Fehlerbehebung können Sie Informationen vom Telefon anfordern. Die Informationen werden im XML-Format ausgegeben. Folgende Informationen stehen zur Verfügung:

- CallInfo: Informationen zu Anrufsitzungen für eine bestimmte Leitung.
- LineInfo: Informationen zur Leitungskonfiguration für das Telefon.
- ModeInfo: Informationen zum Telefonmodus.

## Vorbereitungen

Zum Abrufen der Informationen muss der Webzugriff aktiviert sein.

Das Telefon muss einem Benutzer zugeordnet sein.

## Prozedur

---

**Schritt 1** Geben Sie für Anrufinformationen die folgende URL in einen Browser ein: **http://<phone ip address>/CGI/Java/CallInfo<x>**

Dabei ist

- *<phone ip address>* ist die IP-Adresse des Telefons
- *<x>* ist die Nummer der Leitung, zu der Sie Informationen abrufen möchten.

Der Befehl gibt ein XML-Dokument zurück.

**Schritt 2** Geben Sie für Leitungsinformationen die folgende URL in einen Browser ein: **http://<phone ip address>/CGI/Java/CallInfo**

Dabei ist

- *<phone ip address>* ist die IP-Adresse des Telefons

Der Befehl gibt ein XML-Dokument zurück.

**Schritt 3** Geben Sie für Modellinformationen die folgende URL in einen Browser ein: **http://<phone ip address>/CGI/Java/ModeInfo**

Dabei ist

- *<phone ip address>* ist die IP-Adresse des Telefons

Der Befehl gibt ein XML-Dokument zurück.

---

## Beispielausgabe für „CallInfo“

Der folgende XML-Code ist ein Beispiel für die Ausgabe des Befehls „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>
```

## Beispielausgabe für „LineInfo“

Der folgende XML-Code ist ein Beispiel für die Ausgabe des Befehls „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>

```

## Beispielausgabe für „ModeInfo“

Der folgende XML-Code ist ein Beispiel für die Ausgabe des Befehls „ModeInfo“.

```

<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
  <PlaneTitle>Applications</PlaneTitle>
  <PlaneFieldCount>12</PlaneFieldCount>
  <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
  <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
  <Prompt></Prompt>
  <Notify></Notify>
  <Status></Status>
  <CiscoIPPhoneFields>
    <FieldType>0</FieldType>
    <FieldAttr></FieldAttr>
    <fieldHelpIndex>0</fieldHelpIndex>
    <FieldName>Call History</FieldName>
    <FieldValue></FieldValue>
  </CiscoIPPhoneFields>
  <CiscoIPPhoneFields>
    <FieldType>0</FieldType>
    <FieldAttr></FieldAttr>
    <fieldHelpIndex>0</fieldHelpIndex>
    <FieldName>Preferences</FieldName>
    <FieldValue></FieldValue>
  </CiscoIPPhoneFields>
  ...
</CiscoIPPhoneModeInfo>

```



# KAPITEL 12

## Telefonfehlerbehebung

- [Allgemeine Informationen zur Problembehandlung, auf Seite 161](#)
- [Startprobleme, auf Seite 162](#)
- [Probleme mit dem Zurücksetzen des Telefons, auf Seite 167](#)
- [Das Telefon kann sich nicht mit dem LAN verbinden, auf Seite 169](#)
- [Sicherheitsprobleme auf Cisco IP-Telefon, auf Seite 169](#)
- [Audioprobleme, auf Seite 171](#)
- [Allgemeine Anrufprobleme, auf Seite 172](#)
- [Fehlerbehebungsverfahren, auf Seite 173](#)
- [Debuginformationen von Cisco Unified Communications Manager, auf Seite 177](#)
- [Zusätzliche Informationen zur Problembehandlung, auf Seite 178](#)

## Allgemeine Informationen zur Problembehandlung

Die folgende Tabelle enthält allgemeine Informationen zur Problembehandlung für Cisco IP-Telefon.

**Tabelle 30: Problembehandlung für Cisco IP-Telefone**

Zusammenfassung	Erklärung
Länger dauernde Broadcast-Stürme verursachen, dass IP-Telefone zurückgesetzt werden und Anrufe nicht möglich sind.	Ein länger dauernder Broadcast-Sturm der Ebene 2 (mehrere Minuten) Sprach-VLAN kann verursachen, dass IP-Telefone zurückgesetzt werden. Ein Anruf getrennt wird und kein Anruf getätigt oder angenommen werden. IP-Telefone können nicht verwendet werden, bis ein Broadcast-Sturm beendet ist.
Eine Netzwerkverbindung vom Telefon auf eine Arbeitsstation verlegen	Wenn Sie Ihr Telefon über eine Netzwerkverbindung betreiben und das Netzwerk ausstecken möchten, um es in einen Desktopcomputer einzustecken, müssen Sie vorsichtig vorgehen.  <b>Vorsicht</b> Die Netzwerkkarte im Computer kann keine Energie über eine Netzwerkverbindung empfangen. Wenn Energie über die Netzwerkverbindung übertragen wird, kann die Netzwerkkarte zerstört werden. Um die Netzwerkkarte zu schützen, warten Sie 10 Sekunden oder länger, nachdem Sie das Netzwerk-Kabel aus dem Telefon ausgesteckt haben, bevor Sie das Kabel in den Desktop-Computer stecken. Diese Verzögerung gibt dem Switch genügend Zeit, um zu erkennen, dass kein Telefon auf der Leitung vorhanden ist, und die Energieübertragung zu beenden.

