



## **Cisco IP-Telefon 8800-Serie – Administratorhandbuch für Cisco Unified Communications Manager**

**Erste Veröffentlichung:** 13. Juli 2015

**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 DIESER 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 kodierte 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).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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)

© 2015–2023 Cisco Systems, Inc. Alle Rechte vorbehalten.



## INHALTSVERZEICHNIS

---

### VORWORT:

#### **Einleitung** xiii

Übersicht xiii

Zielgruppe xiii

Handbuchkonventionen xiii

Zugehöriges Dokumentationsmaterial xiv

Dokumentation Cisco IP Phone der Serie 8800 xv

Dokumentation Cisco Unified Communications Manager xv

Dokumentation Cisco Business Edition 6000 xv

Dokumentation, Support und Sicherheitsrichtlinien xv

Übersicht über die Cisco Produktsicherheit xv

---

### 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) 2

Neue und geänderte Informationen zur Firmware-Version 14.0(1) 2

Neue und geänderte Informationen zur Firmware-Version 12.8(1) 3

Neue und geänderte Informationen zur Firmware-Version 12.7(1) 3

Neue und geänderte Informationen zur Firmware-Version 12.6(1) 4

Neue Informationen zur Firmware-Version 12.5(1)SR3 4

Neue Informationen zur Firmware-Version 12.5(1)SR1 4

Neue Informationen zur Firmware-Version 12.1(1)SR1 5

Neue Informationen zur Firmware-Version 12.1(1) 5

Neue Informationen zur Firmware-Version 12.0(1) 6

Neue Informationen zur Firmware-Version 11.7(1) 6

Neue Informationen zur Firmware-Version 11.5(1)SR1 6

Neue Informationen zur Firmware-Version 11.5(1) 7

Neue Informationen zur Firmware Version 11.0 8

---

TEIL I:

**Allgemeines zum Cisco IP-Telefon 11**

---

KAPITEL 2

**Technische Details 13**

Physische und Umgebungsspezifikationen 13

Kabelspezifikationen 14

Pin-Belegungen für Netzwerk- und Computerports 14

Netzwerkport-Stecker 14

Computerport-Stecker 15

Stromversorgung des Telefons 16

Stromausfall 17

Senkung des Stromverbrauchs 17

Energieaushandlung über LLDP 17

Netzwerkprotokolle 18

VLAN-Interaktion 22

Cisco Unified Communications Manager-Interaktion 22

Cisco Unified Communications Manager Express-Interaktion 23

Interaktion mit dem Sprachnachrichtensystem 24

Übersicht über den Startvorgang des Telefons 24

Externe Geräte 26

Informationen zum USB-Port 27

Konfigurationsdateien für Telefone 27

Verhalten des Telefons bei Netzwerküberlastung 28

Telefonverhalten in einem Netzwerk mit zwei Netzwerkroutern 28

Application Programming Interface 28

---

KAPITEL 3

**Cisco IP-Telefon-Hardware 29**

Telefonübersicht 29

Cisco IP Phone 8811 31

Verbindungen mit Multiplattform-Telefonen der Serie 31

Cisco IP-Telefons 8841 und 8845 32

Telefonanschlüsse 32

Cisco IP-Telefons 8851 und 8851NR 33

Verbindungen mit dem	34
Cisco IP-Telefons 8861, 8865 und 8865NR	35
Telefonanschlüsse	35
Tasten und Hardware	36
Softkey-, Leitungs- und Funktionstasten	38
Die Kamera Ihres Videotelefons schützen	39

**TEIL II:****Installation des Cisco IP-Telefon 41****KAPITEL 4****Installation des Cisco IP-Telefon 43**

Netzwerkconfiguration überprüfen	43
Aktivierungscode-Integration für lokale Telefone	44
Aktivierungscode-Integration mit mobilem und Remotezugriff	45
Aktivieren der automatischen Registrierung für Telefone	45
Cisco IP-Telefon installieren	47
Netzwerkverbindung über das Telefon und einen Computer nutzen	49
Telefon über die Einrichtungsmenüs einrichten	49
Anwenden eines Telefonkennworts	50
Text und Menüeintrag vom Telefon	51
Wireless LAN auf dem Telefon aktivieren	51
Wireless LAN über Cisco Unified Communications Manager einrichten	52
Telefon für ein WLAN konfigurieren	53
Anzahl der WLAN-Authentifizierungsversuche festlegen	55
Aktivieren des WLAN-Aufforderungsmodus	55
Wi-Fi-Profil mit Cisco Unified Communications Manager festlegen	56
Wi-Fi-Gruppe mit Cisco Unified Communications Manager festlegen	58
Netzwerkeinstellungen konfigurieren	59
Felder des Ethernet-Setup	59
IPv4-Felder	61
IPv6-Felder	63
Telefon für die Verwendung von DHCP einrichten	65
Telefon so einrichten, dass kein DHCP verwendet wird	65
Software-Server	66
Überprüfung des Telefons beim Starten	66

Telefonservices für Benutzer konfigurieren 66  
 Telefonmodell eines Benutzers ändern 67

---

**KAPITEL 5**

**Cisco Unified Communications Manager – Telefonkonfiguration 69**

- Cisco IP-Telefon einrichten 69
- Die MAC-Adresse des Telefons bestimmen 72
- Methoden zum Hinzufügen von Telefonen 73
  - Einzelne Telefone hinzufügen 73
  - Telefone über eine BAT-Telefonvorlage hinzufügen 73
- Benutzer zu Cisco Unified Communications Manager hinzufügen 74
  - Benutzer aus einem externen LDAP-Verzeichnis hinzufügen 75
  - Einen Benutzer direkt Cisco Unified Communications Manager hinzufügen 75
- Einer Endbenutzergruppe einen Benutzer hinzufügen 76
- Telefone zu Benutzern zuordnen 77
- SRST (Survivable Remote Site Telephony) 77
- E-SRST (Enhanced Survivable Remote Site Telephony) 80
- Anwendungswählregeln 80
  - Anwendungswählregeln konfigurieren 81

---

**KAPITEL 6**

**Verwaltung des Selbstservice-Portals 83**

- Übersicht des Selbstservice-Portals 83
- Den Benutzerzugriff auf das Selbstservice-Portal konfigurieren 83
- Die Ansicht des Selbstservice-Portals anpassen 84

---

**TEIL III:**

**Verwaltung von Cisco IP-Telefon 85**

---

**KAPITEL 7**

**Sicherheit von Cisco IP-Telefonen 87**

- Sicherheitsverbesserungen für Ihr Telefonnetzwerk 87
- Unterstützte Sicherheitsfunktionen 88
  - Einrichten eines LSC (Locally Significant Certificate) 93
  - Aktivieren des FIPS-Modus 94
  - Anrufsicherheit 95
    - Sichere Konferenzanruf-ID 96
    - Sichere Anruf-ID 96

Verschlüsselung für Aufschaltung bereitstellen	97
WLAN-Sicherheit	98
Authentifizierung einrichten	101
Wireless-Sicherheit-Anmeldeinformationen	101
Benutzername und Kennwort einrichten	102
Pre-shared Key – Setup	102
Wireless-Verschlüsselung	103
CA-Zertifikat von ACS mithilfe der Microsoft-Zertifikatdienste exportieren	104
PEAP-Setup	109
Wireless LAN-Sicherheit	110
Verwaltungsseite für das Cisco IP-Telefon	110
SCEP-Konfiguration	113
802.1X-Authentifizierung	114
Auf die 802.1X-Authentifizierung zugreifen	115
Feld „Geräteauthentifizierung“ festlegen	116

---

**KAPITEL 8**

<b>Anpassung des Cisco IP-Telefon</b>	<b>117</b>
Benutzerdefinierte Ruftöne	117
Benutzerdefinierte Hintergrundbilder	117
Breitband-Codec konfigurieren	119
Inaktives Display konfigurieren	120
Den Wählton anpassen	121

---

**KAPITEL 9**

<b>Telefonfunktionen und Konfiguration</b>	<b>123</b>
Übersicht über Telefonfunktionen und Konfiguration	123
Benutzersupport für Cisco IP-Telefon	123
Telefonfunktionen	124
Funktionstasten und Softkeys	142
Telefonfunktion – Konfiguration	144
Einrichten von Telefonfunktionen für alle Telefone	145
Einrichten von Telefonfunktionen für eine Telefongruppe	145
Einrichten von Telefonfunktionen für ein einzelnes Telefon	146
Produktspezifische Konfiguration	146
Bewährte Verfahren für die Konfiguration von Funktionen	168

Umgebungen mit hohem Anrufaufkommen	169
Umgebungen mit mehreren Leitungen	169
Umgebung mit Sitzungsleitungsmodus	169
Feld: Immer Hauptleitung verwenden	170
Transport Layer Security-Schlüssel deaktivieren	170
Anruferverlauf für gemeinsam genutzte Leitung aktivieren	171
Energiesparmodus für Cisco IP-Telefon planen	171
EnergyWise für das Cisco IP-Telefon planen	173
DND konfigurieren	176
Mitarbeiterbegrüßung aktivieren	177
Überwachung und Aufzeichnung konfigurieren	178
Benachrichtigung für Rufumleitung einrichten	178
BLF für Anruflisten aktivieren	179
Energy Efficient Ethernet für Switch-Port und PC-Port einrichten	180
RTP/sRTP-Portbereich konfigurieren	181
Mobil- und Remote Access über Expressway	182
Bereitstellungsszenarien	183
Medienpfade und Interactive Connectivity Establishment	184
Verfügbare Telefonfunktionen für Mobil- und Remote Access über Expressway	184
Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren	186
QR-Code für die MRA-Anmeldung generieren	186
Tool zur Problemmeldung	187
Eine Upload-URL für den Kundensupport konfigurieren	187
Bezeichnung einer Leitung festlegen	188
Informationen für zwei Speicherbänke einrichten	189
Überwachung geparkter Anrufe	189
Timer für Überwachung geparkter Anrufe einrichten	189
Parameter zur Überwachung geparkter Anrufe für Verzeichnisnummern einrichten	191
Überwachung geparkter Anrufe für Hunt Lists einrichten	192
Audio- und Videoport-Bereiche einrichten	192
Einrichten des Cisco IP Manager Assistant	194
Visual Voicemail einrichten	196
Visual Voicemail für einen bestimmten Benutzer einrichten	197
Visual Voicemail-Setup für eine Benutzergruppe	197



	Zugesicherte Dienste für SIP	198
	Direkte Migration Ihres Telefons zu einem Multiplattform-Telefon	199
	MLPP (Multilevel Precedence and Preemption)	199
	Softkey-Vorlagen konfigurieren	199
	Vorlagen für Telefontasten	201
	Telefontastenvorlage ändern	201
	Telefontastenvorlage für alle Anrufe zuweisen	202
	PAB oder Kurzwahl als IP-Telefonservice konfigurieren	203
	Telefontastenvorlage für das persönliche Adressbuch oder die Schnellwahl ändern	204
	VPN-Konfiguration	205
	Zusätzliche Leitungstasten einrichten	206
	Im erweiterten Leitungsmodus verfügbare Funktionen	206
	TLS-Fortsetzungs-Timer einrichten	209
	Intelligent Proximity aktivieren	210
	Auflösung für Videoübertragung einrichten	210
	Headset-Verwaltung für ältere Versionen von Cisco Unified Communications Manager	211
	Standard-Konfigurationsdatei für Headset herunterladen	212
	Standard-Konfigurationsdatei für das Headset ändern	213
	Installieren der Standardkonfigurationsdatei in Cisco Unified Communications Manager	215
	Cisco TFTP-Server neu starten	215
<hr/>		
<b>KAPITEL 10</b>	<b>Unternehmensverzeichnis und persönliches Verzeichnis</b>	<b>217</b>
	Konfiguration des Firmenverzeichnisses	217
	Konfiguration des persönlichen Verzeichnisses	217
	Konfiguration der Benutzereinträge im persönlichen Verzeichnis	218
	Synchronizer für das Adressbuch des Cisco IP-Telefons herunterladen	219
	Bereitstellung des Synchronizers für das Adressbuch des Cisco IP-Telefons	219
	Synchronizer installieren	219
	Synchronizer konfigurieren	220
<hr/>		
<b>TEIL IV:</b>	<b>Problembehandlung für Cisco IP-Telefone</b>	<b>221</b>
<hr/>		
<b>KAPITEL 11</b>	<b>Telefonysteme überwachen</b>	<b>223</b>
	Cisco IP-Telefon-Status	223

Das Fenster Telefoninformationen anzeigen	223
Felder für Telefoninformationen	224
Das Statusmenü anzeigen	224
Statusmeldungen anzeigen	225
Anzeigen des Netzwerk-Info-Bildschirms	230
Bildschirm „Netzwerkstatistik“ anzeigen	230
Bildschirm „Wireless-Statistik“ anzeigen	233
Die Anrufstatistik anzeigen	235
Fenster „Aktueller Zugangspunkt“ anzeigen	237
Webseite für Cisco IP-Telefon	239
Webseite für Telefon öffnen	239
Geräteinformationen	240
Netzwerkkonfiguration	243
Netzwerkstatistik	248
Geräteprotokolle	251
Streaming-Statistik	251
Informationen im XML-Format vom Telefon anfordern	255
Beispielausgabe für „CallInfo“	256
Beispielausgabe für „LineInfo“	257
Beispielausgabe für „ModeInfo“	257
<b>KAPITEL 12</b>	<b>Fehlerbehebung 259</b>
Allgemeine Informationen zur Problembehandlung	259
Startprobleme	260
Cisco IP-Telefon wird nicht normal gestartet	261
Cisco IP-Telefon wird nicht mit Cisco Unified Communications Manager registriert	262
Fehlermeldungen auf dem Telefon	262
Das Telefon kann keine Verbindung mit dem TFTP-Server oder Cisco Unified Communications Manager herstellen	262
Telefon kann keine Verbindung mit dem TFTP-Server herstellen	262
Das Telefon kann sich nicht mit dem Server verbinden	263
Das Telefon kann sich nicht über DNS verbinden	263
Der Cisco Unified Communications Manager- und TFTP-Service werden nicht ausgeführt	263
Die Konfigurationsdatei ist beschädigt	263

Cisco Unified Communications Manager – Telefonregistrierung	264
Cisco IP-Telefon kann keine IP-Adresse abrufen	264
Telefon kann nicht registriert werden	264
Probleme mit dem Zurücksetzen des Telefons	265
Das Telefon wird aufgrund sporadischer Netzwerkausfälle zurückgesetzt	265
Das Telefon wird aufgrund von DHCP-Einstellungsfehlern zurückgesetzt	265
Das Telefon wird aufgrund einer falschen statischen IP-Adresse zurückgesetzt	265
Das Telefon wird bei hoher Netzwerkauslastung zurückgesetzt	266
Das Telefon wird absichtlich zurückgesetzt	266
Das Telefon wird aufgrund von DNS-Problemen oder anderen Verbindungsproblemen zurückgesetzt	266
Das Telefon schaltet sich nicht ein	267
Das Telefon kann sich nicht mit dem LAN verbinden	267
Sicherheitsprobleme auf Cisco IP-Telefon	267
CTL-Dateiprobleme	267
Authentifizierungsfehler, das Telefon kann die CTL-Datei nicht authentifizieren	267
Das Telefon kann die CTL-Datei nicht authentifizieren	268
Die CTL-Datei wird authentifiziert, aber andere Konfigurationsdateien werden nicht authentifiziert	268
Die ITL-Datei wird authentifiziert, aber andere Konfigurationsdateien werden nicht authentifiziert	268
TFTP-Autorisierung fehlgeschlagen	268
Das Telefon wird nicht registriert	269
Signierte Konfigurationsdateien werden nicht angefordert	269
Probleme bei Videoanrufen	269
Keine Videoübertragung zwischen zwei Cisco IP-Videotelefonen	269
Videowiedergabe stolpert oder es werden Frames ausgelassen	270
Videoanruf kann nicht übergeben werden	270
Kein Video während eines Konferenzgesprächs	270
Allgemeine Anrufprobleme	270
Anruf kann nicht hergestellt werden	271
Das Telefon erkennt DTMF-Ziffern nicht oder Ziffern werden verzögert	271
Fehlerbehebungsverfahren	271
Telefonproblembenachrichtigungen im Cisco Unified Communications Manager erstellen	271
Erstellen eines Konsolenprotokolls auf Ihrem Telefon	272

TFTP-Einstellungen überprüfen 272

DNS-Probleme oder Verbindungsprobleme identifizieren 273

DHCP-Einstellungen überprüfen 273

Erstellen einer neuen Konfigurationsdatei für das Telefon 274

Ermitteln, ob bzw. welche 802.1X-Authentifizierungsprobleme bestehen 275

Die DNS-Einstellungen überprüfen 275

Service starten 275

Debuginformationen von Cisco Unified Communications Manager 276

Zusätzliche Informationen zur Problembehandlung 277

---

**KAPITEL 13**

**Wartung 279**

Standardmäßiges Zurücksetzen 279

    Telefon über das Tastenfeld des Telefons auf die Werkseinstellungen zurücksetzen 280

    Alle Einstellungen über das Telefonmenü zurücksetzen 280

    Ihr Telefon über das Backup-Image neu starten 281

Netzwerkconfiguration zurücksetzen 281

Benutzer-Netzwerkconfiguration zurücksetzen 281

CTL-Datei entfernen 282

Quality Report Tool 282

Überwachung der Sprachqualität 282

    Tipps zur Fehlerbehebung bei der Sprachqualität 283

Reinigung des Cisco IP-Telefon 284

---

**KAPITEL 14**

**Unterstützung von Benutzern in anderen Ländern 285**

Unified Communications Manager Installationsprogramm für Endpunktsprache 285

Internationaler Support für Anrufprotokollierung 285

Sprachbeschränkung 286



## VORWORT

# Einleitung

---

- [Übersicht, auf Seite xiii](#)
- [Zielgruppe, auf Seite xiii](#)
- [Handbuchkonventionen, auf Seite xiii](#)
- [Zugehöriges Dokumentationsmaterial, auf Seite xiv](#)
- [Dokumentation, Support und Sicherheitsrichtlinien, auf Seite xv](#)

## Übersicht

Das Nachschlagewerk *Cisco IP-Telefon 8800-Serie – Administratorhandbuch für Cisco Unified Communications Manager* enthält alle relevanten Informationen über Telefone in einem VoIP-Netzwerk: grundlegende Erläuterungen sowie Informationen zur Installation, Konfiguration, Verwaltung und Fehlerbehebung.

Aufgrund der Komplexität eines IP-Telefonienetzwerks werden in diesem Handbuch Vorgänge, die im Cisco Unified Communications Manager bzw. auf anderen Netzwerkgeräten durchgeführt werden müssen, nicht umfassend erläutert.

## Zielgruppe

Netzwerktechniker, Systemadministratoren und Telekommunikationstechniker sollten sich anhand dieses Handbuchs mit den Schritten vertraut machen, die zum Einrichten von Cisco IP-Telefon erforderlich sind. Die in diesem Handbuch beschriebenen Aufgaben umfassen das Konfigurieren der Netzwerkeinstellungen, die nicht für Telefonbenutzer bestimmt sind. Die Aufgaben in diesem Handbuch erfordern, dass Sie mit Cisco Unified Communications Manager vertraut sind.

## Handbuchkonventionen

Dieses Dokument verwendet die folgenden Konventionen:

Konvention	Beschreibung
<b>Fettdruck</b>	Befehle und Schlüsselwörter sind <b>fett</b> markiert.
<i>Kursiv</i>	Argumente, für die Sie Werte angeben, sind <i>kursiv</i> dargestellt.

Konvention	Beschreibung
[]	Elemente in eckigen Klammern sind optional.
{x   y   z}	Alternative Schlüsselwörter sind in geschweiften Klammern gruppiert und durch vertikale Striche getrennt.
[x   y   z]	Optionale alternative Schlüsselwörter sind in Klammern gruppiert und durch vertikale Striche getrennt.
Zeichenfolge	Mehrere Zeichen ohne Anführungszeichen. Setzen Sie die Zeichenfolge nicht in Anführungszeichen, da die Anführungszeichen sonst zur Zeichenfolge gehören.
Bildschirmschrift	Terminalsitzungen und vom System angezeigte Informationen werden in <b>Bildschirmschrift</b> angezeigt.
<b>Eingabeschrift</b>	Informationen, die Sie eingeben müssen, werden in der <b>Eingabeschrift</b> angezeigt.
<i>Kursive</i> Bildschirmschrift	Argumente, für die Sie Werte angeben, sind in <i>kursiver Bildschirmschrift</i> dargestellt.
^	Das Symbol ^ steht für die Strg-Taste. Beispielsweise bedeutet ^D in einer Bildschirmanzeige, dass Sie die Strg-Taste gedrückt halten müssen, während Sie die Taste D drücken.
<>	Nicht druckbare Zeichen, beispielsweise Kennwörter, stehen in spitzen Klammern.



**Hinweis** Dies bedeutet, dass *der Leser auf etwas hingewiesen wird*. Hinweise enthalten nützliche Vorschläge oder Verweise auf Unterlagen, die nicht zur Dokumentation gehören.



**Vorsicht** Dies bedeutet, dass *der Leser etwas beachten muss*. In dieser Situation könnten Sie u.U. einen Vorgang ausführen, der zu einer Beschädigung des Geräts und zum Verlust von Daten führt.

Für Warnungen werden die folgenden Konventionen verwendet:



**Achtung** WICHTIGE SICHERHEITSHINWEISE

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung von Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Hinweisnummer nach der jeweiligen Übersetzung in den Sicherheitshinweisen, die diesem Gerät beiliegt.  
Hinweis 1071

BEWAHREN SIE DIESE HINWEISE GUT AUF.

## Zugehöriges Dokumentationsmaterial

In den folgenden Abschnitten finden Sie zugehörige Informationen.

## Dokumentation Cisco IP Phone der Serie 8800

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

Der Anwendungsleitfaden befindet sich unter folgender URL:

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

## 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 Business Edition 6000

Lesen Sie den *Cisco Business Edition 6000 Dokumentationsleitfaden* und andere Veröffentlichungen für Ihre Cisco Business Edition 6000-Version. Navigieren Sie zur folgenden URL:

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





# 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 2](#)
- [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 3](#)
- [Neue und geänderte Informationen zur Firmware-Version 12.7\(1\), auf Seite 3](#)
- [Neue und geänderte Informationen zur Firmware-Version 12.6\(1\), auf Seite 4](#)
- [Neue Informationen zur Firmware-Version 12.5\(1\)SR3, auf Seite 4](#)
- [Neue Informationen zur Firmware-Version 12.5\(1\)SR1, auf Seite 4](#)
- [Neue Informationen zur Firmware-Version 12.1\(1\)SR1, auf Seite 5](#)
- [Neue Informationen zur Firmware-Version 12.1\(1\), auf Seite 5](#)
- [Neue Informationen zur Firmware-Version 12.0\(1\), auf Seite 6](#)
- [Neue Informationen zur Firmware-Version 11.7\(1\), auf Seite 6](#)
- [Neue Informationen zur Firmware-Version 11.5\(1\)SR1, auf Seite 6](#)
- [Neue Informationen zur Firmware-Version 11.5\(1\), auf Seite 7](#)
- [Neue Informationen zur Firmware Version 11.0, auf Seite 8](#)

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

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

<b>Funktion</b>	<b>Neu oder geändert</b>
Unterstützung für SIP-OAuth für SRST	<a href="#">Sicherheitsverbesserungen für Ihr Telefonnetzwerk, auf Seite 87</a>
Vereinfachte Extension Mobility-Anmeldung mit Cisco-Headset 730-USB-Adapter	<a href="#">Telefonfunktionen, auf Seite 124</a>
Bluetooth-Stummschaltungssynchronisierung für die Cisco-Headset 700 Serie	<a href="#">Telefonfunktionen, auf Seite 124</a>
Neue Einstellungen für die Cisco-Headset 500 Serie: Dock-Ereignis und Modus „Immer an“	<a href="#">Telefonfunktionen, auf Seite 124</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 87</a>
Verbesserte Anruflbenachrichtigung für Sammelanschlussgruppen	<a href="#">Telefonfunktionen, auf Seite 124</a>
Konfigurierbare Rufnummernanzeige für erweiterten Leitungsmodus	<a href="#">Produktspezifische Konfiguration</a>
Konfigurierbare verzögerte PLAR	<a href="#">Telefonfunktionen, auf Seite 124</a>
MRA-Unterstützung für Extension Mobility-Anmeldung mit Cisco-Headsets	<a href="#">Telefonfunktionen, auf Seite 124</a>
Telefonmigration ohne Übergangs-Firmware	<a href="#">Direkte Migration Ihres Telefons zu einem Multiplattform-Telefon, auf Seite 199</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	<a href="#">Produktspezifische Konfiguration, auf Seite 146</a>
SIP-OAuth-Verbesserungen	<a href="#">Sicherheitsverbesserungen für Ihr Telefonnetzwerk, auf Seite 87</a>
Verbesserungen der Benutzeroberfläche	<a href="#">SRST (Survivable Remote Site Telephony), auf Seite 77</a> <a href="#">Telefonfunktionen, auf Seite 124</a>
OAuth-Verbesserungen für MRA	<a href="#">Mobil- und Remote Access über Expressway, auf Seite 182</a>

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	<a href="#">Telefonmodell eines Benutzers ändern, auf Seite 67</a>
Verbesserung der Headset-Aktualisierung	<a href="#">Geräteinformationen, auf Seite 240</a>
Vereinfachen der Extension Mobility mit Cisco-Headsets	<a href="#">Telefonfunktionen, auf Seite 124</a>
Änderungen der Funktionssteuerung	<a href="#">Produktspezifische Konfiguration, auf Seite 146</a> , neue Felder <b>Warnung zur Verringerung der Stimmlautstärke</b> und <b>Anruf als Spam markieren</b>
Allgemeine Änderungen	Wi-Fi und PC-Port klären: <ul style="list-style-type: none"> <li>• <a href="#">Telefon über die Einrichtungsmenüs einrichten, auf Seite 49</a></li> <li>• <a href="#">Wireless LAN auf dem Telefon aktivieren, auf Seite 51</a></li> </ul>
Weitere Informationen zum Feld „Webzugriff“ hinzugefügt	<a href="#">Produktspezifische Konfiguration, auf Seite 146</a>
Nicht unterstützte Funktion entfernen	<a href="#">Telefonfunktionen, auf Seite 124</a>

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

*Tabelle 2: Überarbeitung des Cisco IP-Telefon 8800-Administratorhandbuchs für Firmware-Version 12.7(1)*

Überarbeitung	Aktualisierter Abschnitt
Aktualisiert für Unterstützung von Hintergrundbildern auf den Tastenerweiterungsmodulen.	<a href="#">Benutzerdefinierte Hintergrundbilder, auf Seite 117</a>
Für Cisco Headset 730-Unterstützung aktualisiert	<a href="#">Geräteinformationen, auf Seite 240</a>
Aktualisiert für Cisco-Headset 500 Serie Firmware-Version 2.0	<a href="#">Geräteinformationen, auf Seite 240</a> <a href="#">Headset-Verwaltung für ältere Versionen von Cisco Unified Communications Manager, auf Seite 211</a>
Für eingehende Sammelanschlussgruppen-Anrufe aktualisiert.	<a href="#">Telefonfunktionen, auf Seite 124</a>
E-Hook-Konfigurationsinformationen wurden entfernt.	<a href="#">Produktspezifische Konfiguration, auf Seite 146</a>

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

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

**Tabelle 3: Überarbeitung des Cisco IP-Telefon 8800-Administratorhandbuchs für Firmware-Version 12.6(1)**

Überarbeitung	Aktualisierter Abschnitt
Aktualisierung für die Rückkehr zur Hauptleitung im Sitzungsleitungsmodus.	<a href="#">Produktspezifische Konfiguration, auf Seite 146</a> <a href="#">Umgebung mit Sitzungsleitungsmodus, auf Seite 169</a>

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

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

**Tabelle 4: Überarbeitung des Cisco IP-Telefon 8800-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 45</a>
Unterstützung für die Verwendung des Problembenachrichtigungstools über Cisco Unified Communications Manager.	<a href="#">Telefonproblembenachrichtigungen im Cisco Unified Communications Manager erstellen, auf Seite 271</a>
Neues Thema	<a href="#">Netzwerkverbindung über das Telefon und einen Computer nutzen, auf Seite 49</a>
Neues Thema	<a href="#">Die Kamera Ihres Videotelefons schützen, auf Seite 39</a>

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

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

**Tabelle 5: Überarbeitung des Cisco IP-Telefon 8800-Administratorhandbuchs für Firmware-Version 12.5(1)SR1**

Überarbeitung	Aktualisierter Abschnitt
Unterstützung für Elliptische-Kurven-Unterstützung	<a href="#">Unterstützte Sicherheitsfunktionen, auf Seite 88</a>

Überarbeitung	Aktualisierter Abschnitt
Unterstützung für Anrufprotokoll-Verbesserungen für den erweiterten Leitungsmodus mit Rollover-Leitungen	<a href="#">Im erweiterten Leitungsmodus verfügbare Funktionen, auf Seite 206</a>
Unterstützung für Whisper Paging auf Cisco Unified Communications Manager Express	<a href="#">Cisco Unified Communications Manager Express-Interaktion, auf Seite 23</a>
Unterstützung der chinesischen Sprache	<a href="#">Sprachbeschränkung, auf Seite 286</a>
Unterstützung für das Integrieren des Aktivierungscodes	<a href="#">Aktivierungscode-Integration für lokale Telefone, auf Seite 44</a>
Unterstützung für Medienpfade und Interactive Connectivity Establishment	<a href="#">Medienpfade und Interactive Connectivity Establishment, auf Seite 184</a>
Unterstützung für das Deaktivieren des TLS-Schlüssels	<a href="#">Produktspezifische Konfiguration, auf Seite 146</a>
Unterstützung beim Deaktivieren des Hörers, damit der Audiopfad auf dem Headset aufrechterhalten werden kann	<a href="#">Produktspezifische Konfiguration, auf Seite 146</a>
Unterstützung für die Remote-Konfiguration von Headset-Parametern	<a href="#">Headset-Verwaltung für ältere Versionen von Cisco Unified Communications Manager, auf Seite 211</a>

## Neue Informationen zur Firmware-Version 12.1(1)SR1

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

*Tabelle 6: Überarbeitung des Cisco IP-Telefon 8800-Administratorhandbuchs für Firmware-Version 12.1(1)SR1*

Überarbeitung	Aktualisierter Abschnitt
Enbloc-Wählen für T.302-Erweiterung des Interdigit-Timers.	<a href="#">Produktspezifische Konfiguration, auf Seite 146</a>

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

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

Tabelle 7: Überarbeitung des Cisco IP-Telefon 8800-Administratorhandbuchs für Firmware-Version 12.1(1)

Überarbeitung	Aktualisierter Abschnitt
Der Mobil- und Remote Access über Expressway unterstützt nun den erweiterten Leitungsmodus.	<a href="#">Verfügbare Telefonfunktionen für Mobil- und Remote Access über Expressway, auf Seite 184</a>
	<a href="#">Mobil- und Remote Access über Expressway, auf Seite 182</a>
	<a href="#">Im erweiterten Leitungsmodus verfügbare Funktionen, auf Seite 206</a>
Das Aktivieren oder Deaktivieren von TLS 1.2 für den Webserverzugriff wird nun unterstützt.	<a href="#">Produktspezifische Konfiguration, auf Seite 146</a>
Der G722.2 AMR-WB-Audiocodec wird jetzt unterstützt.	<a href="#">Telefonübersicht, auf Seite 29</a>
	<a href="#">Anrufstatistikfelder, auf Seite 235</a>

## Neue Informationen zur Firmware-Version 12.0(1)

Alle neuen Funktionen wurden zu [Telefonfunktionen, auf Seite 124](#) hinzugefügt.

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

Tabelle 8: Überarbeitung des Cisco IP-Telefon 8800-Administratorhandbuchs für Firmware-Version 12.0(1)

Überarbeitung	Aktualisierter Abschnitt
Aktualisierung in Bezug auf Anruf parken, Anruf parken – Leitungsstatus, Gruppenübernahme und Unterstützung von Sammelanschlüssen im erweiterten Leitungsmodus	<a href="#">Im erweiterten Leitungsmodus verfügbare Funktionen, auf Seite 206</a>

## Neue Informationen zur Firmware-Version 11.7(1)

Für die Firmware-Version 11.7(1) wurden keine Administrationsaktualisierungen benötigt.

## Neue Informationen zur Firmware-Version 11.5(1)SR1

Alle neuen Funktionen wurden zu [Telefonfunktionen, auf Seite 124](#) hinzugefügt.

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

**Table 9: Überarbeitung des Cisco IP-Telefon 8800-Administratorhandbuchs für Firmware-Version 11.5(1)SR1**

Überarbeitung	Aktualisierter Abschnitt
Aktualisiert für Unterstützung des Cisco IP-Telefon 8865NR	<ul style="list-style-type: none"> <li>• <a href="#">Stromversorgung des Telefons</a>, auf Seite 16</li> <li>• <a href="#">Netzwerkprotokolle</a>, auf Seite 18</li> <li>• <a href="#">Telefonübersicht</a>, auf Seite 29</li> <li>• <a href="#">Tasten und Hardware</a>, auf Seite 36</li> </ul>
Aktualisiert für Unterstützung von Aufzeichnung und Überwachung im erweiterten Leitungsmodus	<a href="#">Im erweiterten Leitungsmodus verfügbare Funktionen</a> , auf Seite 206
Aktualisiert für Unterstützung von WLAN-Scanliste	<a href="#">Wireless LAN auf dem Telefon aktivieren</a> , auf Seite 51
	<a href="#">Telefon für ein WLAN konfigurieren</a> , auf Seite 53
	<a href="#">Netzwerkeinstellungen konfigurieren</a> , auf Seite 59
Aktualisiert für Unterstützung der Merkmale MLPP (Vorrangschaltung) und DND (Nicht stören)	<a href="#">DND konfigurieren</a> , auf Seite 176
Aktualisiert für Unterstützung von konfigurierbaren Klingeltönen	<a href="#">Produktspezifische Konfiguration</a> , auf Seite 146
Erhöhte Sicherheit	<a href="#">Sicherheitsverbesserungen für Ihr Telefonnetzwerk</a> , auf Seite 87
Allgemeine Änderungen	<p>Aktualisierung der <a href="#">Webseite für Cisco IP-Telefon</a>, auf Seite 239</p> <p>Neue Präsentation der Telefon-Funktionskonfiguration in Cisco Unified Communications Manager <a href="#">Telefonfunktion – Konfiguration</a>, auf Seite 144</p>

## Neue Informationen zur Firmware-Version 11.5(1)

**Table 10: Überarbeitung des Cisco IP-Telefon 8800-Administratorhandbuchs für Firmware-Version 11.5(1)**

Überarbeitung	Aktualisierter Abschnitt
Erweiterter Leitungsmodus wird unterstützt.	<p><a href="#">Zusätzliche Leitungstasten einrichten</a>, auf Seite 206</p> <p><a href="#">Im erweiterten Leitungsmodus verfügbare Funktionen</a>, auf Seite 206</p>
Die Anzeige von „Nicht stören“ (Ruhefunktion) wurde aktualisiert.	<a href="#">DND konfigurieren</a> , auf Seite 176
Opus-Codec wird unterstützt.	<a href="#">Telefonübersicht</a> , auf Seite 29

Überarbeitung	Aktualisierter Abschnitt
FIPS-Modus wurde hinzugefügt.	<a href="#">Aktivieren des FIPS-Modus, auf Seite 94</a>
WLAN-Setup wurde aktualisiert.	<a href="#">Telefon für ein WLAN konfigurieren, auf Seite 53</a>
WLAN-Profil für Cisco IP-Telefons 8861 und 8865 wird unterstützt.	<a href="#">Wi-Fi-Profil mit Cisco Unified Communications Manager festlegen, auf Seite 56</a>
	<a href="#">Wi-Fi-Gruppe mit Cisco Unified Communications Manager festlegen, auf Seite 58</a>
Festlegen von WLAN-Authentifizierungsversuchen wird unterstützt.	<a href="#">Anzahl der WLAN-Authentifizierungsversuche festlegen, auf Seite 55</a>
Aktivierung des WLAN-Aufforderungsmodus wird unterstützt.	<a href="#">Aktivieren des WLAN-Aufforderungsmodus, auf Seite 55</a>
Anpassung des Wähltons wird unterstützt.	<a href="#">Den Wählton anpassen, auf Seite 121</a>
Anzeige des Netzwerk-Info-Bildschirms wird unterstützt.	<a href="#">Anzeigen des Netzwerk-Info-Bildschirms, auf Seite 230</a>

## Neue Informationen zur Firmware Version 11.0

Alle neuen Funktionen wurden zu [Telefonfunktionen, auf Seite 124](#) hinzugefügt.

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

**Tabelle 11: Überarbeitung des Cisco IP-Telefon 8800-Administratorhandbuchs für Firmware-Version 11.0**

Überarbeitung	Aktualisierter Abschnitt
Aktualisiert – Konkretisierung und Beheben von Unzulänglichkeiten	<ul style="list-style-type: none"> <li>• <a href="#">VPN-Konfiguration, auf Seite 205</a></li> <li>• <a href="#">Netzwerkeinstellungen konfigurieren, auf Seite 59</a></li> <li>• <a href="#">Energy Efficient Ethernet für Switch-Port und PC-Port einrichten, auf Seite 180</a></li> <li>• <a href="#">Auflösung für Videoübertragung einrichten, auf Seite 210</a></li> <li>• <a href="#">E-SRST (Enhanced Survivable Remote Site Telephony), auf Seite 80</a></li> </ul>
Aktualisiert – Verbesserte Einteilung in unterstützte Optionen zum Debuggen des Telefons	<ul style="list-style-type: none"> <li>• <a href="#">Debuginformationen von Cisco Unified Communications Manager, auf Seite 276.</a></li> </ul>



Überarbeitung	Aktualisierter Abschnitt
Aktualisiert – Verbesserte Unterstützung von digitalen EAP-TLS + SCEP-, PEAP-GTC- und X.509-Zertifikaten	<ul style="list-style-type: none"> <li>• <a href="#">WLAN-Sicherheit</a>, auf Seite 98.</li> <li>• <a href="#">Authentifizierung einrichten</a>, auf Seite 101</li> <li>• <a href="#">Wireless-Sicherheit-Anmeldeinformationen</a>, auf Seite 101</li> </ul>
Aktualisiert – Verbesserte Unterstützung des Problembenachrichtigungstools (PRT)	<ul style="list-style-type: none"> <li>• <a href="#">Tool zur Problemmeldung</a>, auf Seite 187.</li> <li>• <a href="#">Eine Upload-URL für den Kundensupport konfigurieren</a>, auf Seite 187.</li> </ul>
Unterstützung durch „Anwendungs-Wählregel“ hinzugefügt	<ul style="list-style-type: none"> <li>• <a href="#">Anwendungswählregeln</a>, auf Seite 80</li> </ul>
Leitungsbeschreibung hinzugefügt	<ul style="list-style-type: none"> <li>• <a href="#">Bezeichnung einer Leitung festlegen</a>, auf Seite 188.</li> </ul>





TEIL **I**

## **Allgemeines zum Cisco IP-Telefon**

- [Technische Details, auf Seite 13](#)
- [Cisco IP-Telefon-Hardware, auf Seite 29](#)





## KAPITEL 2

# Technische Details

- [Physische und Umgebungsspezifikationen, auf Seite 13](#)
- [Kabelspezifikationen, auf Seite 14](#)
- [Stromversorgung des Telefons, auf Seite 16](#)
- [Netzwerkprotokolle, auf Seite 18](#)
- [VLAN-Interaktion, auf Seite 22](#)
- [Cisco Unified Communications Manager-Interaktion, auf Seite 22](#)
- [Cisco Unified Communications Manager Express-Interaktion, auf Seite 23](#)
- [Interaktion mit dem Sprachnachrichtensystem, auf Seite 24](#)
- [Übersicht über den Startvorgang des Telefons, auf Seite 24](#)
- [Externe Geräte, auf Seite 26](#)
- [Informationen zum USB-Port, auf Seite 27](#)
- [Konfigurationsdateien für Telefone, auf Seite 27](#)
- [Verhalten des Telefons bei Netzwerküberlastung, auf Seite 28](#)
- [Telefonverhalten in einem Netzwerk mit zwei Netzwerkroutern, auf Seite 28](#)
- [Application Programming Interface, auf Seite 28](#)

## Physische und Umgebungsspezifikationen

In der folgenden Tabelle werden die Gehäusespezifikationen und die Spezifikationen zur Betriebsumgebung für die Cisco IP-Telefon 8800-Serie aufgeführt.

**Tabelle 12: Physische und Umgebungsspezifikationen**

Spezifikation	Wert oder Bereich
Betriebstemperatur	0 °C bis 40 °C (32 °F bis 104 °F)
Relative Luftfeuchtigkeit beim Betrieb	In Betrieb: 10 % bis 90 % (nicht kondensierend) Außer Betrieb: 10 % bis 95 % (nicht kondensierend)
Lagertemperatur	-10 °C bis 60 °C (14 °F bis 140 °F)
Höhe	229,1 mm
Breite	257,34 mm

Spezifikation	Wert oder Bereich
Tiefe	40 mm
Gewicht	1,19 kg
Netzanschluss	100–240 VAC, 50–60 Hz, 0,5 A bei Verwendung des Netzteils 48 VDC, 0,2 A bei Inline-Stromversorgung über das Netzkabel
Kabel	Kategorie 3/5/5e/6 für 10-Mbit/s-Kabel mit 4 Paaren Kategorie 5/5e/6 für 100-Mbit/s-Kabel mit 4 Paaren Kategorie 5e/6 für 1000-Mbit/s-Kabel mit vier Paaren <b>Hinweis</b> Kabel weisen vier Leiterpaare auf, sodass sich eine Summe von acht ergibt.
Entfernung	Entsprechend der Ethernet-Spezifikation sollte die Kabellänge zwischen einem IP-Telefon und dem Switch höchstens 100 m betragen.

## Kabelspezifikationen

Im Folgenden sind die Kabelspezifikationen aufgeführt:

- RJ-9-Buchse (4 Leiter) für Hörer- und Headset-Port
- RJ-45-Buchse für den LAN 10/100/1000BaseT-Anschluss (10/100/1000-Netzwerk-Port am Telefon)
- RJ-45-Buchse für einen zweiten 10/100/1000BaseT-kompatiblen Anschluss (10/100/1000-Computer-Port am Telefon)
- 3,5-mm-Buchse für Lautsprecheranschluss (nur Cisco IP-Telefon 8861)
- 48-Volt-Netzanschluss
- USB-Ports/-Anschluss: Ein (Cisco IP-Telefon 8851) bzw. zwei USB-Ports (Cisco IP-Telefon 8861)
- 3 Erweiterungsmodulanschlüsse, die beim Cisco IP-Telefon 8851 und beim Cisco IP-Telefon 8861 als USB-Anschluss berücksichtigt werden

## Pin-Belegungen für Netzwerk- und Computerports

Obwohl sowohl der Netzwerk- als auch der Computerport für die Netzwerkverbindung verwendet werden, dienen sie unterschiedlichen Zwecken und weisen unterschiedliche Pin-Belegungen auf.

- Der Netzwerkport ist der 10/100/1000 SW-Port auf dem Cisco IP-Telefon.
- Der Computerport ist der 10/100/1000 PC-Port auf dem Cisco IP-Telefon.

## Netzwerkport-Stecker

In der folgenden Tabelle sind die Pin-Belegungen des Netzwerkport-Steckers aufgeführt.

Tabelle 13: Pin-Belegungen des Netzwerkport-Steckers

Pin-Nummer	Funktion
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
<b>Hinweis</b>	BI steht für bidirektional und DA, DB, DC und DD geben Daten A, Daten B, Daten C und Daten D an.

## Computerport-Stecker

In der folgenden Tabelle sind die Pin-Belegungen des Computerport-Steckers aufgeführt.

Tabelle 14: Pin-Belegungen des Computerport-Steckers

Pin-Nummer	Funktion
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
<b>Hinweis</b>	BI steht für bidirektional und DA, DB, DC und DD geben Daten A, Daten B, Daten C und Daten D an.

# Stromversorgung des Telefons

Cisco IP-Telefon kann über eine externe Stromversorgung oder mit „Power over Ethernet“ (PoE) betrieben werden. Ein separates Netzteil stellt die externe Stromversorgung sicher. Der Switch kann PoE über das Ethernet-Telefonkabel bereitstellen.

Cisco IP-Telefon 8861 und Cisco IP-Telefon 8865 sind Geräte der PoE-Klasse 4 und benötigen zur Unterstützung von Zusatzfunktionen einen Switch oder eine Leitungskarte, die Klasse 4 unterstützen.

Weitere Informationen zur Stromversorgung Ihres Telefons finden Sie im Datenblatt zu Ihrem Telefon.

Wenn Sie ein Telefon installieren, das über eine externe Stromquelle betrieben wird, schließen Sie die Stromversorgung an, bevor Sie das Ethernet-Kabel mit dem Telefon verbinden. Wenn Sie ein Telefon entfernen, das über eine externe Stromquelle betrieben wird, stecken Sie das Ethernet-Kabel vom Telefon aus, bevor Sie die Stromversorgung trennen.

**Tabelle 15: Richtlinien für die Stromversorgung von Cisco IP-Telefonen**

Art der Stromversorgung	Richtlinien
Externe Stromversorgung: Erfolgt über CP-PWR-CUBE-4= externe Stromversorgung	Cisco IP-Telefon verwendet zur Stromversorgung den CP-PWR-CUBE-4.
PoE-Energie: Wird von einem Switch über das Ethernet-Kabel am Telefon bereitgestellt.	Cisco IP-Telefons 8851, 8851NR, 8861, 8865 und 8865NR unterstützen 802.3at PoE Zubehör. Weitere Informationen finden Sie im Datenblatt zu Ihrem Telefon.  Zur Sicherstellung des unterbrechungsfreien Betriebs des Telefons benötigt der Switch Backup-Stromversorgung  Stellen Sie sicher, dass die CatOS- oder IOS-Version, die auf dem Switch ausgeführt wird, die beabsichtigte Telefonbereitstellung unterstützt. Informationen zur Betriebssystemversion finden Sie in der Dokumentation für den Switch.
Universal Power over Ethernet (UPoE)	Cisco IP-Telefon 8865 und 8865NR unterstützen UPoE.

Die Dokumente in der folgenden Tabelle enthalten weitere Informationen zu den folgenden Themen:

- Cisco Switches, die für den Einsatz mit Cisco IP-Telefonen geeignet sind
- Cisco IOS-Versionen, die eine bidirektionale Energieaushandlung unterstützen
- Weitere Anforderungen und Einschränkungen im Zusammenhang mit der Stromversorgung

**Tabelle 16: Zusätzliche Informationen**

Thema des Dokuments	URL
PoE-Lösungen	<a href="http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html">http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html</a>
UPoE	<a href="http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe">http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe</a>
Cisco Catalyst-Switches	<a href="http://www.cisco.com/c/en/us/products/switches/index.html">http://www.cisco.com/c/en/us/products/switches/index.html</a>



Thema des Dokuments	URL
Integrierte Dienst-Router	<a href="http://www.cisco.com/c/en/us/products/routers/index.html">http://www.cisco.com/c/en/us/products/routers/index.html</a>
Cisco IOS Software	<a href="http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html">http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html</a>

## 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 das Cisco IP-Telefon verbraucht.

### Energiesparmodus

Im Energiesparmodus ist die Hintergrundbeleuchtung deaktiviert, wenn das Telefon nicht verwendet wird. Das Telefon verbleibt über die festgelegte Dauer im Energiesparmodus oder bis der Benutzer den Hörer abnimmt oder 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.

## Energieaushandlung über LLDP

Zwischen Telefon und Switch erfolgt eine Energieaushandlung über den Stromverbrauch des Telefons. Für den Betrieb des Cisco IP-Telefons gibt es mehrere Stromeinstellungen, wodurch zum Beispiel der Stromverbrauch gesenkt wird, wenn weniger Strom zur Verfügung steht.

Nach dem Neustart eines Telefons führt der Switch mit einem Protokoll (CDP oder LLDP) die Energieaushandlung durch. Der Switch verbindet sich mit dem ersten Protokoll, das einen Schwellengrenzwert (TLV) enthält, der vom Telefon übertragen wird. Wenn der Systemadministrator das Protokoll auf dem Telefon deaktiviert, kann das Telefon keine Zubehörkomponenten einschalten, da der Switch nicht auf Stromfragen im anderen Protokoll reagiert.

Cisco empfiehlt, bei Verbindungen zu einem Switch, der die Energieaushandlung unterstützt, die Energieaushandlungsfunktion immer aktiviert zu lassen (Standard).

Wenn die Energieaushandlung deaktiviert ist, trennt der Switch die Stromversorgung zum Telefon möglicherweise. Wenn der Switch die Energieaushandlung nicht unterstützt, deaktivieren Sie die

Energieaushandlungsfunktion, bevor Sie Zubehörkomponenten über PoE aktivieren. Wenn die Energieaushandlung deaktiviert ist, kann das Telefon die Zubehörkomponenten bis zum maximalen gemäß IEEE 802.3af-2003-Norm zugelassenen Wert mit Strom versorgen.

**Hinweis**

- Wenn CDP und Energieaushandlung deaktiviert sind, kann das Telefon die Zubehörkomponenten bis zu 15,4 W mit Strom versorgen.

## Netzwerkprotokolle

Die Cisco IP-Telefon 8800-Serie unterstützt verschiedene eigene und Industriestandard-konforme Netzwerkprotokolle, die für die Sprachkommunikation benötigt werden. Die folgende Tabelle enthält eine Übersicht der von den Telefonen unterstützten Netzwerkprotokolle.

**Tabelle 17: Von der Cisco IP-Telefon 8800-Serie unterstützte Netzwerkprotokolle**

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Bluetooth	Bluetooth ist ein Kurzstrecken-Funkprotokoll (WPAN-Protokoll), das die Kommunikation zwischen Geräten über kurze Distanzen regelt.	Telefone des Typs Cisco IP-Telefon 8845, 8865 und 8851 unterstützen Bluetooth 4.1.  Cisco IP-Telefon 8861 unterstützt Bluetooth 4.0.  Cisco IP-Telefon 8811, 8841, 8851NR und 8865NR unterstützen kein Bluetooth.
Bootstrap Protocol (BootP)	Mit BootP kann ein Netzwerkgerät, beispielsweise Cisco IP-Telefon, bestimmte Startinformationen (z. B. die IP-Adresse) abfragen.	—
Cisco Audio Session Tunnel (CAST)	Mit dem CAST-Protokoll können Telefone und zugehörige Anwendungen Remote-IP-Telefone erkennen und mit diesen kommunizieren, ohne dass Änderungen an den herkömmlichen Komponenten zur Signalübertragung erforderlich sind.	Cisco IP-Telefon verwendet CAST als Schnittstelle zwischen CUVA und Cisco Unified Communications Manager mit Cisco IP-Telefon als SIP-Proxy.
Cisco Discovery Protocol (CDP)	CDP ist ein Protokoll für die Geräteerkennung, das auf allen Geräten von Cisco ausgeführt wird.  Mithilfe von CDP kann sich ein Gerät innerhalb des Netzwerks für andere Geräte erkennbar machen und Informationen über andere Geräte empfangen.	Cisco IP-Telefons nutzen CDP für die Übertragung von Informationen, wie beispielsweise Zusatz-VLAN-ID, Energiemanagementdaten einzelner Ports oder Konfigurationsinformationen zur Quality of Service (QoS), an den Cisco Catalyst-Switch.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP ist ein Cisco-eigenes Protokoll, mit dessen Hilfe für Geräte eine Peer-to-Peer-Hierarchie hergestellt werden kann. Über diese Hierarchie können die in der Hierarchie befindlichen Geräte Firmware-Dateien an die benachbarten Geräte weitergeben.	CPPDP wird von der Funktion „Gemeinsame Firmware für Gruppe“ genutzt.