Zusammenfassung	Erklärung
Die Telefonkonfiguration ändern	<p>Die Einstellungen für das Administratorkennwort sind standardmäßig gesperrt, um zu verhindern, dass die Benutzer Änderungen vornehmen, die die Netzwerkverfügbarkeit beeinträchtigen können. Sie müssen die Einstellungen für das Administratorkennwort entsperren, bevor Sie sie konfigurieren können.</p> <p>Weitere Informationen finden Sie unter <a href="#">Anwenden eines Telefonkennworts</a>, Seite 41.</p> <p><b>Hinweis</b> Wenn im allgemeinen Telefonprofil kein Administratorkennwort festgelegt ist, dann können die Benutzer die Netzwerkeinstellungen ändern.</p>
Codec-Konflikt zwischen dem Telefon und einem anderen Gerät	<p>Die RxType- und TxType-Statistiken zeigen den Codec an, der für die Konversation zwischen diesem Cisco IP-Telefon und anderen Geräten verwendet wird. Die Werte dieser Statistiken sollten übereinstimmen. Wenn die Werte nicht übereinstimmen, überprüfen Sie, ob das andere Gerät die Codec-Konversation verarbeiten kann. Wenn kein Transcoder vorhanden ist, um den Service abzuwickeln. Weitere Informationen hierzu finden Sie unter <a href="#">Das Fenster „Anrufstatistik“ anzeigen, auf Seite 14</a>.</p>
Sound-Sample-Konflikt zwischen dem Telefon und einem anderen Gerät	<p>Die RxType- und TxType-Statistiken zeigen die Größe der Sprachpakete an, die während einer Konversation zwischen diesem Cisco IP-Telefon und anderen Geräten verwendet werden. Die Werte dieser Statistiken sollten übereinstimmen. Weitere Informationen hierzu finden Sie unter <a href="#">Das Fenster „Anrufstatistik“ anzeigen, auf Seite 14</a>.</p>
Loopback	<p>Ein Loopback kann unter folgenden Bedingungen auftreten:</p> <ul style="list-style-type: none"> <li>• Die Option SW-Portkonfiguration auf dem Telefon ist auf 10 Halbduplex (10-BaseT/Halbduplex) festgelegt</li> <li>• Das Telefon wird über eine externe Stromversorgung betrieben.</li> <li>• Das Telefon ist ausgeschaltet (die Stromversorgung ist getrennt).</li> </ul> <p>In diesem Fall kann der Switch-Port auf dem Telefon deaktiviert werden und folgende Meldung wird im Switch-Konsolenprotokoll angezeigt:</p> <pre>HALF_DUX_COLLISION_EXCEED_THRESHOLD</pre> <p>Um das Problem zu beheben, aktivieren Sie den Port erneut.</p>

## Startprobleme

Nachdem Sie ein Telefon im Netzwerk installiert und zu Cisco Unified Communications Manager hinzugefügt haben, sollte das Telefon, wie im entsprechenden Abschnitt beschrieben, gestartet werden.

Wenn das Telefon nicht richtig gestartet wird, lesen Sie die Informationen zur Fehlerbehebung in den folgenden Abschnitten.

### Verwandte Themen

[Telefonstart überprüfen](#), auf Seite 54

# Cisco IP-Telefon wird nicht normal gestartet

## Problem

Wenn Sie ein Cisco IP-Telefon in den Netzwerkport einstecken, durchläuft das Telefon den im entsprechenden Thema beschriebenen Startprozess nicht und auf dem Telefonbildschirm werden keine Informationen angezeigt.

## Ursache

Die Ursache dafür, dass das Telefon den Startprozess nicht durchläuft, können defekte Kabel, schlechte Verbindungen, Netzwerkausfälle oder Funktionsstörungen des Telefons sein.

## Lösung

Um festzustellen, ob das Telefon funktioniert, führen Sie die folgenden Aktionen aus, um andere potenzielle Probleme auszuschließen.

- Stellen Sie sicher, dass der Netzwerkport funktionsfähig ist:
  - Ersetzen Sie die Ethernet-Kabel durch Kabel, die nachweislich funktionieren.
  - Stecken Sie ein funktionierendes Cisco IP-Telefon von einem anderen Port aus und stecken Sie es in den Netzwerkport, um zu überprüfen, ob der Port aktiv ist.
  - Stecken Sie das Cisco IP-Telefon, das nicht gestartet wird, in einen anderen Netzwerkport ein, der nachweislich funktioniert.
  - Stecken Sie das Cisco IP-Telefon, das nicht gestartet wird, in den Port auf dem Switch, um die Patchpanel-Verbindung auszuschließen.
- Stellen Sie sicher, dass das Telefon mit Strom versorgt wird:
  - Wenn Sie eine externe Stromquelle verwenden, überprüfen Sie, ob die Steckdose funktioniert.
  - Für Inline-Strom verwenden Sie die externe Stromversorgung.
  - Wenn Sie die externe Stromversorgung verwenden, wechseln Sie zu einer Einheit, die funktioniert.
- Wenn das Telefon immer noch nicht richtig gestartet wird, schalten Sie das Telefon über das Sicherungs-Software-Image ein.
- Wenn das Telefon immer noch nicht richtig gestartet wird, setzen Sie es auf die Werkseinstellungen zurück.
- Wenn auf dem Display des Cisco IP-Telefon nach mindestens fünf Minuten keine Zeichen angezeigt werden, wenden Sie sich an den technischen Support von Cisco.

## Verwandte Themen

[Telefonstart überprüfen](#), auf Seite 54

## Cisco IP-Telefon wird nicht mit Cisco Unified Communications Manager registriert

Wenn das Telefon die erste Phase des Startprozesses abgeschlossen hat (die LEDs blinken), aber die Meldungen auf dem Telefonbildschirm durchläuft, wird das Telefon nicht ordnungsgemäß gestartet. Das Telefon startet erst dann erfolgreich, nachdem es sich mit dem Ethernet-Netzwerk verbunden und bei einem Cisco Unified Communications Manager-Server registriert hat.

Außerdem können Sicherheitsprobleme verhindern, dass das Telefon ordnungsgemäß gestartet wird. Weitere Informationen finden Sie unter [Fehlerbehebungsverfahren, auf Seite 173](#).

## Fehlermeldungen auf dem Telefon

### Problem

Beim Starten des Telefons werden in Statusmeldungen Fehler gemeldet.

### Lösung

Während das Telefon gestartet wird, können Sie auf Statusmeldungen zugreifen, die Informationen zur Ursache eines Problems anzeigen. Im Abschnitt „Fenster ‚Statusmeldungen‘ anzeigen“ finden Sie Anweisungen für den Zugriff auf Statusmeldungen sowie eine Liste der potenziellen Fehler zusammen mit Erklärungen und Lösungen.

### Verwandte Themen

[Das Fenster „Statusmeldungen“ anzeigen](#), auf Seite 136

## Das Telefon kann keine Verbindung mit dem TFTP-Server oder Cisco Unified Communications Manager herstellen

### Problem

Wenn das Netzwerk zwischen dem Telefon und dem TFTP-Server oder Cisco Unified Communications Manager ausgefallen ist, kann das Telefon nicht richtig starten.

### Lösung

Stellen Sie sicher, dass das Netzwerk aktiv ist.

## Telefon kann keine Verbindung mit dem TFTP-Server herstellen

### Problem

Möglicherweise sind die TFTP-Servereinstellungen falsch.

### Lösung

Überprüfen Sie die TFTP-Einstellungen.

### Verwandte Themen

[TFTP-Einstellungen überprüfen](#), auf Seite 174

## Das Telefon kann sich nicht mit dem Server verbinden

### Problem

Die Felder für IP-Adressen und Routing sind möglicherweise nicht richtig konfiguriert.

### Lösung

Überprüfen Sie die IP-Adressen- und RoutingEinstellungen auf dem Telefon. Wenn Sie DHCP verwenden, sollten diese Werte vom DHCP-Server bereitgestellt werden. Wenn Sie dem Telefon eine statische IP-Adresse zugewiesen haben, müssen Sie diese Werte manuell eingeben.

### Verwandte Themen

[DHCP-Einstellungen überprüfen](#), auf Seite 175

## Das Telefon kann sich nicht über DNS verbinden

### Problem

Die DNS-Einstellungen sind möglicherweise falsch.

### Lösung

Wenn Sie DNS für den Zugriff auf den TFTP-Server oder Cisco Unified Communications Manager verwenden, müssen Sie einen DNS-Server angeben.

### Verwandte Themen

[Die DNS-Einstellungen überprüfen](#), auf Seite 176

## Der Cisco Unified Communications Manager- und TFTP-Service werden nicht ausgeführt

### Problem

Wenn der Cisco Unified Communications Manager- oder der TFTP-Service nicht ausgeführt wird, können die Telefone möglicherweise nicht ordnungsgemäß gestartet werden. In diesem Fall tritt wahrscheinlich ein systemweiter Ausfall auf und andere Telefone und Geräte können nicht richtig gestartet werden.

### Lösung

Wenn der Cisco Unified Communications Manager-Service nicht ausgeführt wird, werden alle Geräte im Netzwerk beeinträchtigt, die für Anrufe von diesem Service abhängig sind. Wenn der TFTP-Service nicht ausgeführt wird, können viele Geräte nicht gestartet werden. Weitere Informationen hierzu finden Sie unter [Service starten, auf Seite 176](#).

## Die Konfigurationsdatei ist beschädigt

### Problem

Wenn weiterhin Probleme mit einem bestimmten Telefon auftreten, die mit den anderen Vorschlägen in diesem Kapitel nicht behoben werden können, ist möglicherweise die Konfigurationsdatei beschädigt.

### Lösung

Erstellen einer neuen Konfigurationsdatei für das Telefon.

### Verwandte Themen

[Erstellen einer neuen Konfigurationsdatei für das Telefon](#), auf Seite 175

## Cisco Unified Communications Manager – Telefonregistrierung

### Problem

Das Telefon wird nicht mit Cisco Unified Communications Manager registriert

### Lösung

Ein Cisco IP-Telefon kann sich nur mit einem Cisco Unified Communications Manager-Server registrieren, wenn das Telefon zum Server hinzugefügt wird oder die automatische Registrierung aktiviert ist. Lesen Sie die Informationen und Verfahren in [Methoden zum Hinzufügen von Telefonen, auf Seite 62](#), um sicherzustellen, dass das Telefon zur Cisco Unified Communications Manager-Datenbank hinzugefügt wurde.

Um zu überprüfen, ob sich das Telefon in der Cisco Unified Communications Manager-Datenbank befinden, wählen Sie **Gerät > Telefon** in der Cisco Unified Communications Manager-Verwaltung aus. Klicken Sie auf **Suchen**, um das Telefon basierend auf der MAC-Adresse zu suchen. Weitere Informationen zum Bestimmen der MAC-Adresse finden Sie unter [Die MAC-Adresse des Telefons bestimmen, auf Seite 62](#).

Wenn sich das Telefon bereits in der Cisco Unified Communications Manager-Datenbank befindet, ist die Konfigurationsdatei möglicherweise beschädigt. Siehe [Die Konfigurationsdatei ist beschädigt, auf Seite 166](#), falls Sie Hilfe benötigen.

## Cisco IP-Telefon kann keine IP-Adresse abrufen

### Problem

Wenn ein Telefon während des Starts keine IP-Adresse abrufen kann, befindet sich das Telefon möglicherweise nicht im gleichen Netzwerk oder VLAN wie der DHCP-Server oder der Switch-Port, mit dem das Telefon verbunden ist, ist deaktiviert.

### Lösung

Stellen Sie sicher, dass das Netzwerk oder VLAN, mit dem das Telefon die Verbindung herstellt, auf den DHCP-Server zugreifen kann, und der Switch-Port aktiviert ist.



# Probleme mit dem Zurücksetzen des Telefons

Wenn Benutzer melden, dass ihre Telefone während eines Anrufs oder im inaktiven Zustand zurückgesetzt werden, untersuchen Sie die Ursache. Wenn die Netzwerkverbindung und Cisco Unified Communications Manager-Verbindung stabil sind, sollte sich das Telefon nicht zurücksetzen.

Üblicherweise wird ein Telefon zurückgesetzt, wenn beim Verbinden mit dem Netzwerk oder Cisco Unified Communications Manager ein Problem auftritt.

## Das Telefon wird aufgrund sporadischer Netzwerkausfälle zurückgesetzt

### Problem

Das Netzwerk kann sporadisch ausfallen.

### Lösung

Sporadische Netzwerkausfälle wirken sich unterschiedlich auf den Daten- und Sprachnachrichtenverkehr aus. Das Netzwerk ist möglicherweise sporadisch ausgefallen, ohne dass dies bemerkt wurde. In diesem Fall kann der Datenverkehr verloren gegangene Pakete erneut senden und sicherstellen, dass die Pakete empfangen und gesendet wurden. Beim Sprachdatenverkehr können verloren gegangene Pakete jedoch nicht erneut gesendet werden. Anstatt zu versuchen, über eine unterbrochene Netzwerkverbindung weiter zu übertragen, wird das Telefon zurückgesetzt und es wird versucht, die Netzwerkverbindung wiederherzustellen. Weitere Informationen zu bekannten Problemen im Sprachnetzwerk erhalten Sie vom Systemadministrator.

## Das Telefon wird aufgrund von DHCP-Einstellungsfehlern zurückgesetzt

### Problem

Die DHCP-Einstellungen sind möglicherweise falsch.

### Lösung

Überprüfen Sie, ob das Telefon richtig für DHCP konfiguriert ist. Überprüfen Sie, ob der DHCP-Server richtig konfiguriert ist. Überprüfen Sie, die DHCP-Leasedauer. Wir empfehlen, eine Leasedauer von 8 Tagen festzulegen.

### Verwandte Themen

[DHCP-Einstellungen überprüfen](#), auf Seite 175

## Das Telefon wird aufgrund einer falschen statischen IP-Adresse zurückgesetzt

### Problem

Die statische IP-Adresse, die dem Telefon zugewiesen ist, ist möglicherweise ungültig.

**Lösung**

Wenn Sie dem Telefon eine statische IP-Adresse zuweisen, überprüfen Sie, ob Sie die richtigen Einstellungen eingegeben haben.

## Das Telefon wird bei hoher Netzwerkauslastung zurückgesetzt

**Problem**

Wenn das Telefon bei einer hohen Netzwerkauslastung zurückgesetzt wird, ist wahrscheinlich kein Sprach-VLAN aktiviert.

**Lösung**

Wenn Sie die Telefone in einem separaten zusätzlichen VLAN isolieren, wird die Qualität des Sprachverkehrs verbessert.