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Dynamic Host Configuration Protocol (DHCP)	<p>DHCP reserviert und weist IP-Adressen zu Netzwerkgeräten zu.</p> <p>DHCP ermöglicht das Einbinden eines IP-Telefons in ein Netzwerk, wobei das Telefon anschließend betriebsbereit ist, ohne dass manuell eine IP-Adresse zugewiesen oder zusätzliche Netzwerkparameter konfiguriert werden müssen.</p>	<p>DHCP ist standardmäßig aktiviert. Wenn DHCP deaktiviert ist, müssen Sie die IP-Adresse, die Subnetzmaske, das Gateway und einen TFTP-Server auf jedem Telefon manuell konfigurieren.</p> <p>Wir empfehlen, die angepasste DHCP-Option 150 zu verwenden. Mit dieser Methode können Sie die IP-Adresse des TFTP-Servers als Optionswert konfigurieren. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.</p> <p><b>Hinweis</b> Wenn Sie Option 150 nicht nutzen können, empfiehlt sich die DHCP-Option 66.</p>
Hypertext Transfer Protocol (HTTP)	HTTP ist das Standardprotokoll zum Übertragen von Informationen und Dokumenten im Internet und dem Web.	Cisco IP-Telefons nutzen HTTP für XML-Dienste und zur Fehlerbehebung.
Hypertext Transfer Protocol Secure (HTTPS)	HTTPS ist eine Kombination der Übertragungsprotokolle HTTP und SSL/TLS, die eine Verschlüsselung und sichere Identifizierung von Servern ermöglicht.	Webanwendungen, die sowohl HTTP als auch HTTPS unterstützen, verfügen zu diesem Zweck über zwei konfigurierte URLs. Cisco IP-Telefons, die HTTPS unterstützen, wählen die HTTPS-URL aus.
IEEE 802.1X	<p>Der Standard IEEE 802.1X definiert ein Protokoll zur Client-Server-basierten Zugriffskontrolle und Authentifizierung, das dafür sorgt, dass sich ausschließlich autorisierte Clients über öffentlich zugängliche Ports mit einem LAN verbinden können.</p> <p>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.</p>	<p>Die Implementierung des Standards IEEE 802.1X erfolgt auf dem Cisco IP-Telefon durch Unterstützung der Authentifizierungsmethoden EAP-FAST und EAP-TLS.</p> <p>Wenn auf dem Telefon die 802.1X-Authentifizierung aktiviert ist, sollten Sie das PC-Port- und Sprach-VLAN deaktivieren.</p>
IEEE 802.11n/802.11ac	<p>Der Standard IEEE 802.11 regelt die Kommunikation von Geräten in einem lokalen Funknetzwerk (WLAN).</p> <p>Teilstandard 802.11n arbeitet sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzbereich, während 802.11ac nur für den 5-GHz-Frequenzbereich zuständig ist.</p>	<p>Die 802.11-Schnittstelle ist insbesondere in Situationen, in denen keine Ethernet-Verkabelung zur Verfügung steht bzw. eingesetzt werden soll, eine geeignete Bereitstellungsalternative.</p> <p>Nur Cisco IP-Telefon 8861 und 8865 unterstützen WLAN.</p>

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Internet Protocol (IP)	IP ist ein Messaging-Protokoll, das Pakete im Netzwerk verarbeitet und sendet.	<p>Damit Netzwerkgeräte mittels IP kommunizieren können, müssen ihnen eine IP-Adresse, ein Subnetz und ein Gateway zugewiesen sein.</p> <p>Wenn Sie für Cisco IP-Telefon DHCP (Dynamic Host Configuration Protocol) nutzen, erfolgt die Zuweisung von IP-Adresse, Subnetz und Gateway automatisch. Wenn Sie DHCP nicht verwenden, müssen Sie diese Eigenschaften jedem Telefon manuell zuweisen.</p> <p>Cisco IP-Telefons unterstützen die Verwendung von IPv6-Adressen. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.</p>
Link Layer Discovery Protocol (LLDP)	LLDP ist ein standardisiertes Netzwerkerkennungsprotokoll (ähnlich wie CDP), das auf einigen Geräten von Cisco und Drittanbietern unterstützt wird.	Das Cisco IP-Telefon unterstützt LLDP auf dem PC-Port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED ist eine Erweiterung des LLDP-Standards speziell für Produkte zur Sprachübertragung.	<p>Das Cisco IP-Telefon unterstützt LLDP-MED auf dem SW-Port, um folgende Informationen weiterzugeben:</p> <ul style="list-style-type: none"> <li>• Sprach-VLAN-Konfiguration</li> <li>• Geräteerkennung</li> <li>• Energieverwaltung</li> <li>• Bestandsverwaltung</li> </ul>
Real-Time Transport Protocol (RTP)	RTP ist ein Protokoll zur Übertragung von Echtzeitdaten (z. B. interaktive Sprachübertragung) in Datennetzwerken.	Cisco IP-Telefons verwenden das RTP-Protokoll, um Echtzeit-Sprachverkehr zu senden und von anderen Telefonen und Gateways zu empfangen.
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 Codec-Typen, DTMF-Erkennung oder Komfortauschen vom Cisco Unified Communications Manager oder dem Medien-Gateway im laufenden Betrieb global konfiguriert. Bei manchen SIP-Endgeräten können diese Parameter jedoch direkt auf dem Endgerät konfiguriert werden.

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
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 abbrechen.	SIP ist wie andere VoIP-Protokolle für die Funktionen des Signalübertragungs- und Sitzungsmanagements innerhalb eines Netzwerks für paketbasierte Telefonie zuständig. Mittels Signalübertragung können Anrufinformationen über Netzwerkgrenzen hinweg transportiert werden, während das Sitzungsmanagement die Steuerung der Attribute eines End-to-End-Anrufs ermöglicht.  Cisco IP-Telefons unterstützen das SIP-Protokoll sowohl beim Betrieb im reinen IPv6-Modus und im reinen IPv4-Modus wie auch im kombinierten IPv4/IPv6-Modus.
Transmission Control Protocol (TCP)	TCP ist ein verbindungsorientiertes Transportprotokoll.	Cisco IP-Telefons nutzen TCP für die Verbindung mit dem Cisco Unified Communications Manager sowie für den Zugriff auf XML-Dienste.
Transport Layer Security (TLS)	TLS ist ein Standardprotokoll zum Schützen und Authentifizieren der Kommunikation.	Wenn entsprechende Sicherheitseinstellungen konfiguriert sind, verwenden Cisco IP-Telefons das TLS-Protokoll zum sicheren Registrieren beim Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP ermöglicht die Dateiübertragung über das Netzwerk.  Auf dem Cisco IP-Telefon ermöglicht TFTP das Abrufen einer für den Telefontyp spezifischen Konfigurationsdatei.	Für TFTP muss im Netzwerk ein TFTP-Server vorhanden sein, den der DHCP-Server automatisch identifizieren kann. Wenn das Telefon einen anderen als den vom DHCP-Server festgelegten TFTP-Server verwenden soll, müssen Sie die IP-Adresse dieses TFTP-Servers manuell über das Menü „Netzwerkkonfiguration“ des Telefons zuweisen.  Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.
User Datagram Protocol (UDP)	UDP ist ein verbindungsloses Protokoll für die Übertragung von Datenpaketen.	Dieses Protokoll wird ausschließlich für RTP-Datenströme verwendet. Von der SIP-Signalübertragung der Telefone wird UDP nicht unterstützt.

Weitere Informationen zur Unterstützung von LLDP-MED können Sie dem „Whitepaper LLDP-MED and Cisco Discovery Protocol“ (LLDP-MED und das Cisco Discovery Protocol) entnehmen, das unter folgender Adresse abrufbar ist:

[http://www.cisco.com/en/US/tech/tk652/tk701/technologies\\_white\\_paper0900aecd804cd46d.shtml](http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml)

#### Verwandte Themen

[802.1X-Authentifizierung](#), auf Seite 114

[Netzwerkeinstellungen konfigurieren](#)

[Überprüfung des Telefons beim Starten](#), auf Seite 66

[VLAN-Interaktion](#), auf Seite 22

[Cisco Unified Communications Manager-Interaktion](#), auf Seite 22

[Cisco Unified Communications Manager Express-Interaktion](#), auf Seite 23

[Audio- und Videoport-Bereiche einrichten](#), auf Seite 192

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

## VLAN-Interaktion

Das Cisco IP-Telefon enthält einen internen Ethernet-Switch, über den Pakete an das Telefon, an den Computerport und an den Netzwerkport auf der Rückseite des Telefons weitergeleitet werden können.

Wenn ein Computer an den Computerport angeschlossen ist, verwenden der Computer und das Telefon dieselbe physische Verbindung mit dem Switch und denselben Port am Switch. Dies wirkt sich folgendermaßen auf die VLAN-Konfiguration im Netzwerk aus:

- Die derzeit vorhandenen VLANs können auf IP-Subnetz-Basis konfiguriert werden. Möglicherweise sind jedoch keine zusätzlichen IP-Adressen verfügbar, die dem Telefon im gleichen Subnetz wie andere Geräte, die sich mit dem gleichen Port verbinden, zugewiesen werden können.
- Durch den bei Telefonen mit VLAN-Unterstützung vorhandenen Datenverkehr wird möglicherweise die Qualität des VoIP-Datenverkehrs verringert.
- Die Netzwerksicherheit meldet möglicherweise einen Bedarf zur Trennung des VLAN-Sprachdatenverkehrs vom VLAN-Datenverkehr.

Diese Probleme können Sie lösen, indem Sie den Sprachdatenverkehr in ein separates VLAN verlegen. Der Switch-Port, an den das Telefon angeschlossen ist, wird für separate VLANs für Folgendes konfiguriert:

- Weiterleitung des Sprachdatenverkehrs zum und vom IP-Telefon (zusätzliches VLAN z. B. in der Cisco Catalyst 6000-Serie)
- Datenverkehr zum und vom PC, der über den Computerport des IP-Telefons an den Switch angeschlossen ist (systemeigenes VLAN)

Durch die Verlegung der Telefone in ein separates, zusätzliches VLAN wird die Qualität des Sprachdatenverkehrs verbessert, und Sie können eine große Anzahl von Telefonen zu einem bestehenden Netzwerk hinzufügen, das eigentlich nicht genügend IP-Adressen für alle Telefone besitzt.

Weitere Informationen finden Sie in der Dokumentation für den Cisco Switch. Außerdem finden Sie Informationen zu Switches unter folgender URL:

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

## 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 Konferenzzanrufe 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 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 xv

## 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.

Sowohl der Sitzungsleitungsmodus als auch der erweiterte Leitungsmodus werden im CME-Modus unterstützt.

# 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.

# Übersicht über den Startvorgang des Telefons

Beim Herstellen einer Verbindung mit dem VoIP-Netzwerk durchläuft das Cisco IP-Telefon einen Standardstartvorgang. Je nach Netzwerkkonfiguration kommen nicht alle der folgenden Schritte bei Ihrem Cisco IP-Telefon zur Anwendung.

1. Schließen Sie das Telefon zur Stromversorgung an den Switch an. Wenn ein Telefon keine externe Stromzufuhr bezieht, sorgt der Switch für die interne Stromversorgung über das angeschlossene Ethernet-Kabel.
2. (Nur für Cisco IP-Telefon 8861 und 8865 im Wireless LAN) Führen Sie einen Scan nach einem Access Point durch. Cisco IP-Telefon 8861 und 8865 scannen mit dem Funksignal den HF-Bereich. Das Telefon durchsucht die Netzwerkprofile und scannt nach Access Points, die eine passende SSID und einen passenden Authentifizierungstyp enthalten. Das Telefon ordnet sich dem Access Point mit dem höchsten RSSI zu, der mit dem Netzwerkprofil übereinstimmt.
3. (Nur für Cisco IP-Telefon 8861 und 8865 im Wireless LAN) Authentifizieren Sie sich am Access Point. Das Cisco IP-Telefon startet den Authentifizierungsvorgang. In der folgenden Tabelle wird der Authentifizierungsvorgang beschrieben:

Authentifizierungstyp	Schlüsselverwaltungsoptionen	Beschreibung
Offen	Keine	Jedes Gerät kann sich beim Access Point authentifizieren. Als zusätzliche Sicherheitsmaßnahme können Sie optional die statische WEP-Verschlüsselung verwenden.



Authentifizierungstyp	Schlüsselverwaltungsoptionen	Beschreibung
Gemeinsamer Schlüssel	Keine	Das Telefon verschlüsselt den Text mithilfe des WEP-Schlüssels, und der Access Point muss den WEP-Schlüssel verifizieren, mit dem der Text verschlüsselt wurde, bevor der Netzwerkzugriff verfügbar ist.
PEAP oder EAP-FAST	Keine	Der RADIUS-Server authentifiziert den Benutzernamen und das Kennwort, bevor der Netzwerkzugriff verfügbar ist.

4. Laden Sie das gespeicherte Telefon-Image. Beim Startvorgang führt das Telefon ein Bootstrapladeprogramm aus, mit dem ein im Flash-Speicher gespeichertes Telefonfirmware-Image geladen wird. Dieses Image verwendet das Telefon zur Initialisierung der Soft- und Hardware.
5. Konfigurieren Sie das VLAN. Wenn das Cisco IP-Telefon mit einem Cisco Catalyst-Switch verbunden ist, informiert der Switch das Telefon nun über das Sprach-VLAN, das auf dem Switch definiert ist. Das Telefon muss die VLAN-Mitgliedschaft kennen, bevor es mit der DHCP-Anfrage (Dynamic Host Configuration Protocol) nach einer IP-Adresse fortfahren kann.
6. Rufen Sie eine IP-Adresse ab. Wenn das Cisco IP-Telefon die IP-Adresse über DHCP erhält, startet das Telefon eine entsprechende Anfrage an den DHCP-Server. Wenn Sie in Ihrem Netzwerk kein DHCP verwenden, müssen Sie jedem Telefon lokal eine statische IP-Adresse zuweisen.
7. Rufen Sie die CTL-Datei ab. Der TFTP-Server speichert die CTL-Datei. Diese Datei enthält die für die Herstellung einer sicheren Verbindung zwischen dem Telefon und Cisco Unified Communications Manager erforderlichen Zertifikate.  
Weitere Informationen hierzu finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
8. Rufen Sie die ITL-Datei ab. Das Telefon ruft die ITL-Datei nach der CTL-Datei ab. Die ITL-Datei enthält die Zertifikate der für das Telefon vertrauenswürdigen Entitäten. Die Zertifikate werden für die Authentifizierung einer sicheren Verbindung zu den Servern oder einer von den Servern signierten digitalen Signatur verwendet. Cisco Unified Communications Manager 8.5 und höher unterstützt die ITL-Datei.
9. Konfigurieren Sie den Zugriff auf einen TFTP-Server. Der DHCP-Server weist nicht nur eine IP-Adresse zu, er leitet das Cisco IP-Telefon auch an einen TFTP-Server weiter. Wenn das Telefon eine statisch definierte IP-Adresse besitzt, müssen Sie den TFTP-Server lokal auf dem Telefon konfigurieren. Das Telefon kontaktiert den TFTP-Server dann direkt.


**Hinweis**

Sie können auch einen alternativen TFTP-Server zuweisen, der anstelle des vom DHCP-Protokoll zugewiesenen Servers verwendet werden soll.

10. Rufen Sie die Konfigurationsdatei ab. Der TFTP-Server besitzt Konfigurationsdateien, in denen die Parameter für das Herstellen einer Verbindung zu Cisco Unified Communications Manager und andere Informationen für das Telefon definiert sind.
11. Stellen Sie eine Verbindung mit Cisco Unified Communications Manager her. In der Konfigurationsdatei ist festgelegt, wie das Cisco IP-Telefon mit Cisco Unified Communications Manager kommuniziert,

und es wird eine Software-ID für das Telefon bereitgestellt. Nachdem das Telefon die Datei vom TFTP-Server abgerufen hat, versucht es, eine Verbindung mit der Cisco Unified Communications Manager-Version mit der höchsten Priorität in der Liste herzustellen.

Wenn das Sicherheitsprofil des Telefons für die sichere Signalisierung (verschlüsselt oder authentifiziert) konfiguriert ist und Cisco Unified Communications Manager auf den sicheren Modus eingestellt ist, stellt das Telefon eine TLS-Verbindung her. Andernfalls stellt das Telefon eine nicht sichere TCP-Verbindung her.

Wenn das Telefon manuell zur Datenbank hinzugefügt wurde, wird es von Cisco Unified Communications Manager identifiziert. Wenn das Telefon nicht manuell zur Datenbank hinzugefügt wurde und die automatische Registrierung in Cisco Unified Communications Manager aktiviert ist, versucht das Telefon, sich selbst automatisch in der Cisco Unified Communications Manager-Datenbank zu registrieren.



---

**Hinweis** Wenn Sie den CTL-Client konfiguriert haben, ist die automatische Registrierung deaktiviert. In diesem Fall müssen Sie das Telefon manuell zur Cisco Unified Communications Manager-Datenbank hinzufügen.

---

#### Verwandte Themen

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

## Externe Geräte

Wir empfehlen die Verwendung von qualitativ hochwertigen, externen Geräten, die gegen unerwünschte RF-Signale (Radiofrequenz) und AF-Signale (Audiofrequenz) geschirmt sind. Externe Geräte sind beispielsweise Headsets, Kabel und Steckverbinder.

Je nach der Qualität dieser Geräte und deren Abstand zu anderen Geräten wie Mobiltelefonen oder Funkgeräten, kann trotzdem ein geringes Rauschen auftreten. In diesen Fällen empfehlen wir eine oder mehrere der folgenden Maßnahmen:

- Vergrößern Sie den Abstand zwischen dem externen Gerät und der RF- oder AF-Signalquelle.
- Verlegen Sie die Anschlusskabel des externen Geräts in einem möglichst großen Abstand zur RF- oder AF-Signalquelle.
- Verwenden Sie für das externe Gerät abgeschirmte Kabel oder Kabel mit hochwertiger Abschirmung und hochwertigen Anschlusssteckern.
- Kürzen Sie das Anschlusskabel des externen Geräts.
- Führen Sie die Kabel des externen Geräts durch einen Ferritkern oder eine ähnliche Vorrichtung.

Cisco kann keine Garantie für die Leistung von externen Geräten, Kabeln und Steckern übernehmen.



---

**Vorsicht** Verwenden Sie in EU-Ländern ausschließlich externe Lautsprecher, Mikrofone und Headsets, die mit der EU-Richtlinie 89/336/EWG konform sind.

---

## Informationen zum USB-Port

Cisco IP-Telefon 8851, 8851NR, 8861, 8865 und 8865NR unterstützen maximal fünf Geräte, die an den einzelnen USB-Ports angeschlossen sind. Jedes an das Telefon angeschlossene Gerät wird bei der Anzahl der maximal zulässigen Geräte berücksichtigt. Ihr Telefon kann beispielsweise am seitlichen Anschluss fünf USB-Geräte und am hinteren Anschluss fünf zusätzliche USB-Standardgeräte unterstützen. Viele USB-Produkte von Drittherstellern zählen jedoch als mehrere USB-Geräte, beispielsweise kann ein Gerät, das einen USB-Hub und ein Headset enthält, als zwei USB-Geräte zählen. Weitere Informationen hierzu finden Sie in der Dokumentation für das jeweilige USB-Gerät.



### Hinweis

- Hubs ohne Stromversorgung werden nicht unterstützt; Hubs mit Stromversorgung mit mehr als vier Ports werden ebenfalls nicht unterstützt.
- USB-Headsets, die über einen USB-Hub an das Telefon angeschlossen sind, werden nicht unterstützt.

Jedes an das Telefon angeschlossene Erweiterungsmodul wird als USB-Gerät gezählt. Wenn drei Tastenerweiterungsmodule an das Telefon angeschlossen sind, zählen diese als drei USB-Geräte.

## 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.

### Verwandte Themen

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

## Verhalten des Telefons bei Netzwerküberlastung

Alles, was zu einer Verschlechterung der Netzwerkleistung führt, kann auch die Audio- und Videoqualität 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.

## Telefonverhalten in einem Netzwerk mit zwei Netzwerk Routern

Die Cisco IP-Telefon 8800-Serie verwendet eine Firewall zum Schutz vor Cyber-Angriffen wie z. B. einem Man-in-the-Middle-Angriff. Diese Firewall kann nicht deaktiviert werden. Wenn Sie Ihr Netzwerk mit zwei Netzwerk Routern im gleichen Subnetz und IP-Umleitung konfigurieren, kann dies dazu führen, dass der Datenverkehr auf einem Telefon gestoppt wird.

Die Telefon-Firewall stoppt den Datenverkehr, da dieses Netzwerk-Setup einem Man-in-the-Middle-Angriff ähnelt. Das Telefon empfängt Umleitungspakete für verschiedene Ziel-IPs in einem anderen Subnetz als das Telefon. Das Telefon befindet sich in einem Netzwerk mit mehreren Routern, und der Standardrouter sendet Datenverkehr an einen zweiten Router.

Wenn Sie den Verdacht haben, dass der Datenverkehr durch die Firewall gestoppt wurde, überprüfen Sie die Telefonprotokolle. Suchen Sie nach einer Benachrichtigung mit Fehlercode 1, die während eines Verbindungsversuchs vom Betriebssystem ausgegeben wurde. Eine der möglichen Signaturen lautet:

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

Ein Netzwerk mit zwei Netzwerk Routern im gleichen Subnetz und IP-Umleitung ist keine gängige Konfiguration. Wenn Sie dieses Netzwerk-Setup verwenden, sollten Sie in Betracht ziehen, nur einen Router in einem Subnetz zu verwenden. Wenn jedoch zwei Netzwerk Router im gleichen Subnetz erforderlich sind, deaktivieren Sie die IP-Umleitung auf dem Router, und starten Sie das Telefon neu.

## 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](#).



## KAPITEL 3

# Cisco IP-Telefon-Hardware

- [Telefonübersicht, auf Seite 29](#)
- [Cisco IP Phone 8811, auf Seite 31](#)
- [Cisco IP-Telefons 8841 und 8845, auf Seite 32](#)
- [Cisco IP-Telefons 8851 und 8851NR, auf Seite 33](#)
- [Cisco IP-Telefons 8861, 8865 und 8865NR, auf Seite 35](#)
- [Tasten und Hardware, auf Seite 36](#)
- [Die Kamera Ihres Videotelefons schützen, auf Seite 39](#)

## Telefonübersicht

Die Cisco IP-Telefon 8800-Serie ermöglicht die Sprachkommunikation über ein IP-Netzwerk (Internetprotokoll). Die Funktionen eines Cisco IP-Telefon ähneln denen anderer digitaler Bürotelefone: Sie können Anrufe tätigen und Funktionen wie Stummschaltung, Halten, Anrufübergabe usw. nutzen. Da Ihr Telefon zudem mit dem Datennetzwerk verbunden ist, bietet es erweiterte IP-Telefoniefunktionen, z. B. den Zugriff auf Netzwerkinformationen und -dienste sowie anpassbare Funktionen und Dienste.

Cisco IP-Telefon 8811 verfügt über ein LCD-Graustufendisplay. Cisco IP-Telefons 8841, 8845, 8851, 8851NR, 8861, 8865 und 8865NR weisen ein 24-Bit-LCD-Farbdisplay auf.

Die Anzahl der verfügbaren Leitungstasten ist begrenzt, wenn Sie weitere Funktionen zu den Leitungstasten hinzufügen. Sie können nicht mehr Funktionen als Leitungstasten zu Ihrem Telefon hinzufügen.

Cisco IP-Telefone haben folgende Funktionen:

- Programmierbare Funktionstasten, die bis zu fünf Leitungen im Sitzungsleitungsmodus bzw. bis zu 10 Leitungen im erweiterten Leitungsmodus unterstützen
- Umfassende Videofunktionen (nur Cisco IP-Telefons 8845, 8865 und 8865NR)
- Gigabit Ethernet-Verbindung
- Bluetooth-Unterstützung für kabellose Headsets (nur Cisco IP-Telefons 8845, 8851, 8861 und 8865. Diese Funktion wird auf Cisco IP-Telefon 8811, 8841, 8851NR und 8865NR nicht unterstützt.)
- Unterstützung für ein externes Mikrofon und externe Lautsprecher (nur Cisco IP-Telefon 8861, 8865 und 8865NR)
- Netzwerkverbindungen per Wi-Fi (nur Cisco IP-Telefon 8861 und 8865. Auf Cisco IP-Telefon 8865NR wird Wi-Fi nicht unterstützt.)

- USB-Ports:
  - Ein USB-Port für Cisco IP-Telefon 8851 und 8851NR
  - Zwei USB-Ports für Cisco IP-Telefon 8861, 8865 und 8865NR

Cisco IP-Telefon 8845, 8865 und 8865NR unterstützen Videoanrufe mit einer integrierten Videokamera. Verwenden Sie diese Funktion für die Zusammenarbeit mit Freunden und Kollegen oder für Videokonferenzen über das Telefon.



---

**Hinweis** Bewahren Sie die Box und die Verpackung für das Cisco IP-Telefon 8845, 8865 und 8865NR auf. Die Kameras dieser Telefone sind zerbrechlich. Wenn Sie das Telefon an einen anderen Standort bewegen, sollten Sie das Telefon in die Originalverpackung packen, um die Kamera zu schützen. Weitere Informationen hierzu finden Sie unter [Die Kamera Ihres Videotelefons schützen, auf Seite 39](#).

---

Ein Videoanruf umfasst folgende Funktionen:

- BiB – Sie können vier Positionen auswählen: Unten rechts, oben rechts, unten links und oben links. Sie können BiB auch deaktivieren.
- Wechseln – Wechselt die Ansichten in der BiB-Ansicht. Der Softkey „Wechseln“ ist deaktiviert, wenn BiB ausgeschaltet ist.
- Selbstansichtsvideo – Wählen Sie die Selbstansicht aus, um Ihr Bild wie im Video dargestellt anzuzeigen.
- Video-UI und Konferenz/Übertragung initiieren – Wählen Sie diese Option aus, um eine Konferenz zu starten.

Weitere Informationen zu Videoanrufen finden Sie im *Benutzerhandbuch für die Cisco IP-Telefon 8800-Serie* sowie in der Dokumentation für Ihre jeweilige Cisco Unified Communications Manager-Version.

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
- iSAC



**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.

#### **Verwandte Themen**

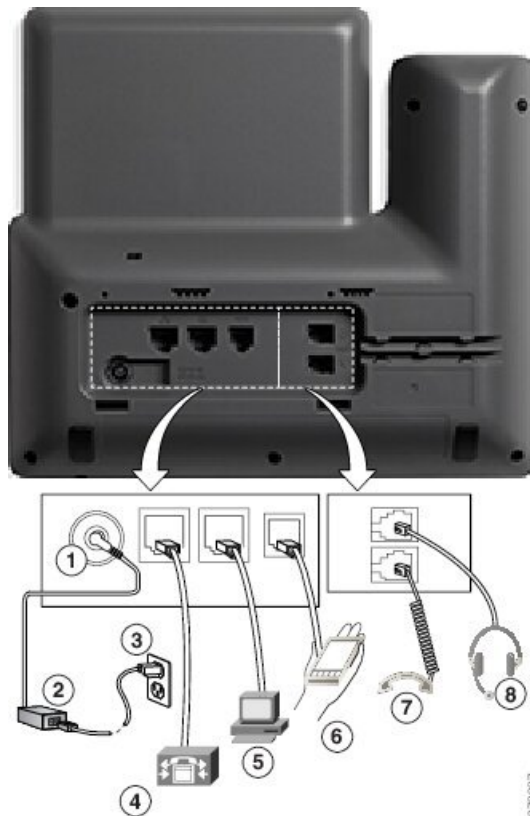
[Dokumentation Cisco Unified Communications Manager](#), auf Seite xv

## **Cisco IP Phone 8811**

Im folgenden Abschnitt werden die Merkmale von Cisco IP Phone 8811 beschrieben.

### **Verbindungen mit Multiplattform-Telefonen der Serie**

Schließen Sie das Telefon an das IP-Telefonienetzwerk des Unternehmens an, wie in der folgenden Abbildung dargestellt.



1	Netzkabel-Port (Gleichstrom, 48 V)	5	Access-Port (10/100/1000 PC)
2	Netzteil mit Wechselstromeingang und Gleichstromausgang (optional)	6	AUX-Port
3	Wechselstrom-Netzstecker (optional)	7	Höreranschluss
4	Netzwerk-Port (10/100/1000 SW), kompatibel mit IEEE 802.3at	8	Analoger Headset-Port (optional)



**Hinweis** Cisco IP Phone 8811 unterstützt kein Erweiterungsmodul.

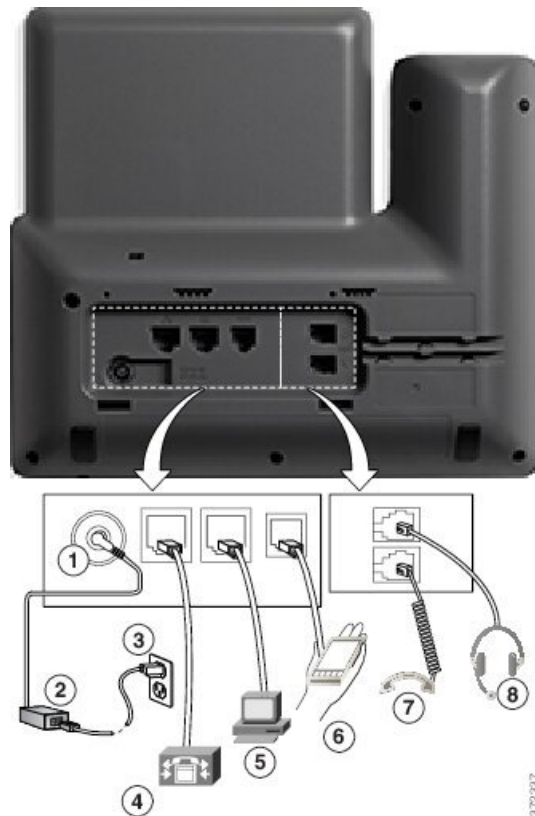
## Cisco IP-Telefons 8841 und 8845

Im folgenden Abschnitt werden die Merkmale der Cisco IP-Telefons 8841 und 8845 beschrieben.

### Telefonanschlüsse

Schließen Sie Ihr Telefon an das IP-Telefonienetzwerk des Unternehmens an. Orientieren Sie sich hierbei an der folgenden Abbildung.





1	Netzstecker-Port (Gleichstrom, 48 V)	5	Access-Port (10/100/1000 PC)
2	Netzteil mit Wechselstromeingang und Gleichstromausgang (optional)	6	AUX-Port
3	Wechselstrom-Netzstecker (optional)	7	Höreranschluss
4	Netzwerk-Port (10/100/1000 SW), kompatibel mit IEEE 802.3at	8	Analoger Headset-Port (optional)



**Hinweis** Cisco IP-Telefon 8841 und 8845 unterstützen kein Erweiterungsmodul.

## Cisco IP-Telefons 8851 und 8851NR

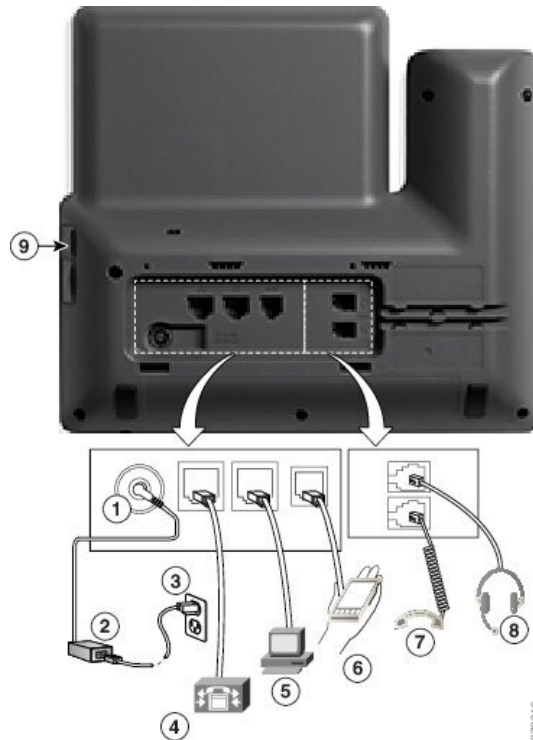
Im folgenden Abschnitt werden die Merkmale der Cisco IP-Telefons 8851 und 8851NR beschrieben.



**Hinweis** Das Cisco IP-Telefon 8851NR unterstützt Bluetooth nicht. Ansonsten unterstützen die Cisco IP-Telefons 8851 und 8851NR die gleichen Funktionen.

## Verbindungen mit dem

Schließen Sie Ihr Telefon an das IP-Telefonienetzwerk des Unternehmens an, wie in der folgenden Abbildung dargestellt.



1	Netzstecker-Port (Gleichstrom, 48 V)	6	AUX-Port
2	Netzteil mit Wechselstromeingang und Gleichstromausgang (optional)	7	Höreranschluss
3	Wechselstrom-Netzstecker (optional)	8	Analoger Headset-Port (optional)
4	Netzwerk-Port (10/100/1000 SW), kompatibel mit IEEE 802.3at	9	USB-Port
5	Access-Port (10/100/1000 PC)		



**Hinweis** Jeder USB-Port unterstützt den Anschluss von maximal fünf unterstützten und nicht unterstützten Geräten. Jedes Gerät, das an das Telefon angeschlossen ist, wird bei der Anzahl der maximal zulässigen Geräte berücksichtigt. Beispielsweise kann das Telefon am seitlichen Port fünf USB-Geräte (wie zwei Erweiterungsmodule, ein Headset, einen Hub und ein anderes Standard-USB-Gerät) unterstützen. Viele USB-Produkte von Drittherstellern zählen jedoch als mehrere USB-Geräte, beispielsweise kann ein Gerät, das einen USB-Hub und ein Headset enthält, als zwei USB-Geräte zählen. Weitere Informationen hierzu finden Sie in der Dokumentation für das jeweilige USB-Gerät.

# Cisco IP-Telefons 8861, 8865 und 8865NR

Im folgenden Abschnitt werden die Merkmale der Cisco IP-Telefons 8861, 8865 und 8865NR beschrieben.

## Telefonanschlüsse

Schließen Sie Ihr Telefon an das IP-Telefonienetzwerk des Unternehmens an, wie in der folgenden Abbildung dargestellt.



1	Netzstecker-Port (Gleichstrom, 48 V)	7	Höreranschluss
2	Netzteil mit Wechselstromeingang und Gleichstromausgang (optional)	8	Analoger Headset-Port (optional)
3	Wechselstrom-Netzstecker (optional)	9	USB-Port
4	Netzwerk-Port (10/100/1000 SW), kompatibel mit IEEE 802.3at	10	Audio-Ein-/Ausgang
5	Access-Port (10/100/1000 PC)	11	USB-Port
6	AUX-Port		



**Hinweis** Jeder USB-Port unterstützt den Anschluss von maximal fünf unterstützten und nicht unterstützten Geräten. Jedes Gerät, das an das Telefon angeschlossen ist, wird bei der Anzahl der maximal zulässigen Geräte berücksichtigt. Beispielsweise kann das Telefon am seitlichen Port fünf USB-Geräte (wie zwei Erweiterungsmodule, ein Headset, ein Hub und ein anderes Standard-USB-Gerät) und am rückwärtigen Port fünf zusätzliche Standard-USB-Geräte unterstützen. Viele USB-Produkte von Drittherstellern zählen jedoch als mehrere USB-Geräte, beispielsweise kann ein Gerät, das einen USB-Hub und ein Headset enthält, als zwei USB-Geräte zählen. Weitere Informationen hierzu finden Sie in der Dokumentation für das jeweilige USB-Gerät.

## Tasten und Hardware

Die Cisco IP Phone 8800-Serie hat zwei verschiedene Hardwaretypen:

- Cisco IP-Telefon 8811, 8841, 8851, 8851NR und 8861 haben keine Kamera.
- Cisco IP-Telefon 8845, 8865 und 8865NR sind mit einer integrierten Kamera ausgestattet.

Die folgende Abbildung zeigt Cisco IP-Telefon 8845.

**Abbildung 1: Tasten und Hardware des Cisco IP-Telefon 8845**







In der folgenden Tabelle werden die Tasten der Cisco IP-Telefon 8800-Serie beschrieben.

**Tabelle 18: Cisco IP-Telefon 8800-Serie – Tasten**

1	Hörer mit Leuchtanzeige	Zeigt einen eingehenden Anruf (rot blinkend) oder eine neue Voicemail (rot leuchtend) an.
2	Kamera Nur Cisco IP-Telefon 8845, 8865 und 8865NR	Verwendung der Kamera für Videoanrufe.

3	Programmierbare Funktionstasten und Leitungstasten	 Zugriff auf Ihre Telefonleitungen, Funktionen und Anrufsitzungen. Die Anzahl der verfügbaren Leitungstasten ist begrenzt, wenn Sie weitere Funktionen zu den Leitungstasten hinzufügen. Sie können nicht mehr Funktionen als Leitungstasten zu Ihrem Telefon hinzufügen. Weitere Informationen finden Sie im Abschnitt „Softkey-, Leitungs- und Funktionstasten“ im Kapitel „Cisco IP-Telefon – Hardware“.
4	Softkeys	 Zugriff auf Funktionen und Dienste. Weitere Informationen finden Sie im Abschnitt „Softkey-, Leitungs- und Funktionstasten“ im Kapitel „Cisco IP-Telefon – Hardware“.
5	<b>Zurück</b> , Navigationsbereich und <b>Freigabe</b>	<b>Zurück</b>  Kehrt zum vorherigen Bildschirm oder Menü zurück. Navigationsbereich  Navigationsrad und <b>Auswahl-Taste</b> – Blättert durch Menüs, markiert Elemente und wählt das markierte Element aus. <b>Freigabe</b>  Beendet einen verbundenen Anruf oder eine Sitzung.
6	<b>Halten/Fortsetzen, Konferenz und Übergabe</b>	<b>Halten/Fortsetzen</b>  Hält einen aktiven Anruf und setzt den gehaltenen Anruf fort. <b>Konferenz</b>  Initiiert einen Konferenzanruf. <b>Übergabe</b>  Übergibt einen Anruf.
7	<b>Lautsprecher, Stummschaltung und Headset</b>	<b>Lautsprecher</b>  Schaltet den Lautsprecher ein bzw. aus. Wenn der Lautsprecher aktiviert ist, leuchtet die Taste. <b>Stummschaltung</b>  Schaltet das Mikrofon ein bzw. aus. Wenn das Mikrofon stummgeschaltet ist, leuchtet die Taste. <b>Headset</b>  Schaltet das Headset ein. Wenn das Headset aktiviert ist, leuchtet die Taste. Um den Headset-Modus zu verlassen, nehmen Sie den Hörer ab oder wählen Sie <b>Lautsprecher</b>  aus.





8	<b>Kontakte, Anwendungen und Nachrichten</b>	<p><b>Kontakte</b>  Greift auf persönliche Verzeichnisse und Firmenverzeichnisse zu.</p> <p><b>Anwendungen</b>  Greift auf die Anrufliste, Benutzervoreinstellungen, Telefoneinstellungen und Modellinformationen zu.</p> <p><b>Nachrichten</b>  Ruft das Voicemail-System automatisch an.</p>
9	<b>Lautstärke-Taste</b>	 Passt die Lautstärke des Hörers, des Headsets und des Lautsprechers (abgenommen) sowie des Ruftons (aufgelegt) an.



## Softkey-, Leitungs- und Funktionstasten

Sie können die Funktionen Ihres Telefons wie folgt verwenden:

- Softkeys ermöglichen Ihnen den Zugriff auf die Funktionen, die auf dem Bildschirm über dem Softkey angezeigt werden. Die Softkeys ändern sich abhängig vom Vorgang, den Sie gerade ausführen. Der Softkey **Mehr ...** zeigt an, dass weitere Funktionen verfügbar sind.
- Die Funktions- und Leitungstasten, die sich an der Seite des Bildschirms befinden, ermöglichen Ihnen den Zugriff auf die Telefonfunktionen und Telefonleitungen.
  - Funktionstasten – Verwenden Sie diese Tasten für Funktionen wie **Kurzwahl** oder **Anrufübernahme** und zum Anzeigen Ihres Status auf einer anderen Leitung.
  - Leitungstasten: Verwenden Sie die Leitungstasten, um einen Anruf anzunehmen oder einen gehaltenen Anruf fortzusetzen. Wenn die Leitungstasten nicht für einen aktiven Anruf verwendet werden, initiieren sie Telefonfunktionen, um beispielsweise verpasste Anrufe anzuzeigen.

Durch das Aufleuchten der Funktions- und Leitungstasten wird der Status angezeigt.

LED-Farbe und Status	Normaler Leitungsmodus: Leitungstasten	Normaler Leitungsmodus: Funktionstasten Erweiterter Leitungsmodus
 Konstant grün leuchtende LED	Aktiver Anruf oder bidirektionaler Intercom-Anruf, gehaltener Anruf, Privatfunktion aktiviert	Aktiver Anruf oder bidirektionaler Intercom-Anruf, Privatfunktion aktiviert
 Grün blinkende LED	Nicht zutreffend	Anruf in der Warteschleife
 Konstant gelb leuchtende LED	Eingehender Anruf, zurückgestellter Anruf, unidirektionaler Intercom-Anruf, bei einer Sammelanschlussgruppe angemeldet	Unidirektionaler Intercom-Anruf, bei einer Sammelanschlussgruppe angemeldet
 Gelb blinkende LED	Nicht zutreffend	Eingehender Anruf, zurückgestellter Anruf

LED-Farbe und Status	Normaler Leitungsmodus: Leitungstasten	Normaler Leitungsmodus: Funktionstasten Erweiterter Leitungsmodus
 Konstant rot leuchtende LED	Remote-Leitung wird verwendet, Remote-Leitung wird gehalten, Ruhfunktion aktiv	Remote-Leitung wird verwendet, Ruhfunktion aktiv
 Rot blinkende LED	Nicht zutreffend	Anruf wird extern gehalten

Der Administrator kann einige Funktionen als Softkeys oder Funktionstasten konfigurieren. Sie können auch mit Softkeys oder zugeordneten Tasten auf einige Funktionen zugreifen.

## Die Kamera Ihres Videotelefons schützen

Die Kamera Ihres Videotelefons ist zerbrechlich und kann während des Transports des Telefons kaputtgehen.

### Vorbereitungen

Sie benötigen eine der folgenden Optionen:

- Original-Telefonbox und das Verpackungsmaterial
- Verpackungsmaterial wie Schaumstoff oder Luftpolsterfolie

### Prozedur

#### Schritt 1

Wenn Sie die Originalbox haben:

- Platzieren Sie den Schaumstoff so auf der Kamera, dass die Linse gut geschützt ist.
- Legen Sie das Telefon in die Originalbox.

#### Schritt 2

Wenn Sie die Box nicht mehr haben, unwickeln Sie das Telefon sorgfältig mit Schaumstoff oder Luftpolsterfolie, um die Kamera zu schützen. Achten Sie darauf, dass der Schaumstoff die Kamera auf jeder Seite schützt und umgibt, damit nichts gegen die Kamera gedrückt und die Kamera beim Transport nicht beschädigt werden kann.







## TEIL II

# Installation des Cisco IP-Telefon

- [Installation des Cisco IP-Telefon, auf Seite 43](#)
- [Cisco Unified Communications Manager – Telefonkonfiguration, auf Seite 69](#)
- [Verwaltung des Selbstservice-Portals, auf Seite 83](#)





## KAPITEL 4

# Installation des Cisco IP-Telefon

---

- Netzwerkkonfiguration überprüfen, auf Seite 43
- Aktivierungscode-Integration für lokale Telefone, auf Seite 44
- Aktivierungscode-Integration mit mobilem und Remotezugriff, auf Seite 45
- Aktivieren der automatischen Registrierung für Telefone, auf Seite 45
- Cisco IP-Telefon installieren, auf Seite 47
- Telefon über die Einrichtungsmenüs einrichten, auf Seite 49
- Wireless LAN auf dem Telefon aktivieren, auf Seite 51
- Netzwerkeinstellungen konfigurieren, auf Seite 59
- Überprüfung des Telefons beim Starten, auf Seite 66
- Telefonservices für Benutzer konfigurieren, auf Seite 66
- Telefonmodell eines Benutzers ändern, auf Seite 67

## Netzwerkkonfiguration überprüfen

Wenn ein neues IP-Telefonssystem 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 xv

# 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 Aktivierungscode 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 Aktivierungscode 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-Telefon 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 verwendet werden. 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-Telefon 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-Telefon 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**.
- 

# Cisco IP-Telefon installieren

Nach dem Verbinden des Telefons mit dem Netzwerk wird das Telefon gestartet, und das Gerät wird bei Cisco Unified Communications Manager registriert. Um die Installation des Telefons fertigzustellen, konfigurieren Sie die Netzwerkeinstellungen auf dem Telefon; dabei ist zu berücksichtigen, ob Sie den DHCP-Dienst aktivieren oder deaktivieren.

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.



---

**Hinweis** Bevor Sie externe Geräte verwenden, lesen Sie [Externe Geräte, auf Seite 26](#).

---

Weitere Informationen zur Installation von Zubehör finden Sie im *Handbuch für Zubehör der Cisco IP-Telefon 7800- und 8800-Serie für Cisco Unified Communications Manager*.

Wenn Sie nur ein LAN-Kabel an Ihrem Schreibtisch haben, können Sie das Telefon über den SW-Port an das LAN anschließen und dann den Computer mit dem PC-Port verbinden. Weitere Informationen hierzu finden Sie unter [Netzwerkverbindung über das Telefon und einen Computer nutzen, auf Seite 49](#).

Sie können auch zwei Telefone miteinander verketteten. Verbinden Sie den PC-Port des ersten Telefons mit dem SW-Port des zweiten Telefons.



---

**Vorsicht** Verbinden Sie die SW- und PC-Ports nicht mit dem LAN.

---

## Prozedur

---

### Schritt 1

Wählen Sie die Stromquelle für das Telefon aus:

- Power over Ethernet (PoE)
- Externes Netzteil

Weitere Informationen hierzu finden Sie unter [Stromversorgung des Telefons, auf Seite 16](#).

### Schritt 2

Schließen Sie den Hörer an den Höreranschluss an und drücken Sie das Kabel in die Führung im Telefon.

Der breitbandfähige Hörer wurde speziell für Cisco IP-Telefon entworfen. Der Hörer verfügt über eine Leuchtanzeige, die eingehende Anrufe und wartende Sprachnachrichten signalisiert.

**Vorsicht** Wenn das Kabel nicht in die Führung am Telefon gedrückt wird, kann die Leiterplatte Schaden nehmen. Die Kabelführung reduziert die Belastung des Anschlusses und der Leiterplatte.

### Schritt 3

Schließen Sie ein Headset oder ein Wireless-Headset an. Sie können ein Headset zu einem späteren Zeitpunkt anschließen.

Drücken Sie das Kabel in die Kabelführung.

**Vorsicht** Wenn das Kabel nicht in die Kabelführung am Telefon gedrückt wird, kann die Leiterplatte im Telefon Schaden nehmen. Die Kabelführung reduziert die Belastung des Anschlusses und der Leiterplatte.

### Schritt 4

Verbinden Sie ein nicht gekreuztes Ethernet-Kabel vom Switch zum Netzwerk-Port am Cisco IP-Telefon, der die Beschriftung 10/100/1000 SW trägt. Im Lieferumfang jedes Cisco IP-Telefon ist ein Ethernet-Kabel enthalten.

Verwenden Sie Kabel der Kategorie 3, 5, 5e oder 6 für 10 Mbps Verbindungen; Kategorie 5, 5e oder 6 für 100 Mbps Verbindungen und Kategorie 5e oder 6 für 1000 Mbps Verbindungen. Weitere Informationen finden Sie unter [Pin-Belegungen für Netzwerk- und Computerports, auf Seite 14](#).

### Schritt 5

Schließen Sie ein nicht gekreuztes Ethernet-Kabel von einem anderen Netzwerkgerät (z. B. einem Desktop-Computer), am PC-Port des Cisco IP-Telefon an. Sie können ein Netzwerkgerät zu einem späteren Zeitpunkt anschließen.

Verwenden Sie Kabel der Kategorie 3, 5, 5e oder 6 für 10 Mbps Verbindungen; Kategorie 5, 5e oder 6 für 100 Mbps Verbindungen und Kategorie 5e oder 6 für 1000 Mbps Verbindungen. Weitere Informationen finden Sie unter [Pin-Belegungen für Netzwerk- und Computerports, auf Seite 14](#).

### Schritt 6

Wenn sich das Telefon auf einem Schreibtisch befindet, passen Sie den Ständer an. Bei einem an der Wand befestigten Telefon muss die Hörerstation möglicherweise eingestellt werden, damit der Hörer nicht aus seiner Halterung rutscht.

### Schritt 7

Überwachen Sie den Startprozess des Telefons. Bei diesem Schritt werden dem Telefon eine primäre und eine sekundäre Verzeichnisnummer sowie Funktionen hinzugefügt, die Verzeichnisnummern zugeordnet sind, außerdem wird überprüft, ob das Telefon ordnungsgemäß konfiguriert ist.

### Schritt 8

Wenn Sie die Netzwerkeinstellungen auf dem Telefon konfigurieren, können Sie unter Verwendung von DHCP oder manuell eine IP-Adresse für das Telefon angeben.

Siehe [Netzwerkeinstellungen konfigurieren, auf Seite 59](#) und [Netzwerkconfiguration, auf Seite 243](#).

### Schritt 9

Aktualisieren Sie das Telefon mit dem aktuellen Firmware-Image.



Firmware-Updates über die WLAN-Schnittstelle dauern länger als Updates über die verkabelte Schnittstelle (abhängig von der Qualität und Bandbreite der drahtlosen Verbindung). Einige Updates können über eine Stunde dauern.

**Schritt 10** Tätigen Sie Anrufe mit Cisco IP-Telefon, um sicherzustellen, dass das Telefon richtig funktioniert.

Siehe das *Benutzerhandbuch für das Cisco IP Phone 8800-Serie*.

**Schritt 11** Informieren Sie die Benutzer über die Verwendung der Telefone und die Konfiguration der Telefonoptionen. Durch diesen Schritt wird sichergestellt, dass Benutzer hinreichend informiert sind, um ihr Cisco IP-Telefon umfassend zu nutzen.

---

## Netzwerkverbindung über das Telefon und einen Computer nutzen

Sowohl Ihr Telefon als auch Ihr Computer müssen mit dem Netzwerk verbunden sein, damit dies funktioniert. Wenn Sie nur einen Ethernet-Port haben, können Ihre Geräte die Netzwerkverbindung gemeinsam nutzen.

### Vorbereitungen

Der Administrator muss den PC-Port in Cisco Unified Communications Manager aktivieren, bevor Sie ihn verwenden können.

### Prozedur

---

**Schritt 1** Schließen Sie den Telefon-SW-Port mit einem Ethernet-Kabel an das LAN an.

**Schritt 2** Schließen Sie Ihren Computer mit einem Ethernet-Kabel an den PC-Port des Telefons an.

---

## Telefon über die Einrichtungsmenüs einrichten

Cisco IP-Telefon enthält die folgenden Konfigurationsmenüs:

- **Netzwerk-Setup:** Bietet Optionen zum Anzeigen und Konfigurieren von Netzwerkeinstellungen, wie z. B. Nur IPv4, Nur IPv6, WLAN und Ethernet.
- **Ethernet-Setup:** Die Menüelemente in diesem Untermenü bieten Konfigurationsoptionen zum Konfigurieren des Cisco IP-Telefon über ein Ethernet-Netzwerk.
- **WLAN-Client-Einrichtung:** Die Menüelemente in diesem Untermenü bieten Konfigurationsoptionen zum Konfigurieren des Cisco IP-Telefon über das drahtlose lokale Netzwerk (WLAN). Nur Cisco IP-Telefon 8861 und 8865 unterstützen Wi-Fi.