## Das Telefon wird absichtlich zurückgesetzt

**Problem**

Wenn Sie nicht der einzige Administrator mit Zugriff auf Cisco Unified Communications Manager sind, sollten Sie sicherstellen, dass kein anderer Administrator die Telefone absichtlich zurückgesetzt hat.

**Lösung**

Sie können prüfen, ob Cisco IP-Telefon einen Befehl zum Zurücksetzen von Cisco Unified Communications Manager empfangen hat; drücken Sie dazu **Einstellungen** auf dem Telefon, und wählen Sie **Administratoreinstellungen > Status > Netzwerkstatistik**.

- Wenn im Feld Grund für den Neustart Zurücksetzen-Zurücksetzen angezeigt wird, hat das Telefon den Befehl Zurücksetzen/Zurücksetzen von Cisco Unified Communications Manager empfangen.
- Wenn im Feld Grund für den Neustart Zurücksetzen-Neustart angezeigt wird, wurde das Telefon heruntergefahren, da es den Befehl Zurücksetzen/Neustart von Cisco Unified Communications Manager empfangen hat.

## Das Telefon wird aufgrund von DNS-Problemen oder anderen Verbindungsproblemen zurückgesetzt

**Problem**

Das Telefon wird fortlaufend zurückgesetzt und Sie vermuten, dass ein DNS-Problem oder anderes Verbindungsproblem aufgetreten ist.

**Lösung**

Wenn das Telefon fortlaufend zurückgesetzt wird, beheben Sie DNS-Probleme oder andere Verbindungsprobleme, indem Sie das Verfahren in [DNS-Probleme oder Verbindungsprobleme identifizieren, auf Seite 174](#) ausführen.

## Das Telefon schaltet sich nicht ein

### Problem

Das Telefon scheint nicht eingeschaltet zu sein.

### Lösung

In den meisten Fällen wird ein Telefon neu gestartet, wenn es mit einer externen Stromquelle eingeschaltet wird, aber die Verbindung getrennt und zu PoE gewechselt wird. Ein Telefon kann auch neu gestartet werden, wenn es mit PoE eingeschaltet und anschließend mit einer externen Stromquelle verbunden wird.

## Das Telefon kann sich nicht mit dem LAN verbinden

### Problem

Möglicherweise ist die physische Verbindung mit dem LAN beschädigt.

### Lösung

Stellen Sie sicher, dass die Ethernet-Verbindung, mit dem das Telefon verbunden ist, aktiv ist. Überprüfen Sie beispielsweise, ob der spezifische Port oder Switch, mit dem das Telefon verbunden ist, ausgeschaltet ist, und der Switch nicht neu gestartet wird. Stellen Sie außerdem sicher, dass kein Kabel beschädigt ist.

## Sicherheitsprobleme auf Cisco IP-Telefon

Die folgenden Abschnitte enthalten Informationen zur Problembehandlung für die Sicherheitsfunktionen auf Cisco IP-Telefon. Weitere Informationen zu den Lösungen für diese Probleme und zur Behandlung von Sicherheitsproblemen finden Sie im *Cisco Unified Communications Manager Sicherheitshandbuch*.

## CTL-Dateiprobleme

In den folgenden Abschnitten wird das Beheben von Problemen mit der CTL-Datei beschrieben.

### Authentifizierungsfehler, das Telefon kann die CTL-Datei nicht authentifizieren

#### Problem

Ein Geräteauthentifizierungsfehler tritt auf.

#### Ursache

Die CTL-Datei hat kein Cisco Unified Communications Manager-Zertifikat oder ein ungültiges Zertifikat.

#### Lösung

Installieren Sie ein gültiges Zertifikat.

## Das Telefon kann die CTL-Datei nicht authentifizieren

### Problem

Das Telefon kann die CTL-Datei nicht authentifizieren.

### Ursache

Der Sicherheitstoken, der die aktualisierte CTL-Datei signiert hat, ist in der CTL-Datei auf dem Telefon nicht vorhanden.

### Lösung

Ändern Sie den Sicherheitstoken in der CTL-Datei und installieren Sie die neue Datei auf dem Telefon.

## Die CTL-Datei wird authentifiziert, aber andere Konfigurationsdateien werden nicht authentifiziert

### Problem

Das Telefon kann keine Konfigurationsdateien, außer der CTL-Datei, authentifizieren.

### Ursache

Es ist ein ungültiger TFTP-Eintrag vorhanden oder die Konfigurationsdatei wurde möglicherweise nicht vom entsprechenden Zertifikat in der Vertrauensliste des Telefons signiert.

### Lösung

Überprüfen Sie den TFTP-Eintrag und das Zertifikat in der Vertrauensliste.

## Die ITL-Datei wird authentifiziert, aber andere Konfigurationsdateien werden nicht authentifiziert

### Problem

Das Telefon kann keine Konfigurationsdateien, außer der ITL-Datei, authentifizieren.

### Ursache

Die Konfigurationsdatei wurde möglicherweise nicht vom entsprechenden Zertifikat in der Vertrauensliste des Telefons signiert.

### Lösung

Signieren Sie die Konfigurationsdatei erneut mit dem richtigen Zertifikat.

## TFTP-Autorisierung fehlgeschlagen

### Problem

Das Telefon meldet einen TFTP-Autorisierungsfehler.

**Ursache**

Die TFTP-Adresse des Telefons ist nicht in der CTL-Datei vorhanden.

Wenn Sie eine neue CTL-Datei mit einem neuen TFTP-Eintrag erstellt haben, enthält die CTL-Datei auf dem Telefon keinen Eintrag für den neuen TFTP-Server.

**Lösung**

Überprüfen Sie die Konfiguration der TFTP-Adresse in der CTL-Datei auf dem Telefon.

## Das Telefon wird nicht registriert

**Problem**

Das Telefon wird nicht mit Cisco Unified Communications Manager registriert.

**Ursache**

Die CTL-Datei enthält nicht die richtigen Informationen für den Cisco Unified Communications Manager-Server.

**Lösung**

Ändern Sie die Cisco Unified Communications Manager-Serverinformationen in der CTL-Datei.

## Signierte Konfigurationsdateien werden nicht angefordert

**Problem**

Das Telefon fordert keine signierten Konfigurationsdateien an.

**Ursache**

Die CTL-Datei enthält keine TFTP-Einträge mit Zertifikaten.

**Lösung**

Konfigurieren Sie TFTP-Einträge mit Zertifikaten in der CTL-Datei.

# Audioprobleme

In den folgenden Abschnitten wird das Beheben von Audioproblemen beschrieben.

## Kein Sprachpfad

**Problem**

Mindestens eine Person in einem Anruf hört nichts.

**Lösung**

Wenn mindestens eine Person bei einem Anruf keinen Ton empfängt, besteht keine IP-Verbindung zwischen den Telefonen. Überprüfen Sie die Konfiguration der Router und Switches, um sicherzustellen, dass die IP-Verbindung ordnungsgemäß konfiguriert ist.

## Abgehackte Sprache

**Problem**

Ein Benutzer beschwert sich über die abgehackte Sprache in einem Anruf.

**Ursache**

Möglicherweise liegt ein Konflikt in der Jitter-Konfiguration vor.

**Lösung**

Überprüfen Sie die AvgJtr- und MaxJtr-Statistik. Eine große Abweichung zwischen diesen Statistiken weist auf ein Problem mit dem Jitter im Netzwerk oder zeitweise hohe Netzwerkaktivitäten hin.

## Ein Telefon im Daisy-Chain-Modus funktioniert nicht

**Problem**

Im Daisy-Chain-Modus funktioniert eines der Konferenztelefone nicht.

**Lösung**

Überprüfen Sie, ob die am Smart-Adapter angeschlossenen Kabel korrekt sind. Die beiden breiteren Kabel verbinden die Telefone mit dem Smart-Adapter. Das schmalere Kabel verbindet den Smart-Adapter mit dem Netzteil.

**Verwandte Themen**

[Daisy-Chain-Modus](#), auf Seite 31

[Konferenztelefon im Daisy-Chain-Modus installieren](#), auf Seite 38

## Allgemeine Anrufprobleme

In den folgenden Abschnitt wird die Behebung allgemeiner Anrufprobleme beschrieben.

### Anruf kann nicht hergestellt werden

**Problem**

Ein Benutzer beschwert sich, dass er keine Anrufe tätigen kann.

**Ursache**

Das Telefon hat keine DHCP IP-Adresse und kann sich nicht mit Cisco Unified Communications Manager registrieren. Telefone mit einem LCD-Display zeigen die Meldung `IP konfigurieren` oder `Registrieren an`. Auf Telefonen ohne LCD-Display wird der Umleitungston (anstatt der Wählton) im Hörer ausgegeben, wenn der Benutzer versucht, einen Anruf zu tätigen.

**Lösung**

1. Überprüfen Sie Folgendes:
  1. Das Ethernet-Kabel ist angeschlossen.
  2. Der Cisco Call Manager-Service wird auf dem Cisco Unified Communications Manager-Server ausgeführt.
  3. Beide Telefone sind mit dem gleichen Cisco Unified Communications Manager registriert.
2. Die Debug- und Erfassungsprotokolle des Audioservers sind für beide Telefone aktiviert. Falls erforderlich, aktivieren Sie Java Debug.

## Das Telefon erkennt DTMF-Ziffern nicht oder Ziffern werden verzögert

**Problem**

Der Benutzer beschwert sich, dass Nummern fehlen oder verzögert werden, wenn er das Tastenfeld verwendet.

**Ursache**

Wenn die Tasten zu schnell gedrückt werden, können Ziffern fehlen oder verzögert werden.

**Lösung**

Die Tasten sollten nicht zu schnell gedrückt werden.

## Fehlerbehebungsverfahren

Mit diesen Verfahren können Probleme identifiziert und behoben werden.

## Telefonproblemlerichte im Cisco Unified Communications Manager erstellen

Sie können einen Problemlericht für die Telefone im Cisco Unified Communications Manager generieren. Diese Aktion führt zu denselben Informationen, die der Softkey "Problemlerichtstool (PRT)" auf dem Telefon generiert.

Der Problemlericht enthält Informationen über das Telefon und die Headsets.

**Prozedur****Schritt 1**

Wählen Sie **Gerät > Telefon** in der Cisco Unified CM Administration aus.

**Schritt 2**

Klicken Sie auf **Suchen**, und wählen Sie ein oder mehrere Cisco IP-Telefone aus.

- Schritt 3** Klicken Sie auf **Generate PRT for Selected** (PRT für ausgewählte generieren), um PRT-Protokolle für die Headsets zu erfassen, die auf den ausgewählten Cisco IP-Telefonen verwendet werden.
- 

## TFTP-Einstellungen überprüfen

### Prozedur

---

- Schritt 1** Überprüfen Sie das Feld „TFTP-Server 1“.
- Wenn Sie dem Telefon eine statische IP-Adresse zugewiesen haben, müssen Sie manuell einen Wert für die Option TFTP-Server 1 eingeben.
- Wenn Sie DHCP verwenden, ruft das Telefon die Adresse für den TFTP-Server vom DHCP-Server ab. Überprüfen Sie, ob die IP-Adresse in Option 150 konfiguriert ist.
- Schritt 2** Sie können das Telefon auch für die Verwendung eines alternativen TFTP-Servers konfigurieren. Diese Einstellung ist insbesondere nützlich, wenn das Telefon kürzlich an einen anderen Standort verlegt wurde.
- Schritt 3** Wenn der lokale DHCP-Server nicht die richtige TFTP-Adresse ausgibt, aktivieren Sie das Telefon für die Verwendung eines alternativen TFTP-Servers.
- Dies ist oft in VPN-Szenarien erforderlich.
- 

## DNS-Probleme oder Verbindungsprobleme identifizieren

### Prozedur

---

- Schritt 1** Verwenden Sie das Menü Einstellungen zurücksetzen, um die Telefoneinstellungen auf die Standardwerte zurückzusetzen.
- Schritt 2** Ändern Sie die DHCP- und IP-Einstellungen:
- Deaktivieren Sie DHCP.
  - Weisen Sie dem Telefon statische IP-Werte zu. Verwenden Sie die gleiche Standardroutereinstellungen wie für die anderen funktionierenden Telefone.
  - Weisen Sie einen TFTP-Server zu. Verwenden Sie den gleichen TFTP-Server wie für die anderen funktionierenden Telefone.
- Schritt 3** Überprüfen Sie auf dem Cisco Unified Communications Manager-Server, ob in den lokalen Hostdateien dem Cisco Unified Communications Manager-Servernamen die richtige IP-Adresse zugewiesen ist.
- Schritt 4** Wählen Sie **System > Server** in Cisco Unified Communications Manager aus und überprüfen Sie, ob die IP-Adresse, nicht der DNS-Name, auf den Server verweist.
- Schritt 5** Wählen Sie **Gerät > Telefon** in der Cisco Unified Communications Manager-Verwaltung aus. Klicken Sie auf **Suchen**, um das Telefon zu suchen. Überprüfen Sie, ob Sie Cisco IP-Telefon die richtige MAC-Adresse zugewiesen haben.