---

**Hinweis** Der Telefonport am PC ist deaktiviert, wenn Wi-Fi auf dem Telefon aktiviert ist.

---

- **IPv4-Setup und IPv6-Setup:** Diese Untermenüs im Menü „Ethernet-Setup“ und im Menü „WLAN-Client-Einrichtung“ bieten zusätzliche Netzwerkooptionen.

- **Sicherheits-Setup:** Bietet Optionen zum Anzeigen und Konfigurieren von Sicherheitseinstellungen, wie z. B. Sicherheitsmodus, Vertrauensliste und 802.1X-Authentifizierung.

Bevor Sie die Optionseinstellungen im Menü „Netzwerk-Setup“ ändern können, müssen Sie die Optionen zum Bearbeiten entsperren.





**Hinweis** Sie können festlegen, ob ein Telefon auf das Menü Einstellungen oder die Optionen in diesem Menü unter Verwendung der Felder Zugriff auf Einstellungen im Fenster Telefonkonfiguration von Cisco Unified Communications Manager-Verwaltung zugreifen kann. Im Feld „Zugriff auf Einstellungen“ werden die folgenden Werte akzeptiert:

- **Aktiviert:** Erlaubt den Zugriff auf das Menü Einstellungen.
- **Deaktiviert:** Verhindert den Zugriff auf das Menü Einstellungen.
- **Eingeschränkt:** Erlaubt den Zugriff auf das Menü Benutzereinstellungen und das Speichern von Lautstärkeinstellungen. Verhindert den Zugriff auf andere Optionen im Menü Einstellungen.

Wenn Sie eine Option im Menü „Administrator Einst.“ nicht aufrufen können, überprüfen Sie die Einstellungen im Feld „Zugriff auf Einstellungen“.

### Prozedur

- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Administratoreinstellungen** aus.
- Schritt 3** Wählen Sie **Netzwerk-Setup** oder **Sicherheits-Setup**.
- Schritt 4** Geben Sie Ihre Benutzer-ID und ggf. Ihr Kennwort ein, und klicken Sie auf **Anmelden**.
- 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** Drücken Sie zum Beenden eines Menüs **Beenden** oder den Zurück-Pfeil .

## Anwenden eines Telefonkennworts

Sie können ein Kennwort für das Telefon festlegen. In diesem Fall können an den Verwaltungsoptionen auf dem Telefon ohne Kennworteingabe auf dem Telefonbildschirm „Administratoreinstellungen“ keine Änderungen vorgenommen werden.

### 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 vom Telefon

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

- Verwenden Sie die Pfeile auf dem Navigationsrad, um die Felder zu markieren, die Sie bearbeiten möchten, und drücken Sie **Auswählen** auf dem Navigationsrad, 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 bei falscher Eingabe den Pfeil-Softkey . Dieser Softkey löscht die Zeichen links vom Cursor.
- Drücken Sie **Abbruch**, bevor Sie **Speich.** drücken, um alle von Ihnen vorgenommenen Änderungen zu verwerfen.
- Zum Eingeben einer IP-Adresse geben Sie Werte in vier bereits getrennt vorgegebene Segmente ein. Wenn Sie die Ziffern ganz links vor dem ersten Punkt eingegeben haben, springen Sie mithilfe des Pfeils nach rechts zum nächsten Segment. Der auf die Ziffern ganz links folgende Punkt wird automatisch eingefügt.
- 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.

**Verwandte Themen**

[Standardmäßiges Zurücksetzen](#), auf Seite 279

[Anwenden eines Telefonkennworts](#), auf Seite 50

## Wireless LAN auf dem Telefon aktivieren

Bevor Sie ein Wireless LAN einrichten, überprüfen Sie, ob Ihr Telefon die WLAN-Nutzung unterstützt. Die Cisco IP-Telefons 8861 und 8865 unterstützen eine Wireless LAN-Bereitstellung. Das Cisco IP-Telefon 8865NR unterstützt kein Wireless LAN.

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

Wenn Sie die Wi-Fi-Verbindung für Sprache aktiviert haben und den EAP-FAST- oder PEAP-Sicherheitsmodus verwenden, authentifizieren Sie das Wi-Fi-Netzwerk mit der WLAN-Anmeldungsanwendung. Zur Authentifizierung im WLAN-Netzwerk können Sie WEP, PSK und offene Sicherheitsmodi verwenden.

Für Wi-Fi-Benutzer wird eine Fast-Secure-Roaming-Methode empfohlen.



**Hinweis** Der Telefonport am PC ist deaktiviert, wenn Wi-Fi auf dem Telefon aktiviert ist.

Ausführliche Informationen zur Konfiguration finden Sie im *Cisco IP-Telefon 8800 Wireless LAN Deployment Guide* (WLAN-Bereitstellungshandbuch für das Cisco IP-Telefon 8800) unter:

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


Das *Cisco IP-Telefon 8800 Wireless LAN Deployment Guide* (WiFi-Bereitstellungshandbuch) enthält folgende 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 **Anwendungen** .
- Schritt 2** Navigieren Sie zu **Administratoreinstellungen > Netzwerk-Setup > WLAN-Client-Einrichtung > Netzwerkname**.  
Daraufhin wird eine Liste der verfügbaren Wireless Access Points angezeigt, mit denen Sie eine Verbindung herstellen können.
- Schritt 3** Aktivieren Sie das Wireless-Netzwerk.
- 

## Wireless LAN über Cisco Unified Communications Manager einrichten

Für das Cisco Wireless IP-Telefon 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 Bürotelefon**.
- 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**.

## Telefon für ein WLAN konfigurieren

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** Der Telefonport am PC ist deaktiviert, wenn Wi-Fi auf dem Telefon aktiviert ist.



**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 die Cisco IP-Telefon 8800-Serie*, 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>

Über das Feld **Vom Benutzer änderbar** im Wireless LAN-Profil wird die Möglichkeit des Benutzers zum Konfigurieren von Sicherheitsmodi auf dem Telefon gesteuert. Wenn ein Benutzer Felder nicht ändern kann, werden diese grau angezeigt.

### Vorbereitungen

Konfigurieren Sie das Wireless LAN in Cisco Unified Communications Manager.

### Prozedur

#### Schritt 1

Drücken Sie **Anwendungen** .

#### 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 19: Menüoptionen für die WLAN-Client-Konfiguration**

Option	Beschreibung	Änderung
Netzwerkname	Gibt die SSIP (Service Set Identifier) an, eine eindeutige ID für den Zugriff auf Wireless Access Points. Zeigt eine Liste der verfügbaren Wireless Access Points an.	Siehe <a href="#">Netzwerkeinstellungen konfigurieren</a> auf <a href="#">Seite 59</a> .
Nur IPv4-Setup	Im Konfigurations-Untermenü „IPv4-Setup“ können Sie folgende Aktionen ausführen: <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> Weitere Informationen zu den IPv4-Adressfeldern finden Sie unter <a href="#">IPv4-Felder</a> , auf <a href="#">Seite 61</a> .	Führen Sie einen Bildlauf zu „IPv4-Setup“ und drücken Sie dann <b>Auswahl</b> .
Nur IPv6-Setup	Im Konfigurations-Untermenü „IPv6-Setup“ können Sie folgende Aktionen ausführen: <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> Weitere Informationen zu den IPv6-Adressfeldern finden Sie unter <a href="#">IPv6-Felder</a> , auf <a href="#">Seite 63</a> .	Führen Sie einen Bildlauf zu „IPv6-Setup“ und drücken Sie dann <b>Auswahl</b> .

Option	Beschreibung	Änderung
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="#">Netzwerkeinstellungen konfigurieren</a> auf <a href="#">Seite 59</a> .

**Schritt 4** Drücken Sie auf **Speichern**, um Änderungen vorzunehmen, oder drücken Sie 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.



**Hinweis** Bei Telefonen, die mithilfe von Mobil- und Remote Access über Expressway mit dem Cisco Unified Communications Manager verbunden werden, können keine Wi-Fi-Profile verwendet werden. Da Sie die SSID, den Authentifizierungsmodus und die Anmeldeinformationen für das Telefon des Benutzers nicht kennen, können Sie kein Wireless LAN-Profil für dessen Telefon konfigurieren.

### 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.

**Hinweis** Das Feld **Netzwerkzugriffsprofil** wird von den Cisco IP-Telefonen 8861 und 8865 nicht unterstützt.

**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**.

---

# Netzwerkeinstellungen konfigurieren

## Prozedur

- 
- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie zum Zugreifen auf das Menü „Netzwerkeinstellungen“ **Administratoreinstellungen > Netzwerk-Setup**.
- Schritt 3** Legen Sie die Felder fest, wie in [Felder des Ethernet-Setup, auf Seite 59](#) beschrieben.
- Schritt 4** Nachdem Sie die Felder konfiguriert haben, wählen Sie **Übernehmen** und **Speichern**.
- Schritt 5** Startet das Telefon neu.
- 

## Felder des Ethernet-Setup

Das Menü „Netzwerk-Setup“ enthält Felder und Untermenüs für IPv4 und IPv6. Um einige Felder zu ändern, muss zunächst DHCP deaktiviert werden.

Beim Herstellen einer VPN-Verbindung werden die Ethernet-Datenfelder überschrieben.

**Tabelle 20: Optionen im Menü „Ethernet-Setup“**

Eintrag	Typ	Beschreibung
IPv4-Setup	Menü	Weitere Informationen finden Sie im Abschnitt „IPv4-Felder“. Diese Option wird nur angezeigt, wenn das Telefon im reinen IPv4-Modus konfiguriert ist.
IPv6-Setup	Menü	Weitere Informationen finden Sie im Abschnitt „IPv6-Felder“.
MAC-Adresse	Zeichenfolge	Eindeutige MAC-Adresse (Media Access Control) des Telefons. Wird nur angezeigt. Der Wert kann nicht konfiguriert werden.
Domänenname	Zeichenfolge	Name der DNS-Domäne (Domain Name System), in der sich das Telefon befindet. Deaktivieren Sie DHCP, um dieses Feld ändern zu können.

Eintrag	Typ	Beschreibung
VLAN-ID (Betrieb)		<p>Zusätzliches VLAN (Virtual Local Area Network), das auf einem Cisco C ist, bei dem das Telefon registriert ist.</p> <p>Wenn das zusätzliche VLAN oder das Verwaltungs-VLAN konfiguriert ist, muss ein Wert angegeben werden.</p> <p>Wenn das Telefon kein zusätzliches VLAN erhalten hat, gibt diese Option keinen Wert an.</p> <p>Das Telefon übernimmt nicht das Betriebs-VLAN vom Verwaltungs-VLAN, wenn das Discovery Protocol oder Link Level Discovery Protocol Media Endpoint Discovery verwendet wird.</p> <p>Wenn Sie eine VLAN-ID manuell zuweisen möchten, verwenden Sie die Option „VLAN-ID (Verwaltung)“.</p>
VLAN-ID (Verwaltung)		<p>Zusätzliches VLAN, bei dem das Telefon registriert ist.</p> <p>Wird nur verwendet, wenn das Telefon kein zusätzliches VLAN vom Switch erhält. Wenn dieser Wert ignoriert wird, wird kein Wert angegeben.</p>
PC-VLAN		<p>Ermöglicht dem Telefon, mit Switches anderer Hersteller zusammenzuarbeiten. Die Option „VLAN-ID (Verwaltung)“ muss festgelegt sein, damit diese Option funktionieren kann.</p>
SW-Port-Setup	<p>Autom. aushandeln</p> <p>1000 Voll</p> <p>100 Halb</p> <p>10 Halb</p> <p>10 Voll</p>	<p>Geschwindigkeit und Duplex-Status des Netzwerk-Ports. Gültige Werte sind:</p> <ul style="list-style-type: none"> <li>• Autom. aushandeln (Standard)</li> <li>• 1000 Voll: 1000-BaseT/Vollduplex</li> <li>• 100 Halb: 100-BaseT/Halbduplex</li> <li>• 100 Voll: 100-BaseT/Vollduplex</li> <li>• 10 Halb: 10-BaseT/Halbduplex</li> <li>• 10 Voll: 10-BaseT/Vollduplex</li> </ul> <p>Wenn das Telefon mit einem Switch verbunden ist, konfigurieren Sie den Switch mit den Einstellungen für Geschwindigkeit wie das Telefon, oder konfigurieren Sie den Switch mit der automatischen Aushandlung.</p> <p>Entsperren Sie die Netzwerkkonfigurationsoptionen, wenn Sie diese Einstellungen ändern. Wenn Sie die Einstellung dieser Option ändern, müssen Sie die Option „Port-Setup“ auf die gleiche Einstellung festlegen.</p>

Eintrag	Typ	Beschreibung
PC-Port-Setup	Autom. aushandeln 1000 Voll 100 Halb 10 Halb 10 Voll	<p>Geschwindigkeit und Duplex-Status des PC-Zugangs-Ports. Zulässig</p> <ul style="list-style-type: none"> <li>• Autom. aushandeln (Standard)</li> <li>• 1000 Voll:1000-BaseT/Vollduplex</li> <li>• 100 Halb: 100-BaseT/Halbduplex</li> <li>• 100 Voll:100-BaseT/Vollduplex</li> <li>• 10 Halb: 10-BaseT/Halbduplex</li> <li>• 10 Voll:10-BaseT/Vollduplex</li> </ul> <p>Wenn das Telefon mit einem Switch verbunden ist, konfigurieren Sie gleichen Einstellungen für Geschwindigkeit wie das Telefon, oder konfigurieren Sie das Telefon für die automatische Aushandlung.</p> <p>Entsperren Sie die Netzwerkkonfigurationsoptionen, wenn Sie diese ändern. Wenn Sie die Einstellung ändern, müssen Sie die Option „SW-Port-Konfiguration“ festlegen.</p> <p>Wenn Sie die Einstellungen für mehrere Telefone gleichzeitig konfigurieren, konfigurieren Sie die Remote-Portkonfiguration im Fenster „Konfiguration des Bürotelefons (des Bürotelefons)“.</p> <p>Wenn die Ports in der Cisco Unified Communications Manager-Verwaltung Remote-Portkonfiguration konfiguriert sind, können die Daten nicht auf</p>

## IPv4-Felder

Tabelle 21: Optionen im Menü „IPv4-Setup“

Eintrag	Beschreibung
DHCP aktiviert	<p>Legt fest, ob DHCP für das Telefon aktiviert oder deaktiviert ist.</p> <p>Wenn DHCP aktiviert ist, weist der DHCP-Server dem Telefon eine IP-Adresse zu. Wenn DHCP deaktiviert ist, muss der Administrator dem Telefon manuell eine IP-Adresse zuweisen.</p> <p>Weitere Informationen hierzu finden Sie unter <a href="#">Telefon für die Verwendung von DHCP einrichten, auf Seite 65</a> und <a href="#">Telefon so einrichten, dass kein DHCP verwendet wird, auf Seite 65</a>.</p>
IP-Adresse	<p>Die IP-Adresse (Internet Protocol) des Telefons.</p> <p>Wenn Sie mit dieser Option eine IP-Adresse zuweisen, müssen Sie auch eine Subnetzmaske und einen Standardrouter zuweisen. Siehe die Optionen „Subnetzmaske“ und „Standardrouter“ in dieser Tabelle.</p>
Subnetzmaske	Die vom Telefon verwendete Subnetzmaske.
Standardrouter	Der vom Telefon verwendete Standardrouter.
DNS-Server 1 DNS-Server 2 DNS-Server 3	Der primäre DNS-Server (DNS Server 1) und optionale DNS-Backupserver (DNS-Server 2 und 3), die das Telefon verwendet.

Eintrag	Beschreibung
Alternativer TFTP-Server	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). Wenn Sie in Ihrem Netzwerk kein DHCP verwenden und diesen Server ändern möchten, müssen Sie die Option „TFTP-Server 1“ verwenden.</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.</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 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>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:</p> <ol style="list-style-type: none"> <li>1. Manuell zugewiesene IPv4-TFTP-Server</li> <li>2. Manuell zugewiesene IPv6-TFTP-Server</li> <li>3. Durch DHCP zugewiesene TFTP-Server</li> <li>4. Durch DHCPv6 zugewiesene TFTP-Server</li> </ol> <p><b>Hinweis</b> Weitere Informationen zur CTL- und ITL-Datei finden Sie im <i>Cisco Unified Communications Manager Security Guide</i> (Sicherheitshandbuch zu Cisco Unified Communications Manager).</p>

Eintrag	Beschreibung
TFTP Server 2	<p>Optionaler Backup-TFTP-Server, den das Telefon verwendet, wenn der primäre TFTP-Server nicht verfügbar ist.</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 eine der beiden Dateien entsperren, bevor Sie die Änderungen an der Option „TFTP-Server 2“ speichern können. In diesem Fall löscht das Telefon eine der beiden Dateien, 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>Wenn Sie vergessen, die CTL- oder ITL-Datei zu entsperren, können Sie die Adresse von TFTP-Server 2 in einer der beiden Dateien ändern und diese dann durch Drücken von „Löschen“ im Menü „Sicherheitskonfiguration“ löschen. Von der Adresse des neuen TFTP-Servers 2 wird eine neue CTL- oder ITL-Datei heruntergeladen.</p> <p>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:</p> <ol style="list-style-type: none"> <li>1. Manuell zugewiesene IPv4-TFTP-Server</li> <li>2. Manuell zugewiesene IPv6-TFTP-Server</li> <li>3. Durch DHCP zugewiesene TFTP-Server</li> <li>4. Durch DHCPv6 zugewiesene TFTP-Server</li> </ol> <p><b>Hinweis</b> Weitere Informationen zur CTL- oder ITL-Datei finden Sie im Cisco Unified Communications Manager Security Guide (Sicherheitshandbuch zu Cisco Unified Communications Manager).</p>
BOOTP-Server	Gibt an, ob das Telefon die IP-Adresse von einem BOOTP-Server statt von einem DHCP-Server erhalten hat.
DHCP-Adressfreigabe	<p>Gibt die von DHCP zugewiesene IP-Adresse frei.</p> <p>Dieses Feld kann bearbeitet werden, wenn DHCP aktiviert ist. Wenn Sie das Telefon aus dem VLAN entfernen und die IP-Adresse für die erneute Zuweisung freigeben möchten, setzen Sie diese Option auf „Ja“, und drücken Sie „Übernehmen“.</p>

## IPv6-Felder

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 erhält und verwendet das Telefon eine IPv4-Adresse und eine IPv6-Adresse. Diese Adressen können je nach Bedarf verwendet werden. Für die Anrufsteuerungssignale verwendet das Telefon entweder die IPv4- oder die IPv6-Adresse.

Weitere Informationen zur IPv6-Bereitstellung finden Sie im [IPv6-Bereitstellungshandbuch für Cisco Collaboration Systems Release 12.0](#).

Sie können IPv6 über eines der folgenden Menüs einrichten:

- Bei deaktiviertem WLAN: **Ethernet-Setup > IPv6-Setup**
- Bei aktiviertem WLAN: **WLAN-Client-Einrichtung > IPv6-Setup**

Verwenden Sie das Tastenfeld des Telefons, um eine IPv6-Adresse einzugeben oder zu bearbeiten. Drücken Sie zum Eingeben eines Doppelpunkts die Sternchentaste (\*) auf dem Tastenfeld. Drücken Sie zum Eingeben der Hexadezimalziffern a, b und c die 2 auf dem Tastenfeld, führen Sie einen Bildlauf bis zur gewünschten Ziffer durch, wählen Sie sie aus, und drücken Sie dann **Eingabe**. Drücken Sie zum Eingeben der Hexadezimalziffern d, e und f die 3 auf dem Tastenfeld, führen Sie einen Bildlauf bis zur gewünschten Ziffer durch, wählen Sie sie aus, und drücken Sie dann **Eingabe**.

In der folgenden Tabelle werden die für IPv6 relevanten Informationen aus dem Menü „IPv6“ beschrieben.

**Tabelle 22: Menüoptionen für das „IPv6-Setup“**

Eintrag	Standardwert	Beschreibung
DHCPv6 aktiviert	Ja	Gibt die Methode an, die das Telefon zur IP-Adressierung verwendet. Wenn DHCPv6 aktiviert ist, ruft das Telefon ein Router-Advertisement vom IPv6-fähigen Router an und weist sich eine zustandsbehaftete (vom DHCPv6-Server) IP-Adresse zu.
IPv6-Adresse	::	Zeigt die aktuelle reine IPv6-Adresse des Telefons an. Eine gültige IPv6-Adresse ist 128 Bit lang. <ul style="list-style-type: none"> <li>• Acht durch Doppelpunkte getrennte Hexadezimalziffern</li> <li>• Komprimiertes Format zur Zusammenfassung von Nullen, das durch einen doppelten Doppelpunkt (::) dargestellt wird</li> </ul> Wenn die IP-Adresse mithilfe dieser Option konfiguriert ist, weist der Standardrouter zu.
Länge des IPv6-Präfixes	0	Zeigt die aktuelle Präfixlänge für das Subnetz an. Die Subnetz-Präfixlänge besteht aus einer Zahl von 0 bis 127.
IPv6 – Standardrouter	::	Zeigt den vom Telefon verwendeten Standard-IPv6-Standardrouter an. Um den Standardrouter einzugeben, drücken Sie <b>Eingabe</b> .
IPv6 – DNS-Server 1	::	Zeigt den primären DNSv6-Server an, dem das Telefon die IP-Adresse festzulegen.
IPv6 – DNS-Server 2	::	Zeigt den sekundären DNSv6-Server an, dem das Telefon die IP-Adresse festzulegen.




Eintrag	Standardwert	Beschreibung
IPv6 – Alternativer TFTP-Server	Nein	Ermöglicht dem Benutzer einen alternativen TFTP-Server festzulegen.
IPv6 – TFTP-Server 1	::	Zeigt den primären IPv6 TFTP-Server festzulegen.
IPv6 – TFTP-Server 2	::	(Optional) Zeigt den sekundären IPv6 TFTP-Server festzulegen, wenn verfügbar ist, oder ermöglicht es dem Benutzer, einen alternativen TFTP-Server festzulegen.
IPv6-Adresse freigegeben	Nein	Ermöglicht es dem Benutzer, die IPv6-Adresse freizugeben.

## Telefon für die Verwendung von DHCP einrichten

Um DHCP zu aktivieren und zuzulassen, dass der DHCP-Server dem Cisco IP-Telefon automatisch eine IP-Adresse zuweist und das Telefon mit einem TFTP-Server verbindet, führen Sie die folgenden Schritte aus:


### Prozedur

- 
- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Verwaltungseinstellungen > Netzwerk-Setup > Ethernet-Setup > IPv4-Setup**.
- Schritt 3** Um DHCP zu aktivieren, setzen Sie „DHCP aktiviert“ auf **Ja**. DHCP ist standardmäßig aktiviert.
- Schritt 4** Um einen alternativen TFTP-Server zu verwenden, setzen Sie „Alternativer TFTP-Server“ auf **Ja**, und geben Sie die IP-Adresse für den TFTP-Server ein.
- Hinweis** Erkundigen Sie sich bei Ihrem Netzwerkverwalter, ob Sie einen alternativen TFTP-Server zuweisen sollten, anstatt den DHCP-zugewiesenen TFTP-Server zu verwenden.
- Schritt 5** Drücken Sie **Übernehmen**.
- 

## Telefon so einrichten, dass kein DHCP verwendet wird

Wenn kein DHCP verwendet wird, müssen Sie IP-Adresse, Subnetzmaske, TFTP-Server und Standardrouter lokal auf dem Telefon konfigurieren.

### Prozedur

- 
- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Verwaltungseinstellungen > Netzwerk-Setup > Ethernet-Setup > IPv4-Setup**.
- Schritt 3** So deaktivieren Sie DHCP und legen manuell eine IP-Adresse fest:
- Setzen Sie „DHCP aktiviert“ auf **Nein**.
  - Geben Sie die statische IP-Adresse für das Telefon ein.
  - Geben Sie die Subnetzmaske ein.

- d) Geben Sie die IP-Adressen für den Standardrouter ein.
- e) Setzen Sie „Alternativer TFTP-Server“ auf **Ja**, und geben Sie die IP-Adresse für TFTP-Server 1 ein.

**Schritt 4**

Drücken Sie **Übernehmen**.

## Software-Server

Der Software-Server dient zur Optimierung der Installationszeit von Firmware-Upgrades für das Telefon. Darüber hinaus wird das WAN entlastet, indem Images lokal gespeichert werden, sodass nicht bei jedem Telefon-Upgrade der WAN-Link verwendet werden muss.

Sie können den Software-Server auf die IP-Adresse oder den Namen eines anderen TFTP-Servers (abweichend von TFTP-Server 1 oder TFTP-Server 2) festlegen, über den die Telefonfirmware für Telefon-Upgrades abgerufen werden kann. Wenn die Option „Software-Server“ festgelegt ist, kontaktiert das Telefon den entsprechenden Server für das Firmware-Upgrade.

**Hinweis**

Mit der Option „Software-Server“ können Sie nur einen alternativen TFTP-Server für Telefon-Upgrades angeben. Zum Abrufen von Konfigurationsdateien verwendet das Telefon weiterhin TFTP-Server 1 oder TFTP-Server 2. Die Option „Software-Server“ ermöglicht keine Verwaltung des Prozesses oder der Dateien (z. B. Dateiübertragung, -komprimierung oder -löschung).

Der Software-Server wird über das Fenster „Konfiguration des Bürotelefons“ konfiguriert. Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **Gerät > Telefon > Konfiguration des Bürotelefons**.

## Überprüfung des Telefons beim Starten

Nachdem das Cisco IP-Telefon an die Stromzufuhr angeschlossen wurde, startet das Gerät den Diagnosevorgang und durchläuft dabei die im Folgenden beschriebenen Schritte.

1. Die Funktions- und Sitzungstasten blinken während der verschiedenen Phasen des Systemstarts nacheinander gelb und grün, während das Gerät die Hardware überprüft.
2. Auf dem Hauptbildschirm wird die Meldung `Registering to Cisco Unified Communications Manager` (Registrierung bei Cisco Unified Communications Manager) angezeigt.

Wenn das Telefon diese Phasen erfolgreich durchläuft, wurde der Startvorgang ordnungsgemäß abgeschlossen, und die **Auswahl**taste bleibt erleuchtet, bis sie ausgewählt wird.

## 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. Zu diesen Diensten gehören XML-Anwendungen und Cisco-signierte Java-Midlets, mit denen auf dem Telefon interaktive Inhalte mit Text und Grafiken angezeigt werden können. Das IP-Telefon verwaltet jeden Service als eine separate Anwendung. Diese Dienste bieten beispielsweise Informationen über das lokale Kinoprogramm, die neuesten Aktienkurse oder den aktuellen Wetterbericht.

Bevor ein Benutzer auf einen Service zugreifen kann:

- Sie müssen Cisco Unified Communications Manager-Verwaltung verwenden, 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 [Verwaltung des Selbstservice-Portals, auf Seite 83](#) für eine Übersicht der Informationen, die Sie an die Benutzer weitergeben müssen.

### Verwandte Themen

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

## 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.

Wenn Sie ein altes Telefon mit SCCP-Firmware gegen ein Modell der Cisco IP Phone der Serie 8800 austauschen, wird das neue Telefon für den Sitzungsleitungsmodus konfiguriert.

Wenn auf dem alten Telefon ein Tasten-Erweiterungsmodell konfiguriert ist, kopiert Unified CM gleichzeitig die Informationen des Erweiterungsmoduls auf das neue Telefon. Wenn der Benutzer ein kompatibles

Tastenerweiterungsmodul mit dem neuen Telefon verbindet, erhält das neue Erweiterungsmodul die Informationen des migrierten Erweiterungsmoduls.

Wenn auf dem alten Telefon ein Tasten-Erweiterungsmodell konfiguriert ist und das neue Telefon kein Erweiterungsmodul unterstützt, kopiert Unified CM die Informationen des Erweiterungsmoduls nicht.

**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 – Telefonkonfiguration

---

- [Cisco IP-Telefon einrichten, auf Seite 69](#)
- [Die MAC-Adresse des Telefons bestimmen, auf Seite 72](#)
- [Methoden zum Hinzufügen von Telefonen, auf Seite 73](#)
- [Benutzer zu Cisco Unified Communications Manager hinzufügen, auf Seite 74](#)
- [Einer Endbenutzergruppe einen Benutzer hinzufügen, auf Seite 76](#)
- [Telefone zu Benutzern zuordnen, auf Seite 77](#)
- [SRST \(Survivable Remote Site Telephony\), auf Seite 77](#)
- [E-SRST \(Enhanced Survivable Remote Site Telephony\), auf Seite 80](#)
- [Anwendungswählregeln, auf Seite 80](#)

## Cisco IP-Telefon 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-Telefon manuell in Cisco Unified Communications Manager konfigurieren. Abhängig von Ihrem System und den Benutzeranforderungen sind einige Aufgaben in diesem Verfahren optional.

Weitere Informationen zur Cisco Unified Communications Manager-Verwaltung finden Sie in der Dokumentation zu Ihrer jeweiligen 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
- Physischer Standort des Telefons
- Name oder Benutzer-ID des Telefonbenutzers

- Gerätepool
- Partition, Anrufsuchraum und Standortinformationen
- Anzahl der Leitungen und zugeordnete Verzeichnisnummern (VNs), die dem Telefon zugewiesen werden sollen
- Cisco Unified Communications Manager-Benutzer, der dem Telefon zugeordnet werden soll
- Informationen zur Telefonnutzung in Bezug auf die Telefontastenvorlage, die Telefonfunktionen, die IP-Telefondienste oder die Telefonanwendungen

Mit diesen Informationen steht Ihnen eine Liste von Konfigurationsanforderungen für die Telefoneinrichtung zur Verfügung, und Sie erkennen, welche vorbereitenden Konfigurationen Sie durchführen müssen, z. B. Telefontastenvorlagen, bevor Sie einzelne Telefone konfigurieren.

**Schritt 2** Stellen Sie sicher, dass genügend Einheitenlizenzen für Ihr Telefon vorhanden sind.

**Schritt 3** Passen Sie ggf. die Telefontastenvorlagen an, indem Sie die Anzahl der Leitungstasten, Kurzwahlstasten oder Dienst-URL-Tasten ändern. Wählen Sie **Gerät > Geräteeinstellungen > Telefontastenvorlage**, um die Vorlagen zu erstellen bzw. zu aktualisieren.

Je nach Bedarf können Sie die Tasten „Privat“, „Alle Anrufe“ oder „Mobilität“ hinzufügen.

Weitere Informationen hierzu finden Sie unter [Vorlagen für Telefontasten, auf Seite 201](#).

**Schritt 4** Definieren Sie die Gerätepools. Wählen Sie **System > Gerätepool** aus.

Gerätepools definieren allgemeine Eigenschaften für Geräte, beispielsweise die Region, die Datum/Uhrzeit-Gruppe, die Softkey-Vorlage und MLPP-Informationen.

**Schritt 5** 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 6** Definieren Sie einen Anrufsuchraum. Klicken Sie in der Cisco Unified Communications Manager-Verwaltung auf **Anrufweiterleitung > 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 Anrufsuchräume für das Gerät und die Verzeichnisnummer werden zusammen verwendet. Die Verzeichnisnummern-CSS hat Vorrang vor der Geräte-CSS.

**Schritt 7** Konfigurieren Sie ein Sicherheitsprofil für den Gerätetyp und das Protokoll. Wählen Sie **System > Sicherheit > Telefonsicherheitsprofil** aus.

**Schritt 8** Wenn Sie die erforderlichen Felder im Fenster „Telefonkonfiguration“ ausfüllen, können Sie das Telefon hinzufügen und konfigurieren. Erforderliche Felder sind durch ein Sternchen (\*) neben dem Feldnamen gekennzeichnet, z. B. MAC-Adresse und Geräte-Pool.

In diesem Schritt wird das Gerät mit den Standardeinstellungen zur Cisco Unified Communications Manager-Datenbank hinzugefügt.

Weitere Informationen zu produktspezifischen Konfigurationsfeldern finden Sie in der Schaltflächen-Hilfe „?“ im Fenster „Telefonkonfiguration“.

**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.

**Schritt 9** Wenn Sie die erforderlichen Felder im Fenster „Verzeichnisnummerkonfiguration“ ausfüllen, können Sie Verzeichnisnummern (Leitungen) auf dem Telefon hinzufügen und konfigurieren. Erforderliche Felder sind durch ein Sternchen (\*) neben dem Feldnamen gekennzeichnet, z. B. Verzeichnisnummer und Präsenzgruppe. In diesem Schritt werden primäre und sekundäre Verzeichnisnummern und zugehörige Funktionen zum Telefon hinzugefügt.

**Hinweis** Wenn Sie keine primäre Verzeichnisnummer konfigurieren, wird dem Benutzer die Meldung `Nicht bereitgestellt` auf dem Telefon angezeigt.

**Schritt 10** Konfigurieren Sie Kurzwahltasten und weisen Sie Kurzwahlnummern zu.

Im Cisco Unified Communications-Selbsthilfe-Portal können die Benutzer die Kurzwahleinstellungen auf ihrem Telefon ändern.

**Schritt 11** Konfigurieren Sie Cisco Unified IP-Telefondienste, und weisen Sie für die Bereitstellung von IP-Telefondiensten Dienste zu (optional).

Im Cisco Unified Communications-Selbsthilfe-Portal können die Benutzer Dienste auf ihrem Telefon hinzufügen oder ändern.

**Hinweis** Benutzer können den IP-Telefondienst nur abonnieren, wenn das Kontrollkästchen „Unternehmensteilnahme“ bei der Erstkonfiguration des IP-Telefondiensts in der Cisco Unified Communications Manager-Verwaltung deaktiviert ist.

**Hinweis** Einige von Cisco bereitgestellte Dienste sind als „Unternehmensteilnahme“ klassifiziert und können daher nicht von Benutzern im Selbsthilfe-Portal hinzugefügt werden. Diese Dienste befinden sich standardmäßig auf dem Telefon und können nur entfernt werden, wenn Sie sie in der Cisco Unified Communications Manager-Verwaltung deaktivieren.

**Schritt 12** Weisen Sie Dienste programmierbaren Tasten zu (optional), um den Zugriff auf einen IP-Telefondienst oder eine URL bereitzustellen.

**Schritt 13** Fügen Sie Benutzerinformationen durch die Konfiguration der erforderlichen Felder hinzu. Erforderliche Felder sind durch ein Sternchen (\*) neben dem Feldnamen gekennzeichnet, z. B. Benutzer-ID und Nachname. In diesem Schritt fügen Sie Benutzerinformationen zum globalen Verzeichnis für Cisco Unified Communications Manager hinzu.

**Hinweis** Weisen Sie ein Kennwort (für das Selbsthilfe-Portal) und eine PIN (für Cisco Anschlussmobilität und Persönliches Verzeichnis) zu.

**Hinweis** Wenn in Ihrem Unternehmen ein LDAP-Verzeichnis für die Speicherung von Informationen über Benutzer verwendet wird, können Sie Cisco Unified Communications installieren und für die Verwendung Ihres vorhandenen LDAP-Verzeichnisses konfigurieren.

**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.

- Schritt 14** Ordnen Sie einen Benutzer einer Benutzergruppe zu. In diesem Schritt weisen Sie Benutzern eine gemeinsame Liste mit Rollen und Berechtigungen zu, die für alle Benutzer in einer Benutzergruppe gelten. Administratoren können Benutzergruppen, Rollen und Berechtigungen verwalten, um die Zugriffsstufe (und damit die Sicherheitsstufe) für Systembenutzer zu steuern. Beispielsweise müssen Sie Benutzer zur Standardgruppe „Cisco CCM-Endbenutzer“ hinzufügen, damit sie Zugriff auf das Cisco Unified Communications Manager-Selbsthilfe-Portal erhalten.
- Schritt 15** Ordnen Sie einen Benutzer einem Telefon zu (optional). In diesem Schritt verleihen Sie Benutzern die Kontrolle über ihr Telefon, z. B. zum Weiterleiten von Anrufen oder Hinzufügen von Kurzwahlnummern oder Diensten. Einigen Telefone, beispielsweise Telefonen in Konferenzräumen, sind keine Benutzer zugewiesen.
- Schritt 16** Wenn Sie sich nicht bereits im Fenster „Endbenutzerkonfiguration“ befinden, wählen Sie **Benutzerverwaltung > Endbenutzer**, um einige abschließende Konfigurationsschritte durchzuführen. Navigieren Sie über die Suchfelder und die Schaltfläche **Suchen** zum Benutzer (z. B. Fritz Mustermann), und klicken Sie dann auf die Benutzer-ID, um das Fenster „Endbenutzerkonfiguration“ für den Benutzer aufzurufen.
- Schritt 17** Wählen Sie im Bildschirmbereich „Verzeichnisnummernzuordnungen“ in der Dropdownliste die primäre Erweiterung aus.
- Schritt 18** Aktivieren Sie das Kontrollkästchen **Mobilität aktivieren** unter **Mobilitätsinformationen**.
- Schritt 19** Fügen Sie diesen Benutzer im Bereich „Berechtigungsinformationen“ mithilfe der Schaltfläche „Benutzergruppe“ zu einer Benutzergruppe hinzu.  
Beispielsweise können Sie den Benutzer zu einer Gruppen hinzufügen, die als eine CCM-Standardbenutzergruppe definiert ist.
- Schritt 20** Wählen Sie zum Anzeigen aller konfigurierten Benutzergruppen **Benutzerverwaltung > Benutzergruppe**.
- Schritt 21** Aktivieren Sie im Bereich „Anschlussmobilität“ das Kontrollkästchen „Anschlussmobilität über Cluster aktivieren“, wenn der Benutzer die Berechtigung für den Dienst „Clusterübergreifende Anschlussmobilität“ besitzt.
- Schritt 22** Wählen Sie **Speichern** aus.

---

#### Verwandte Themen

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

## 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:

- Drücken Sie auf dem Telefon auf **Anwendungen** , wählen Sie **Telefoninformationen** aus, und überprüfen Sie das Feld „MAC-Adresse“.
- 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 72](#).

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

## Einzelne Telefone hinzufügen

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

### Prozedur

- 
- |                  |  |
|------------------|--|
| <b>Schritt 1</b> | Wählen Sie <b>Gerät &gt; Telefon</b> in der Cisco Unified Communications Manager-Verwaltung aus.   |
| <b>Schritt 2</b> | Klicken Sie auf <b>Neu hinzufügen</b> .  |
| <b>Schritt 3</b> | Wählen Sie den Telefentyp aus.   |
| <b>Schritt 4</b> | Wählen Sie <b>Weiter</b> aus.  |
| <b>Schritt 5</b> | Vervollständigen Sie die Informationen über das Telefon, einschließlich die MAC-Adresse.<br>Die vollständigen Anweisungen und weitere Informationen zu Cisco Unified Communications Manager finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager. |
| <b>Schritt 6</b> | Wählen Sie <b>Speichern</b> aus.   |

---

### Verwandte Themen

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

## 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 xv

## 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 75](#).
- 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 xv

## 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 Firmennummer)

**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 der Zugriff auf die wichtigsten Telefonfunktionen auch bei Verlust der WAN-Verbindungen weiterhin möglich ist. 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 unterstützter Firmware und SRST (Survivable Remote Site Telephony) finden Sie auf der Webseite *Cisco Unified Survivable Remote Site Telephony Compatibility Information* (Kompatibilitätsinformationen für SRST) unter Cisco.com (<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html>).

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

**Tabelle 23: Unterstützte SRST-Funktionen**

Funktion	Unterstützt	Hinweise
Neuer Anruf	Ja	

<b>Funktion</b>	<b>Unterstützt</b>	<b>Hinweise</b>
Anruf beenden	Ja	
Wahlwiederholung	Ja	
Anrufannahme	Ja	
Halten	Ja	
Fortsetzen	Ja	
Konferenz	Ja	
Konferenz für aktive Anrufe (Beitreten)	Nein	Der Softkey „Akt. Anrufe“ wird nicht angezeigt.
Konferenzliste	Nein	
Übergabe	Ja	
Übergabe an aktive Anrufe (direkte Übergabe)	Nein	
Automatische Anrufannahme	Ja	
Anklopfen	Ja	
Anrufer-ID	Ja	
Signalton für wartende Nachrichten	Ja	
Programmierbare Leitungstaste „Alle Anrufe“	Ja	
Programmierbare Leitungstaste „Annehmen“	Ja	
Unified-Sitzungspräsentation	Ja	Konferenz ist aufgrund anderer 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	
Programmierbare Leitungstaste „Dienst-URL“	Ja	
An Voicemail (Sofortumleitung)	Nein	Der Softkey SofUml. wird nicht angezeigt.
Leitungsfilter	Teilweise	Leitungen werden unterstützt, können jedoch nicht gemeinsam genutzt werden.
Überwachung geparkter Anrufe	Nein	Der Softkey Parken wird nicht angezeigt.
Aufschalten	Nein	Der Softkey „Aufsch.“ wird nicht angezeigt.
Erweiterte Nachrichtenanzeige	Nein	Nachrichtenzahlleisten werden auf dem Telefondisplay nicht angezeigt. Es wird nur das Symbol für wartende Nachrichten angezeigt.
Gezieltes Parken	Nein	Der Softkey wird nicht angezeigt.
BLF	Teilweise	Die BLF-Funktionstaste funktioniert wie die Kurzwahlstasten.
Halten zurücksetzen	Nein	Anrufe verbleiben für unbegrenzte Zeit in der Warteschleife.
Extern gehaltener Anruf	Nein	Anrufe werden als lokal gehaltene Anrufe angezeigt.
MeetMe	Nein	Der Softkey MeetMe wird nicht angezeigt.
Übernahme	Nein	Der Softkey führt keine Aktion aus.
Gruppenübernahme	Nein	Der Softkey führt keine Aktion aus.

Funktion	Unterstützt	Hinweise
Andere Übernahme	Nein	Der Softkey führt keine Aktion aus.
Fangschaltung	Nein	Der Softkey führt keine Aktion aus.
QRT	Nein	Der Softkey führt keine Aktion aus.
Sammelanschlussgruppe	Nein	Der Softkey führt keine Aktion aus.
Intercom	Nein	Der Softkey führt keine Aktion aus.
Mobilität	Nein	Der Softkey führt keine Aktion aus.
Privatfunktion	Nein	Der Softkey führt keine Aktion aus.
Rückruf	Nein	Der Softkey Rückruf wird nicht angezeigt.
Video	Ja	Videokonferenzen werden nicht unterstützt.
Video	Ja	Videokonferenzen werden nicht unterstützt.
Gemeinsam genutzte Leitung	Nein	
BLF-Kurzwahl	Ja	

## E-SRST (Enhanced Survivable Remote Site Telephony)

Durch Enhanced Survivable Remote Site Telephony (E-SRST) wird sichergestellt, dass verfügbare zusätzliche Telefonfunktionen weiterhin zugänglich bleiben, wenn die WAN-Verbindung getrennt wird. Neben den von SRST (Survivable Remote Site Telephony) unterstützten Funktionen unterstützt E-SRST Folgendes:

- Gemeinsam genutzte Leitung
- Besetztlampenfeld (BLF)
- Videoanrufe

Weitere Informationen zu unterstützter Firmware und SRST (Survivable Remote Site Telephony) finden Sie auf der Webseite *Cisco Unified Survivable Remote Site Telephony Compatibility Information* (Kompatibilitätsinformationen für SRST) unter Cisco.com (<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html>).

## Anwendungswählregeln

Anwendungswählregeln werden verwendet, um Nummern von mobilen Kontakten in Nummern umzuwandeln, die im Netzwerk gewählt werden können. Die Anwendungswählregeln gelten nicht, wenn der Benutzer eine Nummer manuell wählt oder die Nummer bearbeitet wird, bevor der Benutzer den Anruf tätigt.

Anwendungsregeln werden in Cisco Unified Communications Manager festgelegt.



Weitere Informationen zu Wählregeln finden Sie im *Systemkonfigurationshandbuch für Cisco Unified Communications Manager* im Kapitel zum „Konfigurieren von Wählregeln“.

## Anwendungswählregeln konfigurieren

### Prozedur

---

- Schritt 1** Navigieren Sie in der Cisco Unified Communications Manager-Verwaltung zu **Anruf-Routing > Wählregeln > Anwendungswählregeln**.
- Schritt 2** Wählen Sie **Neu hinzufügen** aus, um eine neue Anwendungswählregel zu erstellen oder eine vorhandene Anwendungswählregel zum Bearbeiten auszuwählen.
- Schritt 3** Füllen Sie die folgenden Felder aus:
- **Name** Dieses Feld enthält einen eindeutigen Namen für die Wählregel, die aus bis zu 20 alphanumerischen Zeichen und einer Kombination aus Leerzeichen, Punkten (.), Bindestrichen (-) und Unterstrichen (\_) bestehen kann.
  - **Beschreibung** Dieses Feld enthält eine kurze Beschreibung, die Sie für die Wählregel eingeben.
  - **Nummer beginnt mit** Dieses Feld enthält die Anfangsziffern der Verzeichnisnummern, für die Sie diese Anwendungswählregel übernehmen möchten.
  - **Anzahl der Ziffern** Dieses erforderliche Feld enthält die Anfangsziffern der Verzeichnisnummern, für die Sie diese Anwendungswählregel übernehmen möchten.
  - **Gesamtanzahl der zu entfernenden Ziffern** Dieses erforderliche Feld enthält die Anzahl der Ziffern, die Cisco Unified Communications Manager aus den Verzeichnisnummern entfernen soll, auf die diese Wählregel angewendet wird.
  - **Präfix mit Muster** Dieses erforderliche Feld enthält das Muster, das Verzeichnisnummern vorangestellt wird, auf die diese Anwendungswählregel angewendet wird.
  - **Priorität der Anwendungswählregel** Dieses Feld wird angezeigt, wenn Sie die Informationen für das Präfix mit Muster eingeben. In diesem Feld können Sie die Priorität der Anwendungswählregeln festlegen.
- Schritt 4** Starten Sie Cisco Unified Communications Manager neu.
-





## KAPITEL 6

# Verwaltung des Selbstservice-Portals

- [Übersicht des Selbstservice-Portals, auf Seite 83](#)
- [Den Benutzerzugriff auf das Selbstservice-Portal konfigurieren, auf Seite 83](#)
- [Die Ansicht des Selbstservice-Portals anpassen, auf Seite 84](#)

## 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 xv

## 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

# Verwaltung von Cisco IP-Telefon

- [Sicherheit von Cisco IP-Telefonen, auf Seite 87](#)
- [Anpassung des Cisco IP-Telefon, auf Seite 117](#)
- [Telefonfunktionen und Konfiguration, auf Seite 123](#)
- [Unternehmensverzeichnis und persönliches Verzeichnis, auf Seite 217](#)





## KAPITEL 7

# Sicherheit von Cisco IP-Telefonen

- [Sicherheitsverbesserungen für Ihr Telefonnetzwerk, auf Seite 87](#)
- [Unterstützte Sicherheitsfunktionen, auf Seite 88](#)

## 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>)

- *Sicherheitsüberblick für die Cisco IP-Telefon 7800- und 8800-Serien*(<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.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>)

**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 Cisco IP-Telefon 8800-Serie entspricht dem FIPS (Federal Information Processing Standard). Um ordnungsgemäß zu funktionieren, ist für den FIPS-Modus eine Schlüssellänge von 2048 Bit oder mehr erforderlich. Wenn das Zertifikat 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 auf dem Telefon angezeigt.

Wenn das Telefon über ein LSC verfügt, müssen Sie die LSC-Schlüssellänge auf 2048 Bit oder mehr aktualisieren, bevor Sie FIPS aktivieren.

Die folgende Tabelle enthält eine Übersicht der von den Telefonen unterstützten Sicherheitsfunktionen. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Um die aktuellen Sicherheitseinstellungen auf einem Telefon anzuzeigen, einschließlich Sicherheitsmodus, Vertrauensliste und 802.1X-Authentifizierung, drücken Sie auf **Anwendungen**  und wählen **Verwaltereinstellungen > Sicherheits-Setup**.

**Tabelle 24: Überblick der Sicherheitsfunktionen**

Funktion	Beschreibung
Imageauthentifizierung	<p>Signierte Binärdateien (mit Dateierweiterung „.sbn“) verhindern das Manipulieren des Firmware-Images vor dem Laden auf das Telefon.</p> <p>Wenn das Image manipuliert wurde, kann das Telefon nicht authentifiziert werden und das Image wird abgelehnt.</p>
Image-Verschlüsselung	<p>Verschlüsselte Binärdateien (mit Dateierweiterung „.sebn“) verhindern das Manipulieren des Firmware-Images vor dem Laden auf das Telefon.</p> <p>Wenn das Image manipuliert wurde, kann das Telefon nicht authentifiziert werden und das Image wird abgelehnt.</p>
Kundenseitiges Installieren von Zertifikaten	<p>Jedes Cisco IP Phone erfordert ein eindeutiges Zertifikat für die Geräteauthentifizierung. Auf den Telefonen ist bereits ein vom Hersteller installiertes Zertifikat (MIC) vorhanden, zusätzliche Sicherheit bietet jedoch die Möglichkeit, die Zertifikatinstallation in der Cisco Unified Communications Manager-Verwaltung mithilfe von CAPF (Certificate Authority Proxy Function) festzulegen. Sie können ein LSC (Locally Significant Certificate) auch über das Menü Sicherheitskonfiguration auf dem Telefon installieren.</p>

Funktion	Beschreibung
Geräteauthentifizierung	Die Geräteauthentifizierung erfolgt zwischen dem Cisco Unified Communications Manager-Server und dem Telefon, wenn jede Entität das Zertifikat der anderen Entität akzeptiert. Bestimmt, ob eine sichere Verbindung zwischen dem Telefon und Cisco Unified Communications Manager hergestellt wird, und erstellt, falls erforderlich, mit dem TLS-Protokoll einen sicheren Signalpfad zwischen den Entitäten. Der Cisco Unified Communications Manager registriert Telefone nur dann, wenn sie authentifiziert werden können.
Dateiauthentifizierung	Überprüft digital signierte Dateien, die das Telefon herunterlädt. Das Telefon validiert die Signatur, um sicherzustellen, dass die Datei nach der Erstellung nicht manipuliert wurde. Dateien, die nicht authentifiziert werden können, werden nicht in den Flash-Speicher auf dem Telefon geschrieben. Das Telefon weist diese Dateien ohne weitere Verarbeitung zurück.
Dateiverschlüsselung	Durch Verschlüsselung wird verhindert, dass bei der Übertragung einer Datei auf das Telefon vertrauliche Informationen preisgegeben werden. Außerdem validiert das Telefon die Signatur, um sicherzustellen, dass die Datei nach der Erstellung nicht manipuliert wurde. Dateien, die nicht authentifiziert werden können, werden nicht in den Flash-Speicher auf dem Telefon geschrieben. Das Telefon weist diese Dateien ohne weitere Verarbeitung zurück.
Signalauthentifizierung	Bei dieser Authentifizierung wird anhand des TLS-Protokolls überprüft, dass die Signalkomponenten während der Übertragung nicht manipuliert wurden.
MIC (Manufacturing Installed Certificate)	Auf jedem Cisco IP-Telefon ist ein eindeutiges, vom Hersteller installiertes Zertifikat (Manufacturing Installed Certificate, MIC) vorhanden, das für die Geräteauthentifizierung verwendet wird. Das MIC dient für das Telefon dauerhaft als eindeutiger Identitätsnachweis und ermöglicht dem Cisco Unified Communications Manager das Authentifizieren des Telefons.
Medienverschlüsselung	Diese stellt mithilfe von SRTP sicher, dass Mediendatenströme zwischen unterstützten Geräten geschützt sind und nur der beabsichtigte Empfänger die Daten erhalten und lesen kann. Erstellt ein primäres Medien-Schlüsselpaar für die Geräte, verteilt die Schlüssel an die Geräte und schützt die Schlüssel, während diese übertragen werden.
CAPF (Certificate Authority Proxy Function)	Implementiert Teile des Prozesses für die Zertifikatsgenerierung, die für das Telefon zu verarbeitungsintensiv sind, und interagiert mit dem Telefon bei der Schlüsselgenerierung und Zertifikatsinstallation. CAPF kann konfiguriert werden, um Zertifikate im Auftrag des Telefons von kundenspezifischen Zertifizierungsstellen anzufordern oder Zertifikate lokal zu generieren.
Sicherheitsprofil	Definiert, ob das Telefon nicht sicher, authentifiziert, verschlüsselt oder geschützt ist. Die weiteren Einträge in dieser Tabelle erläutern Sicherheitsfunktionen.
Verschlüsselte Konfigurationsdateien	Ermöglicht Ihnen, den Datenschutz für Telefonkonfigurationsdateien sicherzustellen.
Optionale Webserver-Deaktivierung für Telefone	Aus Sicherheitsgründen können Sie für ein Telefon den Zugriff auf die Webseiten (diese zeigen verschiedenste Betriebsstatistiken des Telefons an) und das Selbsthilfe-Portal verhindern.