**Schritt 6** Schalten Sie das Telefon aus und wieder ein.

---

**Verwandte Themen**

[Die MAC-Adresse des Telefons bestimmen](#), auf Seite 62

[Konferenztelefon neu starten oder zurücksetzen](#), auf Seite 179

## DHCP-Einstellungen überprüfen

---

**Prozedur**

**Schritt 1** Drücken Sie auf dem Telefon auf **Einstellungen**.

**Schritt 2** Wählen Sie **Administratoreinstellungen > Ethernet-Konfiguration > IPv4-Konfiguration** aus.

**Schritt 3** Überprüfen Sie das Feld „DHCP-Server“.

Wenn Sie dem Telefon eine statische IP-Adresse zugewiesen haben, müssen Sie keinen Wert für den DHCP-Server eingeben. Wenn Sie einen DHCP-Server verwenden, muss diese Option jedoch einen Wert enthalten. Wenn kein Wert gefunden wird, überprüfen Sie das IP-Routing und die VLAN-Konfiguration. Lesen Sie das Dokument *Troubleshooting Switch Port and Interface Problems* unter der folgenden URL:

[https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod\\_tech\\_notes\\_list.html](https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html)

**Schritt 4** Überprüfen Sie die Felder „IP-Adresse“, „Subnetzmaske“ und „Standardrouter“.

Wenn Sie dem Telefon eine statische IP-Adresse zuweisen, müssen Sie manuell Einstellungen für diese Optionen eingeben.

**Schritt 5** Wenn Sie DHCP verwenden, überprüfen Sie die IP-Adressen, die der DHCP-Server verteilt.

Lesen Sie das Dokument *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* unter der folgenden URL:

[https://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a00800f0804.shtml](https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml)

---

## Erstellen einer neuen Konfigurationsdatei für das Telefon

Wenn Sie ein Telefon aus der Cisco Unified Communications Manager-Datenbank entfernen, wird die Konfigurationsdatei vom Cisco Unified Communications Manager TFTP-Server gelöscht. Die Verzeichnisnummer oder Nummern des Telefons verbleiben in der Cisco Unified Communications Manager-Datenbank. Diese Nummern werden als nicht zugewiesene DNS bezeichnet und können für andere Geräte verwendet werden. Wenn nicht zugewiesene DNS nicht von anderen Geräten verwendet werden, löschen Sie diese DNS aus der Cisco Unified Communications Manager-Datenbank. Sie können den Routenplanbericht verwenden, um nicht zugewiesene Referenznummern anzuzeigen und zu löschen. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Wenn Sie die Tasten in einer Telefontastenvorlage ändern oder einem Telefon eine andere Telefontastenvorlage zuordnen, kann auf dem Telefon möglicherweise nicht mehr auf Verzeichnisnummern zugegriffen werden. Die Verzeichnisnummern sind dem Telefon noch in der Cisco Unified Communications Manager-Datenbank

zugewiesen, aber das Telefon hat keine Taste, mit der Anrufe angenommen werden können. Diese Verzeichnisnummern sollten vom Telefon entfernt und gelöscht werden.

### Prozedur

---

- Schritt 1** Wählen Sie in Cisco Unified Communications Manager **Gerät > Telefon** aus und klicken Sie auf **Suchen**, um das Telefon zu suchen, auf dem Probleme aufgetreten sind.
- Schritt 2** Wählen Sie **Löschen** aus, um das Telefon aus der Cisco Unified Communications Manager-Datenbank zu entfernen.
- Hinweis** Wenn Sie ein Telefon aus der Cisco Unified Communications Manager-Datenbank entfernen, wird die Konfigurationsdatei vom Cisco Unified Communications Manager TFTP-Server gelöscht. Die Verzeichnisnummer oder Nummern des Telefons verbleiben in der Cisco Unified Communications Manager-Datenbank. Diese Nummern werden als nicht zugewiesene DNS bezeichnet und können für andere Geräte verwendet werden. Wenn nicht zugewiesene DNS nicht von anderen Geräten verwendet werden, löschen Sie diese DNS aus der Cisco Unified Communications Manager-Datenbank. Sie können den Routenplanbericht verwenden, um nicht zugewiesene Referenznummern anzuzeigen und zu löschen.
- Schritt 3** Fügen Sie das Telefon wieder zur Cisco Unified Communications Manager-Datenbank hinzu.
- Schritt 4** Schalten Sie das Telefon aus und wieder ein.

### Verwandte Themen

[Methoden zum Hinzufügen von Telefonen](#), auf Seite 62

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Die DNS-Einstellungen überprüfen

### Prozedur

---

- Schritt 1** Drücken Sie auf dem Telefon auf **Einstellungen**.
- Schritt 2** Wählen Sie **Administratoreinstellungen > Ethernet-Konfiguration > IPv4-Konfiguration** aus.
- Schritt 3** Stellen Sie sicher, dass das Feld „DNS-Server 1“ ordnungsgemäß eingerichtet ist.
- Schritt 4** Vergewissern Sie sich außerdem, dass im DNS-Server ein CNAME-Eintrag für den TFTP-Server und für das Cisco Unified Communications Manager-System festgelegt ist.
- Sie müssen auch sicherstellen, dass DNS für Reverse-Lookups konfiguriert ist.

## Service starten

Ein Service muss aktiviert werden, bevor er gestartet oder beendet werden kann.

## Prozedur

---

- Schritt 1** Wählen Sie **Cisco Unified Wartbarkeit** in der Dropdown-Liste „Navigation“ in der Cisco Unified Communications Manager-Verwaltung aus und klicken Sie auf **Los**.
- Schritt 2** Wählen Sie **Tools > Control Center – Funktionsservices** aus.
- Schritt 3** Wählen Sie den primären Cisco Unified Communications Manager-Server in der Dropdown-Liste „Server“ aus.
- Im Fenster werden die Servicenamen für den ausgewählten Server, der Status der Services und das Servicefeld zum Starten und Beenden eines Services angezeigt.
- Schritt 4** Wenn ein Service beendet wurde, klicken Sie auf das entsprechende Optionsfeld und anschließend auf **Starten**. Das Servicestatussymbol ändert sich von einem Quadrat in einen Pfeil.
- 

# Debuginformationen von Cisco Unified Communications Manager

Wenn mit dem Telefon Probleme auftreten, die Sie nicht beheben können, kann Cisco TAC Ihnen Unterstützung bieten. Sie müssen das Debugging für das Telefon aktivieren, anschließend das Problem reproduzieren, und dann das Debugging wieder deaktivieren und die Protokolle zur Analyse an TCA senden.

Da beim Debugging detaillierte Informationen erfasst werden, kann es aufgrund der umfangreichen Datenübertragung dazu kommen, dass das Telefon langsamer reagiert. Nach dem Erfassen der Protokolle sollten Sie das Debugging deaktivieren, damit das Telefon wieder ordnungsgemäß funktioniert.

Die Fehlersuchinformationen können einen einstelligen Code enthalten, der den Schweregrad der Situation wiedergibt. Situationen werden wie folgt bewertet:

- 0 - Notfall
- 1 - Alarm
- 2 - Kritisch
- 3 - Fehler
- 4 - Warnung
- 5 - Benachrichtigung
- 6 – Informationen
- 7 – Debuggen

Wenden Sie sich an das Cisco TAC für weitere Informationen und Hilfe.

## Prozedur

---

### Schritt 1

Wählen Sie in der Cisco Unified Communications Manager-Verwaltung eines der folgenden Fenster aus:

- **Gerät > Geräteeinstellungen > Allgemeines Telefonprofil**
- **System > Firmentelefonkonfiguration**
- **Gerät > Telefon**

### Schritt 2

Legen Sie die folgenden Parameter fest:

- Protokollprofil – Werte: Voreinstellung (Standard), Standard, Telefonie, SIP, UI, Netzwerk, Medien, Update, Zubehör, Sicherheit, EnergyWise, MobileRemoteAccess
- Remoteprotokoll – Werte: Deaktivieren (Standard), Aktivieren
- IPv6-Protokollserver oder Protokollserver – IP-Adresse (IPv4- oder IPv6-Adresse)

**Hinweis** Wenn der Protokollserver nicht erreicht werden kann, sendet das Telefon keine Debugmeldungen mehr.

- Das Format der IPv4-Protokollserveradresse ist **address : <port>@@base=<0-7>;pfs=<0-1>**
  - Das Format der IPv6-Protokollserveradresse ist **[address] : <port>@@base=<0-7>;pfs=<0-1>**
  - Dabei gilt:
    - Die IPv4-Adresse wird mit Punkten (.) getrennt.
    - Die IPv6-Adresse wird mit Doppelpunkten (:) getrennt.
- 

## Zusätzliche Informationen zur Problembehandlung

Wenn Sie weitere Fragen zur Fehlerbehebung für Ihr Telefon haben, gehen Sie zur folgenden Cisco Website und navigieren Sie zum gewünschten Telefonmodell:

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



# KAPITEL 13

## Wartung

---

- [Konferenztelefon neu starten oder zurücksetzen](#), auf Seite 179
- [Überwachung der Sprachqualität](#), auf Seite 180
- [Reinigung des Cisco IP-Telefon](#), auf Seite 182

## Konferenztelefon neu starten oder zurücksetzen

Sie können ein Telefon einfach zurücksetzen, um es nach einem Fehler wiederherzustellen. Zudem ist es möglich, die Konfigurations- und Sicherheitseinstellungen auf die werksseitigen Standardeinstellungen zurückzusetzen.

### Konferenztelefon neu starten

Wenn Sie das Telefon neu starten, gehen alle Änderungen an Benutzer- und Netzwerk-Setup, die nicht im Flash-Speicher im Telefon gespeichert wurden, verloren.

#### Prozedur

---

Drücken Sie **Einstellungen** > **Verwaltereinstellungen** > **Einstellungen zurücksetzen** > **Gerät zurücksetzen**.

---

#### Verwandte Themen

[Text und Menüeintrag auf dem Telefon](#), auf Seite 41

## Die Einstellungen des Konferenztelefons über das Telefonmenü zurücksetzen

#### Prozedur

---

- Schritt 1** Drücken Sie **Einstellungen**.
- Schritt 2** Wählen Sie **Verwaltereinstellungen** > **Einstellungen zurücksetzen** aus.
- Schritt 3** Wählen Sie die Art der Zurücksetzung aus.
- **Alle**: Stellt die Werkseinstellungen wieder her.

- **Gerät zurücksetzen:** Setzt das Gerät zurück. Die vorhandenen Einstellungen werden nicht geändert.
- **Netzwerk:** Setzt die Netzwerkkonfiguration auf die Standardeinstellungen zurück.
- **Servicemodus:** Löscht den aktuellen Servicemodus, deaktiviert das VPN und startet das Telefon neu.
- **Sicherheit:** Setzt die Sicherheitskonfiguration auf die Standardeinstellungen zurück. Bei Auswahl dieser Option wird die CTL-Datei gelöscht.

**Schritt 4** Drücken Sie **Zurücksetzen** oder **Abbrechen**.

---

#### Verwandte Themen

[Text und Menüeintrag auf dem Telefon](#), auf Seite 41

## Konferenztelefon über das Tastenfeld auf die Werkseinstellungen zurücksetzen

Wenn Sie das Telefon über das Tastenfeld zurücksetzen, werden die Werkseinstellungen wiederhergestellt.

#### Prozedur

---

**Schritt 1** Stecken Sie das Telefon aus:

- Wenn Sie PoE verwenden, stecken Sie das LAN-Kabel aus.
- Wenn Sie das Netzteil verwenden, stecken Sie es aus.

**Schritt 2** Warten Sie 5 Sekunden lang.

**Schritt 3** Halten Sie # gedrückt und schließen Sie das Telefon wieder an.

**Schritt 4** Wenn das Telefon gestartet wird, leuchtet die LED-Leiste auf. Sobald sich die LED-Leiste einschaltet, drücken Sie nacheinander **123456789\*0#**.

Nachdem Sie diese Tasten gedrückt haben, durchläuft das Telefon den Prozess zum Zurücksetzen auf die Werkseinstellungen.

Wenn Sie die Tasten nicht in der richtigen Reihenfolge drücken, wird das Telefon normal gestartet.

**Vorsicht** Schalten Sie das Telefon nicht aus, bis der Prozess abgeschlossen ist und der Hauptbildschirm angezeigt wird.

---

#### Verwandte Themen

[Text und Menüeintrag auf dem Telefon](#), auf Seite 41

## Überwachung der Sprachqualität

Cisco IP-Telefone verwenden zum Messen der Sprachqualität von innerhalb des Netzwerks gesendeten und empfangenen Anrufen Statistikkennzahlen, die auf Verdeckungsereignissen basieren. DSP gibt Verdeckungsrahmen wieder, um den Rahmenverlust im Sprachpaketstream zu maskieren.

- **Verdeckungsmetrik:** Rate der Verdeckungsrahmen über allen Sprachrahmen anzeigen. Die Intervallrate für die Verdeckung wird alle drei Sekunden berechnet.

- Kennzahl Verdeckungszeit in Sekunden: Anzahl von Sekunden anzeigen, in denen DSP aufgrund von Rahmenverlusten Verdeckungsrahmen wiedergibt. Eine schwerwiegend „verdeckte Sekunde“ ist eine Sekunde, in der DSP Verdeckungsrahmen von mehr als fünf Prozent wiedergibt.



**Hinweis** Die Rate und Sekunden der Verdeckung sind primäre Messungen basierend auf dem Rahmenverlust. Die Verdeckungsrate Null gibt an, dass Rahmen und Pakete pünktlich und ohne Verlust im IP-Netzwerk übermittelt werden.

Sie können auf dem Bildschirm Anrufstatistik auf Cisco IP-Telefon oder remote unter Verwendung der Streaming-Statistik auf die Sprachqualitätsmetrik zugreifen.