Funktion	Beschreibung
Telefonhärtung	<p>Weitere Sicherheitsoptionen, die in der Cisco Unified Communications Manager-Verwaltung festgelegt werden:</p> <ul style="list-style-type: none"> <li>• Deaktivierung des PC-Ports</li> <li>• Deaktivierung von Gratuitous ARP-Paketen</li> <li>• Deaktivierung des PC-Sprach-VLAN-Zugriffs</li> <li>• Deaktivierung des Zugriff auf die Einstellungs-menüs oder Beschränkung des Zugriffs auf ausschließlich das Voreinstellungs-menü und die Speichermöglichkeit für Lautstärkeänderungen</li> <li>• Deaktivierung des Zugriffs des Telefons auf Webseiten</li> <li>• Deaktivierung des Bluetooth-Zubehör-Ports</li> <li>• Einschränkung der TLS-Schlüssel</li> </ul>
802.1X-Authentifizierung	<p>Cisco IP-Telefon kann die 802.1X-Authentifizierung zur Anfrage und Ausführung des Netzwerkzugriffs verwenden. Weitere Informationen finden Sie unter <a href="#">802.1X-Authentifizierung, auf Seite 114</a>.</p>
Sicheres SIP-Failover für SRST	<p>Nachdem Sie eine SRST-Sicherheitsreferenz konfiguriert und anschließend die abhängigen Geräte in der Cisco Unified Communications Manager-Verwaltung zurückgesetzt haben, fügt der TFTP-Server das Zertifikat des SRST-fähigen Gateways zur Datei „cnf.xml“ hinzu und sendet diese an das Telefon. Ein sicheres Telefon verwendet eine TLS-Verbindung, um mit dem SRST-fähigen Router zu kommunizieren.</p>
Verschlüsselung des Signalisierungsverkehrs	<p>Durch diese Verschlüsselung wird gewährleistet, dass alle zwischen dem Gerät und dem Cisco Unified Communications Manager-Server ausgetauschten SIP-Signalisierungsnachrichten verschlüsselt werden.</p>
Warnung bei Aktualisierung der Vertrauensliste	<p>Wenn die auf dem Telefon vorhandene Vertrauensliste aktualisiert wird, erhält der Cisco Unified Communications Manager eine Warnmeldung, die angibt, ob die Aktualisierung erfolgreich war oder nicht. Weitere Informationen finden Sie in der nachstehenden Tabelle.</p>
AES 256-Verschlüsselung	<p>Telefone, die mit Cisco Unified Communications Manager Version 10.5(2) oder höher verbunden sind, unterstützen die AES 256-Verschlüsselung für TLS und SIP für die Signalisierung und Medienverschlüsselung. Diese Telefone können TLS 1.2-Verbindungen mit AES-256-basierten Schlüsseln, die mit SHA-2 (Secure Hash Algorithm) und FIPS (Federal Information Processing Standards) konform sind, initiieren und unterstützen. Die Schlüssel enthalten:</p> <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 Cisco Unified Communications Manager.</p>

Funktion	Beschreibung
Elliptic Curve Digital Signature Algorithm (ECDSA)-Zertifikate	Als Teil der Common Criteria(CC-)Zertifizierung hat Cisco Unified Communications Manager ECDSA-Zertifikate in Version 11.0 hinzugefügt. Dies betrifft alle Voice Operating System-(VOS-)Produkte ab Version CUCM 11.5 und höher.

In der folgenden Tabelle sind die bei Aktualisierung der Vertrauensliste ausgegebenen Warnmeldungen sowie deren Bedeutung aufgeführt. Weitere Informationen finden Sie in der Dokumentation zu Cisco Unified Communications Manager.

**Tabelle 25: Warnmeldungen bei Aktualisierung der Vertrauensliste**

Code und Meldung	Beschreibung
1 – TL_SUCCESS	Neue CTL bzw. ITL erhalten
2 – CTL_INITIAL_SUCCESS	Neue CTL erhalten, keine TL vorhanden
3 – ITL_INITIAL_SUCCESS	Neue ITL erhalten, keine TL vorhanden
4 – TL_INITIAL_SUCCESS	Neue CTL und ITL erhalten, keine TL vorhanden
5 – TL_FAILED_OLD_CTL	Aktualisierung auf neue CTL fehlgeschlagen, aber vorherige TL vorhanden
6 – TL_FAILED_NO_TL	Aktualisierung auf neue TL fehlgeschlagen, und keine frühere TL vorhanden
7 – TL_FAILED	Allgemeiner Fehler
8 – TL_FAILED_OLD_ITL	Aktualisierung auf neue ITL fehlgeschlagen, aber vorherige TL vorhanden
9 – TL_FAILED_OLD_TL	Aktualisierung auf neue TL fehlgeschlagen, aber vorherige TL vorhanden

Im Menü „Sicherheits-Setup“ sind Informationen zu verschiedenen Sicherheitseinstellungen verfügbar. Von dort aus kann auch auf das Menü „Vertrauensliste“ zugegriffen werden, und es ist angegeben, ob die CTL- bzw. ITL-Datei auf dem Telefon installiert ist.

In der folgenden Tabelle sind die im Menü „Sicherheits-Setup“ verfügbaren Optionen aufgeführt.

**Tabelle 26: Menü „Sicherheits-Setup“**

Option	Beschreibung	Änderung
Sicherheitsmodus	Zeigt den für das Telefon konfigurierten Sicherheitsmodus an.	Wählen Sie in der Cisco Unified Communications Manager-Verwaltung <b>Gerät &gt; Telefon</b> . Die Einstellung wird im Bereich „Protokollspezifische Informationen“ des Fensters zur Telefonkonfiguration angezeigt.

Option	Beschreibung	Änderung
LSC	Gibt an, ob auf dem Telefon ein für Sicherheitseinstellungen genutztes LSC (Locally Significant Certificate) installiert ist („Ja“) oder nicht („Nein“).	Informationen zum Verwalten des LSCs für das Telefon finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
Vertrauensliste	<p>Das Menü „Vertrauensliste“ beinhaltet Untermenüs für die CTL, die ITL und für signierte Konfigurationsdateien.</p> <p>Im Untermenü „CTL-Datei“ wird der Inhalt der CTL-Datei angezeigt. Im Untermenü „ITL-Datei“ wird der Inhalt der ITL-Datei angezeigt.</p> <p>Außerdem werden im Menü „Vertrauensliste“ folgende Informationen angezeigt:</p> <ul style="list-style-type: none"> <li>• CTL-Signatur: der SHA-1-Hash-Wert der CTL-Datei</li> <li>• Unified CM-/TFTP-Server: der Namen des Cisco Unified Communications Manager- und TFTP-Servers, der vom Telefon verwendet wird. Wenn für diesen Server ein Zertifikat installiert ist, wird ein Zertifikatssymbol angezeigt.</li> <li>• CAPF-Server: der Name des CAPF-Servers, den das Telefon verwendet. Wenn für diesen Server ein Zertifikat installiert ist, wird ein Zertifikatssymbol angezeigt.</li> <li>• SRST-Router: die IP-Adresse des vertrauenswürdigen SRST-Routers, den das Telefon verwenden kann. Wenn für diesen Server ein Zertifikat installiert ist, wird ein Zertifikatssymbol angezeigt.</li> </ul>	Weitere Informationen hierzu finden Sie unter <a href="#">Einrichten eines LSC (Locally Significant Certificate)</a> , auf Seite 93.
802.1X-Authentifizierung	Hier kann die 802.1X-Authentifizierung für das Telefon aktiviert werden.	Siehe <a href="#">802.1X-Authentifizierung</a> , auf Seite 114.

**Verwandte Themen**

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

## 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** Drücken Sie auf dem Telefon auf **Anwendungen** .

**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.

## Aktivieren des FIPS-Modus

### 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.


**Schritt 3** Legen Sie das Feld **FIPS-Modus** auf „Aktiviert“ fest.

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

## Anrufsicherheit

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 nur auf Verbindungen zwischen zwei Telefonen unterstützt. Einige Funktionen, beispielsweise Konferenzerufe und gemeinsam genutzte Leitungen, sind nicht verfügbar, wenn sichere Anrufe konfiguriert sind.

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 Konferenzanruf-ID

Sie können einen sicheren Konferenzanruf initiieren und die Sicherheitsstufe der Teilnehmer überwachen. Ein sicherer Konferenzanruf 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 Konferenzanrufs 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 Konferenzanrufe, 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 27: Sicherheitseinschränkungen für Konferenzanrufe**

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 <code>Sicherheit nicht erfüllt</code> , Anruf abgelehnt.
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-Telefonielösung 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. Als Authentifizierungsmethoden werden sowohl PEAP-MSCHAPV2 als auch PEAP-GTC 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-Signalkette 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 28: 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

Konfiguration des Cisco IP-Telefon	Konfiguration des Access Points			
EAP-TLS	EAP-TLS	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-GTC	PEAP-GTC	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

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>

## Authentifizierung einrichten

Führen Sie die folgenden Schritte aus, um den Authentifizierungsmodus für dieses Profil auszuwählen:

### Prozedur

**Schritt 1** Wählen Sie das zu konfigurierende Netzwerkprofil.

**Schritt 2** Wählen Sie den Authentifizierungsmodus.

**Hinweis** Je nach Auswahl müssen Sie für die Wireless-Sicherheit oder die Wireless-Verschlüsselung zusätzliche Optionen konfigurieren. Weitere Informationen finden Sie unter [WLAN-Sicherheit](#), auf Seite 98.

**Schritt 3** Klicken Sie auf **Speichern**, um die Änderung zu übernehmen.

## Wireless-Sicherheit-Anmeldeinformationen

Wenn in Ihrem Netzwerk EAP-FAST und PEAP für die Benutzerauthentifizierung verwendet werden, müssen Sie ggf. sowohl den Benutzernamen als auch das Kennwort auf dem Remote Authentication Dial-In User Service (RADIUS) und auf dem Telefon konfigurieren.



**Hinweis** Wenn im Netzwerk Domänen genutzt werden, müssen Sie den Benutzernamen mit dem Domänennamen im Format *Domäne\Benutzername* eingeben.

Die folgenden Aktionen können dazu führen, dass das vorhandene Wi-Fi-Kennwort gelöscht wird:

- Eingeben einer ungültigen Benutzer-ID oder einem ungültigen Kennwort
- Installieren einer ungültigen oder abgelaufenen Stammzertifizierungsstelle, wenn der EAP-Typ auf PEAP-MSCHAPV2 oder PEAP-GTC festgelegt ist
- Deaktivieren des EAP-Typs auf dem RADIUS-Server, der vom Telefon verwendet wird, bevor ein Telefon auf den neuen EAP-Typ geändert wurde

Um EAP-Typen zu ändern, führen Sie in der angegebenen Reihenfolge folgende Schritte durch:

- Aktivieren Sie die neuen EAP-Typen auf dem RADIUS-Server.
- Ändern Sie den EAP-Typ auf einem Telefon in den neuen EAP-Typ.

Behalten Sie die aktuelle EAP-Typ-Konfiguration auf dem Telefon, bis der neue EAP-Typ auf dem RADIUS-Server aktiviert ist. Nachdem der neue EAP-Typ auf dem RADIUS-Server aktiviert ist, können Sie den EAP-Typ des Telefons ändern. Sobald alle Telefone in den neuen EAP-Typ geändert wurden, können Sie den vorherigen EAP-Typ ggf. deaktivieren.

## Benutzername und Kennwort einrichten

Bei der Eingabe bzw. Änderung des Benutzernamens oder des Kennworts für das Netzwerkprofil müssen Sie denselben Benutzernamen und dieselbe Kennwortzeichenfolge eingeben, die auf dem RADIUS-Server konfiguriert sind. Die maximale Länge des Benutzernamens bzw. des Kennworts beträgt 64 Zeichen.

Führen Sie die folgenden Schritte aus, um den Benutzernamen und das Kennwort in den Wireless-Sicherheit-Anmeldeinformationen einzurichten:

### Prozedur

- 
- Schritt 1** Wählen Sie das Netzwerkprofil aus.
  - Schritt 2** Geben Sie im Feld „Benutzername“ den Netzwerkbenutzernamen für dieses Profil ein.
  - Schritt 3** Geben Sie im Feld „Kennwort“ die Zeichenfolge für das Netzwerkkenwort für dieses Profil ein.
  - Schritt 4** Klicken Sie auf **Speichern**, um die Änderung zu übernehmen.
- 

## Pre-shared Key – Setup

Verwenden Sie die folgenden Abschnitte, um Anweisungen zum Einrichten der vorinstallierten Schlüssel zu erhalten.

### Formate für Pre-shared Keys

Das Cisco IP-Telefon unterstützt das ASCII-Format und das Hexadezimalformat. Beim Einrichten eines WPA Pre-shared Keys müssen Sie eines dieser Formate verwenden:

### Hexadezimal

Geben Sie für Hexadezimalschlüssel 64 Hexadezimalziffern (0–9 und A–F) ein; beispielsweise AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C.

### ASCII

Geben Sie für ASCII-Schlüssel eine Zeichenfolge ein, in der die Ziffern 0–9, die Buchstaben A–Z (Groß- und Kleinbuchstaben) sowie Symbole enthalten sein können, wobei die Länge zwischen 8 und 63 Zeichen betragen muss; beispielsweise GREG12356789ZXYW.

## PSK einrichten

Führen Sie die folgenden Schritte aus, um ein PSK im Bereich für Wireless-Anmeldedaten einzurichten:

### Prozedur

- 
- |                  |   |
|------------------|---|
| <b>Schritt 1</b> | Wählen Sie das Netzwerkprofil aus, das den WPA Pre-shared Key oder den WPA2 Pre-shared Key aktiviert.     |
| <b>Schritt 2</b> | Geben Sie im Bereich "Schlüsseltyp" den entsprechenden Schlüssel ein.                                     |
| <b>Schritt 3</b> | Geben Sie im Feld „Passphrase“ bzw. „Pre-shared Key“ eine ASCII-Zeichenfolge bzw. Hexadezimalziffern ein. |
| <b>Schritt 4</b> | Klicken Sie auf <b>Speichern</b> , um die Änderung zu übernehmen.   |
- 

## Wireless-Verschlüsselung

Wenn in Ihrem Wireless-Netzwerk WEP-Verschlüsselung verwendet wird und Sie den Authentifizierungsmodus auf Offen + WEP festlegen, müssen Sie einen WEP-Schlüssel im ASCII- oder Hexadezimalformat eingeben.

Die WEP-Schlüssel für das Telefon müssen mit den WEP-Schlüsseln übereinstimmen, die dem Access Point zugewiesen sind. Das Cisco IP-Telefon und die Cisco Aironet Access Points unterstützen sowohl 40-Bit- als auch 128-Bit-Verschlüsselungsschlüssel.

### WEP-Schlüsselformate

Beim Einrichten eines WEP-Schlüssels müssen Sie eines dieser Formate verwenden:

#### Hexadezimal

Verwenden Sie für Hexadezimalschlüssel eine der folgenden Schlüssellängen:

##### 40 Bit

Sie geben eine zehnstellige Zeichenfolge für den Verschlüsselungsschlüssel ein, der aus Hexadezimalzeichen (0–9 und A–F) besteht, beispielsweise ABCD123456.

##### 128 Bit

Sie geben eine 26-stellige Zeichenfolge für den Verschlüsselungsschlüssel ein, der aus Hexadezimalzeichen (0–9 und A–F) besteht, beispielsweise AB123456789CD01234567890EF.

#### ASCII

Geben Sie für ASCII-Schlüssel eine Zeichenfolge ein, in der die Ziffern 0–9, die Buchstaben A–Z (Groß- und Kleinbuchstaben) sowie alle Symbole enthalten sein können; die Schlüsselzeichenfolge muss eine der folgenden Längen aufweisen:

**40 Bit**

Sie geben eine fünfstellige Zeichenfolge ein, beispielsweise GREG5.

**128 Bit**

Sie geben eine 13-stellige Zeichenfolge ein, beispielsweise GREGSSECRET13.

**WEP-Schlüssel einrichten**

Führen Sie die folgenden Schritte aus, um WEP-Schlüssel einzurichten.

**Prozedur**

- 
- Schritt 1** Wählen Sie das Netzwerkprofil aus, das Offen + WEP oder Gemeinsam genutzt + WEP verwendet.
- Schritt 2** Geben Sie im Bereich "Schlüsseltyp" den entsprechenden Schlüssel ein.
- Schritt 3** Wählen Sie im Bereich für die Schlüssellänge eine der folgenden Zeichenfolgelängen aus:
- 40
  - 128
- Schritt 4** Geben Sie im Feld „Verschlüsselungsschlüssel“ die entsprechende Zeichenfolge basierend auf dem ausgewählten Schlüsseltyp und der ausgewählten Schlüssellänge ein. Siehe [WEP-Schlüsselformate, auf Seite 103](#).
- Schritt 5** Klicken Sie auf **Speichern**, um die Änderung zu übernehmen.
- 

**CA-Zertifikat von ACS mithilfe der Microsoft-Zertifikatdienste exportieren**

Exportieren Sie das Stammzertifikat der Zertifizierungsstelle aus dem ACS-Server. Weitere Informationen hierzu finden Sie in der Dokumentation zur Zertifizierungsstelle oder zu RADIUS.

**Vom Hersteller installiertes Zertifikat**

Im Telefon wurde durch Cisco werksseitig ein MIC (Manufacturing Installed Certificate, vom Hersteller installiertes Zertifikat) integriert.

Während der EAP-TLS-Authentifizierung muss der ACS-Server die Vertrauenswürdigkeit des Telefons überprüfen, während das Telefon die Vertrauenswürdigkeit des ACS-Servers prüfen muss.

Zum Überprüfen des MIC müssen das Manufacturing Root Certificate (Herstellerstammzertifikat) und Manufacturing Certificate Authority Certificate (Hersteller-CA-Zertifikat) von einem Cisco IP-Telefon exportiert und auf dem Cisco ACS-Server installiert werden. Diese beiden Zertifikate sind Teil der vertrauenswürdigen Zertifikatskette, anhand der das MIC vom Cisco ACS-Server überprüft wird.

Zum Überprüfen des Cisco ACS-Zertifikats müssen ein vertrauenswürdiges untergeordnetes Zertifikat (sofern vorhanden) sowie ein Stammzertifikat (erstellt von einer Zertifizierungsstelle) auf dem Cisco ACS-Server exportiert und auf dem Telefon installiert werden. Diese Zertifikate sind Teil der vertrauenswürdigen Zertifikatskette, anhand derer die Vertrauenswürdigkeit des Zertifikats vom ACS-Server überprüft wird.



## Vom Benutzer installiertes Zertifikat

Zur Verwendung eines vom Benutzer installierten Zertifikats wird eine Anforderung zum Signieren des Zertifikats (Certificate Signing Request, CSR) generiert und zur Genehmigung an die Zertifizierungsstelle (Certificate Authority, CA) gesendet. Ein Benutzerzertifikat kann auch von der Zertifizierungsstelle ohne eine CSR generiert werden.

Im Rahmen der EAP-TLS-Authentifizierung überprüft der ACS-Server die Vertrauenswürdigkeit des Telefons, und das Telefon überprüft die Vertrauenswürdigkeit des ACS-Servers.

Zur Überprüfung der Authentizität des vom Benutzer installierten Zertifikats müssen Sie ein vertrauenswürdigen untergeordnetes Zertifikat (falls vorhanden) und ein Stammzertifikat der Zertifizierungsstelle installieren, durch die das Benutzerzertifikat auf dem Cisco ACS-Server genehmigt wurde. Diese Zertifikate sind Teil der vertrauenswürdigen Zertifikatskette, die zur Überprüfung der Vertrauenswürdigkeit des vom Benutzer installierten Zertifikats verwendet wird.

Zur Überprüfung des Cisco ACS-Zertifikats exportieren Sie ein vertrauenswürdigen untergeordnetes Zertifikat (falls vorhanden) und das Stammzertifikat (von einer Zertifizierungsstelle) auf dem Cisco ACS-Server. Die exportierten Zertifikate werden auf dem Telefon installiert. Diese Zertifikate sind Teil der vertrauenswürdigen Zertifikatskette, anhand derer die Vertrauenswürdigkeit des Zertifikats vom ACS-Server überprüft wird.

## EAP-TLS-Authentifizierungszertifikate installieren

Führen Sie zum Installieren von Authentifizierungszertifikaten für EAP-TLS die folgenden Schritte aus.

### Prozedur

---

**Schritt 1** Legen Sie auf der Telefon-Webseite Datum und Uhrzeit des Cisco Unified Communications Manager für das Telefon fest.

**Schritt 2** Wenn Sie das MIC (Manufacturing Installed Certificate, vom Hersteller installiertes Zertifikat) verwenden:

- Exportieren Sie das CA-Stammzertifikat und das Hersteller-CA-Zertifikat von der Telefon-Webseite.
- Installieren Sie in Internet Explorer Zertifikate auf dem Cisco ACS-Server, und bearbeiten Sie die Vertrauensliste.
- Importieren Sie das CA-Stammzertifikat in das Telefon.

Weitere Informationen finden Sie hier:

- [Zertifikate im ACS exportieren und installieren, auf Seite 106](#)
- [CA-Zertifikat von ISE mithilfe der Microsoft-Zertifikatdienste exportieren, auf Seite 107](#)

**Schritt 3** Richten Sie mit dem ACS-Konfigurationstool das Benutzerkonto ein.

Weitere Informationen finden Sie hier:

- [ACS-Benutzerkonto einrichten und Zertifikat installieren, auf Seite 108](#)
- [Benutzerhandbuch für Cisco Secure ACS für Windows](http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html)(<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>)

## Datum und Uhrzeit einstellen

Bei EAP-TLS wird die auf Zertifikaten basierende Authentifizierung verwendet, wobei der interne Zeitgeber im Cisco IP-Telefon ordnungsgemäß eingestellt sein muss. Datum und Uhrzeit auf dem Telefon können sich ändern, wenn das Gerät bei Cisco Unified Communications Manager registriert wird.



**Hinweis** Wenn ein neues Server-Authentifizierungszertifikat angefordert wird und die lokale Zeit hinter der GMT (Greenwich Mean Time) zurückliegt, schlägt die Überprüfung des Authentifizierungszertifikats möglicherweise fehl. Cisco empfiehlt, das lokale Datum und die lokale Uhrzeit so festzulegen, dass sie vor der GMT liegen.

Führen Sie die folgenden Schritte aus, um das lokale Datum und die lokale Uhrzeit korrekt festzulegen.

### Prozedur

- 
- Schritt 1** Wählen Sie im linken Navigationsbereich **Datum und Uhrzeit**.
  - Schritt 2** Wenn sich die Einstellung im Feld „Aktuelles Datum und Uhrzeit des Telefons“ von der im Feld „Lokales Datum und Uhrzeit“ unterscheidet, klicken Sie auf **Telefon auf lokales Datum und lokale Zeit festlegen**.
  - Schritt 3** Klicken Sie auf **Telefon neu starten** und anschließend auf **OK**.
- 

## Zertifikate im ACS exportieren und installieren

Zur Verwendung des MIC müssen Sie das Manufacturing Root Certificate (Stammzertifikat des Herstellers) und das Manufacturing CA Certificate (CA-Zertifikat des Herstellers) exportieren und auf dem Cisco ACS-Server installieren.

Führen Sie zum Exportieren des Manufacturing Root Certificate und des Manufacturing CA Certificate auf den ACS-Server die folgenden Schritte aus.

### Prozedur

- 
- Schritt 1** Wählen Sie auf der Telefon-Webseite **Zertifikate**.
  - Schritt 2** Klicken Sie neben dem Manufacturing Root Certificate auf **Exportieren**.
  - Schritt 3** Speichern Sie das Zertifikat, und kopieren Sie es auf den ACS-Server.
  - Schritt 4** Wiederholen Sie die Schritte 1 und 2 für das Manufacturing CA Certificate.
  - Schritt 5** Geben Sie auf der Seite „ACS-Server – Systemkonfiguration“ den Dateipfad für jedes Zertifikat ein, und installieren Sie die Zertifikate.
- Hinweis** Weitere Informationen zur Verwendung des ACS-Konfigurationstools finden Sie in der Online-Hilfe zu ACS oder im *Benutzerhandbuch für Cisco Secure ACS für Windows* (<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>).
- Schritt 6** Fügen Sie auf der Seite „CTL (Certificate Trust List) bearbeiten“ die Zertifikate hinzu, denen der ACS vertrauen soll.
-

## Methoden zum Exportieren von Zertifikaten aus dem ACS

Je nach Typ des aus dem ACS zu exportierenden Zertifikats ist eine der folgenden Methoden anzuwenden:

- Wenn Sie das CA-Zertifikat vom ACS-Server exportieren möchten, der das vom Benutzer installierte Zertifikat oder das ACS-Zertifikat signiert hat, siehe [CA-Zertifikat von ISE mithilfe der Microsoft-Zertifikatdienste exportieren, auf Seite 107](#).
- Wenn Sie das CA-Zertifikat vom ACS-Server exportieren möchten, der ein selbst signiertes Zertifikat verwendet, siehe [CA-Zertifikat von ACS mit Internet Explorer exportieren, auf Seite 107](#).

### CA-Zertifikat von ISE mithilfe der Microsoft-Zertifikatdienste exportieren

Mit dieser Methode können Sie das CA-Zertifikat vom ISE-Server exportieren, der das vom Benutzer installierte Zertifikat oder das ISE-Zertifikat signiert hat.

Führen Sie, wie auf der Webseite der Microsoft-Zertifikatdienste beschrieben, die folgenden Schritte aus, um das CA-Zertifikat zu exportieren.

#### Prozedur

- 
- |                  |  |
|------------------|--|
| <b>Schritt 1</b> | Wählen Sie <b>Zertifizierungsstellenzertifikat, Zertifikatkette oder Zertifikatsperrliste herunterladen</b> .  |
| <b>Schritt 2</b> | Markieren Sie auf der nächsten Seite das aktuelle CA-Zertifikat im Textfeld, wählen Sie unter „Codierungsmethode“ die Option „DER“, und klicken Sie anschließend auf <b>Zertifizierungsstellenzertifikat herunterladen</b> . |
| <b>Schritt 3</b> | Speichern Sie das CA-Zertifikat.   |
- 

### CA-Zertifikat von ACS mit Internet Explorer exportieren

Verwenden Sie diese Methode, um das CA-Zertifikat vom ACS-Server zu exportieren, der ein selbst signiertes Zertifikat verwendet.

Führen Sie die folgenden Schritte aus, um Zertifikate vom ACS-Server mit dem Internet Explorer zu exportieren.

#### Prozedur

- 
- |                  |  |
|------------------|--|
| <b>Schritt 1</b> | Wählen Sie im Internet Explorer <b>Extras &gt; Internetoptionen</b> , und klicken Sie dann auf die Registerkarte „Inhalte“.                                  |
| <b>Schritt 2</b> | Klicken Sie unter „Zertifikate“ auf <b>Zertifikate</b> , und klicken Sie anschließend auf die Registerkarte „Vertrauenswürdige Stammzertifizierungsstellen“. |
| <b>Schritt 3</b> | Markieren Sie das Stammzertifikat, und klicken Sie auf <b>Exportieren</b> . Der Zertifikatexport-Assistent wird angezeigt.                                   |
| <b>Schritt 4</b> | Klicken Sie auf <b>Weiter</b> .  |
| <b>Schritt 5</b> | Wählen Sie im nächsten Fenster <b>DER-codiert-binär X.509 (.CER)</b> , und klicken Sie dann auf <b>Weiter</b> .  |
| <b>Schritt 6</b> | Geben Sie einen Namen für das Zertifikat an, und klicken Sie auf <b>Weiter</b> .   |
| <b>Schritt 7</b> | Speichern Sie das CA-Zertifikat, damit es auf dem Telefon installiert werden kann.   |
-

## Vom Benutzer installiertes Zertifikat anfordern und importieren

Mithilfe der folgenden Schritte können Sie ein Zertifikat abrufen und auf dem Telefon installieren.

### Prozedur

- 
- Schritt 1** Wählen Sie auf der Telefon-Webseite erst das Netzwerkprofil, das EAP-TLS nutzt, und anschließend im Feld für das EAP-TLS-Zertifikat **Installiert vom Benutzer**.
- Schritt 2** Klicken Sie auf **Zertifikate**.
- Auf der Seite zum Installieren des Benutzerzertifikats sollte der Name im Feld „Allgemeiner Name“ mit dem Benutzernamen für den ACS-Server übereinstimmen.
- Hinweis** Bei Bedarf können Sie das Feld „Allgemeiner Name“ auch bearbeiten. Es muss jedoch sichergestellt sein, dass dessen Inhalt mit dem Benutzernamen für den ACS-Server identisch ist. Siehe [ACS-Benutzerkonto einrichten und Zertifikat installieren, auf Seite 108](#).
- Schritt 3** Geben Sie die Informationen ein, die das Zertifikat enthalten soll, und klicken Sie anschließend auf **Senden**, um die CSR-Datei (Zertifikatssignierungsanforderung) zu generieren.
- 

## Stammzertifikat des Authentifizierungsservers installieren

Führen Sie die folgenden Schritte aus, um das Stammzertifikat des Authentifizierungsservers auf dem Telefon zu installieren.

### Prozedur

- 
- Schritt 1** Exportieren Sie das Stammzertifikat des Authentifizierungsservers aus dem ACS. Siehe [Methoden zum Exportieren von Zertifikaten aus dem ACS, auf Seite 107](#).
- Schritt 2** Navigieren Sie zur Telefon-Webseite, und wählen Sie **Zertifikate**.
- Schritt 3** Klicken Sie neben dem Stammzertifikat des Authentifizierungsservers auf **Importieren**.
- Schritt 4** Starten Sie das Telefon neu.
- 

## ACS-Benutzerkonto einrichten und Zertifikat installieren

Führen Sie die folgenden Schritte aus, um den Namen des Benutzerkontos einzurichten und das MIC-Stammzertifikat für das Telefon im ACS zu installieren.



- 
- Hinweis** Weitere Informationen zur Verwendung des ACS-Konfigurationstools finden Sie in der Online-Hilfe zu ACS oder im *Benutzerhandbuch für Cisco Secure ACS für Windows*.
-

## Prozedur

---

- Schritt 1** Erstellen Sie auf der Benutzer-Setup-Seite des ACS-Konfigurationstools einen Benutzerkontonamen für das Telefon, sofern ein solcher nicht bereits eingerichtet ist.
- In der Regel enthält der Benutzername am Ende die MAC-Adresse des Telefons. Für EAP-TLS ist kein Kennwort erforderlich.
- Hinweis** Vergewissern Sie sich, dass der Benutzername mit dem Eintrag im Feld „Allgemeiner Name“ auf der Seite zum Installieren des Benutzerzertifikats übereinstimmt. Siehe [Vom Benutzer installiertes Zertifikat anfordern und importieren, auf Seite 108](#).
- Schritt 2** Aktivieren Sie auf der Seite „Systemkonfiguration“ im Abschnitt „EAP-TLS“ die folgenden Felder:
- **Allow EAP-TLS (EAP-TLS zulassen)**
  - **Certificate CN comparison (CN-Vergleich für Zertifikate)**
- Schritt 3** Fügen Sie auf der Seite „ACS Certification Authority Setup“ (Einrichtung der ACS-Zertifizierungsstelle) dem ACS-Server das Manufacturing Root Certificate (Herstellerstammzertifikat) und das Manufacturing Certificate Authority Certificate (Hersteller-CA-Zertifikat) hinzu.
- Schritt 4** Aktivieren Sie in der ACS-Zertifikate-Vertrauensliste sowohl das Herstellerstammzertifikat als auch das Hersteller-CA-Zertifikat.
- 

## PEAP-Setup

Protected Extensible Authentication Protocol (PEAP) authentifiziert Clients mit serverseitigen Zertifikaten für öffentliche Schlüssel, indem ein verschlüsselter SSL/TLS-Tunnel zwischen dem Client und dem Authentifizierungsserver hergestellt wird.

Das Cisco IP-Telefon 8865 unterstützt nur ein Serverzertifikat, das entweder über SCEP oder die manuelle Installationsmethode, jedoch nicht über beide, installiert werden kann. Das Telefon unterstützt nicht die TFTP-Methode zur Zertifikatsinstallation.



---

**Hinweis** Die Validierung des Authentifizierungsservers kann durch Importieren des Zertifikats für den Authentifizierungsserver aktiviert werden.

---

## Vorbereitungen

Vergewissern Sie sich vor dem Konfigurieren der PEAP-Authentifizierung für das Telefon, dass die folgenden Cisco Secure ACS-Anforderungen erfüllt sind:

- Das ACS-Stammzertifikat muss installiert sein.
- Ein Zertifikat kann auch installiert werden, um die Servervalidierung für PEAP zu aktivieren. Wenn jedoch ein Serverzertifikat installiert wird, wird auch die Servervalidierung aktiviert.
- Die Einstellung „Allow EAP-MSCHAPv2“ (EAP-MSCHAPv2 zulassen) muss aktiviert sein.
- Benutzerkonto und Kennwort müssen konfiguriert sein.

- Für die Kennwortauthentifizierung können Sie die lokale ACS-Datenbank oder eine externe Datenbank (wie Windows oder LDAP) verwenden.

## PEAP-Authentifizierung aktivieren

### Prozedur

- 
- Schritt 1** Wählen Sie auf der Webseite für die Telefonkonfiguration PEAP als Authentifizierungsmodus aus.
- Schritt 2** Geben Sie einen Benutzernamen und ein Kennwort ein.
- 

## 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.

### Verwandte Themen

[Webseite für Cisco IP-Telefon](#), auf Seite 239

## 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.
  - Drücken Sie auf dem Telefon auf **Anwendungen** , wählen Sie **Telefoninformationen**, und blättern Sie zum Feld „IPv4-Adresse“.
- 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:

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

- 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 Feld „Benutzerinstallation“, und klicken Sie auf **Installieren**.
- Schritt 3** Navigieren Sie zum Zertifikat auf Ihren PC.
- Schritt 4** Geben Sie im Feld **Kennwort extrahieren** das Extraktionskennwort des Zertifikats an.
- Schritt 5** Klicken Sie auf **Hochladen**.
- Schritt 6** 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.
- 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

---

- Schritt 1** Wählen Sie **Gerät > Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Suchen Sie das Telefon.
- Schritt 3** Navigieren Sie zum Bereich **Produktspezifische Konfiguration – Layout**.
- Schritt 4** Aktivieren Sie das Kontrollkästchen **WLAN SCEP-Server**, um den SCEP-Parameter zu aktivieren.
- Schritt 5** Aktivieren Sie das Kontrollkästchen **WLAN-Stammzertifizierungsstellen-Fingerabdruck (SHA256 oder SHA1)**, 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. CDP identifiziert lokal verbundene Arbeitsstationen nicht. Cisco IP-Telefons stellen eine Durchlaufmethode bereit. Diese Methode ermöglicht einer Arbeitsstation, die mit Cisco IP-Telefon verbunden ist, EAPOL-Meldungen an den 802.1X-Authentifikator auf dem LAN-Switch zu übermitteln. Die Durchlaufmethode stellt sicher, dass das IP-Telefon nicht als LAN-Switch agiert, um einen Datenendpunkt zu authentifizieren, bevor das Telefon auf das Netzwerk zugreift.

Cisco IP-Telefons stellen auch eine Proxy-EAPOL-Logoff-Methode bereit. Wenn der lokal verbundene PC vom IP-Telefon getrennt wird, erkennt der LAN-Switch nicht, dass die physische Verbindung unterbrochen wurde, da die Verbindung zwischen dem LAN-Switch und dem IP-Telefon aufrechterhalten wird. Um eine Gefährdung der Netzwerkintegrität zu verhindern, sendet das IP-Telefon im Auftrag des nachgelagerten PCs eine EAPOL-Logoff-Meldung an den Switch, die den LAN-Switch veranlasst, den Authentifizierungseintrag für den nachgelagerten PC zu löschen.

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

- Cisco IP-Telefon: Das Telefon initiiert die Anforderung, um auf das Netzwerk zuzugreifen. Das Cisco IP-Telefon enthält ein 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 Secure Access Control Server (ACS) (oder ein anderer Authentifizierungsserver eines Drittanbieters): Der Authentifizierungsserver und das Telefon müssen beide mit einem Shared Secret konfiguriert werden, mit dem das Telefon authentifiziert werden kann.
- 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 Meldungs austausch 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.
- PC-Port konfigurieren: Der 802.1X-Standard berücksichtigt VLANs nicht und empfiehlt deshalb, dass an einem Switch-Port nur ein Gerät authentifiziert werden sollte. Einige Switches (einschließlich Cisco Catalyst-Switches) unterstützen jedoch die Authentifizierung in mehreren Domänen. Die Switch-Konfiguration bestimmt, ob Sie einen PC in einem PC-Port des Telefon anschließen können.
  - Aktiviert: Wenn Sie einen Switch verwenden, der die Authentifizierung in mehreren Domänen unterstützt, können Sie den PC-Port aktivieren und einen PC anschließen. In diesem Fall unterstützen Cisco IP-Telefons Proxy-EAPOL-Logoff, um die Authentifizierung zwischen dem Switch und dem angeschlossenen PC zu überwachen. Weitere Informationen zur Unterstützung von IEEE 802.1X auf Cisco Catalyst-Switches finden Sie in den Konfigurationshandbüchern für die Cisco Catalyst-Switches:  
[http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)
  - Deaktiviert: Wenn der Switch mehrere 802.1X-konforme Geräte am gleichen Port nicht unterstützt, deaktivieren Sie den PC-Port, wenn die 802.1X-Authentifizierung aktiviert ist. Wenn Sie diesen Port nicht deaktivieren und versuchen, einen PC anzuschließen, verweigert der Switch den Netzwerkzugriff auf das Telefon und den PC.
- Sprach-VLAN konfigurieren: Da VLANs von 802.1X-Standard nicht berücksichtigt werden, sollten Sie diese Einstellung basierend auf der 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 Sie den Port dem systemeigenen VLAN zu.

## Auf die 802.1X-Authentifizierung zugreifen

Führen Sie die folgenden Schritte aus, um auf die Einstellungen für die 802.1X-Authentifizierung zuzugreifen:

### Prozedur

- 
- Schritt 1** Drücken Sie **Anwendungen** .
  - Schritt 2** Wählen Sie **Verwaltereinstellungen > Sicherheits-Setup > 802.1X -Authentifizierung**.
  - Schritt 3** Konfigurieren Sie die Optionen entsprechend der Beschreibung in [802.1X-Authentifizierungsoptionen](#), auf [Seite 116](#).

**Schritt 4** Drücken Sie zum Schließen dieses Menüs **Beenden**.

---

## 802.1X-Authentifizierungsoptionen

In folgender Tabelle sind die Optionen der 802.1X-Authentifizierung beschrieben.


*Tabelle 29: 802.1X-Authentifizierung – Einstellungen*

Option	Beschreibung	Änderung
Geräteauthentifizierung	Diese Option gibt an, ob die 802.1X-Authentifizierung aktiviert ist: <ul style="list-style-type: none"> <li>• Aktiviert: Telefon verwendet die 802.1X-Authentifizierung, um Netzwerkzugriff anzufordern.</li> <li>• Deaktiviert: Standardeinstellung. Das Telefon verwendet CDP zur Anforderung des VLAN- und Netzwerkzugriffs.</li> </ul>	Siehe <a href="#">Feld „Geräteauthentifizierung“</a> auf Seite 116.
Transaktionsstatus	Status: Zeigt den Status der 802.1X-Authentifizierung an: <ul style="list-style-type: none"> <li>• Verbindung getrennt: Zeigt an, dass die 802.1X-Authentifizierung auf dem Telefon nicht konfiguriert ist.</li> <li>• Authentifiziert: Zeigt an, dass das Telefon authentifiziert ist.</li> <li>• Gehalten: Zeigt an, dass die Authentifizierung gerade durchgeführt wird.</li> </ul> Protokoll: Zeigt die EAP-Methode an, die für die 802.1X-Authentifizierung verwendet wird (EAP-FAST oder EAP-TLS).	Wird nur angezeigt. Der Wert kann nicht konfiguriert werden.

## Feld „Geräteauthentifizierung“ festlegen

### Prozedur

---

- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Verwaltereinstellungen** > **Sicherheits-Setup** > **802.1X-Authentifizierung**.
- Schritt 3** Legen Sie die Option „Geräteauthentifizierung“ fest:
- **Ja**
  - **Nein**
- Schritt 4** Drücken Sie **Übernehmen**.
-



## KAPITEL 8

# Anpassung des Cisco IP-Telefon

- Benutzerdefinierte Ruftöne, auf Seite 117
- Benutzerdefinierte Hintergrundbilder, auf Seite 117
- Breitband-Codec konfigurieren, auf Seite 119
- Inaktives Display konfigurieren, auf Seite 120
- Den Wählton anpassen, auf Seite 121

## Benutzerdefinierte Ruftöne

Im Lieferumfang des Telefons sind drei Ruftöne enthalten, die bereits in die Hardware integriert sind: „Sunshine“, „Chirp“ und „Chirp1“.

Zusätzlich bietet der Cisco Unified Communications Manager einen Standardsatz mit weiteren Ruftönen, die in Softwareform (PCM-Dateien) zur Verfügung gestellt werden. Die PCM-Dateien und eine XML-Datei (Ringlist-wb.xml), die die an Ihrem Standort verfügbaren Ruftonlistenoptionen beschreibt, befinden sich im TFTP-Verzeichnis auf den Cisco Unified Communications Manager-Servern.



**Achtung** Bei allen Dateinamen muss die Groß-/Kleinschreibung beachtet werden. Wenn Sie Ringlist-wb.xml als Dateinamen angeben, werden die Änderungen nicht auf dem Telefon übernommen.

Weitere Informationen finden Sie im Kapitel „Custom Phone Rings and Backgrounds“ (Benutzerdefinierte Ruftöne und Hintergründe) im [Funktionskonfigurationshandbuch für Cisco Unified Communications Manager für Cisco Unified Communications Manager Version 12.0\(1\) oder höher](#).

## Benutzerdefinierte Hintergrundbilder

Sie können ein Cisco IP-Telefon mit einem Hintergrundbild personalisieren. Benutzerdefinierte Hintergrundbilder werden gerne genutzt, um Firmenlogos oder Bilder anzuzeigen. Deshalb wählen zahlreiche Unternehmen Hintergrundbilder, mit denen sich ihre Telefone von der Masse abheben.

Ab Firmware-Version 12.7(1) können Sie Ihr Hintergrundbild sowohl auf Ihren Telefonen als auch auf Tastenerweiterungsmodulen individuell anpassen. Sie benötigen jedoch ein Bild für das Telefon und ein weiteres Bild für das Erweiterungsmodul.

Das Telefon analysiert die Hintergrundbildfarben und ändert die Schriftfarben und Symbole so, dass Sie sie gut lesen können. Wenn Ihr Hintergrundbild dunkel ist, ändert das Telefon die Schriftarten und Symbole in weiß. Wenn das Hintergrundbild hell ist, werden die Schriftarten und Symbole schwarz angezeigt.

Es empfiehlt sich, ein einfaches Bild, wie eine Volltonfarbe oder ein Muster, als Hintergrund zu wählen. Vermeiden Sie Bilder mit hohem Kontrast.

Sie können ein benutzerdefiniertes Hintergrundbild auf zwei Arten hinzufügen:

- List-Datei verwenden
- Allgemeines Telefonprofil verwenden

Wenn Sie möchten, dass sich der Benutzer Ihr Bild aus verschiedenen Hintergrundbildern aussuchen kann, die auf dem Telefon verfügbar sind, dann ändern Sie die List-Datei. Wenn Sie das Bild jedoch auf das Telefon übertragen möchten, dann erstellen oder ändern Sie ein vorhandenes allgemeines Telefonprofil.

Beachten Sie Folgendes, unabhängig von Ihrem Ansatz:

- Die Bilder müssen im PNG-Format vorliegen und die Abmessungen des Bildes in voller Größe müssen sich innerhalb der folgenden Werte befinden:
  - Miniaturbilder: 139 Pixel (Breite) zu 109 Pixel (Höhe)
  - Cisco IP-Telefon 8800-Serie: 800 Pixel zu 480 Pixel
  - Tastenerweiterungsmodul für Cisco IP-Telefon 8851 und 8861 mit zwei LCD-Displays: 320 Pixel zu 480 Pixel
  - Tastenerweiterungsmodul für Cisco IP-Telefon 8865 mit zwei LCD-Displays – 320 x 480 Pixel
  - Tastenerweiterungsmodul für Cisco IP-Telefon 8800 mit einem LCD-Display: 272 Pixel zu 480 Pixel
- Laden Sie die Bilder, die Miniaturbilder und die List-Datei auf Ihren TFTP-Server hoch. Das Verzeichnis lautet:
  - Cisco IP-Telefon 8800-Serie: Desktops/800x480x24
  - Tastenerweiterungsmodul für Cisco IP-Telefon 8851 und 8861 mit zwei LCD-Bildschirmen: Desktops/320x480x24
  - Tastenerweiterungsmodul für Cisco IP-Telefon 8865 mit zwei LCD-Displays – Desktops/320x480x24
  - Tastenerweiterungsmodul für das Cisco IP-Telefon 8800 mit einem LCD-Display – Desktops/272x480x24

Starten Sie nach dem Hochladen den TFTP-Server neu.

- Wenn Sie nicht möchten, dass sich Benutzer ihr eigenes Hintergrundbild aussuchen können, dann deaktivieren Sie **Benutzerzugriff auf die Einstellung Telefon-Hintergrundimage aktivieren**. Speichern und übernehmen Sie das Telefonprofil. Starten Sie die Telefone neu, damit Ihre Änderungen übernommen werden.



**Hinweis** Sie können die Hintergrundbilder des Telefons mit dem **allgemeinen Telefonprofil** in einem Massenvorgang übernehmen. Bei einer Massenkongfiguration müssen Sie jedoch die **Benutzerzugriff auf die Einstellung Telefon-Hintergrundimage aktivieren** deaktivieren. Weitere Informationen zur Massenkongfiguration von Hintergrundbildern finden Sie im Kapitel „Configure the Common Phone Profile“ (Konfigurieren des allgemeinen Telefonprofils) der Dokumentation [Customized Wallpapers Best Practices Cisco IP Phone 8800 Series](#) (Bewährte Verfahren für benutzerdefinierte Hintergrundbilder für Cisco IP-Telefon 8800-Serie).

Weitere Informationen zum Anpassen von Hintergrundbildern finden Sie in der folgenden Dokumentation:

- [Customized Wallpapers Best Practices Cisco IP Phone 8800 Series](#) (Bewährte Verfahren für benutzerdefinierte Hintergrundbilder für Cisco IP-Telefon 8800-Serie)
- Kapitel „Custom Phone Rings and Backgrounds“ (Benutzerdefinierte Ruftöne und Hintergrundbilder) im [Funktionskonfigurationshandbuch für Cisco Unified Communications Manager](#) für Cisco Unified Communications Manager Version 12.0(1) oder neuer.
- Kapitel „Settings“ (Einstellungen) im *Benutzerhandbuch für die Cisco IP-Telefon 8800-Serie*.

## Breitband-Codec konfigurieren

Der G.722-Codec ist standardmäßig für das Cisco IP-Telefon aktiviert. Wenn die Konfiguration von Cisco Unified Communications Manager die Verwendung des G.722-Codex vorsieht und das Endgerät G.722 unterstützt, wird bei der Herstellung der Anrufverbindung anstelle des G.711-Codex der G.722-Codec verwendet.

Dies geschieht unabhängig davon, ob der Benutzer ein Wideband-Headset oder einen Wideband-Hörer aktiviert hat, er wird jedoch möglicherweise eine verbesserte Audioempfindlichkeit während der Gespräche feststellen, wenn Headset oder Hörer aktiviert sind. Eine höhere Empfindlichkeit bedeutet eine bessere Audioqualität, aber auch, dass der Remote-Endpunkt mehr Hintergrundgeräusche hört (beispielsweise Papierrascheln oder Gespräche, die in der Nähe stattfinden). Auch ohne ein Breitband-Headset oder einen Breitband-Hörer können einige Benutzer die höhere Empfindlichkeit von G.722 ablenkend empfinden. Andere Benutzer können diese erhöhte Audioempfindlichkeit von G.722 als Vorteil empfinden.

Von der Einstellung des Dienstparameters „G.722 und iSAC Codex ankündigen“ hängt es ab, ob die Wideband-Unterstützung für alle Geräte existiert, die bei diesem Cisco Unified Communications Manager-Server registriert werden, oder nur für ein bestimmtes Telefon, je nachdem, wie der Parameter im Fenster „Cisco Unified Communications Manager-Verwaltung“ konfiguriert wurde.

### Prozedur

#### Schritt 1

So konfigurieren Sie die Wideband-Unterstützung für alle Geräte:

- a) Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **System > Unternehmensparameter**
- b) Nehmen Sie die gewünschten Einstellungen im Feld „G.722 und iSAC Codex ankündigen“ vor.

Der Standardwert dieses Unternehmensparameters lautet **True**, was bedeutet, dass alle bei diesem Cisco Unified Communications Manager registrierten Cisco IP-Telefon-Modelle G.722 anbieten. Wenn alle Endgeräte im Anruf den G.722-Codec in ihrem Funktionssatz unterstützen, wählt Cisco Unified Communications Manager diesen Codec für den Anruf aus.

## Schritt 2

So konfigurieren Sie die Wideband-Unterstützung für ein bestimmtes Gerät:

- a) Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **Gerät > Telefon**.
- b) Nehmen Sie die gewünschte Einstellung für den Parameter „G.722 und iSAC Codecs ankündigen“ im Bereich „Produktspezifische Konfiguration“ vor.

Dieser produktspezifische Parameter ist standardmäßig auf die Verwendung des vom Unternehmensparameter vorgegebenen Werts eingestellt. Wenn Sie diese Einstellung für ein bestimmtes Telefon überschreiben möchten, wählen Sie **Aktiviert** bzw. **Deaktiviert**.

# Inaktives Display konfigurieren

Sie können ein inaktives Display festlegen (nur Text; die Textdatei sollte nicht größer als 1 MB sein), das auf dem Telefon angezeigt wird. Das inaktive Display ist ein XML-Service, der das Telefon startet, wenn das Telefon für eine angegebene Zeitdauer inaktiv ist (nicht verwendet wird) oder keine Funktionsmenü geöffnet ist.

Detaillierte Anweisungen zum Erstellen und Anzeigen des inaktiven Displays finden Sie in *Inaktive URL-Grafik auf Cisco IP-Telefon erstellen* unter dieser URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_tech\\_note09186a00801c0764.shtml](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml)

In der Dokumentation für Ihre Version von Cisco Unified Communications Manager finden Sie die folgenden Informationen:

- Die URL für den XML-Service Inaktives Display angeben:
  - Für ein Telefon: Das Feld „Inaktiv“ im Fenster „Telefonkonfiguration“ in der Cisco Unified Communications Manager-Verwaltung.
  - Für mehrere Telefone: Das Feld URL inaktiv im Fenster Enterprise-Parameterkonfiguration oder das Feld Inaktiv in BAT (Bulk Administration Tool).
- Die Zeitdauer festlegen, die das Telefon nicht verwendet wird, bevor der XML-Service Inaktives Display aktiviert wird:
  - Für ein Telefon: Das Feld „Inaktiv-Timer“ im Fenster „Telefonkonfiguration“ in der Cisco Unified Communications Manager-Verwaltung.
  - Für mehrere Telefone: Das Feld URL inaktive Zeitdauer im Fenster Enterprise-Parameterkonfiguration oder das Feld Inaktiv-Timer in BAT (Bulk Administration Tool).

## Prozedur

### Schritt 1

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



- Schritt 2** Geben Sie im Feld Inaktiv die URL zum XML-Service für inaktive Displays ein.
- Schritt 3** Geben Sie im Feld Inaktiv-Timer die Zeitdauer ein, die das inaktive Telefon wartet, bevor der XML-Service Inaktives Display aktiviert wird.
- Schritt 4** Wählen Sie **Speichern** aus.
- 

## Den Wählton anpassen

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

- Standard: Unterschiedliche Wähltöne 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

---

- Schritt 1** Wählen Sie in Cisco Unified Communications Manager Administration **System > Dienstparameter** aus.
- Schritt 2** Wählen Sie den gewünschten Server aus.
- Schritt 3** Wählen Sie **Cisco CallManager** als Dienst aus.
- Schritt 4** Navigieren Sie zum Bereich „Clusterweite Parameter“.
- Schritt 5** Legen Sie **Immer Wählton verwenden** auf eine der folgenden Einstellungen fest:
- Extern
  - Intern
  - Standard
- Schritt 6** Wählen Sie **Speichern** aus.
- Schritt 7** Starten Sie die Telefone neu.
-





## KAPITEL 9

# Telefonfunktionen und Konfiguration

- [Übersicht über Telefonfunktionen und Konfiguration, auf Seite 123](#)
- [Benutzersupport für Cisco IP-Telefon, auf Seite 123](#)
- [Telefonfunktionen, auf Seite 124](#)
- [Funktionstasten und Softkeys, auf Seite 142](#)
- [Telefonfunktion – Konfiguration, auf Seite 144](#)
- [Softkey-Vorlagen konfigurieren, auf Seite 199](#)
- [Vorlagen für Telefontasten, auf Seite 201](#)
- [VPN-Konfiguration, auf Seite 205](#)
- [Zusätzliche Leitungstasten einrichten, auf Seite 206](#)
- [TLS-Fortsetzungs-Timer einrichten, auf Seite 209](#)
- [Intelligent Proximity aktivieren, auf Seite 210](#)
- [Auflösung für Videoübertragung einrichten, auf Seite 210](#)
- [Headset-Verwaltung für ältere Versionen von Cisco Unified Communications Manager, auf Seite 211](#)

## Übersicht über Telefonfunktionen und Konfiguration

Nachdem Sie Cisco IP-Telefone in Ihrem Netzwerk installiert haben, deren Netzwerkeinstellungen konfiguriert und sie dem Cisco Unified Communications Manager hinzugefügt haben, müssen Sie mit der Cisco Unified Communications Manager-Verwaltung die Telefoniefunktionen konfigurieren, (optional) Telefonvorlagen bearbeiten, Dienste einrichten und Benutzer zuweisen.

Über die Cisco Unified Communications Manager-Verwaltung können Sie weitere Einstellungen für das Cisco IP-Telefon bearbeiten. Mit dieser webbasierten Anwendung können Sie Kriterien für Telefonregistrierung und Anrufschräume festlegen, Unternehmensverzeichnisse und -dienste konfigurieren, Telefontastenvorlagen ändern und weitere Aufgaben ausführen.

Die Anzahl der verfügbaren Leitungstasten ist begrenzt, wenn Sie weitere Funktionen zu den Leitungstasten hinzufügen. Sie können nicht mehr Funktionen als Leitungstasten zu Ihrem Telefon hinzufügen.

## 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

## Telefonfunktionen

Nachdem Sie Cisco IP-Telefon zu Cisco Unified Communications Manager hinzugefügt haben, können Sie den Telefonen Funktionen hinzufügen. In der folgenden Tabelle sind die unterstützten Telefonfunktionen aufgelistet, von denen viele mit der Cisco Unified Communications Manager-Verwaltung konfiguriert werden können.

Weitere Informationen zur Verwendung der meisten dieser Funktionen auf dem Telefon finden Sie im *Benutzerhandbuch für die Cisco IP-Telefon 8800-Serie*. Siehe [Funktionstasten und Softkeys, auf Seite 142](#) für eine Liste der Funktionen, die als programmierbare Tasten sowie zugeordnete Softkeys und Funktionstasten konfiguriert werden können.



### Hinweis

Die Cisco Unified Communications Manager-Verwaltung stellt mehrere Serviceparameter bereit, die Sie zum Konfigurieren der verschiedenen Telefonfunktionen verwenden können. Weitere Informationen zum Zugriff und Konfigurieren der Serviceparameter finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Um weitere Informationen zu den Funktionen eines Dienstes zu erhalten, wählen Sie im Fenster [Produktspezifische Konfiguration](#) den Namen des Parameters oder die **Hilfe-Schaltfläche mit dem Fragezeichen (?)** aus.

Weitere Informationen hierzu finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.

Funktion	Beschreibung und weitere Informationen
Kurzwahlcodes	<p>Ermöglicht dem Benutzer, eine Telefonnummer schnell zu wählen, indem er einen zugewiesenen Indexcode (1-199) auf dem Tastenfeld des Telefons eingibt.</p> <p><b>Hinweis</b> Sie können Kurzwahlcodes bei aufgelegtem oder abgenommenem Hörer verwenden.</p> <p>Index-Codes können von den Benutzern auf dem Selbsthilfe-Portal zugewiesen werden.</p>

Funktion	Beschreibung und weitere Informationen
Aktionshinweis für eingehende Anrufe	<p>Bietet verschiedene Optionen, um Benachrichtigungen über eingehende Anrufe zu steuern. Die können die Benachrichtigung aktivieren oder deaktivieren. Außerdem können Sie die Anzeige der Anrufer-ID aktivieren oder deaktivieren.</p> <p>Siehe „Aktionshinweis für eingehende Anrufe“, <a href="#">Produktspezifische Konfiguration, auf Seite 146</a>.</p>
Unterstützung der AES 256-Verschlüsselung für Telefone	<p>Verbessert die Sicherheit, da TLS 1.2 und andere Schlüssel unterstützt werden. Weitere Informationen hierzu finden Sie unter <a href="#">Unterstützte Sicherheitsfunktionen, auf Seite 88</a>.</p>
Mitarbeiterbegrüßung	<p>Ermöglicht einem Mitarbeiter eine aufgezeichnete Begrüßung zu erstellen oder zu aktualisieren, die zu Beginn eines Kundenanrufs abgespielt wird, bevor der Mitarbeiter das Gespräch mit dem Kunden beginnt. Der Mitarbeiter kann nach Bedarf eine oder mehrere Begrüßungen aufzeichnen.</p> <p>Siehe <a href="#">Mitarbeiterbegrüßung aktivieren, auf Seite 177</a>.</p>
Beliebige Anrufübernahme	<p>Ermöglicht dem Benutzer, einen Anruf auf einer beliebigen Leitung in seiner Anrufübernahmegruppe anzunehmen, unabhängig davon, wie der Anruf an das Telefon geleitet wurde.</p> <p>Siehe die Informationen zur Anrufübernahme in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Anwendungs-Wählregeln	<p>Konvertiert Nummern für gemeinsame genutzte mobile Kontakte in über das Netzwerk wählbare Nummern.</p> <p>Siehe <a href="#">Anwendungswählregeln, auf Seite 80</a>.</p>
Unterstütztes gezieltes Parken	<p>Ermöglicht dem Benutzer, einen Anruf zu parken, indem er eine Taste drückt. Administratoren müssen eine BLF-Taste für das unterstützte direkte Parken von Anrufen konfigurieren. Wenn der Benutzer eine inaktive BLF-Taste für einen aktiven Anruf drückt, wird der Anruf unter der Nummer geparkt, die der Taste für das unterstützte direkte Parken zugewiesen ist.</p> <p>Siehe die Informationen zum unterstützten gezielten Parken in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Signalton für wartende Nachrichten	<p>Ein unterbrochenes Rufzeichen vom Hörer, Headset oder Lautsprecher zeigt an, das ein Benutzer mindestens eine neue Voicemail auf einer Leitung hat.</p> <p><b>Hinweis</b> Das unterbrochene Rufzeichen ist leitungsspezifisch. Er wird nur auf der Leitung mit den wartenden Nachrichten ausgegeben.</p>
Automatische Anrufannahme	<p>Verbindet eingehende Anrufe automatisch nach einem oder zwei Ruftönen.</p> <p>Die automatische Anrufannahme funktioniert mit dem Lautsprecher oder dem Headset. Siehe die Informationen zu Verzeichnisnummern in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>

Funktion	Beschreibung und weitere Informationen
Automatische Portsynchronisierung	<p>Synchronisiert Ports auf die geringste Geschwindigkeit zwischen den Ports eines Telefons, um Paketverlust zu vermeiden.</p> <p>Siehe „Automatische Portsynchronisierung“, <a href="#">Produktspezifische Konfiguration, auf Seite 146</a>.</p>
Automatische Übernahme	<p>Ermöglicht einem Benutzer, mit nur einem einzigen Tastendruck Anrufübernahmefunktionen zu nutzen.</p> <p>Siehe die Informationen zur Anrufübernahme in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Aufschalten	<p>Ermöglicht dem Benutzer, sich in einen Anruf aufzuschalten, indem unter Verwendung der integrierten Konferenzbrücke des Zieltelefons ein Dreiwegen-Konferenzanruf initiiert wird.</p> <p>Siehe „Konferenzanschaltung“ in dieser Tabelle.</p>
Externe Übergabe blockieren	<p>Verhindert, dass Benutzer einen externen Anruf an eine andere externe Nummer übergeben.</p> <p>Siehe die Informationen zum Übergeben externer Anrufe in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Bluetooth-Mehrfachverbindung	<p>Ermöglicht dem Benutzer, mehrere Geräte mit dem Telefon zu koppeln. Auf diese Weise kann der Benutzer ein mobiles Gerät über Bluetooth verbinden und zugleich ein Bluetooth-Headset verwenden.</p> <p>Cisco IP-Telefon 8851NR unterstützt Bluetooth nicht.</p>
Besetztlampenfeld (BLF)	<p>Ermöglicht einem Benutzer, den Anrufstatus einer Verzeichnisnummer zu überwachen, die einer Kurzwahltaste auf dem Telefon zugeordnet ist.</p> <p>Siehe die Informationen zur Anwesenheit in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Besetztlampenfeld (BLF) mit Annahme	<p>Stellt Erweiterungen für die BLF-Kurzwahl bereit. Ermöglicht Ihnen, eine Verzeichnisnummer (DN) zu konfigurieren, die ein Benutzer für eingehende Anrufe überwachen kann. Wenn auf der Verzeichnisnummer ein Anruf eingeht, informiert das System den überwachenden Benutzer, der den Anruf dann übernehmen kann.</p> <p>Siehe die Informationen zur Anrufübernahme in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Rückruf	<p>Gibt ein akustisches und visuelles Signal auf dem Telefon aus, wenn ein besetzter oder nicht verfügbarer Teilnehmer verfügbar wird.</p> <p>Weitere Informationen zu Rückrufen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.</p>
Einschränkungen für die Anrufanzeige	<p>Legt die Informationen fest, die für anrufende oder verbundene Leitungen angezeigt werden, abhängig von den Teilnehmern.</p> <p>Siehe die Informationen zu Routing-Plänen und Anrufanzeigeeinschränkungen in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>

Funktion	Beschreibung und weitere Informationen
Rufumleitung	<p>Ermöglicht den Benutzern, eingehende Anrufe an eine andere Nummer umzuleiten. Die Optionen für die Anrufweiterleitung umfassen Alle Anrufe weiterleiten, Bei besetzt weiterleiten, Bei keiner Antwort weiterleiten und Bei keinem Netz weiterleiten.</p> <p>Weitere Informationen zu Verzeichnisnummern finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager und in <a href="#">Die Ansicht des Selbstservice-Portals anpassen, auf Seite 84</a>.</p>
Schleife beim Weiterleiten aller Anrufe	<p>Erkennt und verhindert Schleifen bei „Alle Anrufe umleiten“. Wenn bei „Alle Anrufe umleiten“ eine Schleife erkannt wird, wird die Konfiguration von „Alle Anrufe umleiten“ ignoriert und der Anruf durchgestellt.</p>
Verhinderung von Schleifen bei „Alle Anrufe umleiten“	<p>Erkennt und verhindert Schleifen bei „Alle Anrufe umleiten“. Wenn bei „Alle Anrufe umleiten“ eine Schleife erkannt wird, wird die Konfiguration von „Alle Anrufe umleiten“ ignoriert und der Anruf durchgestellt.</p>
Anzeige für konfigurierbare Anrufweiterleitung	<p>Verhindert, dass ein Benutzer ein Ziel für „Alle Anrufe umleiten“ direkt auf dem Telefon konfiguriert, das eine Schleife bei „Alle Anrufe umleiten“ oder eine Kette bei „Alle Anrufe umleiten“ mit einer größeren Anzahl von Hops erzeugt, als der vorhandene Dienstparameter „Maximale Hop-Anzahl bei der Anrufweiterleitung“ erlaubt.</p> <p>Siehe die Informationen zu Verzeichnisnummern in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Weiterleitungsziel überschreiben	<p>Ermöglicht Ihnen, CFA (Call Forward All) zu überschreiben, wenn das CFA-Ziel den CFA-Initiator anruft. Diese Funktion ermöglicht dem CFA-Ziel den CFA-Initiator für wichtige Anrufe zu erreichen. Die Überschreibung funktioniert unabhängig davon, ob die CFA-Zielnummer intern oder extern ist.</p> <p>Weitere Informationen zu Verzeichnisnummern finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.</p>
Benachrichtigung für Rufumleitung	<p>Ermöglicht Ihnen, die Informationen zu konfigurieren, die der Benutzer sieht, wenn er einen weitergeleiteten Anruf erhält.</p> <p>Siehe <a href="#">Benachrichtigung für Rufumleitung einrichten, auf Seite 178</a>.</p>
Anrufverlauf für gemeinsam genutzte Leitung	<p>Ermöglicht Ihnen, die Aktivitäten auf der gemeinsam genutzten Leitung im Anrufverlauf anzuzeigen. Diese Funktion führt die folgenden Aktionen aus:</p> <ul style="list-style-type: none"> <li>• Verpasste Anrufe auf der gemeinsam genutzten Leitung werden protokolliert</li> <li>• Alle auf der gemeinsam genutzten Leitung angenommenen und getätigten Anrufe werden protokolliert</li> </ul>

Funktion	Beschreibung und weitere Informationen
Anruf parken	<p>Ermöglicht den Benutzern, einen Anruf zu parken (vorübergehend zu speichern) und den Anruf auf einem anderen Telefon im Cisco Unified Communications Manager-System heranzuholen.</p> <p>Sie können das Feld <b>Eine Leitung für das Parken von Anrufen dedizieren</b> im Fensterbereich <b>Produktspezifischen Konfigurationslayout</b> konfigurieren, um den Anruf in der ursprünglichen oder einer anderen Leitung zu parken.</p> <p>Wenn das Feld aktiviert ist, verbleibt der geparkte Anruf in der Benutzerleitung und kann mit dem Softkey <b>Fortsetzen</b> den Anruf annehmen. Der Benutzer sieht die Durchwahlnummer für den geparkten Anruf auf dem Telefondisplay.</p> <p>Wenn das Feld deaktiviert ist, wird der geparkte Anruf an die Leitung für geparkte Anrufe übergeben. Die Benutzerleitung kehrt in den Status „frei“ zurück und die Parkkennziffer wird in einem Popup-Fenster angezeigt. Der Benutzer wählt die Durchwahl, um den Anruf anzunehmen.</p> <p>Siehe die Informationen zum Parken von Anrufen in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Anrufübernahme	<p>Ermöglicht dem Benutzer, einen Anruf, der auf einem anderen Telefon in seiner Anrufübernahmegruppe eingeht, an sein Telefon umzuleiten.</p> <p>Sie können akustische und visuelle Signale für die primäre Leitung auf dem Telefon konfigurieren. Diese Benachrichtigung teilt dem Benutzer mit, dass ein Anruf in seiner Übernahmegruppe eingeht.</p> <p>Siehe die Informationen zur Anrufübernahme in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Call Recording	<p>Ermöglicht einem Supervisor einen aktiven Anruf aufzuzeichnen. Der Benutzer kann möglicherweise einen Signalton hören, wenn der Anruf aufgezeichnet wird.</p> <p>Wenn ein Anruf geschützt ist, wird der Sicherheitsstatus des Anrufs auf Cisco IP-Telefons als Schloss-Symbol angezeigt. Die verbundenen Teilnehmer hören möglicherweise auch einen Signalton, der angibt, dass der Anruf sicher ist und aufgezeichnet wird.</p> <p><b>Hinweis</b> Während ein aktiver Anruf überwacht oder aufgezeichnet wird, kann der Benutzer Intercom-Anrufe tätigen und annehmen. Wenn der Benutzer jedoch einen Intercom-Anruf tätigt, wird der aktive Anruf gehalten, die Aufzeichnungssitzung wird abgebrochen und die Überwachungssitzung wird angehalten. Um die Überwachungssitzung fortzusetzen, muss der überwachte Teilnehmer den Anruf fortsetzen.</p> <p>Siehe die Informationen zum Mithören und Aufzeichnen in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Anklopfen	<p>Zeigt einen Anruf an, der eingeht, während ein anderer Anruf aktiv ist. Auf dem Telefon werden Informationen zum eingehenden Anruf angezeigt.</p> <p>Weitere Informationen zu Verzeichnisnummern finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.</p>



Funktion	Beschreibung und weitere Informationen
Anklopfton	<p>Bietet Benutzern die Möglichkeit, als Anklopfton einen Rufton anstelle des Standardsignaltons zu verwenden.</p> <p>Als Optionen stehen „Klingeln“ und „Einmal klingeln“ zur Verfügung.</p> <p>Siehe die Informationen zu Verzeichnisnummern in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Anrufer-ID	<p>Die Anrufer-ID, beispielsweise eine Telefonnummer, ein Name oder eine Beschreibung, werden auf dem Telefondisplay angezeigt.</p> <p>Siehe die Informationen zu Routing-Plan, Anrufanzeigeeinschränkungen und Verzeichnisnummern in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Blockierung der Anrufer-ID	<p>Ermöglicht einem Benutzer, seine Telefonnummer oder E-Mail-Adresse für Telefone zu blockieren, auf denen die Anrufer-ID aktiviert ist.</p> <p>Siehe die Informationen zu Routing-Plan und Verzeichnisnummern in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Rufnummernnormalisierung	<p>Die Rufnummernnormalisierung zeigt Anrufe mit einer wählbaren Nummer an. Escapecodes werden zur Nummer hinzugefügt, damit der Benutzer den Anrufer einfach erneut anrufen kann. Die wählbare Nummer kann im Anrufverlauf oder im persönlichen Adressbuch gespeichert werden.</p>
CAST für SIP	<p>Stellt eine Kommunikation zwischen Cisco Unified Video Advantage (CUVA) und Cisco IP-Telefon her, um Video auf dem PC zu unterstützen, auch wenn das IP-Telefon über keine Videofunktion verfügt.</p>
Konferenzaufschaltung	<p>Ermöglicht einem Benutzer, sich auf ein nicht-privates Gespräch auf einer gemeinsam genutzten Leitung aufzuschalten. Mit „KAufsch.“ wird ein Benutzer zu einem Anruf hinzugefügt und der Anruf in eine Konferenz konvertiert, sodass der Benutzer und andere Teilnehmer auf die Konferenzfunktionen zugreifen können. Das Konferenzgespräch wird mithilfe der Konferenzbrückenfunktion von Cisco Unified Communications Manager erstellt.</p> <p>Sie müssen sowohl den Softkey als auch die Konferenzbrückenfunktion aktivieren, damit KAufsch. ordnungsgemäß funktioniert.</p> <p>In Firmware-Version 10.2(2) und höher wird über den Softkey „Aufsch.“ auf die Funktion „KAufsch.“ zugegriffen.</p> <p>Weitere Informationen hierzu finden Sie im Kapitel „Aufschalten“ im <a href="#">Funktionskonfigurationshandbuch für Cisco Unified Communications Manager</a>.</p>
Mobilgerät aufladen	<p>Ermöglicht einem Benutzer, ein Mobilgerät durch Anschließen an den USB-Port des Cisco IP-Telefon aufzuladen.</p> <p>Siehe <i>Benutzerhandbuch für die Cisco IP-Telefon 8800-Serie</i>.</p>

Funktion	Beschreibung und weitere Informationen
Cisco Anschlussmobilität	<p>Ermöglicht es den Benutzern, auf einem gemeinsam genutzten Cisco IP-Telefon auf ihre Cisco IP-Telefon-Konfiguration wie Leitungsanzeigen, Dienste und Kurzwahleinträge zuzugreifen.</p> <p>Cisco Extension Mobility ist hilfreich, wenn die Benutzer an verschiedenen Standorten des Unternehmens arbeiten oder sich einen Arbeitsplatz mit Kollegen teilen.</p>
Cisco Extension Mobility Cross Cluster (EMCC)	<p>Ermöglicht einem Benutzer, der in einem Cluster konfiguriert ist, sich an einem Cisco IP-Telefon in einem anderen Cluster anzumelden. Die Benutzer in einem Heimcluster melden sich an einem Cisco IP-Telefon in einem Besuchercluster an.</p> <p><b>Hinweis</b> Konfigurieren Sie die Cisco Anschlussmobilität auf Cisco IP-Telefons, bevor Sie EMCC konfigurieren.</p>
Cisco IP Manager Assistant (IPMA)	<p>Bietet Anruf-Routing- sowie andere Anrufverarbeitungsfunktionen, mit denen Manager und Assistenten Telefonanrufe effektiver verarbeiten können.</p> <p>Siehe <a href="#">Einrichten des Cisco IP Manager Assistant, auf Seite 194</a>.</p>
<p>Cisco IP Phone 8800-Tastenerweiterungsmodul</p> <p>Tastenerweiterungsmodul für Cisco IP Phone 8851/8861</p> <p>Cisco IP Phone 8865-Tastenerweiterungsmodul</p>	<p>Bietet zusätzliche Schlüssel durch Hinzufügen eines Erweiterungsmoduls zum Telefon.</p> <p>Weitere Informationen zur Installation von Zubehör finden Sie im <i>Handbuch für Zubehör der Cisco IP-Telefon 7800- und 8800-Serie für Cisco Unified Communications Manager</i>.</p>
Cisco IP Phone 8811Support	Bietet Unterstützung für Cisco IP Phone 8811.
Unterstützung für Cisco IP-Telefon 8851NR	Bietet Unterstützung für Cisco IP-Telefon 8851NR.
Cisco Unified Communications Manager Express (Unified CME) – Versionsaushandlung	<p>Cisco Unified Communication Manager Express verwendet ein spezielles Tag in den Informationen, die an das Telefon gesendet werden, um sich zu identifizieren. Dieses Tag ermöglicht dem Telefon, Services für den Benutzer bereitzustellen, die vom Switch unterstützt werden.</p> <p>Weitere Informationen finden Sie hier:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Express System Administrator Guide (Systemadministratorhandbuch für Cisco Unified Communications Manager Express)</i></li> <li>• <a href="#">Cisco Unified Communications Manager Express-Interaktion, auf Seite 23</a></li> </ul>
Cisco Unified Video Advantage (CUVA)	<p>Ermöglicht Benutzern, mit einem Cisco IP-Telefon, einem PC und einer Videokamera Videoanrufe zu tätigen.</p> <p><b>Hinweis</b> Konfigurieren Sie den Parameter Videofunktionen im produktspezifischen Konfigurationsbereich in der Telefonkonfiguration.</p> <p>Siehe Dokumentation zu Cisco Unified Video Advantage.</p>
Cisco WebDialer	Ermöglicht dem Benutzer, Anrufe über Web- und Desktop-Anwendungen zu tätigen.

Funktion	Beschreibung und weitere Informationen
Klassischer Klingelton	<p>Unterstützt Ruftöne, die in der Telefonfirmware integriert sind oder von Cisco Unified Communications Manager heruntergeladen wurden. Diese Funktion vereinheitlicht die verfügbaren Ruftöne mit denen anderer Cisco IP-Telefons.</p> <p>Siehe <a href="#">Benutzerdefinierte Ruftöne, auf Seite 117</a>.</p>
Konferenz	<p>Ermöglicht dem Benutzer, gleichzeitig mit mehreren Teilnehmern zu sprechen, indem er jeden Teilnehmer separat anruft. Die Konferenzfunktionen umfassen Konferenz und MeetMe.</p> <p>Ermöglicht einem Teilnehmer in einer Standardkonferenz (Ad-hoc) andere Teilnehmer hinzuzufügen oder zu entfernen sowie zwei Standardkonferenzen auf einer Leitung zusammenzuführen.</p> <p>Diese Funktionen können Sie mithilfe des Dienstparameters „Ad-hoc-Konferenz erweitern“ aktivieren, der in der Cisco Unified Communications Manager-Verwaltung standardmäßig deaktiviert ist.</p> <p><b>Hinweis</b> Informieren Sie unbedingt Ihre Benutzer, wenn diese Funktionen aktiviert sind.</p>
Konfigurierbares Energy Efficient Ethernet (EEE) für PC- und Switch-Port	<p>Bietet eine Methode zur Steuerung von EEE-Funktionen an PC- und Switch-Port, indem EEE aktiviert oder deaktiviert wird. Die Funktion steuert beide Porttypen separat. Der Standardwert ist Aktiviert.</p> <p>Siehe <a href="#">Energy Efficient Ethernet für Switch-Port und PC-Port einrichten, auf Seite 180</a>.</p>
Konfigurierbare Schriftgröße	<p>Ermöglicht Benutzern, durch Ändern der Schriftgröße die maximale Anzahl von Zeichen zu erhöhen oder zu verringern, die das IP-Telefon im Anrufprotokoll oder im Anrufterfenster anzeigt.</p> <p>Eine kleinere Schriftart erhöht die maximale Anzahl von angezeigten Zeichen, und eine größere Schriftart verringert die maximale Anzahl von angezeigten Zeichen.</p>
CTI-Anwendungen	<p>Ein CTI-Routenpunkt (Computer Telephony Integration) kann ein virtuelles Gerät für die anwendungsgesteuerte Umleitung zuordnen, das mehrere Anrufe gleichzeitig empfangen kann.</p>
Alle umleiten	<p>Ermöglicht einem Benutzer, einen eingehenden, verbundenen oder gehaltenen Anruf direkt an ein Sprachnachrichtensystem zu übergeben. Nachdem ein Anruf umgeleitet wurde, ist die Leitung wieder für das Tätigen oder Empfangen neuer Anrufe verfügbar.</p> <p>Siehe die Informationen zum sofortigen Umleiten in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Vom Gerät aufgerufene Aufzeichnung	<p>Ermöglicht den Benutzern, ihre Anrufe über einen Softkey aufzuzeichnen.</p> <p>Administratoren können Anrufe weiterhin über die CTI-Benutzeroberfläche aufzeichnen.</p> <p>Siehe die Informationen zum Mithören und Aufzeichnen in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>

Funktion	Beschreibung und weitere Informationen
Gezieltes Parken	<p>Ermöglicht einem Benutzer, einen aktiven Anruf an eine für das gezielte Parken verfügbare Nummer zu übergeben. Eine BLF-Taste für das gezielte Parken zeigt an, ob eine Nummer für das gezielte Parken besetzt ist und ermöglicht den Kurzwahlzugriff auf diese Nummer.</p> <p><b>Hinweis</b> Wenn Sie das gezielte Parken implementieren, konfigurieren Sie keinen Softkey. Dies verhindert, dass die Benutzer die zwei Funktionen für das Parken von Anrufen verwechseln.</p> <p>Siehe die Informationen zum Parken von Anrufen in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Symbole für Akkuladestand und Signalstärke anzeigen	<p>Zeigt Akkuladestand und Signalstärke des Mobiltelefons auf dem IP-Telefon an, wenn das Mobiltelefon über Bluetooth mit dem IP-Telefon verbunden ist.</p> <p>Cisco IP-Telefon 8851NR unterstützt Bluetooth nicht.</p>
Eindeutiger Rufton	<p>Benutzer können anpassen, wie sie über eingehende Anrufe und neue Sprachnachrichten informiert werden.</p> <p>Siehe die Informationen zur Anrufübernahme in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Bitte nicht stören (DND)	<p>Wenn die Ruhefunktion eingeschaltet ist, werden während eines klingelnden Anrufs entweder keine Ruftöne oder weder Ruftöne noch visuelle Hinweise ausgegeben.</p> <p>Wenn aktiviert, wird der Überschriftenbereich des Telefonbildschirms rot, und „Nicht stören“ wird auf dem Telefon angezeigt.</p> <p>Wenn MLPP (Vorrangschaltung) konfiguriert ist und der Benutzer einen Prioritätsanruf erhält, ertönt auf dem Telefon ein spezieller Klingelton.</p> <p>Siehe <a href="#">DND konfigurieren, auf Seite 176</a>.</p>
„Über Leitungen hinweg zusammenführen“ (JAL) bzw. „Direkte Übergabe an eine andere Leitung“ (TAL) aktivieren/deaktivieren	<p>Ermöglicht dem Verwalter, die Funktionen „Über Leitungen hinweg zusammenführen“ (JAL) und „Direkte Übergabe an eine andere Leitung“ (TAL) zu steuern.</p> <p>Siehe „Richtlinie für Zusammenführung und direkte Übergabe“, <a href="#">Produktspezifische Konfiguration, auf Seite 146</a>.</p>
EnergyWise	<p>Ermöglicht, dass das IP-Telefon zu festgelegten Zeitpunkten aus- und eingeschaltet wird, um Energie zu sparen.</p> <p>Siehe <a href="#">EnergyWise für das Cisco IP-Telefon planen, auf Seite 173</a>.</p>
Erweiterter Leitungsmodus	<p>Aktivieren Sie den erweiterten Leitungsmodus, um die Tasten auf beiden Seiten des Telefondisplays als Leitungstasten zu verwenden.</p> <p>Siehe <a href="#">Zusätzliche Leitungstasten einrichten, auf Seite 206</a></p>
Erweiterte Secure Extension Mobility Cross Cluster (EMCC)	<p>Verbessert die EMCC-Funktion, indem die Netzwerk- und Sicherheitskonfiguration auf dem angemeldeten Telefon beibehalten wird. Die Sicherheitsrichtlinien werden eingehalten, die Netzwerkbandbreite wird aufrechterhalten und Netzwerkfehler im VC (Visiting Cluster) werden vermieden.</p>

Funktion	Beschreibung und weitere Informationen
Schnellwahldienst	<p>Ermöglicht dem Benutzer, einen Schnellwahlcode einzugeben, um einen Anruf zu tätigen. Schnellwahlcodes können Telefonnummern oder Einträgen im persönlichen Adressbuch zugewiesen werden. Siehe „Dienste“ in dieser Tabelle.</p> <p>Siehe <a href="#">Telefontastenvorlage für das persönliche Adressbuch oder die Schnellwahl ändern, auf Seite 204</a>.</p>
Gruppenanruf übernehmen	<p>Ermöglicht dem Benutzer, einen Anruf anzunehmen, der für eine Verzeichnisnummer in einer anderen Gruppe eingeht.</p> <p>Siehe die Informationen zur Anrufübernahme in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Steuerung des Headset-Eigenechos	<p>Ermöglicht einem Verwalter, die Eigenecho-Lautstärke eines kabelgebundenen Headsets einzustellen.</p>
Halten zurücksetzen	<p>Begrenzt die Zeitdauer, die ein Anruf gehalten werden kann, bevor er zurück auf das Telefon gestellt wird, von dem aus er gehalten wurde, und benachrichtigt den Benutzer.</p> <p>Zurückgestellte Anrufe unterscheiden sich durch einen einzigen Rufton (oder Signalton) von eingehenden Anrufen. Die Benachrichtigung wird in Intervallen wiederholt, wenn der Anruf nicht fortgesetzt wird.</p> <p>Ein Anruf, der „Halten zurücksetzen“ auslöst, zeigt auch ein animiertes Symbol an. Sie können eine Priorität für den Anruf-Fokus festlegen, um eingehenden oder zurückgestellten Anrufen den Vorrang zu geben.</p>
Halten-Status	<p>Ermöglicht Telefonen mit einer gemeinsam genutzten Leitung, lokale Leitungen und Remote-Leitungen, die einen Anruf halten, zu unterscheiden.</p>
Halten/Fortsetzen	<p>Ermöglicht dem Benutzer, einen Anruf vom aktiven Status in den gehaltenen Status zu wechseln.</p> <ul style="list-style-type: none"> <li>• Es ist keine Konfiguration erforderlich, außer wenn Sie die Warteschleifenmusik aktivieren möchten. Weitere Informationen finden Sie unter „Warteschleifenmusik“ in dieser Tabelle.</li> <li>• Siehe „Halten zurücksetzen“ in dieser Tabelle.</li> </ul>
HTTP-Download	<p>Verbessert den Prozess zum Herunterladen von Dateien auf das Telefon, indem HTTP verwendet wird. Wenn der HTTP-Download fehlschlägt, verwendet das Telefon wieder den TFTP-Download.</p>

Funktion	Beschreibung und weitere Informationen
Sammelanschlussgruppe	<p>Ermöglicht die Lastverteilung für Anrufe an die Hauptverzeichnisnummer. Ein Sammelanschluss umfasst mehrere Verzeichnisnummern, die eingehende Anrufe annehmen können. Wenn die erste Verzeichnisnummer des Sammelanschlusses besetzt ist, sucht das System in einer vorgegebenen Reihenfolge nach der nächsten freien Verzeichnisnummer in der Gruppe und leitet den Anruf an dieses Telefon weiter.</p> <p>Sie können die <b>Anrufer-ID</b> (sofern die Anrufer-ID konfiguriert ist), die <b>Verzeichnisnummer</b> und die <b>Pilotnummer für Sammelanschluss</b> in der Benachrichtigung für eingehende Anrufe für den Sammelanschlussanruf anzeigen lassen. Die Sammelanschlussnummer wird nach der Bezeichnung „Sammelanschluss“ angezeigt.</p> <p>Siehe die Informationen zu Sammelanschlussgruppe und Routing-Plänen in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Popup-Timer für eingehenden Anruf	<p>Ermöglicht Ihnen, die Zeitdauer festzulegen, die ein Toast (Benachrichtigung) für einen eingehenden Anruf auf dem Telefondisplay angezeigt wird.</p> <p>Siehe „Toast-Timer für eingehende Anrufe“, <a href="#">Produktspezifische Konfiguration, auf Seite 146</a>.</p>
Intelligent Proximity	<p>Ermöglicht Benutzern, ein Mobilgerät über Bluetooth mit dem Telefon zu koppeln und das Telefon zu verwenden, um mobile Anrufe zu tätigen und zu empfangen.</p> <p>Siehe <a href="#">Intelligent Proximity aktivieren, auf Seite 210</a>.</p> <p>Cisco IP-Telefon 8811, 8841 und 8851NR unterstützen Bluetooth oder Intelligent Proximity nicht.</p>
Intercom	<p>Ermöglicht dem Benutzer unter Verwendung von programmierbaren Telefontasten Intercom-Anrufe zu tätigen und anzunehmen. Die können Intercom-Leistungstasten konfigurieren, um:</p> <ul style="list-style-type: none"> <li>• einen bestimmten Intercom-Anschluss direkt anzuwählen.</li> <li>• einen Intercom-Anruf zu initiieren und den Benutzer aufzufordern, eine gültige Intercom-Nummer einzugeben.</li> </ul> <p><b>Hinweis</b> Wenn der Benutzer sich täglich mit seinem Cisco Anschlussmobilitätsprofil bei demselben Telefon anmeldet, weisen Sie diesem Profil die Telefontastenvorlage zu, die Intercom-Informationen enthält, und weisen Sie das Telefon als Standard-Intercom-Gerät für die Intercom-Leitung zu.</p>
Nur IPv6-Unterstützung	<p>Bietet Unterstützung für die erweiterte IP-Adressierung auf Cisco IP-Telefons. Die Konfiguration von IPv4 und IPv6 wird empfohlen und vollständig unterstützt. Bei einer eigenständigen Konfiguration werden bestimmte Funktionen nicht unterstützt. Nur IPv6-Adresse ist zugewiesen.</p> <p>Siehe <a href="#">Netzwerkeinstellungen konfigurieren, auf Seite 59</a>.</p>
Jitter-Puffer	<p>Die Jitter-Puffer-Funktion kann Jitter von 10 ms (Millisekunden) bis 1.000 ms für Audiostreams kompensieren.</p> <p>Die Funktion wird in einem Anpassungsmodus ausgeführt und passt die Jitter-Intensität dynamisch an.</p>

Funktion	Beschreibung und weitere Informationen
Zusammenführen	Ermöglicht Benutzern, durch Zusammenführen zweier Anrufe auf einer Leitung ein Konferenzgespräch zu erstellen und weiterhin verbunden zu bleiben.
Leitungsstatus für Anruflisten	<p>Ermöglicht dem Benutzer, den Leitungsstatus im Anrufverlauf anzuzeigen. Mögliche Leitungsstatuswerte sind:</p> <ul style="list-style-type: none"> <li>• Offline</li> <li>• Verfügbar</li> <li>• Wird verwendet</li> <li>• Bitte nicht stören</li> </ul> <p>Siehe <a href="#">BLF für Anruflisten aktivieren</a>, auf Seite 179.</p>
Leitungsstatus im Unternehmensverzeichnis	<p>Ermöglicht die Anzeige des Status für einen Kontakt im Unternehmensverzeichnis.</p> <ul style="list-style-type: none"> <li>• Offline</li> <li>• Verfügbar</li> <li>• Wird verwendet</li> <li>• Bitte nicht stören</li> </ul> <p>Siehe <a href="#">BLF für Anruflisten aktivieren</a>, auf Seite 179.</p>
Leitungsbeschreibung	<p>Legt eine Textbezeichnung anstatt eine Verzeichnisnummer für eine Leitung fest.</p> <p>Siehe <a href="#">Bezeichnung einer Leitung festlegen</a>, auf Seite 188.</p>
Abmelden von einem Sammelanschluss	<p>Ermöglicht dem Benutzer, sich von einem Sammelanschluss abzumelden und eingehende Anrufe auf seinem Telefon vorübergehend zu blockieren. Wenn Sie sich von einem Sammelanschluss abmelden, werden Anrufe, die nicht an den Sammelanschluss gerichtet sind, weiterhin an Ihr Telefon durchgestellt.</p> <p>Siehe die Informationen zu Routing-Plänen in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Identifikation böswilliger Anrufer (MCID, Malicious Caller Identification)	Ermöglicht dem Benutzer, den Systemadministrator über verdächtige Anrufe zu benachrichtigen.
MeetMe-Konferenz	Ermöglicht dem Benutzer, eine Meet-Me-Konferenz durchzuführen, in der andere Teilnehmer zu einer geplanten Zeit eine im Voraus festgelegte Rufnummer wählen.
Wartende Nachrichten	<p>Definiert Verzeichnisnummern für die Anzeige von wartenden Nachrichten. Ein direkt verbundenes Sprachnachrichtensystem verwendet die angegebene Verzeichnisnummer, um eine Anzeige für wartende Nachrichten für ein bestimmtes Cisco IP-Telefon zu aktivieren oder zu deaktivieren.</p> <p>Siehe die Informationen zu wartenden Nachrichten und Voicemail in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>

Funktion	Beschreibung und weitere Informationen
Anzeige für wartende Nachrichten	Ein Licht am Hörer, das anzeigt, dass ein Benutzer mindestens eine neue Voicemail hat. Siehe die Informationen zu wartenden Nachrichten und Voicemail in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
Minimale Ruftonlautstärke	Legt eine minimale Ruftonlautstärke für ein IP-Telefon fest.
Protokollierung der Anrufe in Abwesenheit	Ermöglicht dem Benutzer, festzulegen, ob verpasste Anrufe im Verzeichnis verpasster Anrufe für eine bestimmte Leitung protokolliert werden. Siehe die Informationen zu Verzeichnisnummern in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
Mobile Verbindung	Ermöglicht dem Benutzer, geschäftliche Anrufe mit einer einzigen Telefonnummer zu verwalten und aktive Anrufe auf dem Bürotelefon oder einem Remotegerät anzunehmen. Der Benutzer kann die Anrufergruppe basierend auf der Telefonnummer und Tageszeit einschränken. Siehe die Informationen zu Cisco Unified Mobility in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
Mobil- und Remote Access über Expressway	Ermöglicht Remotebenutzern, sich einfach und sicher mit dem Firmennetzwerk zu verbinden, ohne einen VPN-Clientunnel verwenden zu müssen. Siehe <a href="#">Mobil- und Remote Access über Expressway, auf Seite 182</a>
MVA (Mobile Voice Access)	Erweitert die Funktionen für die mobile Verbindung, indem die Benutzer auf ein IVR-System (Interactive Voice Response) zugreifen können, um einen Anruf auf einem Remotegerät zu initiieren. Siehe die Informationen zu Cisco Unified Mobility in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
Überwachung und Aufzeichnung	Ermöglicht einem Supervisor einen aktiven Anruf mitzuhören. Der Supervisor kann vom anderen Teilnehmer nicht gehört werden. Der Benutzer kann möglicherweise einen Signalton hören, wenn der Anruf überwacht wird. Wenn ein Anruf geschützt ist, wird der Sicherheitsstatus des Anrufs auf Cisco IP-Telefons als Schloss-Symbol angezeigt. Die verbundenen Teilnehmer hören möglicherweise auch einen Signalton, der angibt, dass der Anruf sicher ist und überwacht wird. <b>Hinweis</b> Während ein aktiver Anruf überwacht oder aufgezeichnet wird, kann der Benutzer Intercom-Anrufe tätigen und annehmen. Wenn der Benutzer jedoch einen Intercom-Anruf tätigt, wird der aktive Anruf gehalten, die Aufzeichnungssitzung wird abgebrochen und die Überwachungssitzung wird angehalten. Um die Überwachungssitzung fortzusetzen, muss der überwachte Teilnehmer den Anruf fortsetzen.
MLPP (Multilevel Precedence and Preemption)	Ermöglicht es dem Benutzer, dringende oder wichtige Anrufe in speziellen Umgebungen, beispielsweise beim Militär oder bei Behörden, zu tätigen und anzunehmen. Siehe <a href="#">MLPP (Multilevel Precedence and Preemption), auf Seite 199</a> .



Funktion	Beschreibung und weitere Informationen
Mehrere Anrufe pro Leitung	<p>Jede Leitung kann mehrere Anrufe unterstützen. Standardmäßig unterstützt das Telefon zwei aktive Anrufe pro Leitung und maximal sechs aktive Anrufe pro Leitung. Es kann immer nur ein einziger Anruf verbunden sein. Alle anderen Anrufe werden automatisch gehalten, d. h. in die Warteschleife gestellt.</p> <p>Auf dem System können Sie die maximale Anzahl an Anrufen bzw. Auslösern bei Besetztzeichen bis zu einem Maximalwert von 6/6 konfigurieren. Eine Konfiguration über 6/6 wird offiziell nicht unterstützt.</p> <p>Weitere Informationen zu Verzeichnisnummern finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.</p>
Warteschleifenmusik	Gibt Musik wieder, während ein Anruf gehalten wird.
Stummschaltung	Schaltet das Mikrofon des Hörers oder des Headsets stumm.
Kein Alarmname	Macht es dem Benutzer einfacher, übergebene Anruf zu identifizieren, da die Telefonnummer des ursprünglichen Anrufers angezeigt wird. Der Anruf wird als Benachrichtigung gefolgt von der Telefonnummer des Anrufers angezeigt.
Wählen mit aufgelegtem Hörer	Ermöglicht dem Benutzer, eine Nummer zu wählen, ohne den Hörer abzulegen. Der Benutzer kann den Hörer abnehmen oder Wählen drücken.
Andere Gruppenübernahme	<p>Ermöglicht dem Benutzer, einen Anruf anzunehmen, der auf einem Telefon in einer anderen Gruppe eingeht, die mit der Gruppe des Benutzers verknüpft ist.</p> <p>Siehe die Informationen zur Anrufübernahme in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Meldung für Anschlussmobilitäts-Benutzer auf dem Telefondisplay	Mit dieser Funktion wird die Benutzeroberfläche des Telefons durch die Bereitstellung benutzerfreundlicher Meldungen für Anschlussmobilitäts-Benutzer optimiert.
Benachrichtigung für Telefonvertrauensliste in Cisco Unified Communications Manager	<p>Ermöglicht dem Telefon, bei Aktualisierung der Vertrauensliste eine Warnung an Cisco Unified Communications Manager zu senden.</p> <p>Siehe <a href="#">Unterstützte Sicherheitsfunktionen, auf Seite 88</a>.</p>
PLK-Unterstützung für Warteschlangenstatus	Die Funktion „Unterstützung programmierbarer Leitungstasten für Warteschlangenstatistik“ ermöglicht Benutzern, die Anrufwarteschlangenstatistik für Hunt Pilots abzufragen und die Informationen auf dem Telefonbildschirm anzuzeigen.
Pluszeichen wählen	<p>Ermöglicht dem Benutzer das Wählen von E.164-Nummern, denen ein Pluszeichen (+) vorangestellt ist.</p> <p>Um das Pluszeichen zu wählen, muss der Benutzer die Sterntaste (*) mindestens eine Sekunde lang gedrückt halten. Dies gilt für das Wählen der ersten Ziffer für einen Anruf bei aufgelegtem und abgenommenem Hörer.</p>
Energieaushandlung über LLDP	<p>Ermöglicht dem Telefon, die Energie mit LLDP (Link Level Endpoint Discovery Protocol) und CDP (Cisco Discovery Protocol) auszuhandeln.</p> <p>Siehe „Leistungsaushandlung“, <a href="#">Produktspezifische Konfiguration, auf Seite 146</a>.</p>

Funktion	Beschreibung und weitere Informationen
Predictive Dialing	<p>Erleichtert die Durchführung eines Anrufs. In der Anrufliste werden nur die Telefonnummern angezeigt, die der gewählten Nummer ähnlich sind.</p> <p>Predictive Dialing ist verfügbar, wenn der erweiterte Leitungsmodus aktiviert ist. „UI für vereinfachten neuen Anruf“ muss deaktiviert sein, damit Predictive Dialing funktioniert.</p>
Privatfunktion	<p>Verhindert, dass sich Benutzer auf einer gemeinsam genutzten Leitung zum Anruf des anderen Benutzers hinzufügen und dass Informationen zum Anruf des anderen Benutzers auf ihrem Telefondisplay angezeigt werden.</p> <p>Siehe die Informationen zu Aufschaltung und Privatfunktion in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
PLAR (Private Line Automated Ringdown)	<p>Der Cisco Unified Communications Manager-Verwalter kann eine Telefonnummer konfigurieren, die Cisco IP-Telefon wählt, sobald der Hörer abgehoben wird. Dies kann bei Telefonen hilfreich sein, die zum Wählen von Notruf- und „Hotline“-Nummern vorgesehen sind.</p> <p>Der Administrator kann eine Verzögerung von bis zu 15 Sekunden konfigurieren. Dies ermöglicht es dem Benutzer, einen Anruf zu tätigen, bevor das Telefon die standardmäßige Hotline-Nummer anwählt. Der Timer kann über den Parameter <b>Timer Abgehoben bis erste Ziffer</b> unter <b>Geräte &gt; Geräteeinstellungen &gt; SIP-Profil</b> konfiguriert werden.</p> <p>Weitere Informationen finden Sie im <i>Funktionskonfigurationshandbuch für Cisco Unified Communications Manager</i>.</p>
Tool für Problemlberichte	<p>Sendet Telefonprotokolle und Problemlberichte an den Administrator.</p> <p>Siehe <a href="#">Tool zur Problemmeldung, auf Seite 187</a>.</p>
Programmierbare Funktionstasten	<p>Sie können Leitungstasten Funktionen wie „Anruf“, „Rückruf“ und „Rufumleitung“ zuweisen.</p> <p>Siehe die Informationen zur Telefontastenvorlage in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Tool für Qualitätsberichte (QRT)	<p>Ermöglicht den Benutzern das Senden von Informationen zu Anrufproblemen, indem sie eine Taste drücken. QRT kann für zwei Benutzermodi konfiguriert werden, abhängig von der gewünschten Benutzerinteraktion mit QRT.</p>
Letzte	<p>Ermöglicht Benutzern, die letzten 150 Anrufe und Anrufgruppen anzuzeigen. Sie können die zuletzt gewählten Nummern und Anrufe in Abwesenheit anzeigen sowie Anrufdaten löschen.</p>
Wahlwiederholung	<p>Ermöglicht den Benutzern durch das Drücken einer Taste oder des Wahlwiederholung-Softkeys die zuletzt gewählte Telefonnummer zu wählen.</p>

Funktion	Beschreibung und weitere Informationen
Remote-Port-Konfiguration	<p>Ermöglicht Ihnen, die Geschwindigkeit und Duplex-Funktion für die Ethernet-Telefonports in der Cisco Unified Communications Manager-Verwaltung remote zu konfigurieren. Dies verbessert die Leistung für große Bereitstellungen mit bestimmten Porteinstellungen.</p> <p><b>Hinweis</b> Wenn die Ports in Cisco Unified Communications Manager für die Remote-Portkonfiguration konfiguriert sind, können die Daten auf dem Telefon nicht geändert werden.</p> <p>Siehe „Remote-Portkonfiguration“, <a href="#">Produktspezifische Konfiguration</a>, auf Seite 146.</p>
Anrufe an ein Remoteziel an die Büronummer umleiten	<p>Leitet einen Anruf, der auf dem Mobiltelefon des Benutzers eingeht, an die Büronummer um. Wenn ein Anruf am Remoteziel (Mobiltelefon) eingeht, läutet nur das Remoteziel. Das Bürotelefon läutet nicht. Wenn ein Anruf auf dem Mobiltelefon angenommen wird, wird auf dem Bürotelefon die Meldung „Remote genutzt“ angezeigt. Während dieser Anrufe können Benutzer verschiedene Funktionen auf ihrem Mobiltelefon nutzen.</p> <p>Siehe die Informationen zu Cisco Unified Mobility in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Timer für das Entfernen der Aufforderung „Anruf beendet“	<p>Verbessert die Reaktionszeit beim Beenden von Anrufen durch Entfernen der Meldung <code>Anruf beendet</code> vom Telefondisplay.</p>
Ruftoneinstellung	<p>Identifiziert den für eine Leitung verwendeten Ruftontyp, wenn ein anderer Anruf auf einem Telefon aktiv ist.</p> <p>Weitere Informationen zu Verzeichnisnummern finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager und in <a href="#">Benutzerdefinierte Ruftöne</a>, auf Seite 117.</p>
RTCP-Halten für SIP	<p>Stellt sicher, dass gehaltene Anrufe nicht vom Gateway getrennt werden. Das Gateway überprüft den Status des RTCP-Ports, um zu bestimmen, ob einer Anruf aktiv ist. Wenn der Telefonport offen ist, werden gehaltene Anrufe nicht vom Gateway beendet.</p>
Sichere Konferenz	<p>Ermöglicht Konferenzanrufe auf sicheren Telefonen über eine geschützte Konferenzbrücke. Wenn mithilfe der Softkeys „Konfer.“, „Zusf.“ oder „Aufsch.“ oder über eine MeetMe-Konferenz neue Teilnehmer hinzugefügt werden, wird das Symbol für einen sicheren Anruf angezeigt, sofern alle Teilnehmer ein sicheres Telefon verwenden.</p> <p>In der Konferenzliste wird die Sicherheitsstufe der Konferenzteilnehmer angezeigt. Initiatoren können nicht sichere Teilnehmer aus der Konferenzliste entfernen. Teilnehmer können andere Teilnehmer hinzufügen oder entfernen, wenn der Parameter Erweiterte Ad-hoc-Konferenz aktiviert festgelegt ist.</p> <p>Siehe die Informationen zu Konferenzbrücke und Sicherheit in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager und unter <a href="#">Unterstützte Sicherheitsfunktionen</a>, auf Seite 88.</p>
Sicherer EMCC	<p>Verbessert die EMCC-Funktion, da die Sicherheit für einen Benutzer erhöht wird, der sich an einem Remotestandort an seinem Telefon anmeldet.</p>

Funktion	Beschreibung und weitere Informationen
Services	<p>Ermöglicht Ihnen, in der Cisco Unified Communications Manager-Verwaltung im Menü „Konfiguration der Cisco IP-Telefon-Dienste“ die Liste der Telefondienste zu definieren und zu pflegen, die von den Benutzern abonniert werden können.</p> <p>Siehe die Informationen zu Diensten in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Taste „Dienste-URL“	<p>Ermöglicht Benutzern den Zugriff auf Dienste über eine programmierbare Taste anstatt über das Menü „Dienste“ auf einem Telefon.</p> <p>Siehe die Informationen zu Diensten in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p>
Anrufer-ID und Nummer anzeigen	<p>Das Telefon kann die Anrufer-ID und die Nummer von eingehenden Anrufen anzeigen. Die Größe des LCD-Displays des IP-Telefons beschränkt die Länge der angezeigten Anrufer-ID und Anrufernummer.</p> <p>Die Einstellungen Anrufer-ID anzeigen und Anrufernummer sind nur für eingehende Anrufhinweise relevant und ändern die Einstellungen Anruf weiterleiten und Sammelanschluss nicht.</p> <p>Siehe „Anrufer-ID“ in dieser Tabelle.</p>
Vereinfachen der Extension Mobility mit Cisco-Headsets	<p>Ermöglicht dem Benutzer, sich mit seinem Cisco-Headset bei Extension Mobility anzumelden.</p> <p>Wenn sich das Telefon im MRA-Modus befindet, kann sich der Benutzer mit dem Headset am Telefon anmelden.</p> <p>Diese Funktion erfordert Cisco Unified Communications Manager (UCM) Version 11.5(1)SU8, 11.5(1)SU.9, 12.5(1)SU3 oder höher.</p> <p>Weitere Informationen finden Sie im <i>Funktionskonfigurationshandbuch für Cisco Unified Communications Manager</i>, Version 11.5(1)SU8 oder höher oder Version 12.5(1)SU3 oder höher.</p>
Vereinfachte Tablet-Unterstützung	<p>Ermöglicht einem Android- oder iOS-Tablet-Benutzer, das Tablet über Bluetooth mit dem Telefon zu koppeln und das Telefon dann für den Audio-Teil eines Anrufs auf dem Tablet zu verwenden.</p> <p>Siehe <a href="#">Intelligent Proximity aktivieren, auf Seite 210</a>.</p> <p>Cisco IP-Telefon 8851NR unterstützt Bluetooth nicht.</p>
Kurzwahl	<p>Wählt eine angegebene Nummer, die zuvor gespeichert wurde.</p>
SSH-Zugriff	<p>Ermöglicht Ihnen, die SSH-Zugriffseinstellung in der Cisco Unified Communications Manager-Verwaltung zu aktivieren oder zu deaktivieren. Wenn Sie den SSH-Server aktivieren, kann das Telefon SSH-Verbindungen akzeptieren. Wenn Sie die SSH-Serverfunktionalität des Telefons deaktivieren, wird der SSH-Zugriff auf das Telefon gesperrt.</p> <p>Siehe „SSH-Zugriff“, <a href="#">Produktspezifische Konfiguration, auf Seite 146</a>.</p>

Funktion	Beschreibung und weitere Informationen
Tageszeit-Routing	Beschränkt den Zugriff auf Telefoniefunktionen in Abhängigkeit vom Zeitraum. Siehe die Informationen zu Zeitraum und Tageszeit-Routing in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
Aktualisierung der Zeitzone	Aktualisiert Cisco IP-Telefon mit Zeitonenänderungen. Siehe die Informationen zu Datum und Uhrzeit in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
Übergabe	Ermöglicht Benutzern, verbundene Anrufe von ihrem Telefon an eine andere Nummer umzuleiten.
Übergabe – direkte Übergabe	Übergabe: Der erste Aufruf von „Übergabe“ initiiert immer einen neuen Anruf mit derselben Verzeichnisnummer, nachdem der aktive Anruf in die Warteschleife gestellt wurde. Mit der Funktion „Aktiven Anruf übergeben“ kann der Benutzer Anrufe direkt übergeben. Einige JTAPI-/TAPI-Anwendungen sind nicht mit der Implementierung der Funktion „Zusammenführen und direkte Übergabe“ auf dem Cisco IP-Telefon kompatibel. Daher müssen Sie möglicherweise die Richtlinie für Zusammenführen und direkte Übergabe konfigurieren, um das Zusammenführen und die direkte Übergabe auf derselben Leitung oder u. U. über Leitungen hinweg zu deaktivieren. Siehe die Informationen zu Verzeichnisnummern in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
TVS	TVS (Trust Verification Services) ermöglicht Telefonen, signierte Konfigurationen und andere Server oder Peers zu authentifizieren, ohne die CTL (Certificate Trust List) zu vergrößern oder das Herunterladen einer aktualisieren CTL-Datei auf das Telefon zu erfordern. TVS ist standardmäßig aktiviert. TVS-Informationen werden auf dem Telefon im Menü „Sicherheitseinstellungen“ angezeigt.
UCR 2013	Cisco IP-Telefons unterstützen UCR (Unified Capabilities Requirements) 2013 durch Bereitstellung der folgenden Funktionen: <ul style="list-style-type: none"> <li>• Unterstützung für FIPS (Federal Information Processing Standard) 140-2</li> <li>• Unterstützung für 80-Bit SRTCP-Markierung</li> </ul> Als IP-Telefonverwalter müssen Sie spezifische Parameter in der Cisco Unified Communications Manager-Verwaltung einrichten.
Benachrichtigung über nicht konfigurierte Hauptleitung	Informiert den Benutzer, wenn die Hauptleitung nicht konfiguriert wurde. Dem Benutzer wird auf dem Telefondisplay die Meldung <code>Nicht bereitgestellt</code> angezeigt.
Aktualisierungen der Benutzeroberfläche für „Liste“, „Warnung“ und „Visual Voicemail“	Vergrößert das Anwendungsfenster, um gekürzte Zeichenfolgen zu minimieren.