## Tipps zur Fehlerbehebung bei der Sprachqualität

Wenn Sie signifikante und permanente Änderungen der Metrik bemerken, verwenden Sie die folgende Tabelle, die Informationen zur allgemeinen Fehlerbehebung enthält.

**Tabelle 31: Änderungen der Sprachqualitätsmetrik**

Metrikänderung	Bedingung
Die Verdeckungsrate und Sekunden der Verdeckung nehmen wesentlich zu	Netzwerkstörung durch Paketverlust und hohen Jitter.
Die Verdeckungsrate ist Null oder beinahe Null, aber die Sprachqualität ist schlecht.	<ul style="list-style-type: none"> <li>• Rauschen oder Verzerrung im Audiokanal, beispielsweise Echo oder Audiopegel.</li> <li>• Aufeinanderfolgende Anrufe, die mehrmals codiert/decodiert werden, beispielsweise Anrufe in einem Mobilfunknetz oder Callingcard-Netzwerk.</li> <li>• Akustische Probleme verursacht vom Lautsprecher, Mobiltelefon oder drahtlosen Headset.</li> </ul> <p>Überprüfen Sie die Paketübermittlung (TxCnt) und den Paketempfang (RxCnt), um sicherzustellen, dass die Sprachpakete gesendet werden.</p>
Die MOS LQK-Anzahl verringert sich wesentlich	<p>Netzwerkstörung durch Paketverlust und hohen Jitter:</p> <ul style="list-style-type: none"> <li>• Die durchschnittliche MOS LQK-Anzahl verringert sich und kann auf eine weitverbreitete und einheitliche Verminderung hinweisen.</li> <li>• Einzelne MOS LQK-Verminderungen können auf eine stoßweise Verminderung hinweisen.</li> </ul> <p>Überprüfen Sie die Verdeckungsrate und Sekunden der Verdeckung auf einen Hinweis auf Paketverlust und Jitter.</p>

Metrikänderung	Bedingung
Die MOS LQK-Anzahl erhöht sich wesentlich	<ul style="list-style-type: none"> <li>• Überprüfen Sie, ob das Telefon einen anderen als den erwarteten Codec verwendet (RxType und TxType).</li> <li>• Überprüfen Sie, ob sich die MOS LQK-Version geändert hat, nachdem eine Firmware aktualisiert wurde.</li> </ul>



**Hinweis** Die Sprachqualitätsmetrik berücksichtigt Geräusche und Verzerrungen nicht, nur den Rahmenverlust.

## Reinigung des Cisco IP-Telefon

Reinigen Sie die Oberflächen und den Telefonbildschirm Ihres Cisco IP-Telefons nur mit einem weichen, trockenen Tuch. Tragen Sie Flüssigkeiten oder Reinigungsmittel nicht direkt auf das Telefon auf. Wie bei allen nicht witterungsbeständigen elektronischen Geräten können Flüssigkeiten oder pulverförmige Stoffe die Komponenten beschädigen und Fehlfunktionen verursachen.

Wenn sich das Telefon im Energiesparmodus befindet, ist das Display leer und die Auswahltaste leuchtet nicht. In diesem Zustand können Sie das Display des Telefons reinigen, sofern Sie sich sicher sind, dass das Telefon bis zum Abschluss der Reinigung im Energiesparmodus verbleiben wird.





## KAPITEL 14

# Unterstützung von Benutzern in anderen Ländern

- [Unified Communications Manager Installationsprogramm für Endpunktsprache](#), auf Seite 183
- [Internationaler Support für Anrufprotokollierung](#), auf Seite 183
- [Sprachbeschränkung](#), auf Seite 184

## Unified Communications Manager Installationsprogramm für Endpunktsprache

Cisco IP-Telefone sind standardmäßig für das Gebietsschema Englisch (USA) konfiguriert. Um Cisco IP-Telefone in anderen Gebietsschemata verwenden zu können, müssen Sie die gebietsschemaspezifische Version des Unified Communications Manager-Sprachinstallationspakets für Endgeräte auf jedem Cisco Unified Communications Manager-Server im Cluster installieren. Der Locale Installer installiert den neuesten übersetzten Text für die Benutzeroberfläche des Telefons und länderspezifische Telefonsignale auf Ihrem System, damit diese für Cisco IP-Telefon verfügbar sind.

Um auf das Sprachinstallationspaket für eine bestimmte Version zuzugreifen, öffnen Sie die Seite [Software-Download](#), navigieren Sie zu Ihrem Telefonmodell und wählen Sie den Link „Unified Communications Manager Endpoints Locale Installer“ aus.

Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.



**Hinweis** Die aktuelle Version des Locale Installer ist möglicherweise nicht sofort verfügbar. Sehen Sie regelmäßig auf der Webseite nach, ob Aktualisierungen vorhanden sind.

### Verwandte Themen

[Dokumentation Cisco Unified Communications Manager](#), auf Seite 14

## Internationaler Support für Anrufprotokollierung

Wenn Ihr Telefonsystem für die internationale Anrufprotokollierung (Anrufernormalisierung) konfiguriert ist, zeigen die Einträge für die Anrufprotokolle, die Wahlwiederholung oder das Anrufverzeichnis möglicherweise ein Pluszeichen (+) an, das die internationale Escapesequenz für Ihren Standort darstellt.

Abhängig von der Konfiguration Ihres Telefonsystems kann das Pluszeichen durch die richtige internationale Vorwahl ersetzt werden oder Sie müssen die Nummer vor dem Wählen bearbeiten, um das Pluszeichen durch die internationale Escapesequenz für Ihren Standort zu ersetzen. Obwohl im Anrufprotokoll oder Verzeichniseintrag die vollständige internationale Nummer des eingehenden Anrufs angezeigt wird, kann auf dem Telefondisplay die gekürzte lokale Version der Nummer ohne Landesvorwahl angezeigt werden.

## Sprachbeschränkung

Für die folgenden asiatischen Gebietsschemata besteht keine lokalisierte KATE-Unterstützung (Keyboard Alphanumeric Text Entry):

- Chinesisch (China)
- Chinesisch (Hongkong)
- Chinesisch (Taiwan)
- Japanisch (Japan)
- Koreanisch (Korea, Republik)

Stattdessen wird der standardmäßige englische KATE (USA) für den Benutzer angezeigt.

Beispiel: Auf dem Telefonbildschirm wird Text in Koreanisch angezeigt, die Taste **2** auf dem Tastenfeld zeigt aber **a b c 2 A B C** an.

Über diese Übersetzung

Cisco kann in einigen Regionen Übersetzungen dieses Inhalts in die Landessprache bereitstellen. Bitte beachten Sie, dass diese Übersetzungen nur zu Informationszwecken zur Verfügung gestellt werden. Bei Unstimmigkeiten hat die englische Version dieses Inhalts Vorrang.