Funktion	Beschreibung und weitere Informationen
Videomodus	<p>Ermöglicht einem Benutzer, in Abhängigkeit von den im System konfigurierten Modi den Videomodus auszuwählen, der zum Anzeigen einer Videokonferenz verwendet wird.</p> <p>Siehe die Informationen zum Video in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.</p> <p>Auf Cisco IP-Telefon 8845, 8865 und 8865NR verfügbar.</p>
Videomodus	<p>Ermöglicht Videounterstützung auf dem Telefon. Für Videoanrufe muss der Parameter „Videofunktionen“ im Fenster „Telefonkonfiguration“ von Cisco Unified Communications Manager aktiviert sein. Der Parameter ist standardmäßig aktiviert.</p> <p>Auf Cisco IP-Telefon 8845, 8865 und 8865NR verfügbar.</p>
Video über den PC	<p>Ermöglicht Benutzern, mit ihrem Cisco Unified IP-Telefon, einem PC und einer externen Videokamera Videoanrufe zu tätigen.</p> <p>Darüber hinaus ermöglicht die Funktion Benutzern, mit Cisco Jabber oder Cisco Unified Video Advantage-Produkten Videoanrufe zu tätigen.</p>
Visual Voicemail	<p>Ersetzt die Voicemail-Audio-Aufforderungen durch eine grafische Benutzeroberfläche.</p> <p>Siehe <i>Installation and Configuration Guide for Visual Voicemail</i> (Installations- und Konfigurationshandbuch für Visual Voicemail) unter <a href="http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3">http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3</a>.</p>
Voicemail-System	<p>Ermöglicht dem Anrufer, eine Nachricht zu hinterlassen, wenn ein Anruf nicht angenommen wird.</p> <p>Siehe die Informationen zu Voicemail in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager und unter <a href="#">Visual Voicemail einrichten</a>, auf Seite 196.</p>
VPN	<p>Stellt mithilfe von SSL eine VPN-Verbindung (Virtual Private Network, virtuelles privates Netzwerk) auf dem Cisco Unified IP-Telefon her, wenn sich dieses außerhalb eines vertrauenswürdigen Netzwerks befindet oder wenn der Netzwerkdatenverkehr zwischen dem Telefon und Unified Communications Manager nicht vertrauenswürdige Netzwerke durchlaufen muss.</p>
Standardmäßig deaktivierter Webzugriff	<p>Verbessert die Sicherheit, da der Zugriff auf alle Webservices, beispielsweise HTTP, deaktiviert wird. Benutzer können nur auf Webdienste zugreifen, wenn Sie den Webzugriff aktivieren.</p>

#### Verwandte Themen

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

## Funktionstasten und Softkeys

Die folgende Tabelle enthält Informationen zu den Funktionen, die auf Softkeys und Funktionstasten verfügbar sind und die Sie als programmierbare Funktionstasten konfigurieren müssen. Ein Eintrag „Unterstützt“ in der Tabelle zeigt an, dass die Funktion für den entsprechenden Tastentyp oder Softkey unterstützt wird. Nur programmierbare Funktionstasten müssen in der Cisco IP-Telefon-Verwaltung konfiguriert werden.

Für Informationen zu programmierbaren Funktionstasten siehe [Vorlagen für Telefontasten, auf Seite 201](#).

**Table 30: Funktionen und entsprechende Tasten und Softkeys**

<b>Funktionsname</b>	<b>Spezielle Funktionstaste</b>	<b>Programmierbare Funktionstaste</b>	<b>Softkey</b>
Hinweisanrufe	Nicht unterstützt	Unterstützt	Nicht unterstützt
Alle Anrufe	Nicht unterstützt	Unterstützt	Nicht unterstützt
Anrufannahme	Nicht unterstützt	Unterstützt	Unterstützt
Konferenzanschaltung	Nicht unterstützt	Nicht unterstützt	Unterstützt
Rückruf	Nicht unterstützt	Unterstützt	Unterstützt
Rufumleitung Alle Anrufe	Nicht unterstützt	Nicht unterstützt	Unterstützt
Anruf parken	Nicht unterstützt	Unterstützt	Unterstützt
Anruf parken – Leitungsstatus	Nicht unterstützt	Unterstützt	Nicht unterstützt
Anrufübernahme	Nicht unterstützt	Unterstützt	Unterstützt
Anruf übernehmen – Leitungsstatus	Nicht unterstützt	Unterstützt	Nicht unterstützt
Konferenz	Unterstützt	Nicht unterstützt	Unterstützt
Umleiten	Nicht unterstützt	Nicht unterstützt	Unterstützt
Bitte nicht stören	Nicht unterstützt	Unterstützt	Unterstützt
Gruppenübernahme	Nicht unterstützt	Unterstützt	Unterstützt
Halten	Unterstützt	Nicht unterstützt	Unterstützt
Sammelanschlussgruppen	Nicht unterstützt	Unterstützt	Nicht unterstützt
Intercom	Nicht unterstützt	Unterstützt	Nicht unterstützt
Identifizierung böswilliger Anrufer (Fangschaltung)	Nicht unterstützt	Unterstützt	Unterstützt
MeetMe	Nicht unterstützt	Unterstützt	Unterstützt
Zusammenführen	Nicht unterstützt	Nicht unterstützt	Unterstützt
Mobile Verbindung (Mobilität)	Nicht unterstützt	Unterstützt	Unterstützt
Stummschaltung	Unterstützt	Nicht unterstützt	Nicht unterstützt

Funktionsname	Spezielle Funktionstaste	Programmierbare Funktionstaste	Softkey
Andere Übernahme	Nicht unterstützt	Unterstützt	Unterstützt
Unterstützung programmierbarer Leitungstasten für Warteschlangenstatus	Nicht unterstützt	Nicht unterstützt	Unterstützt
Privatfunktion	Nicht unterstützt	Unterstützt	Nicht unterstützt
Warteschlangenstatus	Nicht unterstützt	Unterstützt	Nicht unterstützt
Tool für Qualitätsberichte (QRT)	Nicht unterstützt	Unterstützt	Unterstützt
Aufzeichnen	Nicht unterstützt	Nicht unterstützt	Unterstützt
Wahlwiederholung	Nicht unterstützt	Unterstützt	Unterstützt
Kurzwahl	Nicht unterstützt	Unterstützt	Nicht unterstützt
Kurzwahl – Leitungsstatus	Nicht unterstützt	Unterstützt	Nicht unterstützt
Unterstützung für Halten-Taste auf USB-Headsets	Nicht unterstützt	Nicht unterstützt	Unterstützt
Übergabe	Unterstützt	Nicht unterstützt	Unterstützt

## 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.

## Einrichten von Telefonfunktionen für alle Telefone

### Prozedur

---

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

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

---

## 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.
-

## 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.
- 

## Produktspezifische Konfiguration

In der folgenden Tabelle werden die Felder im Bereich „Produktspezifische Konfiguration – Layout“ beschrieben.

**Tabelle 31: Felder im Bereich „Produktspezifische Konfiguration“**

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Lautsprecher deaktivieren	Kontrollkästchen	Deaktiviert	Die Lautsprecherfunktion des Telefons wird deaktiviert.
Freisprechanlage und Headset deaktivieren	Kontrollkästchen	Deaktiviert	Die Lautsprecherfunktion und das Headset des Telefons werden deaktiviert.
Hörer deaktivieren	Kontrollkästchen	Deaktiviert	Die Hörerfunktion des Telefons wird deaktiviert.
PC-Port	Aktiviert Deaktiviert	Aktiviert	Legt fest, ob der PC-Port zum Verbinden eines Computers mit dem LAN verwendet werden kann.
Zugriff auf Einstellungen	Deaktiviert Aktiviert Eingeschränkt	Aktiviert	Aktiviert, deaktiviert oder schränkt den Zugriff auf die lokalen Telefonkonfigurationseinstellungen in der App „Einstellungen“ ein. <ul style="list-style-type: none"> <li>• Deaktiviert – Im Menü „Einstellungen“ werden keine Optionen angezeigt.</li> <li>• Aktiviert – Auf alle Einträge im Menü „Einstellungen“ kann zugegriffen werden.</li> <li>• Eingeschränkt – Es kann nur auf das Menü „Telefonereinstellungen“ zugegriffen werden.</li> </ul>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
PC-Sprach-VLAN-Zugriff	Aktiviert Deaktiviert	Aktiviert	<p>Gibt an, ob ein Gerät, das am PC-Port angeschlossen ist, auf das Sprach-VLAN des Telefons zugreifen kann.</p> <ul style="list-style-type: none"> <li>• Deaktiviert – Der PC kann keine Daten über das Sprach-VLAN oder über das Telefon senden und empfangen.</li> <li>• Aktiviert – Der PC kann Daten über das Sprach-VLAN oder über das Telefon senden und empfangen. Legen Sie dieses Feld auf „Aktiviert“ fest, wenn eine Anwendung auf dem Computer ausgeführt wird, die den Telefon-Datenverkehr überwacht. Dazu können Überwachungs- und Aufzeichnungsanwendungen sowie die Verwendung von Netzwerküberwachungssoftware für Analysezwecke zählen.</li> </ul>
Videofunktionen	Aktiviert Deaktiviert	8845, 8865 und 8865NR: Aktiviert  8811, 8851, 8851NR, 8861: Deaktiviert	Ermöglicht Benutzern, mit einem Cisco IP-Telefon, einem PC und einer Videokamera Videoanrufe zu tätigen.
Webzugriff	Deaktiviert Aktiviert	Deaktiviert	<p>Aktiviert oder deaktiviert den Zugriff auf die Webseiten des Telefons über einen Webbrowser.</p> <p><b>Vorsicht</b> Wenn Sie dieses Feld aktivieren, legen Sie möglicherweise vertrauliche Daten über das Telefon offen.</p>
TLS 1.0 und TLS 1.1 für Webzugriff deaktivieren	Deaktiviert Aktiviert	Deaktiviert	<p>Steuert die Verwendung von TLS 1.2 für eine Webserververbindung.</p> <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 und Richtlinien für die Verwendung
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>
Display nicht aktiv – Tage	Tage der Woche		<p>Definiert die Tage, an denen sich das Telefondisplay nicht automatisch zur im Feld „Anzeige einschalten – Uhrzeit“ eingetragenen 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>
Display eingeschaltet – Uhrzeit	hh:mm		<p>Definiert die Uhrzeit, zu der sich das Telefondisplay jeden Tag automatisch einschaltet (außer an den im Feld „Anzeige 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 das Display beispielsweise um 07:00 Uhr (0700) einzuschalten, geben Sie 07:00 ein. Um das Display um 14.00 Uhr (1400) einzuschalten, geben Sie 14:00 ein.</p> <p>Wenn in dieses Feld nichts eingegeben wird, schaltet sich das Display automatisch um 00:00 Uhr ein.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Display eingeschaltet – Dauer	hh:mm		<p>Definiert den Zeitraum, für den das Telefondisplay eingeschaltet bleibt, nachdem es sich zur im Feld „Anzeige einschalten – Uhrzeit“ angegebenen Uhrzeit eingeschaltet hat.</p> <p>Um das Display beispielsweise für vier Stunden und 30 Minuten zu aktivieren, nachdem es automatisch aktiviert wurde, 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 „Anzeige einschalten – Uhrzeit“ der Wert „00:00“ eingetragen und im Feld „Anzeige eingeschaltet – Dauer“ kein Wert (oder „24:00“) vorhanden ist, wird das Display nicht ausgeschaltet.</p>
Display Laufzeitbeschränkung	hh:mm	01:00	<p>Definiert den Zeitraum, für den das Telefon inaktiv gewesen sein muss, bevor sich das Display abschaltet. 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 Stunden:Minuten 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 01:30 ein.</p> <p>Weitere Informationen hierzu finden Sie unter <a href="#">Inaktives Display konfigurieren, auf Seite 120</a>.</p>
Anzeige bei eingehendem Anruf aktivieren	Deaktiviert Aktiviert	Aktiviert	Schaltet das inaktive Display ein, wenn ein Anruf eingeht.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
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>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
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>
Telefon ausschalten – Uhrzeit	hh:mm		<p>Ermittelt 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>
Telefon ausschalten - Leerlauf-Timeout	20 bis 1440 Minuten	60	<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>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Signalton aktivieren	Kontrollkästchen	Deaktiviert	Wenn diese Option aktiviert ist, gibt das Telefon 10 Minuten vor der angegebenen Ausschaltzeit einen Signalton aus.  Dieses Kontrollkästchen ist nur relevant, wenn im Listenfeld Power Save Plus aktivieren mindestens ein Tag ausgewählt ist.
EnergyWise-Domäne	Bis zu 127 Zeichen		Ermittelt die EnergyWise-Domäne, in der sich das Telefon befindet.
EnergyWise-Secret	Bis zu 127 Zeichen		Ermittelt das Kennwort der Sicherheitsabfrage, das in der Kommunikation mit den Endgeräten in der EnergyWise-Domäne verwendet wird.
EnergyWise-Überschreibung zulassen	Kontrollkästchen	Deaktiviert	Bestimmt, ob die Controller-Richtlinie der EnergyWise-Domäne aktualisierte Energiepegelraten an die Telefone senden darf. Es gelten die folgenden Bedingungen: <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>



Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Richtlinie für Zusammenführung und direkte Übergabe	Gleiche Leitung, mehrere Leitungen aktivieren  Nur gleiche Leitung aktivieren  Gleiche Leitung, mehrere Leitungen deaktivieren	Gleiche Leitung, mehrere Leitungen aktivieren	Steuert die Möglichkeit eines Benutzers, Anrufen beitreten und diese zu übergeben. <ul style="list-style-type: none"> <li>• Gleiche Leitung, mehrere Leitungen aktivieren – Benutzer können einen Anruf auf der aktuellen Leitung an einen Anruf auf einer anderen Leitung übergeben oder diesem beitreten.</li> <li>• Nur gleiche Leitung aktivieren – Benutzer können Anrufe nur direkt übergeben oder an diesen teilnehmen, wenn beide Anrufe auf derselben Leitung stattfinden.</li> <li>• Gleiche Leitung, mehrere Leitungen deaktivieren – Benutzer können keine Anrufe auf derselben Leitung übergeben oder an diesen teilnehmen. Die Beitritts- und Übergabefunktionen sind deaktiviert, und der Benutzer kann diese Funktionen nicht verwenden.</li> </ul>
An PC-Port weiterleiten	Deaktiviert Aktiviert	Deaktiviert	Gibt an, ob das Telefon Pakete, die über den Netzwerk-Port gesendet und empfangen werden, an den Access-Port weiterleitet.
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>
Cisco Discovery Protocol (CDP): Switchport	Deaktiviert Aktiviert	Aktiviert	Steuert das CDP (Cisco Discovery Protocol) für den SW-Port des Telefons.
Cisco Discovery Protocol (CDP): PC-Port	Deaktiviert Aktiviert	Aktiviert	Steuert das CDP (Cisco Discovery Protocol) für den PC-Port des Telefons.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Link Layer Discovery Protocol – Media Endpoint Discover (LLDP-MED): Switchport	Deaktiviert Aktiviert	Aktiviert	Aktiviert LLDP-MED für den SW-Port.
Link Layer Discovery Protocol – (LLDP): PC-Port	Deaktiviert Aktiviert	Aktiviert	Aktiviert LLDP für den PC-Port.
LLDP Asset-ID	Zeichenfolge mit bis zu 32 Zeichen		Identifiziert die Asset-ID, die dem Telefon für die Bestandsverwaltung zugewiesen wird.
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 Aktiviert Deaktiviert	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>
Automatische Portsynchronisierung	Deaktiviert Aktiviert	Deaktiviert	Synchronisiert Ports auf die geringste Geschwindigkeit zwischen den Ports eines Telefons, um Paketverlust zu vermeiden.
Remotekonfiguration für Switchport	Deaktiviert Aktiviert	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.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Remotekonfiguration für PC-Port	Deaktiviert Aktiviert	Deaktiviert	Ermöglicht es Ihnen, die Geschwindigkeit und Duplex-Funktion für den PC-Port des Telefons remote zu konfigurieren. Dies verbessert die Leistung für große Bereitstellungen mit bestimmten Porteinstellungen.  Wenn die 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).
Popup-Timer für eingehenden Anruf	0, 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, 60	5	Gibt die Zeitdauer, die ein Toast angezeigt wird, in Sekunden an. Die Zeitdauer umfasst das Ein- und Ausblenden des Fensters.  0 bedeutet, dass der Hinweis bei eingehendem Anruf deaktiviert ist.
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.
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	Gibt an, ob ein Anruf auf einer gemeinsam genutzten Leitung im Anrufprotokoll aufgezeichnet werden soll.
Minimale Ruftonlautstärke	0-Stumm 1–15	0-Stumm	Steuert die minimale Ruftonlautstärke für das Telefon.  Sie können ein Telefon so einstellen, dass der Klingelton deaktiviert werden kann.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
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		<p>Identifiziert den alternativen IPv4-Server, den das Telefon verwendet, um Firmware und Updates abzurufen.</p> <p>Das Format für die Adresse lautet:  <b>address : &lt;port&gt;@@base=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b></p>
IPv6 – Lastserver	Zeichenfolge mit bis zu 256 Zeichen		<p>Identifiziert den alternativen IPv6-Server, den das Telefon verwendet, um Firmware und Updates abzurufen.</p> <p>Das Format für die Adresse lautet:  <b>[address] : &lt;port&gt;@@base=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b></p>
Wideband-Headset	Deaktiviert Aktiviert	Aktiviert	<p>Ermöglicht es dem Benutzer, den Wideband-Codec für ein analoges Headset zu verwenden.</p>
Wideband-Headset	Deaktiviert Aktiviert	Aktiviert	<p>Aktiviert oder deaktiviert die Verwendung eines Wideband-Headsets auf dem Telefon. Zusammen mit benutzergesteuertem Wideband-Headset verwendet.</p> <p>Weitere Informationen hierzu finden Sie unter <a href="#">Breitband-Codec konfigurieren, auf Seite 119</a>.</p>

<b>Feldname</b>	<b>Feldtyp oder Auswahlmöglichkeiten</b>	<b>Standard</b>	<b>Beschreibung und Richtlinien für die Verwendung</b>
WLAN	Deaktiviert Aktiviert	Aktiviert	Ermöglicht es den Cisco IP-Telefonen 8861 und 8865, eine Verbindung mit dem Wi-Fi-Netzwerk herzustellen.  Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.
USB-Port hinten	Deaktiviert Aktiviert	8861, 8865 und 8865NR: Aktiviert	Legt fest, ob der USB-Port an der Rückseite der Cisco IP-Telefone 8861 und 8865 verwendet werden kann.  Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.
Seitlicher USB-Port	Deaktiviert Aktiviert	Aktiviert	Legt fest, ob der USB-Port an der Seite der Cisco IP-Telefone 8851, 8851NR, 8861, 8865 und 8865NR verwendet werden kann.  Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.
Konsolenzugriff	Deaktiviert Aktiviert	Deaktiviert	Gibt an, ob die serielle Konsole aktiviert oder deaktiviert ist.
Bluetooth	Deaktiviert Aktiviert	Aktiviert	Aktiviert oder deaktiviert die Bluetooth-Option auf dem Telefon. Wenn diese Option deaktiviert ist, kann der Benutzer Bluetooth auf dem Telefon nicht aktivieren. Auf den Cisco IP-Telefonen 8845, 8851, 8861 und 8865 unterstützt.  Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.
Importieren von Bluetooth-Kontakten zulassen	Deaktiviert Aktiviert	Aktiviert	Ermöglicht es dem Benutzer, Kontakte von einem verbundenen Mobilgerät über Bluetooth zu importieren. Wenn diese Option deaktiviert ist, kann der Benutzer keine Kontakte von einem verbundenen Mobilgerät auf das Telefon importieren. Auf den Cisco IP-Telefonen 8845, 8851, 8861 und 8865 unterstützt.  Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Bluetooth-Mobilfreisprechmodus zulassen	Deaktiviert Aktiviert	Aktiviert	<p>Ermöglicht es Benutzern, die akustischen Eigenschaften des Telefons für ihr Mobilgerät oder Tablet zu nutzen. Der Benutzer koppelt das Mobilgerät oder Tablet über Bluetooth mit dem Telefon. Wenn diese Option deaktiviert ist, kann der Benutzer das Mobilgerät oder Tablet nicht mit dem Telefon koppeln.</p> <p>Mit einem gekoppelten Mobilgerät kann der Benutzer Mobiltelefon-Anrufe über das Telefon tätigen und annehmen. Bei einem Tablet kann der Benutzer den Audio-Anruf vom Tablet auf das Telefon umleiten.</p> <p>Benutzer können mehrere Mobilgeräte, Tablets und ein Bluetooth-Headset mit dem Telefon koppeln. Es können jedoch nur jeweils ein Gerät und ein Headset gleichzeitig angeschlossen sein.</p> <p>Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.</p>
Bluetooth-Profile	Freisprechen Eingabegeräte	Freisprechen	<p>Gibt an, welche Bluetooth-Profile auf dem Telefon aktiviert oder deaktiviert sind.</p> <p>Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.</p>
ARP unnötig	Deaktiviert Aktiviert	Deaktiviert	<p>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.</p>
Alle Anrufe auf der Hauptleitung anzeigen	Deaktiviert Aktiviert	Deaktiviert	<p>Gibt an, ob alle Anrufe für dieses Telefon auf der Hauptleitung angezeigt werden.</p> <p>Der Zweck dieses Feldes ist es, es dem Benutzer zu erleichtern, alle Anrufe auf allen Leitungen auf einen Blick zu sehen, anstatt eine Leitung zu wählen, um die Anrufe auf dieser Leitung zu sehen. Mit anderen Worten: Wenn mehrere Leitungen auf dem Telefon konfiguriert sind, ist es in der Regel sinnvoller, alle Anrufe auf allen Leitungen in einer kombinierten Anzeige sehen zu können. Wenn diese Funktion aktiviert ist, werden alle Anrufe auf der Hauptleitung angezeigt, Sie können jedoch weiterhin eine bestimmte Leitung wählen, um die Anzeige zu filtern und nur die Anrufe für diese spezifische Leitung anzuzeigen.</p>
HTTPS-Server	HTTP und HTTPS aktiviert Nur HTTPS	HTTP und HTTPS aktiviert	<p>Steuert die Art der Kommunikation mit dem Telefon. Wenn Sie „Nur HTTPS“ auswählen, ist die Telefonkommunikation besser geschützt.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
IPv6 – Protokollserver	Zeichenfolge mit bis zu 256 Zeichen		Identifiziert den IPv6-Protokollserver. 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.
Protokollprofil	Standard Voreinstellung Telefonie SIP UI Netzwerk Medien Upgrade Zubehörteil Sicherheit WLAN VPN EnergyWise MobileRemoteAc	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>• Wi-Fi – Protokolliert Wi-Fi-Informationen.</li> <li>• VPN – Protokolliert Informationen zum virtuellen privaten Netzwerk.</li> <li>• EnergyWise – Protokolliert Energiesparinformationen.</li> <li>• MobileRemoteAC – Protokolliert Informationen zum Mobil- und Remotezugriff über Expressway.</li> </ul>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
G.722 und iSAC Codecs ankündigen	Systemstandard verwenden  Deaktiviert  Aktiviert	Systemstandard verwenden	<p>Gibt an, ob das Telefon die Codecs G.722 und iSAC auf dem Cisco Unified Communications Manager ankündigt.</p> <ul style="list-style-type: none"> <li>• Systemstandard verwenden – Verwendet die im Unternehmensparameter „G.722 Codec ankündigen“ festgelegte Einstellung.</li> <li>• Deaktiviert – Kündigt G.722 nicht auf dem Cisco Unified Communications Manager an.</li> <li>• Aktiviert – Kündigt G.722 auf dem Cisco Unified Communications Manager an.</li> </ul> <p>Weitere Informationen finden Sie unter dem Hinweis im Anschluss an die Tabelle.</p>
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-Unifed CM/SRST.</p> <ul style="list-style-type: none"> <li>• Normal – Unified CM-Verbindungsfehler werden in der Standardsystemgeschwindigkeit erkannt. Wählen Sie diesen Wert für eine schnellere Erkennung eines Unified CM-Verbindungsfehlers.</li> <li>• Verzögert – Die Erkennung eines Unified CM-Verbindungsfailovers ist etwa vier Mal langsamer als bei „Normal“. Wählen Sie diesen Wert, wenn Sie den Failover etwas verzögern möchten, um zu versuchen, die Verbindung wiederherzustellen.</li> </ul> <p>Der genaue Zeitunterschied zwischen Normal und Verzögert hängt von mehreren Faktoren ab, die sich ständig ändern.</p> <p>Dieses Feld gilt nur für verkabelte Ethernet-Verbindungen.</p>
Leistungsaushandlung	Deaktiviert  Aktiviert	Aktiviert	<p>Ermöglicht dem Telefon, die Energie mit LLDP (Link Level Endpoint Discovery Protocol) und CDP (Cisco Discovery Protocol) auszuhandeln.</p> <p>Die Energieaushandlung sollte nicht deaktiviert werden, wenn das Telefon mit einem Switch verbunden ist, der die Energieaushandlung unterstützt. Wenn die Energieaushandlung deaktiviert ist, kann der Switch das Telefon ausschalten.</p>



Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Wählton über Freigabetaste	Deaktiviert Aktiviert	Deaktiviert	Steuert, ob der Benutzer einen Wählton hört, wenn die Freigabetaste gedrückt wird. <ul style="list-style-type: none"> <li>• Deaktiviert – Der Benutzer hört keinen Wählton.</li> <li>• Aktiviert – Der Benutzer hört einen Wählton.</li> </ul>
Hintergrundbild	Zeichenfolge mit bis zu 64 Zeichen		Gibt die Standard-Hintergrundbild-Datei an. Wenn ein Standard-Hintergrundbild festgelegt ist, kann der Benutzer das Telefon-Hintergrundbild nicht ändern.
UI für vereinfachten neuen Anruf	Deaktiviert Aktiviert	Deaktiviert	Steuert die Benutzeroberfläche beim Wählen. Wenn aktiviert, kann der Benutzer keine Nummer aus der Anrufliste auswählen.  Wenn aktiviert, enthält dieses Feld ein vereinfachtes Fenster für den Benutzer, um einen Anruf zu tätigen. Der Benutzer sieht das Popup-Fenster mit der Anrufliste nicht, das angezeigt wird, wenn der Hörer abgehoben wird. Die Anzeige des Popup-Fensters wird als nützlich betrachtet, daher ist „UI für vereinfachten neuen Anruf“ standardmäßig deaktiviert.
Zurückkehren zu allen Anrufen	Deaktiviert Aktiviert	Deaktiviert	Gibt an, ob das Telefon zu „Alle Anrufe“ zurückkehrt, wenn ein Anruf beendet ist und der Anruf einen Filter außer „Hauptleitung“, „Alle Anrufe“ oder „Eingehender Anruf“ aufweist.
Anrufverlauf nur für ausgewählte Leitung anzeigen	Deaktiviert Aktiviert	Deaktiviert	Steuert die Anzeige der Anrufliste. <ul style="list-style-type: none"> <li>• Deaktiviert – Die Anrufliste zeigt das Anrufprotokoll für alle Leitungen an.</li> <li>• Aktiviert – Die Anrufliste zeigt das Anrufprotokoll für die ausgewählte Leitung an.</li> </ul>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Aktionshinweis für eingehende Anrufe	Deaktiviert Für alle eingehenden Anrufe anzeigen Für unsichtbaren eingehenden Anruf anzeigen	Für alle eingehenden Anrufe anzeigen	Steuert den Typ der Benachrichtigung für eingehende Anrufe, die auf dem Telefonbildschirm angezeigt wird. Der Zweck dieses Felds ist es, die Anzahl der Tasten zu reduzieren, die zum Annehmen eines Anrufs durch den Benutzer gedrückt werden müssen. <ul style="list-style-type: none"> <li>• Deaktiviert – Der Aktionshinweis für eingehende Anrufe ist deaktiviert, und der Benutzer sieht die herkömmliche Popup-Benachrichtigung für eingehende Anrufe.</li> <li>• Für alle eingehenden Anrufe anzeigen – Der Aktionshinweis für eingehende Anrufe wird für alle Anrufe angezeigt, unabhängig von der Sichtbarkeit.</li> <li>• Für unsichtbaren eingehenden Anruf anzeigen – Der Aktionshinweis für eingehende Anrufe wird für Anrufe angezeigt, die nicht auf dem Telefon angezeigt werden. Dieser Parameter verhält sich ähnlich wie der Popup-Hinweis „Signal f. eingeh. Anruf“.</li> </ul>
DF-Bit	0 1	0	Steuert, wie Netzwerkpakete gesendet werden. Pakete können in Blöcken (Fragmenten) unterschiedlicher Größe gesendet werden. Wenn das DF-Bit in der Paketkopfzeile auf 1 gesetzt ist, wird die Netzwerknutzlast auf dem Weg durch Netzwerkgeräte wie Switches und Router nicht fragmentiert. Ohne Fragmentierung wird eine fehlerhafte Analyse auf der Empfangsseite vermieden, dies vermindert jedoch die Geschwindigkeit etwas. Die DF-Bit-Einstellung gilt nicht für ICMP-, VPN-, VXC-VPN- oder DHCP-Datenverkehr.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Standardleitungsfilter	Liste von durch Komma getrennten Telefongerätenamen		<p>Zeigt die Liste der Telefone an, die im Standardfilter enthalten sind.</p> <p>Wenn der Standardleitungsfilter konfiguriert ist, können Benutzer einen Filter mit dem Namen <code>Tageszeitplan</code> in den <b>Anrufbenachrichtigungen</b> im Menü <b>Einstellungen &gt; Voreinstellungen</b> des Telefons sehen. Dieser Tageszeitplanfilter ist zusätzlich zum voreingestellten Filter „Alle Anrufe“ verfügbar.</p> <p>Wenn der Standardleitungsfilter nicht konfiguriert ist, überprüft das Telefon alle bereitgestellten Leitungen. Bei entsprechender Konfiguration überprüft das Telefon die auf dem Cisco Unified Communications Manager festgelegten Leitungen, wenn der Benutzer den Standardfilter als aktiven Filter wählt oder wenn keine benutzerdefinierten Filter vorhanden sind.</p> <p>Benutzerdefinierte Leitungsfilter ermöglichen es Ihnen, Leitungen mit hoher Priorität zu filtern, um die Meldungsaktivität zu reduzieren. Sie können die Benachrichtigungspriorität für eingehende Anrufe für einen Teil der Leitungen festlegen, auf die ein Hinweisfilter angewendet wird. Der benutzerdefinierte Filter erzeugt für eingehende Anrufe auf den ausgewählten Leitungen entweder herkömmliche Popup-Hinweise oder Hinweise, aus denen heraus direkt eine Aktion durchgeführt werden kann. Jeder Filter erzeugt nur für die abgedeckten Leitungen Hinweise. Diese Funktion bietet eine Möglichkeit für Benutzer mit mehreren Leitungen, die Hinweisaktivität zu reduzieren, indem Hinweise gefiltert und nur diejenigen von Leitungen mit hoher Priorität angezeigt werden. Die Benutzer können dies selbst konfigurieren. Alternativ können Sie den Standardleitungsfilter programmieren und ihn auf das Telefon übertragen.</p>
Niedrigste Priorität für Eingangsleitungsstatus	Deaktiviert Aktiviert	Deaktiviert	<p>Gibt den Benachrichtigungsstatus an, wenn Sie gemeinsam genutzte Leitungen verwenden.</p> <ul style="list-style-type: none"> <li>• Deaktiviert – Wenn ein Anruf auf der gemeinsam genutzten Leitung eingeht, gibt das LED-/Leitungsstatussymbol den Status an und nicht „Remote genutzt“.</li> <li>• Aktiviert – Wenn ein Anruf auf einer gemeinsam genutzten Leitung eingeht, sieht der Benutzer das Symbol „Remote genutzt“.</li> </ul>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Einspaltenanzeige für Erweiterungsmodul	Deaktiviert Aktiviert	Deaktiviert	<p>Steuert die Anzeige auf dem Erweiterungsmodul.</p> <ul style="list-style-type: none"> <li>• Deaktiviert – Das Erweiterungsmodul verwendet den Zweispaltenmodus.</li> <li>• Aktiviert – Das Erweiterungsmodul verwendet den Einspaltenmodus.</li> </ul> <p>Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.</p>
Energy Efficient Ethernet (EEE): PC-Port	Deaktiviert Aktiviert	Deaktiviert	Steuert EEE für den PC-Port.
Energy Efficient Ethernet (EEE): SW-Port	Deaktiviert Aktiviert	Deaktiviert	Steuert EEE für den Switch-Port.
Videoport starten			<p>Definiert den Start des Portbereichs für Videoanrufe.</p> <p>Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.</p>
Videoport stoppen			<p>Definiert das Ende des Portbereichs für Videoanrufe.</p> <p>Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.</p>
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 vorgegeben.</p> <p>Weitere Informationen finden Sie im Abschnitt <a href="#">Mobil- und Remote Access über Expressway</a>, auf Seite 182.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Upload-URL für Kundensupport	Zeichenfolge mit bis zu 256 Zeichen		<p>Stellt die URL für das Tool für Problemberichte (PRT) bereit.</p> <p>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.</p> <p>Weitere Informationen finden Sie im Abschnitt <a href="#">Mobil- und Remote Access über Expressway</a>, auf Seite 182.</p>
Webadministrator	Deaktiviert Aktiviert	Deaktiviert	<p>Aktiviert oder deaktiviert den Zugriff des Administrators auf die Webseiten des Telefons über einen Webbrowser.</p> <p>Weitere Informationen finden Sie im Abschnitt <a href="#">Konfigurieren der Verwaltungsseite für das Telefon</a>, auf Seite 110.</p> <p>Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.</p>
Administratorkennwort	Zeichenfolge von 8 bis 127 Zeichen		<p>Definiert das Administratorkennwort, wenn Sie als Administrator auf die Telefon-Webseiten zugreifen.</p> <p>Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.</p>
WLAN SCEP-Server	Zeichenfolge mit bis zu 256 Zeichen		<p>Gibt den SCEP-Server an, den das Telefon verwendet, um Zertifikate für die WLAN-Authentifizierung zu erhalten. Geben Sie den Hostnamen oder die IP-Adresse (im IP-Standardformat) des Servers ein.</p> <p>Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.</p>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
WLAN-Stammzertifizierungsstelle (SHA256 oder SHA1)	Zeichenfolge mit bis zu 95 Zeichen		<p>Gibt den SHA256- oder SHA1-Fingerabdruck der Stammzertifizierungsstelle zur Validierung während des SCEP-Prozesses an, wenn Zertifikate für die WLAN-Authentifizierung ausgestellt werden. Wir empfehlen die Verwendung des SHA256-Fingerabdrucks, der über OpenSSL abgerufen werden kann (z. B. openssl x509 -in rootca.cer -noout -sha256 -fingerprint), oder die Verwendung eines Webbrowsers, um die Zertifikatsinformationen zu überprüfen.</p> <p>Geben Sie den 64-Hexadezimalzeichenwert für den SHA256-Fingerabdruck oder den 40-Hexadezimalzeichenwert für den SHA1-Fingerabdruck mit einem allgemeinen Trennzeichen (Doppelpunkt, Bindestrich, Punkt, Leerzeichen) oder ohne Trennzeichen ein. Wenn Sie ein Trennzeichen verwenden, sollte das Trennzeichen bei SHA256-Fingerabdrücken konsistent nach allen 2, 4, 8, 16 oder 32 Hexadezimalzeichen bzw. bei SHA1-Fingerabdrücken nach allen 2, 4 oder 8 Hexadezimalzeichen platziert werden.</p> <p>Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.</p>
WLAN-Authentifizierung			Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.
Aufforderungsmodus für WLAN-Profil 1	Deaktiviert Aktiviert	Deaktiviert	Auf Telefonen, die diese Funktion nicht unterstützen, wird das Feld nicht angezeigt.
Leitungsmodus	Sitzungsleitungsmodus Erweiterter Leitungsmodus	Sitzungsleitungsmodus	<p>Steuert die Leitungsanzeige auf dem Telefon.</p> <ul style="list-style-type: none"> <li>• Sitzungsleitungsmodus – Die Schaltflächen auf einer Seite des Bildschirms sind Leitungstasten.</li> <li>• Erweiterter Leitungsmodus – Die Tasten auf beiden Seiten des Telefonbildschirms sind Leitungstasten. Predictive Dialing und Aktionshinweise für eingehende Anrufe sind im erweiterten Leitungsmodus standardmäßig aktiviert.</li> </ul>
Konfigurierbarer Admin-Klingelton	Deaktiviert Sunrise Chirp1 Chirp2	Deaktiviert	<p>Steuert den Klingelton und die Möglichkeit für Benutzer, den Klingelton festzulegen.</p> <ul style="list-style-type: none"> <li>• Wenn diese Option auf <b>Deaktiviert</b> eingestellt ist, können Benutzer den Standardklingelton auf ihrem Telefon konfigurieren.</li> <li>• Bei allen anderen Werten können Benutzer den Klingelton nicht ändern. Das Menüelement <b>Klingelton</b> im Menü <b>Einstellungen</b> ist abgeblendet.</li> </ul>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
Verwendung des Kunden-Supports	Zeichenfolge mit bis zu 64 Zeichen	Leer	Nur für die Verwendung von Cisco TAC.
TLS-Schlüssel deaktivieren	Siehe <a href="#">Transport Layer Security-Schlüssel deaktivieren</a> , auf Seite 170.	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.  Die Auswahl aller Telefonschlüssel wirkt sich auf den TLS-Dienst des Telefons aus.
Benachrichtigung für das Verringern der Stimmlautstärke	Aktiviert Deaktiviert	Aktiviert	Steuert die Funktion zum Verringern der Stimmlautstärke.  <ul style="list-style-type: none"> <li>• Deaktiviert: <ul style="list-style-type: none"> <li>• Das Menüelement <b>Stimmlautstärke verringern</b> wird im Menü <b>Einstellungen</b> nicht angezeigt.</li> <li>• Benutzer sehen die Nachricht nicht auf ihrem Bildschirm, wenn sie laut sprechen.</li> </ul> </li> <li>• Aktiviert: <ul style="list-style-type: none"> <li>• Die Benutzer steuern die Funktion über das Menüelement <b>Stimmlautstärke verringern</b> im Menü <b>Einstellungen</b>. Das Feld ist standardmäßig auf <b>Ein</b> festgelegt.</li> </ul> </li> </ul>
Anruf als Spam markieren	Aktiviert Deaktiviert	Aktiviert	Steuert die Funktion „Anruf als Spam markieren“.  <ul style="list-style-type: none"> <li>• Deaktiviert: <ul style="list-style-type: none"> <li>• Das Telefon zeigt den Softkey <b>Als Spam markieren</b> nicht an.</li> <li>• Das Element <b>Spam-Liste</b> im Menü <b>Einstellungen</b> wird nicht angezeigt.</li> <li>• Wenn eine Spam-Liste vorhanden ist, wird die Liste gelöscht und kann nicht wiederhergestellt werden.</li> </ul> </li> <li>• Aktiviert: <ul style="list-style-type: none"> <li>• Das Telefon zeigt den Softkey <b>Als Spam markieren</b> an.</li> <li>• Das Element <b>Spam-Liste</b> im Menü <b>Einstellungen</b> wird angezeigt.</li> </ul> </li> </ul>

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung und Richtlinien für die Verwendung
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.
Anzeige der Leitungsbezeichnung im ELM	Deaktiviert Aktiviert	Aktiviert	Steuert die Anzeige der Leitungsbezeichnungen während eines Anrufs, wenn der erweiterte Leitungsmodus konfiguriert ist <ul style="list-style-type: none"> <li>• Aktiviert <ul style="list-style-type: none"> <li>• Wenn der Name des Anrufers konfiguriert ist, werden der Name in der ersten Zeile der Anrufsituation und die lokale Leitungsbezeichnung in der zweiten Zeile angezeigt.</li> <li>• Wenn der Name des Anrufers nicht konfiguriert ist, werden die Remote-Nummer in der ersten und die lokale Leitungsbezeichnung in der zweiten Zeile angezeigt.</li> </ul> </li> <li>• Deaktiviert <ul style="list-style-type: none"> <li>• Wenn der Name des Anrufers konfiguriert ist, werden der Name in der ersten Zeile der Anrufsituation und die Nummer in der zweiten Zeile angezeigt.</li> <li>• Wenn der Name des Anrufers nicht konfiguriert ist, wird <b>nur</b> die Remote-Nummer angezeigt.</li> </ul> </li> </ul> <p>Dieses Feld ist ein Pflichtfeld.</p>



**Hinweis** Die Codec-Aushandlung besteht aus zwei Schritten:

1. Das Telefon kündigt den unterstützten Codec auf dem Cisco Unified Communications Manager an. Nicht alle Endgeräte unterstützen den gleichen Satz von Codecs.
2. Wenn der Cisco Unified Communications Manager die Liste der unterstützten Codecs von allen Telefonen erhält, die am Anrufversuch beteiligt sind, wählt dieser einen allgemein unterstützten Codec basierend auf verschiedenen Faktoren aus, einschließlich der Regionskoppelungseinstellung.

## Bewährte Verfahren für die Konfiguration von Funktionen

Sie können die Telefonfunktionen entsprechend den Anforderungen der Benutzer konfigurieren. Wir haben allerdings einige Empfehlungen für bestimmte Situationen und Bereitstellungen, die Sie möglicherweise hilfreich finden.



## Umgebungen mit hohem Anrufaufkommen

In einer Umgebung mit hohem Anrufaufkommen wird empfohlen, einige Funktionen in einer bestimmten Weise zu konfigurieren.

Feld	Verwaltungsbereich	Empfohlene Einstellung
Immer Hauptleitung verwenden	Geräteinformationen	Aktiviert oder deaktiviert  Weitere Informationen hierzu finden Sie unter <a href="#">Feld: Immer Hauptleitung verwenden, auf Seite 170</a> .
Aktionshinweis für eingehende Anrufe	Produktspezifische Konfiguration – Layout	Für alle eingehenden Anrufe anzeigen
Alle Anrufe auf der Hauptleitung anzeigen	Produktspezifische Konfiguration – Layout	Aktiviert
Zurückkehren zu allen Anrufen	Produktspezifische Konfiguration – Layout	Aktiviert

## Umgebungen mit mehreren Leitungen

In einer Umgebung mit mehreren Leitungen wird empfohlen, einige Funktionen in einer bestimmten Weise zu konfigurieren.

Feld	Verwaltungsbereich	Empfohlene Einstellung
Immer Hauptleitung verwenden	Geräteinformationen	Aus  Weitere Informationen hierzu finden Sie unter <a href="#">Feld: Immer Hauptleitung verwenden, auf Seite 170</a> .
Aktionshinweis für eingehende Anrufe	Produktspezifische Konfiguration – Layout	Für alle eingehenden Anrufe anzeigen
Alle Anrufe auf der Hauptleitung anzeigen	Produktspezifische Konfiguration – Layout	Aktiviert
Zurückkehren zu allen Anrufen	Produktspezifische Konfiguration – Layout	Aktiviert

## Umgebung mit Sitzungsleitungsmodus

Der erweiterte Leitungsmodus ist das bevorzugte Tool für die meisten Anrufumgebungen. Wenn der erweiterte Leitungsmodus jedoch nicht Ihre Anforderungen erfüllt, können Sie auch den Sitzungsleitungsmodus verwenden.

Feld	Verwaltungsbereich	Empfohlene Einstellung für Sitzungsleitungsmodus
Alle Anrufe auf der Hauptleitung anzeigen	Produktspezifische Konfiguration – Layout	Deaktiviert
Zurückkehren zu allen Anrufen	Produktspezifische Konfiguration – Layout	Deaktiviert
Aktionshinweis für eingehende Anrufe	Produktspezifische Konfiguration – Layout	Standardmäßig aktiviert (Firmware-Version 11.5(1) und höher).

#### Verwandte Themen

[Zusätzliche Leitungstasten einrichten](#), auf Seite 206

[Im erweiterten Leitungsmodus verfügbare Funktionen](#), auf Seite 206

## Feld: Immer Hauptleitung verwenden

Dieses Feld gibt an, ob die Hauptleitung auf einem IP-Telefon gewählt wird, wenn ein Benutzer den Hörer abnimmt. Wenn dieser Parameter auf „True“ festgelegt ist und bei einem Telefon der Hörer abgenommen wird, wird die Hauptleitung gewählt und wird zur aktiven Leitung. Auch wenn ein Anruf auf der zweiten Leitung des Benutzers eingeht und beim Telefon der Hörer abgenommen wird, wird nur die Hauptleitung aktiv geschaltet. Der eingehende Anruf auf der zweiten Leitung wird nicht angenommen. In diesem Fall muss der Benutzer die zweite Leitung wählen, um den Anruf anzunehmen. Standardmäßig ist der Wert auf „False“ festgelegt.

Der Zweck des Feldes „Immer Hauptleitung verwenden“ ist ähnlich wie die Kombination aus „Alle Anrufe auf der Hauptleitung anzeigen“ und „Zurückkehren zu allen Anrufen“, wenn beide Funktionen aktiviert sind. Der Hauptunterschied besteht jedoch darin, dass eingehende Anrufe nicht auf der zweiten Leitung angenommen werden, wenn „Immer Hauptleitung verwenden“ aktiviert ist. Nur auf der Hauptleitung ist der Wählton zu hören. Es gibt bestimmte Umgebungen mit hohem Anrufaufkommen, in denen dies das gewünschte Verhalten ist. Im Allgemeinen ist es von Vorteil, dieses Feld deaktiviert zu lassen, wenn Sie nicht in einer Umgebung mit hohem Anrufaufkommen arbeiten, in der diese Funktion benötigt wird.

## 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>).

## Anrufverlauf für gemeinsam genutzte Leitung aktivieren

Ermöglicht Ihnen, die Aktivitäten auf der gemeinsam genutzten Leitung im Anrufverlauf anzuzeigen. Diese Funktion:

- Protokolliert Anrufe in Abwesenheit auf der gemeinsam genutzten Leitung.
- Protokolliert alle auf der gemeinsam genutzten Leitung angenommenen und getätigten Anrufe.

### Vorbereitungen

Deaktivieren Sie die Privatfunktion, bevor Sie den Anrufverlauf für gemeinsam genutzte Leitungen aktivieren. Andernfalls werden im Anrufverlauf nicht die Anrufe angezeigt, die andere Benutzer annehmen.

### 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 gewünschte Telefon.   |
| <b>Schritt 3</b> | Navigieren Sie zu der Dropdown-Liste "Anrufverlauf für gemeinsam genutzte Leitung aufzeichnen" im produktspezifischen Konfigurationsbereich. |
| <b>Schritt 4</b> | Wählen Sie in der Dropdown-Liste <b>Aktiviert</b> .  |
| <b>Schritt 5</b> | Wählen Sie <b>Speichern</b> aus.   |
- 

## 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.

Weitere Informationen hierzu finden Sie unter [Produktspezifische Konfiguration, auf Seite 146](#)

## 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

**Table 32: 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.
Display eingeschaltet – Uhrzeit	Die Uhrzeit, zu der das Display jeden Tag automatisch eingeschaltet wird (außer an den festgelegten Tagen). Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (00:00 ist Mitternacht). 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> . Wenn das Feld leer ist, wird das Display automatisch um 0:00 aktiviert.
Display eingeschaltet – Dauer	Die Zeitdauer, die das Display eingeschaltet bleibt, nachdem es zum festgelegten Zeitpunkt eingeschaltet wurde. Geben Sie den Wert in diesem Feld im Format <i>Stunden:Minuten</i> ein. Um das Display beispielsweise für vier Stunden und 30 Minuten zu aktivieren, nachdem es automatisch aktiviert wurde, geben Sie <b>04:30</b> ein. Wenn das Feld leer ist, wird das Telefon am Ende des Tages (0:00) ausgeschaltet. <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.

Feld	Beschreibung
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.

Weitere Informationen hierzu finden Sie unter [Produktspezifische Konfiguration, auf Seite 146](#)

### 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 33: 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>
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>

Feld	Beschreibung
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. 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>
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>

Feld	Beschreibung
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“ (Ruhefunktion) aktiviert ist, ertönt bei einem eingehenden Anruf kein Rufton, oder es erfolgt keine hörbare bzw. visuelle Benachrichtigung.

Wenn „Nicht stören“ (Ruhefunktion) aktiviert ist, ändert sich die Farbe des Überschriftenbereichs des Telefonbildschirms, und `Nicht stören` wird angezeigt.

Sie können das Telefon mit einer Telefontastenvorlage konfigurieren, in der DND eine ausgewählte Funktion ist.

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.  
Wählen Sie nicht „Anrufzurückweisung“, wenn Sie möchten, dass Prioritätsanrufe (MLPP) an dieses Telefon gehen, wenn „Nicht stören“ (Ruhefunktion) eingeschaltet ist.
- 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 xv

## Mitarbeiterbegrüßung aktivieren

Über die Funktion Mitarbeiterbegrüßung kann ein Mitarbeiter eine aufgezeichnete Begrüßung erstellen oder aktualisieren, die zu Beginn eines Anrufs, beispielsweise bei einem Kundenanruf, abgespielt wird, bevor der Mitarbeiter das Gespräch mit dem Kunden beginnt. Der Mitarbeiter kann eine oder mehrere Begrüßungen aufzeichnen sowie Begrüßungen erstellen und aktualisieren.

Bei einem Kundenanruf hören sowohl der Mitarbeiter als auch der Anrufer die aufgezeichnete Begrüßung. Der Mitarbeiter kann bis zum Ende der Begrüßung stumm bleiben oder den Anruf annehmen, während die Begrüßung abgespielt wird.

Alle für das Telefon unterstützten Codecs werden auch für Anrufe mit Mitarbeiterbegrüßungen unterstützt.

Weitere Informationen zum Aufschalten und zur Privatfunktion 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** Klicken Sie auf das IP-Telefon, das Sie konfigurieren müssen.
- Schritt 3** Navigieren Sie zu den Geräteinformationen und legen Sie **Integrierte Brücke** auf Ein oder Standard fest.
- Schritt 4** Wählen Sie **Speichern** aus.
- Schritt 5** Überprüfen Sie die Einstellung der Brücke:
  - a) Wählen Sie **System > Serviceparameter** aus.
  - b) Wählen Sie den entsprechenden Server und Service aus.
  - c) Navigieren Sie zum Bereich Clusterweite Parameter (Gerät - Telefon) und legen Sie **Integrierte Brücke** auf Ein fest.
  - d) Wählen Sie **Speichern** aus.

---

#### Verwandte Themen

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

## Überwachung und Aufzeichnung konfigurieren

Die Funktion Überwachung und Aufzeichnung ermöglicht einem Supervisor, einen aktiven Anruf zu überwachen. Keiner der Teilnehmer kann den Supervisor hören. Der Benutzer kann möglicherweise einen Signalton hören, wenn der Anruf überwacht wird.

Wenn ein Anruf sicher ist, wird ein Schloss-Symbol angezeigt. Die Teilnehmer können möglicherweise einen Signalton hören, der angibt, dass der Anruf überwacht wird. Die verbundenen Teilnehmer hören möglicherweise auch einen Signalton, der angibt, dass der Anruf sicher ist und überwacht wird.

Während ein aktiver Anruf überwacht oder aufgezeichnet wird, kann der Benutzer Intercom-Anrufe tätigen und annehmen. Wenn der Benutzer jedoch einen Intercom-Anruf tätigt, wird der aktive Anruf gehalten. Diese Aktion verursacht, dass die Aufzeichnungssitzung abgebrochen und die Überwachungssitzung angehalten wird. Um die Überwachungssitzung fortzusetzen, muss die überwachte Person den Anruf fortsetzen.

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

Das folgende Verfahren fügt einen Benutzer zu den überwachenden Standardbenutzergruppen hinzu.

### Vorbereitungen

Cisco Unified Communications Manager muss konfiguriert werden, um die Überwachung und Aufzeichnung zu unterstützen.

### Prozedur

- 
- Schritt 1** Wählen Sie **Benutzerverwaltung > Anwendungsbenutzer** in der Cisco Unified Communications Manager-Verwaltung aus.
  - Schritt 2** Aktivieren Sie die Benutzergruppen Standard-CTI Anrufüberwachung zulassen und Standard-CTI Anrufaufzeichnung zulassen.
  - Schritt 3** Klicken Sie auf **Auswahl hinzufügen**.
  - Schritt 4** Klicken Sie auf **Zur Benutzergruppe hinzufügen**.
  - Schritt 5** Fügen Sie die Benutzertelefone zur Liste der gesteuerten Geräte der Anwendungsbenutzer hinzu.
  - Schritt 6** Wählen Sie **Speichern** aus.

### Verwandte Themen

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

## 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.
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.

## BLF für Anruflisten aktivieren

Das Feld BLF für Anruflisten steuert auch den Leitungsstatur für die Firmenverzeichnisfunktion.

### Prozedur

**Schritt 1** Wählen Sie **System > Enterprise-Parameter** in der Cisco Unified Communications Manager-Verwaltung aus.

**Schritt 2** Aktivieren oder deaktivieren Sie die Funktion für das Feld BLF für Anruflisten.

Die Funktion ist standardmäßig deaktiviert.

Die Parameter, die Sie im produktspezifischen Konfigurationsbereich festlegen, werden möglicherweise auch im Fenster Gerätekonfiguration für verschiedene Geräte und im Fenster Firmentelefonkonfiguration angezeigt. Wenn Sie diese Parameter auch in den anderen Fenstern festlegen, wird die Einstellung, die Vorrang hat, in der folgenden Reihenfolge bestimmt:

1. Einstellungen im Fenster Gerätekonfiguration

2. Einstellungen im Fenster Allgemeines Telefonprofil
3. Einstellungen im Fenster Firmentelefonkonfiguration

**Schritt 3** Wählen Sie **Speichern** aus.

## Energy Efficient Ethernet für Switch-Port und PC-Port einrichten

IEEE 802.3az Energy Efficient Ethernet (EEE) ist eine Erweiterung des IEEE 802.3-Standards, der eine Methode zum Verringern des Energieverbrauchs bietet, ohne dass dabei die unverzichtbare Funktion von Netzwerkschnittstellen beeinträchtigt wird. Mit dem konfigurierbaren EEE können Administratoren EEE-Funktionen für den PC-Port und den Switch-Port steuern.



**Hinweis** Administratoren müssen sich vergewissern, dass auf allen entsprechenden USM-Seiten das Kontrollkästchen „Überschreiben“ aktiviert ist; andernfalls funktioniert EEE nicht.

Der Administrator steuert die EEE-Funktionen mit den folgenden beiden Parametern:

- **Energy Efficient Ethernet: PC-Port:** Hiermit wird die nahtlose Verbindung mit PCs hergestellt. Der Administrator kann die Funktion durch Auswahl der Optionen „Aktiviert“ und „Deaktiviert“ steuern.
- **Energy Efficient Ethernet: Switch-Port:** Hiermit wird eine nahtlose Verbindung hergestellt.

Für weitere Informationen siehe [Produktspezifische Konfiguration, auf Seite 146](#)

### Prozedur

**Schritt 1** Wählen Sie in der Cisco Unified Communications Manager-Verwaltung eines der folgenden Fenster aus:

- **Gerät > Telefon**
- **Gerät > Geräteeinstellungen > Allgemeines Telefonprofil**
- **System > Firmentelefonkonfigurationen**

Wenn Sie die Parameter in mehreren Fenstern konfigurieren, müssen Sie folgende Reihenfolge einhalten:

1. **Gerät > Telefon**
2. **Gerät > Geräteeinstellungen > Allgemeines Telefonprofil**
3. **System > Firmentelefonkonfigurationen**

**Schritt 2** Falls erforderlich, suchen Sie das Telefon.

**Schritt 3** Legen Sie die Felder **Energieeffizientes Ethernet: PC-Port** und **Energieeffizientes Ethernet: Switch-Port** fest.

- Energy Efficient Ethernet: PC-Port
- Energieeffizientes Ethernet: Switch-Port

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

## RTP/sRTP-Portbereich konfigurieren

Die Portwerte für RTP (Real-Time Transport Protocol) und sRTP (secure Real-Time Transport Protocol) werden im SIP-Profil konfiguriert. Die RTP- und sRTP-Portwerte liegen im Bereich von 2048 bis 65535 mit einem Standardbereich von 16384 bis 32764. Einige Portwerte im RTP- und sRTP-Portbereich sind für andere Telefondienste bestimmt. Sie können diese Ports nicht für RTP und sRTP konfigurieren.

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

### Prozedur

---

- Schritt 1** Wählen Sie **Gerät > Geräteeinstellungen > SIP-Profil** aus.
- Schritt 2** Wählen Sie die Suchkriterien aus und klicken Sie auf **Suchen**.
- Schritt 3** Wählen Sie das zu ändernde Profil aus.
- Schritt 4** Konfigurieren Sie den Medien-Start-Port und Medien-End-Port, um den Start und das Ende des Portbereichs einzubeziehen.

In der folgenden Liste sind die UDP-Ports aufgeführt, die für andere Telefonservices verwendet werden und nicht für RTP und sRTP verfügbar sind:

#### Port 4051

Wird für die PFS-Funktion (Peer Firmware Sharing) verwendet

#### Port 5060

Wird für SIP über UDP-Transport verwendet

#### Portbereich 49152 bis 53247

Wird für lokale temporäre Ports verwendet

#### Portbereich 53248 bis 65535

Wird für die VPN-Funktion VxC-Einfachtunnel verwendet

- Schritt 5** Klicken Sie auf **Speichern**.
- Schritt 6** Klicken Sie auf **Konfiguration übernehmen**.
- 

### Verwandte Themen

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

## 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).

---

Mobil- und Remote Access über Expressway unterstützt den erweiterten Leitungsmodus.

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 den folgenden Abschnitten sind verschiedene Bereitstellungsszenarien für Mobil- und Remote Access über Expressway aufgeführt.

### **Innerhalb des Unternehmens meldet sich der Benutzer am Unternehmensnetzwerk an.**

Melden Sie sich nach der Bereitstellung von Mobil- und Remote Access über Expressway am Unternehmensnetzwerk an, wenn Sie vor Ort sind. Das Telefon erkennt das Netzwerk und führt eine Registrierung bei Cisco Unified Communications Manager durch.

### **Außerhalb des Unternehmens meldet sich der Benutzer am Unternehmensnetzwerk an**

Wenn Sie sich nicht im Büro befinden, erkennt das Telefon, dass es sich im nicht lokalen Modus befindet. Das Mobil- und Remote Access über Expressway-Anmeldefenster wird angezeigt und Sie stellen eine Verbindung zum Unternehmensnetzwerk her.

Beachten Sie Folgendes:

- Sie müssen über gültige Daten für Servicedomäne, Benutzername und Kennwort verfügen, um eine Verbindung mit dem Netzwerk herzustellen.
- Setzen Sie den Servicemodus zurück, um die Einstellung für „Alternativer TFTP-Server“ zu löschen, ehe Sie versuchen, auf das Unternehmensnetzwerk zuzugreifen. Dadurch werden die Werte der Einstellung „Alternativer TFTP-Server“ gelöscht, sodass das Telefon das externe Netzwerk erkennt und verhindert, dass das Gerät eine VPN-Verbindung herstellt. Überspringen Sie diesen Schritt aus, wenn ein Telefon zum ersten Mal bereitgestellt wird.
- Wenn Sie die DHCP-Option 150 oder 66 auf dem Netzwerkrouter aktiviert haben, können Sie sich unter Umständen nicht beim Unternehmensnetzwerk anmelden. Setzen Sie Ihren Servicemodus zurück, um in den MRA-Modus zu wechseln.

### **Außerhalb des Unternehmens meldet sich der Benutzer mit VPN am Unternehmensnetzwerk an**

Außerhalb des Unternehmens melden Sie sich nach der Bereitstellung von Mobil- und Remote Access über Expressway mit VPN beim Unternehmensnetzwerk an.

Führen Sie ein standardmäßiges Zurücksetzen durch, um Ihre Telefonkonfigurationen zurückzusetzen, wenn bei Ihrem Telefon ein Fehler auftritt.

Sie müssen die Alternativ-TFTP-Einstellung konfigurieren (**Administratoreinstellungen > Netzwerkeinstellungen > IPv4, Feld Alternativer TFTP-Server 1**).

**Verwandte Themen**

[Standardmäßiges Zurücksetzen](#), auf Seite 279

**Medienpfade und Interactive Connectivity Establishment**

Sie können Interactive Connectivity Establishment (ICE) bereitstellen, um die Zuverlässigkeit von Mobil- und Remote Access-Anrufen (MRA) zu verbessern, die eine Firewall oder eine Network Address Translation (NAT) überschreiten. ICE ist eine optionale Bereitstellung, bei der Serial Tunneling- und Traversal Using Relays around NAT-Dienste verwendet werden, um den optimalen Medienpfad für einen Anruf auszuwählen.

Sekundärer Turn-Server und Turn-Server-Failover werden nicht unterstützt.

Weitere Informationen zu MRA und ICE finden Sie im *Systemkonfigurationshandbuch für Cisco Unified Communications Manager, Version 12.0(1)* oder höher. Zusätzliche Informationen finden Sie auch in der Internet Engineering Task Force-(IETF-)Anforderung für Kommentardokumente:

- *Traversal Using Relays around NAT (TURN): Relais-Erweiterungen für Session Traversal Utilities for NAT (STUN)*(RFC 5766)
- *Interactive Connectivity Establishment (ICE): Ein Protokoll für Network Address Translator (NAT) Traversal für Angebots-/Antwort-Protokolle* (RFC 5245)

**Verfügbare Telefonfunktionen für Mobil- und Remote Access über Expressway**

Mobil- und Remote Access über Expressway ermöglicht den sicheren Zugriff auf Services für die Zusammenarbeit für Mobil- und Remotebenutzer. Um die Netzwerksicherheit aufrechtzuerhalten, ist der Zugriff auf einige Telefonfunktionen jedoch eingeschränkt.

In der folgenden Liste sind die Telefonfunktionen für Mobil- und Remote Access über Expressway aufgelistet.

**Tabelle 34: Unterstützte Funktionen und Mobil- und Remote Access über Expressway**

Telefonfunktion	Telefon-Firmwareversion
Kurzwahlcodes	10.3(1) und höher
Ältesten annehmen	11.5(1)SR1 und höher
Unterstütztes gezieltes Parken	10.3(1) und höher
Automatische Anrufannahme	11.5(1)SR1 und höher
Aufschaltung und Konferenzaufschaltung	11.5(1)SR1 und höher
Besetztlampenfeld (BLF)	10.3(1) und höher
Besetztlampenfeld (BLF) mit Annahme	10.3(1) und höher
Besetzt-Anzeige (BLF) mit Kurzwahl	10.3(1) und höher
Rückruf	10.3(1) und höher
Rufumleitung	10.3(1) und höher
Benachrichtigung für Rufumleitung	10.3(1) und höher



Telefonfunktion	Telefon-Firmwareversion
Anruf parken	10.3(1) und höher
Anrufübernahme	10.3(1) und höher
Cisco Unified Serviceability	11.5(1)SR1 und höher
Clientzugriffslizenz (Client Access License, CAL)	11.5(1)SR1 und höher
Konferenz	10.3(1) und höher
Konferenzliste/Teilnehmer entfernen	11.5(1)SR1 und höher
Unternehmensverzeichnis	11.5(1)SR1 und höher
CTI-Anwendungen (CTI-gesteuert)	11.5(1)SR1 und höher
Direkte Übergabe	10.3(1) und höher
Gezieltes Parken	10.3(1) und höher
Eindeutiger Rufton	11.5(1)SR1 und höher
Umleiten	10.3(1) und höher
Erweiterter Leitungsmodus	12.1(1) und höher
Umleiten	10.3(1) und höher
Forced Access Codes (FAC) und Client Matter Codes (CMC)	11.5(1)SR1 und höher
Gruppenanruf übernehmen	10.3(1) und höher
Halten/Fortsetzen	10.3(1) und höher
Halten zurücksetzen	10.3(1) und höher
Sofort umleiten	10.3(1) und höher
Beitreten	10.3(1) und höher
Identifikation böswilliger Anrufer (MCID, Malicious Caller Identification)	11.5(1)SR1 und höher
MeetMe-Konferenz	10.3(1) und höher
Anzeige für wartende Nachrichten	10.3(1) und höher
Mobile Verbindung	10.3(1) und höher
MVA (Mobile Voice Access)	10.3(1) und höher
Multilevel Precedence and Preemption (MLPP)	11.5(1)SR1 und höher
IP-Telefon	11.5(1)SR1 und höher

Telefonfunktion	Telefon-Firmwareversion
Warteschleifenmusik	10.3(1) und höher
Stummschaltung	10.3(1) und höher
Netzwerkprofile (automatisch)	11.5(1)SR1 und höher
Wählen mit abgehobenem Hörer	10.3(1) und höher
Wählen bei aufgelegtem Hörer	10.3(1) und höher
Pluszeichen wählen	10.3(1) und höher
Privatfunktion	11.5(1)SR1 und höher
PLAR (Private Line Automated Ringdown)	11.5(1)SR1 und höher
Wahlwiederholung	10.3(1) und höher
Kurzwahl (Pause wird nicht unterstützt)	10.3(1) und höher
Taste „Dienste-URL“	11.5(1)SR1 und höher
Übergabe	10.3(1) und höher
URI-Wahl (Uniform Resource Identifier)	10.3(1) und höher

## 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 144

[Produktspezifische Konfiguration](#), auf Seite 146

## QR-Code für die MRA-Anmeldung generieren

Benutzer, deren Telefon mit einer Kamera ausgestattet ist, können einen QR-Code scannen, um sich bei MRA anzumelden und müssen nicht manuell die Servicedomäne und ihren Benutzernamen eingeben.

### Prozedur

#### Schritt 1

Generieren Sie mit einem QR-Code-Generator einen QR-Code mit der Servicedomäne oder mit der Servicedomäne und dem Benutzernamen, die durch ein Komma voneinander getrennt sind. Beispiel: mra.beispiel.com oder mra.beispiel.com,benutzername.

**Schritt 2** Drucken Sie den QR-Code aus, und übergeben Sie ihn dem Benutzer.

## Tool zur Problemmeldung

Die Benutzer senden Problembereiche mit dem Tool für Problembereiche (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 Problembereich zu erstellen, greifen die Benutzer auf das Tool für Problembereiche 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.
- 

## Informationen für zwei Speicherbänke einrichten

Gehen Sie zum Einrichten von Informationen für zwei Speicherbänke wie folgt vor:

### Prozedur

---

- Schritt 1** Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **Gerät > Gerätestandardwerte**.
- Schritt 2** Prüfen Sie die Software-Informationen im Feld mit den Informationen zu inaktiver Software.
- Schritt 3** Wählen Sie **Massenverwaltung > Importieren/Exportieren > Exportieren > Gerätestandardwerte**, und planen Sie einen Export-Auftrag.
- Schritt 4** Laden Sie die exportierte TAR-Datei herunter, und entpacken Sie diese.
- Schritt 5** Überprüfen Sie das Dateiformat in der exportierten CSV-Datei, und stellen Sie sicher, dass die CSV-Datei über eine Spalte mit Informationen zur inaktiven Software verfügt, in der der korrekte Wert angegeben ist.
- Hinweis** Der Wert in der CSV-Datei muss mit dem Gerätestandardwert im Fenster der Cisco Unified Communications Manager-Verwaltung übereinstimmen.
- 

## Überwachung geparkter Anrufe

Die Überwachung geparkter Anrufe wird nur unterstützt, wenn ein Anruf von einem Cisco IP-Telefon geparkt wird. Der Status eines geparkten Anrufs wird dann von der Überwachung geparkter Anrufe überwacht. Die Anrufblase für die Überwachung geparkter Anrufe verschwindet erst, wenn der geparkte Anruf abgerufen oder nicht angenommen wird. Dieser geparkte Anruf kann über die gleiche Anrufblase auf dem Telefon abgerufen werden, das den Anruf geparkt hat.

## Timer für Überwachung geparkter Anrufe einrichten

In der Cisco Unified Communications Manager-Verwaltung gibt es drei clusterübergreifende Dienstzeitgeberparameter für die Überwachung geparkter Anrufe: „Wiederholungstimer für die Überwachung geparkter Anrufe“, „Periodischer Wiederholungstimer für die Überwachung geparkter Anrufe“ und „Timer für die Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel“. Für jeden Dienstparameter gibt es einen Standard, und es ist keine spezielle Konfiguration erforderlich. Diese Zeitgeberparameter sind nur für die

Überwachung geparkter Anrufe vorgesehen. „Anzeigetimer für geparkte Anrufe“ und „Wiederholungstimer für geparkte Anrufe“ werden für die Überwachung geparkter Anrufe nicht verwendet. Eine Beschreibung dieser Parameter finden Sie in der folgenden Tabelle.

Die Zeitgeber werden auf der Seite „Cisco Unified Communications Manager – Dienstparameter“ konfiguriert.

## Prozedur

### Schritt 1

Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **System > Dienstparameter**.

### Schritt 2

Aktualisieren Sie die Felder „Wiederholungstimer für die Überwachung geparkter Anrufe“, „Periodischer Wiederholungstimer für die Überwachung geparkter Anrufe“ und „Timer für die Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel“ im Bereich „Clusterübergreifende Parameter“ („Funktion – Allgemein“).

**Tabelle 35: Dienstparameter für die Überwachung geparkter Anrufe**

Feld	Beschreibung
Wiederholungstimer für die Überwachung geparkter Anrufe	<p>Die Standardeinstellung ist 60 Sekunden. Mit diesem Parameter wird festgelegt, wie viele Sekunden vergehen sollen, bis der Cisco Unified Communications Manager den Benutzer dazu auffordert, ihm selbst geparkten Anruf wieder abzurufen. Dieser Timer beginnt zu laufen, wenn der Benutzer ein Telefon „Parken“ wählt. Nach Ablauf des Timers wird eine Erinnerung ausgegeben.</p> <p>Den Wert, den dieser Dienstparameter angibt, können Sie im Abschnitt „Überwachung geparkter Anrufe“ im Fenster zur Verzeichnisnummernkonfiguration für jede Leitung separat überschreiben (wählen Sie die Cisco Unified Communications Manager-Verwaltung <b>Anrufrouting &gt; Verzeichnisnummern</b>). Wenn Sie den Wert „0“ eingeben, können Sie sofort den periodischen Zurücksetzungsintervall nutzen. Wenn Sie den Dienstparameter „Periodischer Wiederholungstimer für die Überwachung geparkter Anrufe“ auf null setzen (Weitere Informationen hierzu finden Sie in der folgenden Beschreibung.) Wenn beispielsweise der Dienstparameter auf null und „Periodischer Wiederholungstimer für die Überwachung geparkter Anrufe“ auf 15 eingestellt ist, wird der Benutzer sofort und danach alle 15 Sekunden dazu aufgefordert, den geparkten Anruf abzurufen, bis „Timer für die Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel“ (siehe folgende Beschreibung) abläuft.</p>
Periodischer Wiederholungstimer für die Überwachung geparkter Anrufe	<p>Die Standardeinstellung ist 30 Sekunden. Dieser Parameter bestimmt den Intervall (in Sekunden), in dem der Cisco Unified Communications Manager wartet, bevor der Benutzer erneut dazu aufgefordert wird, den geparkten Anruf abzurufen. Nehmen Sie den Hörer ab, wenn die Aufforderung erneut erscheint, um eine Verbindung mit dem geparkten Anruf herzustellen. Cisco Unified Communications Manager fordert den Benutzer weiterhin dazu auf, den geparkten Anruf abzurufen, solange der Anruf geparkt bleibt. Wenn der „Timer für die Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel“ abläuft (siehe folgende Beschreibung). Geben Sie zum Deaktivieren der regelmäßigen Aufforderungen zu dem geparkten Anruf den Wert „0“ an.</p>

Feld	Beschreibung
Timer für die Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel	Die Standardeinstellung ist 300 Sekunden. Dieser Parameter gibt die Anzahl der Sekunden an, bevor Erinnerungsmeldungen über den geparkten Anruf gesendet werden, bevor der geparkte Anruf zum Ziel für „Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel“ weiterleitet, das in der Verzeichnisnummernkonfiguration angegeben wird. (Wenn in der Cisco Unified Communications Manager-Verwaltung kein Weiterleitungsziel angegeben wird, kehrt der Anruf zu der Leitung zurück, der der Anruf geparkt wurde.) Dieser Parameter startet, wenn die Zeit abgelaufen ist, die der Parameter „Wiederholungstimer für die Überwachung geparkter Anrufe“ angibt. Wenn „Timer für die Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel“ abgelaufen ist, wird der Anruf aus der Liste der geparkten Anrufe entfernt und zum angegebenen Ziel weitergeleitet, oder er kehrt zu der Leitung zurück, der der Anruf geparkt wurde.

## Parameter zur Überwachung geparkter Anrufe für Verzeichnisnummern einrichten

Im Abschnitt „Überwachung geparkter Anrufe“ im Fenster zur Verzeichnisnummernkonfiguration können Sie drei Parameter konfigurieren.

### Prozedur

#### Schritt 1

Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **Anruf-Routing > Verzeichnisnummer**.

#### Schritt 2

Konfigurieren Sie die Felder zur Überwachung geparkter Anrufe entsprechend den Angaben in der folgenden Tabelle.

**Tabelle 36: Parameter für die Überwachung geparkter Anrufe**

Feld	Beschreibung
Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel, extern	Wenn es sich beim geparkten Teilnehmer um einen externen Teilnehmer handelt, wird der Anruf an das Ziel umgeleitet, das im Parameter „Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel, extern“ des den Anruf parkenden Teilnehmers angegeben ist. Wenn das Feld „Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel, extern“ keinen Wert enthält, wird der geparkte Teilnehmer wieder auf die Leitung des den Anruf parkenden Teilnehmers umgeleitet.
Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel, intern	Wenn es sich beim geparkten Teilnehmer um einen internen Teilnehmer handelt, wird der Anruf an das Ziel umgeleitet, das im Parameter „Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel, intern“ des den Anruf parkenden Teilnehmers angegeben ist. Wenn das Feld „Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel, intern“ keinen Wert enthält, wird der geparkte Teilnehmer wieder auf die Leitung des den Anruf parkenden Teilnehmers umgeleitet.

Feld	Beschreibung
Wiederholungstimer für die Überwachung geparkter Anrufe	<p>Mit diesem Parameter wird festgelegt, wie viele Sekunden vergehen sollen, bis der Cisco Unified Communications Manager den Benutzer dazu auffordert, einen von ihm selbst geparkten Anruf wieder abzurufen. Dieser Timer beginnt zu laufen, wenn der Benutzer auf dem Telefon „Parken“ wählt. Nach Ablauf des Timers wird eine Erinnerung ausgegeben.</p> <p>Standardwert: 60 Sekunden</p> <p>Wenn Sie einen anderen Wert als null eingeben, überschreibt dieser Wert den Wert des im Fenster „Dienstparameter“ eingestellten Parameters. Bei Eingabe des Werts „0“ wird dagegen der im Fenster „Dienstparameter“ eingestellte Parameterwert verwendet.</p>

## Überwachung geparkter Anrufe für Hunt Lists einrichten

Wenn ein über die Hunt List weitergeleiteter Anruf geparkt wurde, wird bei Ablauf des Timers für „Überwachung geparkter Anrufe, Weiterleiten, kein Abruf“ der Wert des Parameters „Hunt Pilot, Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel“ verwendet (sofern dieser nicht leer ist).

### Prozedur

**Schritt 1** Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **Anrufrouting > /Route/Hunt > Hunt Pilot**.

**Schritt 2** Legen Sie den Parameter „Hunt Pilot, Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel“ fest.

Wenn der Wert des Parameters „Hunt Pilot, Überwachung geparkter Anrufe, Weiterleiten, kein Abrufziel“ leer ist, wird der Anruf bei Ablauf des Timers für „Überwachung geparkter Anrufe, Weiterleiten, kein Abruf“ an das Ziel weitergeleitet, das im Fenster „Konfiguration der Verzeichnisnummer“ konfiguriert ist.

## Audio- und Videoport-Bereiche einrichten

Zur Erhöhung der Quality of Service (QoS) können Audio- und Videodatenverkehr jeweils an unterschiedliche RTP-Port-Bereiche gesendet werden.

Die Port-Bereiche werden in der Cisco Unified Communications Manager-Verwaltung mithilfe der folgenden Felder festgelegt:

- Audioports
  - Medienport starten (standardmäßig: 16384)
  - Medienport beenden (standardmäßig: 32766)
- Videoports
  - Video starten (damit wird der Port zum Starten von Videos festgelegt).



- Minimum: 2048
  - Maximum: 65535
- Video stoppen (damit wird der Port zum Stoppen von Videos festgelegt).
- Minimum: 2048
  - Maximum: 65535

Für das Konfigurieren der Videoport-Felder gelten folgende Regeln:

Wenn die Felder „Start Video-RTP-Port“ und „End-Video-RTP-Port“ konfiguriert sind, verwendet das Telefon für den Videodatenverkehr Ports innerhalb dieses Videoport-Bereiches. Für den Audiodatenverkehr werden die Medienports genutzt.

Bei einer Überschneidung von Audio- und Videoport-Bereich laufen über diejenigen Ports, die in beiden Bereichen vorhanden sind, sowohl Audio- als auch Videodatenverkehr. Wenn der Videoport-Bereich nicht ordnungsgemäß konfiguriert wurde, verwendet das Telefon stattdessen die konfigurierten Audioports sowohl für Audio- als auch für Videodatenverkehr.

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

### Prozedur

- 
- Schritt 1** Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **Gerät > Geräteeinstellungen > SIP-Profil**.
- Schritt 2** Legen Sie anhand der Felder „Medienport starten“ und „Medienport beenden“ den Audioport-Bereich fest.
- Schritt 3** Wählen Sie **Speichern** aus.
- Schritt 4** Wählen Sie eines der folgenden Fenster aus:
- **System > Firmentelefonkonfiguration**
  - **Gerät > Geräteeinstellungen > Allgemeines Telefonprofil**
  - **Gerät > Telefon > Telefonkonfiguration**
- Schritt 5** Legen Sie anhand der Felder „Start-Video-RTP-Port“ und „End-Video-RTP-Port“ den erforderlichen Port-Bereich fest.
- Für das Konfigurieren der Videoport-Felder gelten folgende Regeln:
- Der Wert im Feld „End-Video-RTP-Port“ muss größer sein als der Wert im Feld „Start-Video-RTP-Port“.
  - Die Differenz der Werte in den Feldern „Start-Video-RTP-Port“ und „End-Video-RTP-Port“ muss mindestens 16 betragen.
- Schritt 6** Wählen Sie **Speichern** aus.

---

### Verwandte Themen

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

## Einrichten des Cisco IP Manager Assistant

Cisco IP Manager Assistant (IPMA) bietet Anrufweiterleitungs- sowie andere Anrufverarbeitungsfunktionen, mit denen Manager und Assistenten Telefonanrufe effektiver verarbeiten können.

Bevor Sie auf IPMA-Dienste zugreifen können, müssen diese Dienste im Cisco Unified Communications Manager konfiguriert werden. Detaillierte Informationen zur IPMA-Konfiguration finden Sie im *Funktionskonfigurationshandbuch für Cisco Unified Communications Manager*.

IPMA besteht aus drei Hauptkomponenten:

### Manager

Die Anrufe für einen Manager werden vom Anruf-Routing-Dienst abgefangen.

### Assistent

Ein Assistent verarbeitet Anrufe im Auftrag eines Managers.

### Assistent Console

Die Assistent Console ist eine Desktop-Anwendung, über die Assistenten Aufgaben durchführen und die meisten Funktionen verwalten können.

IPMA unterstützt zwei Betriebsmodi: Unterstützung für Proxy-Leitungen und Unterstützung für gemeinsam genutzte Leitungen. Beide Modi unterstützen mehrere Anrufe pro Leitung für den Manager. Der IPMA-Dienst unterstützt die Unterstützung für Proxy-Leitungen und gemeinsam genutzte Leitungen in einem Cluster.

Im Modus für gemeinsam genutzte Leitungen teilen sich der Manager und der Assistent eine Verzeichnisnummer; Anrufe werden in der gemeinsam genutzten Leitung bearbeitet. Wenn ein Anruf in der gemeinsam genutzten Leitung eingeht, läuten sowohl das Telefon des Managers als auch das Telefon des Assistenten. Im Modus für gemeinsam genutzte Leitungen werden die Standard-Assistentenauswahl, die Assistentenüberwachung, die Anruffilterung oder die Umleitung aller Anrufe nicht unterstützt.

Wenn Sie Cisco IPMA im Modus für gemeinsam genutzte Leitungen konfigurieren, teilen sich der Manager und der Assistent eine Verzeichnisnummer, beispielsweise 1701. Der Assistent verarbeitet unter der gemeinsamen Verzeichnisnummer Anrufe für einen Manager. Wenn ein Manager einen Anruf unter der Verzeichnisnummer 1701 erhält, klingelt sowohl das Telefon des Managers als auch das des Assistenten.

Nicht alle IPMA-Funktionen sind im Modus für gemeinsam genutzte Leitungen verfügbar. Dazu gehören die Standard-Assistentenauswahl, die Assistentenüberwachung, die Anruffilterung und die Umleitung aller Anrufe. Den Assistenten werden diese Funktionen nicht in der Assistent Console angezeigt und sie können auch nicht darauf zugreifen. Das Telefon des Assistenten weist nicht den Softkey für die Funktion „Alle umleit.“ auf. Das Telefon des Managers weist nicht die Softkeys für die Funktionen „Asst. Überw.“, „Alle umleit.“ oder „Abfangen“ auf.

Um auf den Benutzergeräten auf die Unterstützung für gemeinsam genutzte Leitungen zugreifen zu können, müssen Sie zuerst über die Cisco Unified Communications Manager-Verwaltung den Cisco IP Manager Assistant-Dienst konfigurieren und starten.

Im Modus für Proxy-Leitungen verarbeitet der Assistent Anrufe im Namen eines Managers mithilfe einer Proxy-Nummer. Der Modus für Proxy-Leitungen unterstützt alle IPMA-Funktionen.

Wenn Sie Cisco IPMA im Modus für Proxy-Leitungen konfigurieren, haben Manager und Assistent keine gemeinsame Verzeichnisnummer. Der Assistent verarbeitet Anrufe für einen Manager mithilfe einer Proxy-Nummer. Die Proxy-Nummer ist nicht die Verzeichnisnummer für den Manager. Es handelt sich um eine alternative Nummer, die vom System gewählt und von einem Assistenten verwendet wird, um Anrufe des Managers zu bearbeiten. Im Modus für Proxy-Leitungen haben ein Manager und ein Assistent Zugriff

auf alle in IPMA verfügbaren Funktionen, einschließlich Standard-Assistentenauswahl, Assistentenüberwachung, Anruffilterung und Umleiten aller Anrufe.

Um auf den Benutzergeräten auf die Unterstützung für Proxy-Leitungen zugreifen zu können, müssen Sie zuerst über die Cisco Unified Communications Manager-Verwaltung den Cisco IP Manager Assistant-Dienst konfigurieren und starten.

Sie können über Softkeys und Telefondienste auf die IPMA-Funktionen zugreifen. Die Softkey-Vorlage wird im Cisco Unified Communications Manager konfiguriert. IPMA unterstützt die folgenden Standard-Softkey-Vorlagen:

### Standard-Manager

Unterstützt den Manager für den Proxy-Modus.

### Standard-Manager im gemeinsam genutzten Modus

Unterstützt den Manager für den gemeinsam genutzten Modus.

### Standard-Assistent

Unterstützt den Assistenten im Proxy- oder gemeinsam genutzten Modus.

In der folgenden Tabelle sind die in den Softkey-Vorlagen verfügbaren Softkeys aufgeführt.

**Tabelle 37: IPMA-Softkeys**

Softkey	Call State (Anrufstatus)	Beschreibung
Umleiten	Läuten, Verbunden, Gehalten	Der ausgewählte Anruf wird an ein vorkonfiguriertes Ziel umgeleitet.
Übernehmen	Alle Status	Ein Anruf wird vom Telefon des Assistenten an das Telefon des Managers umgeleitet und automatisch beantwortet.
Überwachen	Alle Status	Der Status eines Anrufs, der von einem Assistenten bearbeitet wird, wird angezeigt.
TransVM (Weiterleiten an Voicemail)	Läuten, Verbunden, Gehalten	Der ausgewählte Anruf wird an die Voicemail des Managers weitergeleitet.
Alle umleiten	Alle Status	Alle an den Manager geleiteten Anrufe werden an ein vorkonfiguriertes Ziel umgeleitet.



**Hinweis** „Abfangen“, „Überwachen“ und „Alle umleiten“ sollten nur für ein Manager-Telefon im Modus für Proxy-Leitungen konfiguriert werden.

Die folgende Vorgehensweise bietet einen Überblick über die erforderlichen Schritte.

### Prozedur

---

- Schritt 1** Konfigurieren Sie die Telefone und Benutzer.
  - Schritt 2** Ordnen Sie die Telefone den Benutzern zu.
  - Schritt 3** Aktivieren Sie den Cisco IP Manager Assistant-Dienst im Fenster für die Dienstaktivierung.
  - Schritt 4** Konfigurieren Sie die Parameter der Systemverwaltung.
  - Schritt 5** Konfigurieren Sie bei Bedarf IPMA-clusterweite Dienstparameter.
  - Schritt 6** (optional) Konfigurieren Sie das Benutzer-CAPF-Profil.
  - Schritt 7** (optional) Konfigurieren Sie die IPMA-Dienstparameter für die Sicherheit.
  - Schritt 8** Halten Sie den IPMA-Dienst an, und starten Sie ihn neu.
  - Schritt 9** Konfigurieren Sie die Einstellungen für Telefonparameter, Manager und Assistenten, einschließlich der Softkey-Vorlagen.
  - Schritt 10** Konfigurieren Sie die Anwendung Cisco Unified Communications Manager Assistant.
  - Schritt 11** Konfigurieren Sie Wählregeln.
  - Schritt 12** Installieren Sie die Anwendung Assistant Console.
  - Schritt 13** Konfigurieren Sie die Anwendungen Manager und Assistant Console.
- 

## Visual Voicemail einrichten

Visual Voicemail wird in der Cisco Unified Communications Manager-Verwaltung für alle Cisco IP-Telefons oder für einen Einzelbenutzer bzw. eine einzelne Gruppe von Benutzern konfiguriert.



**Hinweis** Weitere Informationen zur Konfiguration finden Sie in der Dokumentation für Cisco Visual Voicemail unter <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

Der visuelle Voicemail-Client wird auf den Cisco IP 8800-Telefonen nicht als Midlet unterstützt.

### Prozedur

---

- Schritt 1** Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **Gerät > Geräteeinstellungen > Telefondienste**.
- Schritt 2** Wählen Sie **Neu hinzufügen**, um einen neuen Dienst für Visual Voicemail zu erstellen.
- Schritt 3** Geben Sie im Konfigurationsfenster für die IP-Telefondienste in den entsprechenden Feldern die folgenden Informationen ein:
  - Dienstname: Geben Sie **VisualVoiceMail** ein.
  - ASCII-Servicename: Geben Sie **VisualVoiceMail** ein.
  - Dienst-URL: Geben Sie **Application: Cisco/VisualVoiceMail** ein.
  - Servicekategorie: Wählen Sie im Pulldown-Menü **XML-Dienst**.
  - Servicetyp: Wählen Sie im Pulldown-Menü **Nachrichten**.
- Schritt 4** Aktivieren Sie die Option **Aktivieren**, und klicken Sie dann auf **Speichern**.

**Hinweis** Vergewissern Sie sich, dass **Unternehmensteilnahme** nicht aktiviert ist.

**Schritt 5** Klicken Sie im Fenster für Informationen zu Dienstparametern auf **Neuer Parameter**, und geben Sie in den entsprechenden Feldern die folgenden Informationen ein:

- Parametername. Geben Sie „voicemail\_server“ ein.
- Parameter-Anzeigename. Geben Sie „voicemail\_server“ ein.
- Standardwert. Geben Sie den Host-Namen des primären Unity Servers ein.
- Parameterbeschreibung

**Schritt 6** Aktivieren Sie die Option **Parameter ist erforderlich**, und klicken Sie auf **Speichern**.

**Hinweis** **Parameter ist Kennwort (Inhalt verbergen)** darf nicht aktiviert sein.

**Schritt 7** Schließen Sie das Fenster, und wählen Sie im Konfigurationsfenster für Telefondienste erneut **Speichern**.

---

## Visual Voicemail für einen bestimmten Benutzer einrichten

Gehen Sie wie folgt vor, um Visual Voicemail für einen bestimmten Benutzer zu konfigurieren.



**Hinweis** Informationen zur Konfiguration finden Sie in der Dokumentation zu Cisco Visual Voicemail unter <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

---

### Prozedur

- Schritt 1** Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **Gerät > Telefon**.
- Schritt 2** Wählen Sie das Gerät aus, das dem von Ihnen gesuchten Benutzer zugeordnet ist.
- Schritt 3** Wählen Sie in der Dropdown-Liste „Weiterführende Links“ die Option **Dienste abonnieren/Abonnement kündigen**, und klicken Sie dann auf **Los**.
- Schritt 4** Wählen Sie den von Ihnen erstellten Visual Voicemail-Dienst und anschließend **Weiter > Abonnieren**.

---

## Visual Voicemail-Setup für eine Benutzergruppe

Um Cisco Unified Communications Manager mit einem Visual Voicemail-Abonnement eine Gruppe von Cisco IP-Telefons hinzuzufügen, erstellen Sie für jeden Telefentyp und in jeder Telefonvorlage eine Telefonvorlage im BAT-Tool. Sie können anschließend den Visual Voicemail-Dienst abonnieren und die Telefone mithilfe der Vorlage einfügen.

Wenn Ihre Cisco IP-Telefons bereits registriert sind und Sie für die Telefone den Visual Voicemail-Dienst abonnieren möchten, erstellen Sie eine Telefonvorlage in BAT, abonnieren Sie den Visual Voicemail-Dienst in der Vorlage, und aktualisieren Sie anschließend die Telefone mithilfe des BAT-Tools.

Weitere Informationen finden Sie unter <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>.

## Zugesicherte Dienste für SIP

Assured Services SIP (AS-SIP) ist eine Sammlung an Funktionen und Protokollen, die einen äußerst sicheren Anrufdienst für Cisco IP-Telefon und Drittanbieter-Telefone bieten. Die folgenden Funktionen werden zusammen als AS-SIP bezeichnet:

- Multilevel Precedence and Preemption (MLPP)
- Differentiated Services Code Point (DSCP)
- Transport Layer Security (TLS) und Secure Real-Time Transport Protocol (SRTP)
- Internetprotokoll Version 6 (IPv6)

AS-SIP wird häufig mit Multilevel Precedence and Preemption (MLPP) verwendet, um Anrufe bei einem Notfall zu priorisieren. Mit MLPP weisen Sie Ihren ausgehenden Anrufen eine Prioritätsstufe von Stufe 1 (niedrig) bis Stufe 5 (hoch) zu. Wenn Sie einen Anruf erhalten, wird das Symbol für die Prioritätsstufe auf dem Telefon angezeigt, das die Anrufpriorität angibt.

Um AS-SIP zu konfigurieren, führen Sie die folgenden Aufgaben in Cisco Unified Communications Manager durch:

- Einen Digest-Benutzer konfigurieren: Konfigurieren Sie den Endbenutzer so, dass er die Digest-Authentifizierung für SIP-Anforderungen verwendet.
- Sicheren Port für SIP-Telefon konfigurieren: Cisco Unified Communications Manager verwendet diesen Port, um SIP-Telefone für SIP-Leitungsregistrierungen über TLS abzuhören.
- Dienste neu starten: Starten Sie nach der Konfiguration des sicheren Ports die Cisco Unified Communications Manager- und Cisco CTL Provider-Dienste neu. Ein SIP-Profil für AS-SIP konfigurieren: Konfigurieren Sie ein SIP-Profil mit SIP-Einstellungen für Ihre AS-SIP-Endpunkte und für Ihre SIP-Trunks. Die telefonspezifischen Parameter werden nicht auf das AS-SIP-Telefon eines Drittanbieters heruntergeladen. Sie werden nur von Cisco Unified Manager verwendet. Drittanbieter-Telefone müssen lokal dieselben Einstellungen konfigurieren.
- Telefonsicherheitsprofil für AS-SIP konfigurieren: Sie können das Sicherheitsprofil des Telefons verwenden, um Sicherheitseinstellungen wie TLS, SRTP und Digest-Authentifizierung zuzuweisen.
- AS-SIP-Endpunkt konfigurieren: Konfigurieren Sie ein Cisco IP-Telefon oder einen Drittanbieter-Endpunkt mit AS-SIP-Unterstützung.
- Gerät mit Endpunkt zuweisen: Weisen Sie den Endpunkt einem Benutzer zu.
- SIP-Trunk-Sicherheitsprofil für AS-SIP konfigurieren: Sie können das SIP-Trunk-Sicherheitsprofil verwenden, um Sicherheitsfunktionen, wie TLS oder Digest-Authentifizierung, einem SIP-Trunk zuzuweisen.
- SIP-Trunk für AS-SIP konfigurieren: Konfigurieren Sie einen SIP-Trunk mit AS-SIP-Unterstützung.
- AS-SIP-Funktionen konfigurieren: Konfigurieren Sie zusätzliche AS-SIP-Funktionen wie MLPP, TLS, V.150 und IPv6.

Detaillierte Informationen zur AS-SIP-Konfiguration finden Sie im Kapitel "AS-SIP-Endpunkte konfigurieren" im *Systemkonfigurationsleitfaden für Cisco Unified Communications Manager*.

## 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)

## MLPP (Multilevel Precedence and Preemption)

Mit Multilevel Precedence and Preemption (MLPP) können Sie Anrufe Notfällen oder anderen Krisensituationen priorisieren. Sie weisen Ihren ausgehenden Anrufen eine Priorität von 1 bis 5 zu. Bei eingehenden Anrufen wird ein Symbol angezeigt, das die Anrufpriorität angibt. Authentifizierte Benutzer können Anrufe entweder an Zielstellen weiterleiten oder über vollständig ausgelastete TDM-Trunks durchschalten.

Diese Funktion sichert hochrangiges Personal für die Kommunikation für wichtige Organisationen und Mitarbeiter.

MLPP wird häufig mit Assured Services SIP (AS-SIP) verwendet. Detaillierte Informationen zur MLPP-Konfiguration finden Sie im Kapitel "Multilevel Precedence and Preemption konfigurieren" im *Systemkonfigurationshandbuch für Cisco Unified Communications Manager*.

## Softkey-Vorlagen konfigurieren

Mit der Cisco Unified Communications Manager-Verwaltung können Sie vom Telefon unterstützte Anwendungen zu insgesamt maximal 18 Softkeys zuordnen. Cisco Unified Communications Manager unterstützt die Softkey-Vorlagen Standardbenutzer und Standardfunktionen.

Einer Anwendung, die Softkeys unterstützt, sind eine oder mehrere Standard-Softkey-Vorlagen zugeordnet. Sie können eine Standard-Softkey-Vorlage ändern, indem Sie sie kopieren, umbenennen und die neue Vorlage anschließend aktualisieren. Sie können auch eine nicht standardisierte Softkey-Vorlage ändern.

Der Parameter „Softkey-Steuerung“ gibt an, ob Softkeys eines Telefons durch die Softkey-Vorlagenfunktion gesteuert werden. Der Parameter „Softkey-Steuerung“ ist ein erforderliches Feld.

Weitere Informationen zum Konfigurieren dieser Funktion finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.

Die Cisco IP-Telefons unterstützen nicht alle Softkeys, die in der Softkey-Vorlagenkonfiguration in der Cisco Unified Communications Manager-Verwaltung konfiguriert werden können. Der Cisco Unified Communications Manager ermöglicht es Ihnen, einige Softkeys in den Konfigurationseinstellungen der Steuerungsrichtlinie zu aktivieren oder zu deaktivieren. In der folgenden Tabelle werden die Funktionen und Softkeys aufgelistet, die in einer Softkey-Vorlage konfiguriert werden können; zudem wird angegeben, ob sie für die Cisco IP-Telefons unterstützt werden.



---

**Hinweis**

Cisco Unified Communications Manager ermöglicht Ihnen, einen beliebigen Softkey in einer Softkey-Vorlage zu konfigurieren, aber nicht unterstützte Softkeys werden nicht auf dem Telefon angezeigt.

---

Tabelle 38: Konfigurierbare Softkeys

Funktion	Konfigurierbare Softkeys in der Softkey-Vorlagenkonfiguration	Unterstützt als Softkey
Anrufannahme	Annehmen (Annehm.)	Unterstützt
Rückruf	Rückruf (Rückruf)	Unterstützt
Rufumleitung Alle Anrufe	Alle Anrufe weiterleiten (Rufuml.)	Unterstützt
Anruf parken	Anruf parken (Parken)	Unterstützt
Anrufübernahme	Übernahme (Übernah.)	Unterstützt
Aufschalten	Aufschalten	Unterstützt
Konferenzanschaltung	Konferenz anschalten	Unterstützt
Konferenz	Konferenz (Konfer.)	Unterstützt
Konferenzliste	Konferenzliste (KonfList)	Unterstützt
Umleiten	Sofort umleiten (SofUml.)	Unterstützt
Bitte nicht stören	„Bitte nicht stören“ (Ruhefunktion) ein-/ausschalten	Unterstützt
Anruf beenden	Anruf beenden (Auflegen)	Unterstützt
Gruppenübernahme	Gruppenübernahme (GrÜbern.)	Unterstützt
Halten	Halten (Halten)	Unterstützt
Sammelanschlussgruppe	HLog (HLog)	Unterstützt
Beitreten	Zusammenführen (Zusf.)	Nicht unterstützt
Identifizierung böswilliger Anrufer	Identifizierung böswilliger Anrufer umschalten	Unterstützt
MeetMe	MeetMe (MeetMe)	Unterstützt
Mobile Verbindung	Mobilität (Mobilität)	Unterstützt
Neuer Anruf	Neuer Anruf (Anruf)	Unterstützt
Andere Übernahme	Andere Übernahme (APickUp)	Unterstützt
PLK-Unterstützung für Warteschlangenstatus	Warteschlangenstatus	Nicht unterstützt
Quality Reporting Tool	Tool für Qualitätsberichte (QRT)	Unterstützt



Funktion	Konfigurierbare Softkeys in der Softkey-Vorlagenkonfiguration	Unterstützt als Softkey
Wahlwiederholung	Wahlwiederholung (Wahlw.)	Unterstützt
Letzten Konferenzteilnehmer entfernen	Letzten Konferenzteilnehmer entfernen (Entfernen)	Nicht unterstützt
Heranholen	Fortsetzen (Forts.)	Unterstützt
Auswahl	Auswahl (Auswahl)	Nicht unterstützt
Kurzwahl	Kurzwahlcodes (KWCodes)	Unterstützt
Übergabe	Übergabe (Übergabe)	Unterstützt
Videomodus-Befehl	Videomodus-Befehl (VidModus)	Nicht unterstützt

### Prozedur

#### Schritt 1

Wählen Sie in der Cisco Unified Communications Manager-Verwaltung eines der folgenden Fenster aus:

- Wählen Sie zum Konfigurieren von Softkey-Vorlagen **Gerät > Geräteeinstellungen > Softkey-Vorlage**.
- Um eine Softkey-Vorlage einem Telefon zuzuweisen, wählen Sie **Gerät > Telefon**, und konfigurieren Sie das Feld „Softkey-Vorlage“.

#### Schritt 2

Speichern Sie die Änderungen.

### Verwandte Themen

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

## Vorlagen für Telefontasten

Mit Telefontastenvorlagen können Sie programmierbaren Tasten eine Kurzwahl oder Anruffunktion zuordnen. Die Anruffunktionen, die Tasten zugeordnet werden können, umfassen Annehmen, Mobilität und Alle Anrufe.

Sie sollten Vorlagen ändern, bevor Sie Telefone im Netzwerk registrieren. Auf diese Weise können Sie während der Registrierung in Cisco Unified Communications Manager auf die Optionen für benutzerdefinierte Telefontastenvorlagen zugreifen.

## Telefontastenvorlage ändern

Weitere Informationen zu IP-Telefondiensten und zum Konfigurieren von Leitungstasten finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.

### Prozedur

---

- Schritt 1** Wählen Sie **Gerät > Geräteeinstellungen > Telefontastenvorlage** in der Cisco Unified Communications Manager-Verwaltung aus.
- Schritt 2** Klicken Sie auf **Suchen**.
- Schritt 3** Wählen Sie das Telefonmodell aus.
- Schritt 4** Wählen Sie **Kopieren** aus, geben Sie den Namen für die neue Vorlage ein und wählen Sie **Speichern** aus.  
Das Fenster Konfiguration der Telefontastenvorlage wird geöffnet.
- Schritt 5** Identifizieren Sie die Taste, die Sie zuweisen möchten, und wählen Sie **Service-URL** in der Dropdown-Liste Funktionen aus, die der Leitung zugeordnet ist.
- Schritt 6** Wählen Sie **Speichern** aus, um eine neue Telefontastenvorlage zu erstellen, die die Service-URL verwendet.
- Schritt 7** Wählen Sie **Gerät > Telefon** aus und öffnen Sie das Fenster Telefonkonfiguration für das Telefon.
- Schritt 8** Wählen Sie die neue Telefontastenvorlage in der Dropdown-Liste Telefontastenvorlage aus.
- Schritt 9** Wählen Sie **Speichern** aus, um die Änderung zu speichern, und anschließend **Konfiguration übernehmen**, um die Änderung zu implementieren.
- Der Benutzer des Telefons kann nun auf das Self Care Portal zugreifen und dem Service eine Taste auf dem Telefon zuweisen.

### Verwandte Themen

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

## Telefontastenvorlage für alle Anrufe zuweisen

Weisen Sie in der Telefonvorlage eine Taste „Alle Anrufe“ für Benutzer mit mehreren gemeinsam genutzten Leitungen zu.

Wenn Sie eine Taste „Alle Anrufe“ auf dem Telefon konfigurieren, können Benutzer die Taste „Alle Anrufe“ für Folgendes verwenden:

- Anzeigen einer zusammengefassten Liste der aktuellen Anrufe für alle Leitungen des Telefons
- Anzeigen einer Liste aller Anrufe in Abwesenheit für alle Leitungen des Telefons (unter „Anrufprotokoll“)
- Tätigen eines Anrufs auf der Hauptleitung des Benutzers, wenn der Benutzer den Hörer abhebt. „Alle Anrufe“ verwendet standardmäßig die Hauptleitung des Benutzers für alle ausgehenden Anrufe.

### Prozedur

---

- Schritt 1** Bearbeiten Sie die Telefontastenvorlage, um die Taste „Alle Anrufe“ darin aufzunehmen.
- Schritt 2** Weisen Sie die Vorlage dem Telefon zu.
-

## PAB oder Kurzwahl als IP-Telefonservice konfigurieren

Sie können eine Telefontastenvorlage ändern, um einer programmierbaren Taste eine Service-URL zuzuordnen. Anschließend können die Benutzer mit einer Taste auf PAB und Kurzwahlen zugreifen. Vor dem Ändern der Telefontastenvorlage müssen Sie das persönliche Adressbuch bzw. die Kurzwahl als IP-Telefondienst konfigurieren. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Um PAB oder Kurzwahlen als IP-Telefonservice zu konfigurieren, führen Sie die folgenden Schritte aus:

### Prozedur

- 
- Schritt 1** Wählen Sie **Gerät > Geräteeinstellungen > Telefonservices** in der Cisco Unified Communications Manager-Verwaltung aus.
- Das Fenster IP-Telefonservices suchen und auflisten wird angezeigt.
- Schritt 2** Klicken Sie auf **Neu hinzufügen**.
- Das Fenster IP-Telefonservicekonfiguration wird geöffnet.
- Schritt 3** Geben Sie die folgenden Einstellungen ein:
- Servicename: Geben Sie **Persönliches Adressbuch** ein.
  - Servicebeschreibung: Geben Sie eine optionale Beschreibung für den Service ein.
  - Service-URL
    - Für PAB geben Sie die folgende URL ein:  
**http://<Unified CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**
    - Für die Schnellwahl geben Sie die folgende URL ein:  
**http://<Unified-CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**
  - Sichere Service-URL
    - Für PAB geben Sie die folgende URL ein:  
**https://<Unified CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab**
    - Für die Schnellwahl geben Sie die folgende URL ein:  
**https://<Unified-CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd**
  - Servicekategorie: Wählen Sie **XML-Service** aus.
  - Servicetyp: Wählen Sie **Verzeichnisse** aus.
  - Aktiviert: Aktivieren Sie das Kontrollkästchen.  
*http://<IP\_address>* oder *https://<IP\_address>* (je nach dem vom Cisco IP-Telefon unterstützten Protokoll)
- Schritt 4** Wählen Sie **Speichern** aus.

**Hinweis** Wenn Sie die Service-URL ändern, entfernen Sie einen IP-Telefonserviceparameter oder ändern Sie den Namen des Telefonserviceparameters für einen Telefonservice, den die Benutzer abonniert haben. Sie müssen auf **Abonnements aktualisieren** klicken, um alle aktuellen Benutzer mit den Änderungen zu aktualisieren. Ansonsten müssen die Benutzer den Service erneut abonnieren, um die korrekte URL zu erstellen.

---

#### Verwandte Themen

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

## Telefontastenvorlage für das persönliche Adressbuch oder die Schnellwahl ändern

Sie können eine Telefontastenvorlage ändern, um einer programmierbaren Taste eine Service-URL zuzuordnen. Anschließend können die Benutzer mit einer Taste auf PAB und Kurzwahlen zugreifen. Vor dem Ändern der Telefontastenvorlage müssen Sie das persönliche Adressbuch bzw. die Kurzwahl als IP-Telefondienst konfigurieren.

Weitere Informationen zu IP-Telefondiensten und zum Konfigurieren von Leitungstasten finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.

#### Prozedur

- 
- Schritt 1** Wählen Sie **Gerät > Geräteeinstellungen > Telefontastenvorlage** in der Cisco Unified Communications Manager-Verwaltung aus.
  - Schritt 2** Klicken Sie auf **Suchen**.
  - Schritt 3** Wählen Sie das Telefonmodell aus.
  - Schritt 4** Wählen Sie **Kopieren** aus, geben Sie den Namen für die neue Vorlage ein und wählen Sie **Speichern** aus. Das Fenster Konfiguration der Telefontastenvorlage wird geöffnet.
  - Schritt 5** Identifizieren Sie die Taste, die Sie zuweisen möchten, und wählen Sie **Service-URL** in der Dropdown-Liste Funktionen aus, die der Leitung zugeordnet ist.
  - Schritt 6** Wählen Sie **Speichern** aus, um eine neue Telefontastenvorlage zu erstellen, die die Service-URL verwendet.
  - Schritt 7** Wählen Sie **Gerät > Telefon** aus und öffnen Sie das Fenster Telefonkonfiguration für das Telefon.
  - Schritt 8** Wählen Sie die neue Telefontastenvorlage in der Dropdown-Liste Telefontastenvorlage aus.
  - Schritt 9** Wählen Sie **Speichern** aus, um die Änderung zu speichern, und anschließend **Konfiguration übernehmen**, um die Änderung zu implementieren.

Der Benutzer des Telefons kann nun auf das Self Care Portal zugreifen und dem Service eine Taste auf dem Telefon zuweisen.

---

#### Verwandte Themen

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

# VPN-Konfiguration

Durch die Cisco VPN-Funktion bleibt die Netzwerksicherheit erhalten, während die Benutzer über eine sichere, zuverlässige Methode verfügen, um eine Verbindung mit Ihrem Unternehmensnetzwerk herzustellen.

Verwenden Sie diese Funktion in folgenden Situationen:

- Ein Telefon befindet sich außerhalb eines vertrauenswürdigen Netzwerks
- Der Netzwerkverkehr zwischen dem Telefon und Cisco Unified Communications Manager verläuft durch ein nicht vertrauenswürdiges Netzwerk

Bei einem VPN gibt es drei gängige Ansätze in Bezug auf die Client-Authentifizierung:

- Digitale Zertifikate
- Kennwörter
- Benutzername und Kennwort

Jede Methode bietet ihre Vorteile. Sofern dies von der Sicherheitsrichtlinie Ihres Unternehmens zugelassen wird, empfiehlt es sich jedoch, einen auf Zertifikaten basierenden Ansatz zu verwenden, da Zertifikate eine nahtlose Anmeldung ohne jegliche Benutzerintervention ermöglichen. Es werden sowohl LSC- als auch MIC-Zertifikate unterstützt.

Um die VPN-Funktionen zu konfigurieren, stellen Sie das Gerät zunächst am Standort vor Ort bereit; anschließend können Sie das Gerät für externe Standorte bereitstellen.

Weitere Informationen zum Authentifizieren mit Zertifikaten und zum Arbeiten mit einem VPN-Netzwerk finden Sie im Technischen Hinweis *AnyConnect VPN Phone with Certificate Authentication on an ASA Configuration Example* (Beispiel für ein AnyConnect VPN-Telefon mit Zertifikatauthentifizierung in einer ASA-Konfiguration). Dieses Dokument kann unter der URL <http://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html> abgerufen werden.

Bei einem Ansatz mit Kennwort oder Benutzername und Kennwort werden Benutzer aufgefordert, Anmeldeinformationen anzugeben. Legen Sie die Anmeldeinformationen für Benutzer entsprechend der Sicherheitsrichtlinie Ihres Unternehmens fest. Sie können auch die Einstellung „Dauerhaftes Kennwort festlegen“ so konfigurieren, dass das Benutzerkennwort auf dem Telefon gespeichert wird. Das Benutzerkennwort bleibt gespeichert, bis ein Anmeldeversuch fehlschlägt, das Kennwort von einem Benutzer manuell gelöscht wird, das Telefon zurückgesetzt wird oder die Stromversorgung unterbrochen wird.

Ein weiteres hilfreiches Tool ist die Einstellung „Automatische Netzwerkerkennung aktivieren“. Wenn Sie dieses Kontrollkästchen aktivieren, kann der VPN-Client nur ausgeführt werden, wenn er erkennt, dass er sich außerhalb des Unternehmensnetzwerks befindet. Diese Einstellung ist standardmäßig deaktiviert.

Ihr Cisco Telefon unterstützt Cisco SVC IP-Telefon Client v1.0 als Client-Typ.

Weitere Informationen zum Warten, Konfigurieren und Betreiben eines virtuellen privaten Netzwerks mit einem VPN finden Sie im *Sicherheitshandbuch zu Cisco Unified Communications Manager* im Kapitel zum Einrichten des Virtual Private Network („Virtual Private Network Setup“). Dieses Dokument kann unter der URL <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html> abgerufen werden.

Die Cisco VPN-Funktion nutzt SSL (Secure Sockets Layer), um die Netzwerksicherheit zu erhalten.



**Hinweis** Machen Sie Angaben für die Einstellung „Alternativer TFTP-Server“, wenn Sie ein Telefon an einem externen Standort für SSL VPN in ASA mit einem integrierten Client konfigurieren.

## Zusätzliche Leitungstasten einrichten

Aktivieren Sie den erweiterten Leitungsmodus, um die Tasten auf beiden Seiten des Telefonbildschirms als Leitungstasten zu verwenden. Predictive Dialing und Aktionshinweise für eingehende Anrufe sind im erweiterten Leitungsmodus standardmäßig aktiviert.

### Vorbereitungen

Sie müssen eine neue, benutzerdefinierte Telefontastenvorlage erstellen.

### 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 Bereich „Produktspezifische Konfiguration“, und setzen das Feld **Leitungsmodus** auf **Erweiterter Leitungsmodus**.
  - Schritt 4** Navigieren Sie zum Bereich „Geräteinformationen“, und legen Sie im Feld **Telefontastenvorlage** eine benutzerdefinierte Vorlage fest.
  - Schritt 5** Wählen Sie **Konfiguration übernehmen**.
  - Schritt 6** Wählen Sie **Speichern** aus.
  - Schritt 7** Starten Sie das Telefon neu.

### Verwandte Themen

[Umgebung mit Sitzungsleitungsmodus](#), auf Seite 169

## Im erweiterten Leitungsmodus verfügbare Funktionen

Der erweiterte Leitungsmodus (ELM) kann mit Mobil- und Remote Access über Expressway verwendet werden.

Der ELM kann auch mit einer Rollover-Leitung verwendet werden. Hierbei handelt es sich um die Konfiguration eines Anruf-Routings, bei der Anrufe an eine andere gemeinsam genutzte Leitung weitergeleitet werden, wenn die anfängliche gemeinsam genutzte Leitung besetzt ist. Wenn ELM mit einer Rollover-Leitung verwendet wird, werden die letzten Anrufe an gemeinsam genutzte Leitungen unter einer einzelnen Verzeichnisnummer zusammengefasst. Weitere Informationen zu Rollover-Leitungen finden Sie in *Funktionskonfigurationshandbuch für Cisco Unified Communications Manager* für Cisco Unified Communications Manager 12.0(1) oder höher.

ELM unterstützt die meisten, jedoch nicht alle Funktionen. Wenn Sie eine Funktion aktivieren, heißt das nicht automatisch, dass diese auch unterstützt wird. Sehen Sie in der folgenden Tabelle nach, um sicherzustellen, dass eine bestimmte Funktion unterstützt wird.

Tabelle 39: Funktionsunterstützung und erweiterter Leitungsmodus

Funktion	Unterstützt	Firmwareversion
Anrufannahme	Ja	11.5(1) und höher
Anrufe automatisch annehmen	Ja	11.5(1) und höher
Aufschalten/KAufsch.	Ja	11.5(1) und höher
Gezieltes Parken von Anrufen mit Besetztlampenfeld	Ja	12.0(1) und höher
Bluetooth-Smartphone-Integration	Nein	-
Bluetooth-USB-Headsets	Ja	11.5(1) und höher
Rückruf	Ja	11.5(1) und höher
Anrufe beaufsichtigen	Nein	-
Rufumleitung Alle Anrufe	Ja	11.5(1) und höher
Anruf parken	Ja	12.0(1) und höher
Anruf parken – Leitungsstatus	Ja	12.0(1) und höher
Anrufübernahme	Ja	11.5(1) und höher
Anruf übernehmen – Leitungsstatus	Ja	11.5(1) und höher
Call Forward All (Rufumleitung Alle Anrufe) auf mehreren Leitungen	Ja	11.5(1) und höher
Cisco Extension Mobility Cross Cluster	Ja	12.0(1) und höher unterstützt diese Funktion.
Cisco IP Manager Assistant (IPMA)	Nein	-
Cisco Unified Communications Manager Express	Nein	-
Konferenz	Ja	11.5(1) und höher
CTI-Anwendungen (Computer Telephony Integration, Integration von Computertelefonie)	Ja	11.5(1) und höher
Ablehnen	Ja	11.5(1) und höher
Vom Gerät aufgerufene Aufzeichnung	Ja	11.5(1)SR1 und höher
Bitte nicht stören	Ja	11.5(1) und höher

<b>Funktion</b>	<b>Unterstützt</b>	<b>Firmwareversion</b>
Erweiterte SRST	Nein	-
Anschlussmobilität	Ja	11.5(1) und höher
Gruppenübernahme	Ja	12.0(1) und höher unterstützt diese Funktion.
Halten	Ja	11.5(1) und höher
Sammelanschlussgruppen	Ja.	12.0(1) und höher
Benachrichtigung für eingehende Anrufe mit konfigurierbarem Timer	Nein	-
Intercom	Ja	11.5(1) und höher
Tastenerweiterungsmodul	Cisco IP-Telefon 8851/8861 Erweiterungsmodul und Cisco IP-Telefon 8865 Erweiterungsmodul unterstützen den erweiterten Leitungsmodus	12.0(1) und höher
Identifizierung böswilliger Anrufer (Fangschaltung)	Ja	11.5(1) und höher
MeetMe	Ja	11.5(1) und höher
Mobile Verbindung	Ja	11.5(1) und höher
MLPP (Multilevel Precedence and Preemption)	Nein	-
Stummschaltung	Ja	11.5(1) und höher
Andere Übernahme	Ja	12.0(1) und höher
Unterstützung programmierbarer Leitungstasten für Warteschlangenstatus	Ja	11.5(1) und höher
Privatfunktion	Ja	11.5(1) und höher
Warteschlangenstatus	Ja	11.5(1) und höher
Tool für Qualitätsberichte (QRT)	Ja	11.5(1) und höher
Unterstützung für Gebietsschemata, bei denen von rechts nach links geschrieben wird	Nein	-
Wahlwiederholung	Ja	11.5(1) und höher
Stilles Mithören und Aufzeichnen	Ja	11.5(1)SR1 und höher



Funktion	Unterstützt	Firmwareversion
Kurzwahl	Ja	11.5(1) und höher
Survivable Remote Site Telephony (SRST)	Ja	11.5(1) und höher
Übergabe	Ja	11.5(1) und höher
URI-Wahl (Uniform Resource Identifier)	Ja	11.5(1) und höher
Videoanrufe	Ja	11.5(1) und höher
Visuelle Voicemail	Ja	11.5(1) und höher
Voicemail	Ja	11.5(1) und höher

#### Verwandte Themen

[Umgebung mit Sitzungsleitungsmodus](#), auf Seite 169

## TLS-Fortsetzungs-Timer einrichten

Durch die TLS-Fortsetzung kann eine TLS-Sitzung fortgesetzt werden, ohne den gesamten TLS-Authentifizierungsvorgang wiederholen zu müssen. Die Zeit, die eine TLS-Verbindung zum Austausch von Daten benötigt, kann somit entscheidend verringert werden.

Die Telefone unterstützen zwar TLS-Sitzungen, jedoch unterstützen nicht alle TLS-Sitzungen die TLS-Fortsetzung. Die folgende Liste führt die verschiedenen Sitzungen sowie deren Unterstützung der TLS-Fortsetzung auf:

- TLS-Sitzung für SIP-Signale: unterstützt die Fortsetzung
- HTTPS-Client: unterstützt die Fortsetzung
- CAPF: unterstützt die Fortsetzung
- TVS: unterstützt die Fortsetzung
- EAP-TLS: unterstützt die Fortsetzung nicht
- EAP-FAST: unterstützt die Fortsetzung nicht
- VPN-Client: unterstützt die Fortsetzung nicht

Weitere Informationen 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

Legen Sie den Parameter „TLS-Fortsetzungs-Timer“ fest.

Der zulässige Bereich für den Timer ist 0 bis 3600, der Standardwert ist 3600. Wenn das Feld auf 0 gesetzt wird, ist die Fortsetzung der TLS-Sitzung deaktiviert.

---

#### Verwandte Themen

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

## Intelligent Proximity aktivieren



---

**Hinweis** Diese Vorgehensweise gilt nur für Bluetooth-fähige Telefone. Die Cisco IP-Telefons 8811, 8841, 8851NR und 8865NR unterstützen kein Bluetooth.

---

Mit Intelligent Proximity können Benutzer die akustischen Eigenschaften des Telefons für ihr Mobilgerät oder Tablet nutzen. Der Benutzer koppelt das Mobilgerät oder Tablet über Bluetooth mit dem Telefon.

Mit einem gekoppelten Mobilgerät kann der Benutzer Mobiltelefon-Anrufe über das Telefon tätigen und annehmen. Bei einem Tablet kann der Benutzer den Audio-Anruf vom Tablet auf das Telefon umleiten.

Benutzer können mehrere Mobilgeräte, Tablets, und ein Bluetooth-Headset mit dem Telefon koppeln. Es können jedoch nur jeweils ein Gerät und ein Headset gleichzeitig angeschlossen sein.

#### Prozedur

---

- Schritt 1** Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **Telefon > Gerät**.
  - Schritt 2** Suchen Sie das Telefon, an dem eine Änderung vorgenommen werden soll.
  - Schritt 3** Suchen Sie nach dem Feld „Bluetooth“, und ändern Sie dessen Einstellung auf **Aktiviert**.
  - Schritt 4** Suchen Sie nach dem Feld „Bluetooth-Mobil-Freisprechmodus zulassen“, und ändern Sie dessen Einstellung auf **Aktiviert**.
  - Schritt 5** Speichern Sie die Änderungen, und übernehmen Sie sie für das Telefon.
- 

## Auflösung für Videoübertragung einrichten

Die Cisco IP-Telefons 8845, 8865 und 8865NR unterstützen die folgenden Videoformate:

- 720p (1280 x 720)
- WVGA (800 x 480)
- 360p (640 x 360)
- 240p (432 x 240)
- VGA (640 x 480)
- CIF (352 x 288)

- SIF (352 x 240)
- QCIF (176 x 144)

Cisco IP-Telefons mit Videofunktion handeln die optimale Auflösung für Bandbreite entsprechend der Telefonkonfiguration bzw. der Einschränkungen hinsichtlich der Auflösung aus. Beispiel: Bei einem Direktanruf von 88 x 5 nach 88 x 5 wird von den Telefonen nicht der tatsächliche Videotyp 720p, sondern 800 x 480 gesendet. Diese Einschränkung geht ausschließlich auf die 5-Zoll-WVGA-Bildschirmauflösung zurück, bei der 88 x 5 mit 800 x 480 gleichgesetzt wird.

Videotyp	Videoauflösung	fps (Frames per Second, Bilder pro Sekunde)	Video-Bitraten-Bereich
720 p	1280 x 720	30	1360–2500 Kb/s
720 p	1280 x 720	15	790–1359 Kb/s
WVGA	800 x 480	30	660–789 Kb/s
WVGA	800 x 480	15	350–399 Kb/s
360p	640 x 360	30	400–659 Kb/s
360p	640 x 360	15	210–349 Kb/s
240p	432 x 240	30	180–209 Kb/s
240p	432 x 240	15	64–179 Kb/s
VGA	640 x 480	30	520–1500 Kb/s
VGA	640 x 480	15	280–519 Kb/s
CIF	352 x 288	30	200–279 Kb/s
CIF	352 x 288	15	120–199 Kb/s
SIF	352 x 240	30	200–279 Kb/s
SIF	352 x 240	15	120–199 Kb/s
QCIF	176 x 144	30	94–119 Kb/s
QCIF	176 x 144	15	64–93 Kb/s

## Headset-Verwaltung für ältere Versionen von Cisco Unified Communications Manager

Wenn Sie eine Version von Cisco Unified Communications Manager älter als 12.5 (1) SU1 haben, können Sie die Cisco Headset-Einstellungen remote für die Verwendung mit On-Premises-Telefonen konfigurieren.

Die Remote-Headset-Konfiguration in der Cisco Unified Communication Manager-Version 10.5 (2), 11.0 (1), 11.5 (1), 12.0 (1) und 12.5 (1) erfordert, dass Sie eine Datei von der [Cisco Software-Download-Website](#)

herunterladen, die Datei bearbeiten und die Datei anschließend auf den TFTP-Server von Cisco Unified Communications Manager hochladen. Die Datei ist eine JSON-Datei (JavaScript Object Notification). Die aktualisierte Headset-Konfiguration wird für die Unternehmens-Headsets für einen Zeitraum von 10 bis 30 Minuten angewendet, um einen Rückstau auf dem TFTP-Server zu verhindern.




---

**Hinweis** Sie können Headsets über die Cisco Unified Communications Manager Administration Version 11.5 (1) SU7 verwalten und konfigurieren.

---

Beachten Sie Folgendes, wenn Sie mit der JSON-Datei arbeiten:

- Die Einstellungen werden nicht angewendet, wenn Sie eine Klammer oder Klammern im Code vergessen. Verwenden Sie ein Online-Tool wie JSON Formatter und prüfen Sie das Format.
- Legen Sie die Einstellung **updatedTime** auf die aktuelle Epochenzeit fest oder die Konfiguration wird nicht angewendet. Alternativ können Sie den Wert **updatedTime** um + 1 erhöhen, um ihn gegenüber der vorherigen Version zu erhöhen.
- Ändern Sie nicht den Parameternamen. Andernfalls wird die Einstellung nicht angewendet.

Weitere Informationen zum TFTP-Dienst finden Sie im Kapitel "Geräte-Firmware verwalten" im *Administratorhandbuch für Cisco Unified Communications Manager und IM und Präsenzdienst*.

Aktualisieren Sie Ihre Telefone auf die neueste Firmware-Version, bevor Sie die Datei `defaultheadsetconfig.json` anwenden. In der folgenden Tabelle werden die Standardeinstellungen beschrieben, die Sie mit der JSON-Datei anpassen können.

## Standard-Konfigurationsdatei für Headset herunterladen

Bevor Sie die Headset-Parameter remote konfigurieren, müssen Sie die neueste JSON-Beispieldatei (JavaScript Object Notation) herunterladen.

### Prozedur

---

- Schritt 1** Gehen Sie zur folgenden URL:<https://software.cisco.com/download/home/286320550>.
  - Schritt 2** Wählen Sie **Headsets 500-Serie**.
  - Schritt 3** Wählen Sie Ihre Headset-Serie aus.
  - Schritt 4** Wählen Sie einen Freigabeordner aus und wählen Sie die ZIP-Datei aus.
  - Schritt 5** Klicken Sie auf die Schaltfläche **Download** oder **Zum Warenkorb hinzufügen** und folgen Sie den Eingabeaufforderungen.
  - Schritt 6** Entpacken Sie die zip-Datei in einem Verzeichnis auf Ihrem PC.
- 

### Nächste Maßnahme

[Standard-Konfigurationsdatei für das Headset ändern, auf Seite 213](#)

## Standard-Konfigurationsdatei für das Headset ändern

Beachten Sie Folgendes, wenn Sie mit der Datei JavaScript Object Notation (JSON) arbeiten:

- Die Einstellungen werden nicht angewendet, wenn Sie eine Klammer oder Klammern im Code vergessen. Verwenden Sie ein Online-Tool wie JSON Formatter und prüfen Sie das Format.
- Legen Sie die Einstellung "**UpdatedTime**" auf die aktuelle Epochenzeit fest oder die Konfiguration wird nicht angewendet.
- Überprüfen Sie, ob **firmwareName**LATEST lautet. Andernfalls werden die Konfigurationen nicht angewendet.
- Ändern Sie keinen Parameternamen; andernfalls wird die Einstellung nicht angewendet.

### Prozedur

#### Schritt 1

Öffnen Sie die Datei `defaultheadsetconfig.json` mit einem Texteditor.

#### Schritt 2

Bearbeiten Sie den Wert **updatedTime** und die Parameterwerte, die sich ändern möchten.

Im Folgenden finden Sie ein Beispielskript. Dieses Skript dient nur zu Referenzzwecken. Verwenden Sie es als Leitfaden für die Konfiguration der Headset-Parameter. Verwenden Sie die JSON-Datei, die mit Ihrer Firmware geliefert wurde.

```
{
  "headsetConfig": {
    "templateConfiguration": {
      "configTemplateVersion": "1",
      "updatedTime": 1537299896,
      "reportId": 3,
      "modelSpecificSettings": [
        {
          "modelSeries": "530",
          "models": [
            "520",
            "521",
            "522",
            "530",
            "531",
            "532"
          ],
          "modelFirmware": [
            {
              "firmwareName": "LATEST",
              "latest": true,
              "firmwareParams": [
                {
                  "name": "Speaker Volume",
                  "access": "Both",
                  "usageId": 32,
                  "value": 7
                },
                {
                  "name": "Microphone Gain",
                  "access": "Both",
                  "usageId": 33,
                  "value": 2
                }
              ]
            }
          ]
        }
      ]
    }
  }
}
```

```

        "name": "Sidetone",
        "access": "Both",
        "usageId": 34,
        "value": 1
    },
    {
        "name": "Equalizer",
        "access": "Both",
        "usageId": 35,
        "value": 3
    }
]
}
},
{
    "modelSeries": "560",
    "models": [
        "560",
        "561",
        "562"
    ],
    "modelFirmware": [
        {
            "firmwareName": "LATEST",
            "latest": true,
            "firmwareParams": [
                {
                    "name": "Speaker Volume",
                    "access": "Both",
                    "usageId": 32,
                    "value": 7
                },
                {
                    "name": "Microphone Gain",
                    "access": "Both",
                    "usageId": 33,
                    "value": 2
                },
                {
                    "name": "Sidetone",
                    "access": "Both",
                    "usageId": 34,
                    "value": 1
                },
                {
                    "name": "Equalizer",
                    "access": "Both",
                    "usageId": 35,
                    "value": 3
                },
                {
                    "name": "Audio Bandwidth",
                    "access": "Admin",
                    "usageId": 36,
                    "value": 0
                },
                {
                    "name": "Bluetooth",
                    "access": "Admin",
                    "usageId": 39,
                    "value": 0
                }
            ]
        }
    ]
}
}

```

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

**Schritt 3** Speichern Sie die Datei `defaultheadsetconfig.json`.

---

#### Nächste Maßnahme

Installieren Sie die Standardkonfigurationsdatei.

## Installieren der Standardkonfigurationsdatei in Cisco Unified Communications Manager

Nachdem Sie die Datei `defaultheadsetconfig.json` bearbeitet haben, installieren Sie diese mit Hilfe des TFTP Dateimanagement-Tools im Cisco Unified Communications Manager.

#### Prozedur

- 
- Schritt 1** Wählen Sie in der Cisco Unified OS-Administration **Software Upgrades > TFTP Dateimanagement**
  - Schritt 2** Wählen Sie **Datei hochladen**.
  - Schritt 3** Wählen Sie **Datei auswählen** und gehen Sie zu der Datei `defaultheadsetconfig.json`.
  - Schritt 4** Wählen Sie **Datei hochladen**.
  - Schritt 5** Klicken Sie auf **Schließen**.
- 

## Cisco TFTP-Server neu starten

Nachdem Sie die Datei `defaultheadsetconfig.json` in das TFTP-Verzeichnis hochgeladen haben, starten Sie den Cisco TFTP-Server erneut und setzen Sie die Telefone zurück. Nach etwa 10 - 15 Minuten beginnt der Download und die neuen Konfigurationen werden auf die Headsets angewendet. Es dauert weitere 10 bis 30 Minuten, bis die Einstellungen angewendet werden.

## Prozedur

---

- Schritt 1** Melden Sie sich bei Cisco Unified Serviceability an und wählen **Tools > Control Center - Funktionsdienste**.
- Schritt 2** Wählen Sie in der Dropdown-Liste **Server** den Server aus, auf dem der Cisco TFTP-Dienst läuft.
- Schritt 3** Klicken Sie auf die Schaltfläche, die dem **Cisco TFTP**-Dienst entspricht.
- Schritt 4** Klicken Sie auf **Neu starten**.
-





## KAPITEL 10

# Unternehmensverzeichnis und persönliches Verzeichnis

---

- [Konfiguration des Firmenverzeichnisses, auf Seite 217](#)
- [Konfiguration des persönlichen Verzeichnisses, auf Seite 217](#)
- [Konfiguration der Benutzereinträge im persönlichen Verzeichnis, auf Seite 218](#)

## 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.

Cisco IP-Telefone verwenden eine dynamische Zuweisung für SecureApp auf Clients und Servern. Dadurch wird sichergestellt, dass Ihr Telefon Zertifikate lesen kann, die größer als 4KB sind. Zusätzlich wird die Häufigkeit von Fehlermeldungen `Host nicht gefunden` reduziert, wenn ein Benutzer auf das Verzeichnis zugreift.

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 xv

## Konfiguration des persönlichen Verzeichnisses

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

Das persönliche Verzeichnis umfasst folgende Features:

- Persönliches Adressbuch (PAB)
- Kurzwahl
- Adressbuch-Synchronisierungstool (TABSynch)

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.
- Von einer Microsoft Windows-Anwendung aus können Benutzer mithilfe des TABSynch-Tools ihre PABs mit dem Microsoft Windows-Adressbuch (WAB) synchronisieren. Kunden, die das Microsoft Outlook-Adressbuch (OAB) verwenden möchten, müssen die Daten zuerst aus dem OAB in das WAB importieren. Anschließend kann das WAB mithilfe von TabSynch mit dem persönlichen Verzeichnis synchronisiert werden. Weitere Informationen zu TABSynch finden Sie unter [Synchronizer für das Adressbuch des Cisco IP-Telefons herunterladen, auf Seite 219](#) und [Synchronizer konfigurieren, auf Seite 220](#).

Cisco IP-Telefone verwenden eine dynamische Zuweisung für SecureApp auf Clients und Servern. Dadurch wird sichergestellt, dass Ihr Telefon Zertifikate lesen kann, die größer als 4KB sind. Zusätzlich wird die Häufigkeit von Fehlermeldungen `Host nicht gefunden` reduziert, wenn ein Benutzer auf das Verzeichnis zugreift.

Um sicherzustellen, dass die Benutzer, die den Synchronizer für das Adressbuch auf Cisco IP-Telefon verwenden, nur auf ihre Benutzerdaten zugreifen können, aktivieren Sie den Cisco UXL-Webservice in der Cisco Unified Wartbarkeit.

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.

## Konfiguration der Benutzereinträge im persönlichen Verzeichnis

Die Benutzer können Einträge im persönlichen Verzeichnis auf Cisco IP-Telefon konfigurieren. Um ein persönliches Verzeichnis zu konfigurieren, muss der Benutzer auf Folgendes zugreifen können:

- Selbstservice-Portal: Stellen Sie sicher, dass die Benutzer wissen, wie sie auf das Selbstservice-Portal zugreifen können. Weitere Informationen hierzu finden Sie unter [Den Benutzerzugriff auf das Selbstservice-Portal konfigurieren, auf Seite 83](#).
- Synchronizer für das Adressbuch des Cisco IP-Telefon: Geben Sie den Benutzern das Installationsprogramm. Siehe [Synchronizer für das Adressbuch des Cisco IP-Telefons herunterladen, auf Seite 219](#).



---

**Hinweis** Die Synchronisierung für das Cisco IP-Telefonadressbuch wird nur auf nicht unterstützten Versionen von Windows (z. B. Windows XP und älter) unterstützt. Das Tool wird in neueren Versionen von Windows nicht unterstützt. In Zukunft wird es aus der Liste der Cisco Unified Communications Manager-Plug-ins entfernt.

---

## Synchronizer für das Adressbuch des Cisco IP-Telefons herunterladen

Um eine Kopie des Synchronizers herunterzuladen und an die Benutzer zu senden, führen Sie die folgenden Schritte aus:

### Prozedur

---

- Schritt 1** Wählen Sie **Anwendung** > **Plugins** in der Cisco Unified Communications Manager-Verwaltung aus.
  - Schritt 2** Wählen Sie **Download** neben dem Namen des Synchronizers für das Adressbuch des Cisco IP-Telefon aus.
  - Schritt 3** Wenn das Dialogfeld Datei-Download angezeigt wird, wählen Sie **Speichern** aus.
  - Schritt 4** Senden Sie die Datei TabSyncInstall.exe und die Anweisungen in [Bereitstellung des Synchronizers für das Adressbuch des Cisco IP-Telefons, auf Seite 219](#) an alle Benutzer, die diese Anwendung benötigen.
- 

## Bereitstellung des Synchronizers für das Adressbuch des Cisco IP-Telefons

Der Synchronizer für das Adressbuch des Cisco IP-Telefon synchronisiert die Daten, die in Ihrem Microsoft Windows-Adressbuch gespeichert sind, mit dem Cisco Unified Communications Manager-Verzeichnis und dem persönlichen Adressbuch im Selbstservice-Portal.



---

**Tipp** Um das Windows-Adressbuch mit dem persönlichen Adressbuch zu synchronisieren, müssen alle Benutzer im Windows-Adressbuch eingegeben werden, bevor Sie die folgenden Verfahren ausführen.

---

## Synchronizer installieren

Um den Synchronizer für das Adressbuch auf Cisco IP-Telefon zu installieren, führen Sie die folgenden Schritte aus:

### Prozedur

---

- Schritt 1** Die Installationsdatei für den Synchronizer für das Adressbuch auf Cisco IP-Telefon erhalten Sie vom Systemadministrator.
- Schritt 2** Doppelklicken Sie auf die Datei TabSyncInstall.exe, die Sie vom Administrator erhalten haben.
- Schritt 3** Wählen Sie **Ausführen** aus.

- Schritt 4** Wählen Sie **Weiter** aus.
  - Schritt 5** Lesen Sie die Lizenzvereinbarung und wählen Sie **Ich stimme zu** aus. Wählen Sie **Weiter** aus.
  - Schritt 6** Wählen Sie das Verzeichnis aus, in dem die Anwendung installiert werden soll, und klicken Sie auf **Weiter**.
  - Schritt 7** Wählen Sie **Installieren** aus.
  - Schritt 8** Wählen Sie **Fertig stellen** aus.
  - Schritt 9** Um den Prozess abzuschließen, führen Sie die Schritte in [Synchronizer konfigurieren, auf Seite 220](#) aus.
- 

## Synchronizer konfigurieren

Um den Synchronizer für das Adressbuch auf Cisco IP-Telefon zu konfigurieren, führen Sie die folgenden Schritte aus:

### Prozedur

---

- Schritt 1** Öffnen Sie den Synchronizer für das Adressbuch auf dem Cisco IP-Telefon.  
Wenn Sie das vorgegebene Installationsverzeichnis übernommen haben, können Sie die Anwendung öffnen, indem Sie **Start > Alle Programme > Cisco Systems > TabSync** auswählen.
  - Schritt 2** Um die Benutzerinformationen zu konfigurieren, wählen Sie **Benutzer** aus.
  - Schritt 3** Geben Sie den Benutzernamen und das Kennwort für Cisco IP-Telefon ein und wählen Sie **OK** aus.
  - Schritt 4** Um die Cisco Unified Communications Manager-Serverinformationen zu konfigurieren, wählen Sie **Server** aus.
  - Schritt 5** Geben Sie die IP-Adresse oder den Hostnamen und die Portnummer des Cisco Unified Communications Manager-Servers ein und wählen Sie **OK** aus.  
Wenn Ihnen diese Angaben unbekannt sind, wenden Sie sich an den Systemadministrator.
  - Schritt 6** Um die Verzeichnissynchronisierung zu starten, wählen Sie **Synchronisieren** aus.  
Im Fenster Synchronisierungsstatus wird der Status der Adressbuchsynchronisierung angezeigt. Wenn Sie die Regel für manuelles Bearbeiten von doppelten Einträgen auswählen und doppelte Adressbucheinträge vorhanden sind, wird das Fenster Doppelte Auswahl angezeigt.
  - Schritt 7** Wählen Sie den Eintrag aus, der in das persönliche Adressbuch eingefügt werden soll, und klicken Sie auf **OK**.
  - Schritt 8** Wenn der Synchronisierungsvorgang abgeschlossen ist, wählen Sie **Bearbeiten** aus, um das Cisco Unified CallManager-Adressbuch zu schließen.
  - Schritt 9** Um zu überprüfen, ob die Synchronisierung funktioniert hat, melden Sie sich am Selbstservice-Portal an und wählen Sie **Persönliches Adressbuch** aus. Die Benutzer in Ihrem Windows-Adressbuch werden aufgelistet.
-



## TEIL **IV**

# Problembehandlung für Cisco IP-Telefone

- [Telefonsysteme überwachen, auf Seite 223](#)
- [Fehlerbehebung, auf Seite 259](#)
- [Wartung, auf Seite 279](#)
- [Unterstützung von Benutzern in anderen Ländern, auf Seite 285](#)





# KAPITEL 11

## Telefonsysteme überwachen

---

- [Cisco IP-Telefon-Status](#), auf Seite 223
- [Webseite für Cisco IP-Telefon](#), auf Seite 239
- [Informationen im XML-Format vom Telefon anfordern](#), auf Seite 255

### Cisco IP-Telefon-Status

In diesem Abschnitt wird beschrieben, wie Sie Modellinformationen, Statusmeldungen und Netzwerkstatistiken auf Telefonen der Serie Cisco IP-Telefon 8800 anzeigen können.

- **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.

Weitere Informationen zur Fehlerbehebung finden Sie unter [Fehlerbehebung](#), auf Seite 259.

### Das Fenster Telefoninformationen anzeigen

Führen Sie die folgenden Schritte aus, um den Bildschirm „Modellinformationen“ anzuzeigen.

#### Prozedur

---

##### Schritt 1

Drücken Sie **Anwendungen** .

##### Schritt 2

Wählen Sie **Telefoninfo**.

Wenn der Benutzer mit einem sicheren oder authentifizierten Server verbunden ist, wird ein entsprechendes Symbol (Schloss oder Zertifikat) auf dem Bildschirm Telefoninformationen rechts neben der Serveroption angezeigt. Wenn der Benutzer nicht mit einem sicheren oder authentifizierten Server verbunden ist, wird kein Symbol angezeigt.

**Schritt 3** Um den Bildschirm „Modellinformationen“ zu verlassen, drücken Sie **Beenden**.

## Felder für Telefoninformationen

In der folgenden Tabelle werden die Einstellungen für Telefoninformationen beschrieben.

**Tabelle 40: Einstellungen für Telefoninformationen**

Option	Beschreibung
Modellnummer	Die Modellnummer des Telefons.
IPv4-Adresse	IP-Adresse des Telefons.
Host-Name	Host-Name des Telefons.
Aktive Software	Version der derzeit auf dem Telefon installierten Firmware. Der Benutzer kann <b>Details</b> drücken, um weitere Informationen zu erhalten.
Inaktive Software	<p>„Inaktive Software“ wird nur angezeigt, wenn ein Download ausgeführt wird. Außerdem werden ein Download-Symbol und der Status „Upgrade läuft“ oder „Upgrade fehlgeschlagen“ angezeigt. Wenn ein Benutzer während eines laufenden Upgrades <b>Details</b> drückt, werden der Dateiname und die Komponenten des Downloads aufgeführt.</p> <p>Der Download eines neuen Firmware-Image kann vor einem Wartungszeitfenster festgelegt werden. Somit muss nicht gewartet werden, bis alle Telefone die Firmware heruntergeladen haben. Stattdessen wechselt das System schneller vom Zurücksetzen einer vorhandenen Software in den Inaktiv-Status und zum Installieren der neuen Software.</p> <p>Nach Abschluss des Downloads wechselt das Symbol und zeigt nun den Fertigstellungsstatus an; ein Häkchen wird für einen erfolgreichen Download angezeigt, ein „X“ gibt an, dass der Download fehlgeschlagen ist. Sofern möglich, wird versucht, den Rest der Firmware weiter herunterzuladen.</p>
Letzte Aktualisierung	Datum des letzten Firmware-Upgrades.
Aktiver Server	Domänenname des Servers, bei dem das Telefon registriert ist.
Standby-Server	Domänenname des Standby-Servers.

## Das Statusmenü anzeigen

Das Menü „Status“ enthält folgende Optionen, die Informationen zum Telefon und dessen Aktivitäten geben:


- Statusmeldungen: Zeigt den Bildschirm für Statusmeldungen an, der ein Protokoll mit wichtigen Systemmeldungen enthält.



- Ethernet-Statistik: Zeigt den Bildschirm für Ethernet-Statistik an, auf dem statistische Daten zum Ethernet-Datenverkehr aufgeführt sind.
- Wireless-Statistik: Zeigt (sofern zutreffend) den Bildschirm für die Wireless-Statistik an.
- Anrufstatistik: Zeigt Zählerstände und Statistiken für den derzeitigen Anruf an.
- Aktueller Zugangspunkt: Zeigt (sofern zutreffend) den Bildschirm für den aktuellen Access Point an.

Zum Anzeigen des Menüs „Status“ müssen Sie folgende Schritte ausführen:


**Prozedur**

- Schritt 1** Um das Statusmenü anzuzeigen, drücken Sie auf **Anwendungen** .
- Schritt 2** Wählen Sie **Verwaltungseinstellungen > Status**.
- Schritt 3** Drücken Sie zum Verlassen des Menüs „Status“ auf **Beenden**.

**Statusmeldungen anzeigen**

Im Fenster „Statusmeldungen“ werden die 30 letzten vom Telefon generierten Statusmeldungen angezeigt. Sie können diesen Bildschirm jederzeit aufrufen, selbst wenn der Startvorgang des Telefons noch nicht abgeschlossen wurde.

**Prozedur**

- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Verwaltungseinstellungen > Status > Statusmeldungen**.
- Schritt 3** Drücken Sie zum Entfernen der aktuellen Statusmeldungen **Leeren**.
- Schritt 4** Drücken Sie zum Schließen des Bildschirms „Statusmeldungen“ **Beenden**.

**Statusmeldungen**

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

*Tabelle 41: Statusmeldungen des Cisco Unified IP-Telefons*

Nachricht	Beschreibung	Mögliche Erklärung und durch
CFG TFTP-Größenfehler	Die Konfigurationsdatei ist zu groß für das Dateisystem auf dem Telefon.	Schalten Sie das Telefon aus u
Prüfsummenfehler	Die heruntergeladene Softwaredatei ist beschädigt.	Beziehen Sie eine neue Kopie speichern Sie diese im TFTP Dateien nur in dieses Verzeich TFTP-Serversoftware deaktiv ansonsten beschädigt werden k

Nachricht	Beschreibung	Mögliche Erklärung und durchzuführen
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 eine IP-Adresse für das Telefon verfügbar hat.
CTL und ITL installiert	Auf dem Telefon sind sowohl die CTL- als auch die ITL-Datei installiert.	Keine. Diese Meldung ist nur für ITL-Dateien bestimmt. Zuvor war weder die CTL- noch die ITL-Datei installiert.
CTL installiert	Auf dem Telefon ist eine CTL-Datei installiert.	Keine. Diese Meldung ist nur für ITL-Dateien bestimmt. Zuvor war keine CTL-Datei installiert.
CTL-Aktualisierungsfehler	Das Telefon konnte die CTL-Datei nicht aktualisieren.	Auf dem TFTP-Server ist ein Problem mit der CTL-Datei aufgetreten.
DHCP-Zeitüberschreitung	Der DHCP-Server antwortet nicht.	Netzwerk ist ausgelastet: Die Fehler beheben, wenn die Netzwerklast reduziert wird. Keine Netzwerkverbindung zwischen Telefon: Überprüfen Sie die Netzwerkeinstellungen. DHCP-Server ist ausgefallen: Prüfen Sie den Status des DHCP-Servers. Fehler weiterhin vorhanden: Ziehen Sie die Verwendung einer statischen IP-Adresse in Erwägung.
DNS-Zeitüberschreitung	Der DNS-Server antwortet nicht.	Netzwerk ist ausgelastet: Die Fehler beheben, wenn die Netzwerklast reduziert wird. Keine Netzwerkverbindung zwischen Telefon: Überprüfen Sie die Netzwerkeinstellungen. DNS-Server ist ausgefallen: Prüfen Sie den Status des DNS-Servers.
Unbekannter DNS-Host	DNS konnte den Namen des TFTP-Servers bzw. des Cisco Unified Communications Managers nicht auflösen.	Kontrollieren Sie, ob die Host-Namen des TFTP-Servers bzw. des Cisco Unified Communications Managers ordnungsgemäß definiert sind. Ziehen Sie die Verwendung von IP-Adressen für die Host-Namen in Erwägung.
Doppelte IP	Ein anderes Gerät verwendet die IP-Adresse, die dem Telefon zugewiesen ist.	Wenn das Telefon eine statische IP-Adresse verwendet, stellen Sie sicher, dass keine doppelte IP-Adresse verwendet wird. Wenn Sie DHCP verwenden, überprüfen Sie die DHCP-Serverkonfiguration.
CTL- und ITL-Dateien löschen	Löschen Sie die CTL- oder ITL-Datei.	Keine. Diese Meldung ist nur für ITL-Dateien bestimmt.

Nachricht	Beschreibung	Mögliche Erklärung und durch
Fehler beim Aktualisieren des Gebietschemas	Im Verzeichnis „TFTPPath“ konnten eine oder mehrere Lokalisierungsdateien nicht gefunden werden bzw. waren nicht gültig. Das Gebietschema wurde geändert.	Überprüfen Sie von der Admin Unified-Betriebssystems aus, ob der TFTP-Dateiverwaltung folgende sind: <ul style="list-style-type: none"> <li>• Im Unterverzeichnis, das Netzwerkgebietschema hat <ul style="list-style-type: none"> <li>• tones.xml</li> </ul> </li> <li>• Mit dem gleichen Namen Benutzergebietschema im gespeichert: <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 das Telefon zur Cisco Unified Manager-Datenbank hinzugefügt nicht in der Cisco Unified Com Manager-Datenbank vorhanden. TFTP-Server eine <b>CFG-Datei gefunden</b> -Antwort. <ul style="list-style-type: none"> <li>• Das Telefon ist nicht mit Communications Manager. Sie müssen das Telefon mit Communications Manager automatische Registrierung zulassen. Weitere Informationen <a href="#">Methoden zum Hinzufügen 73</a>.</li> <li>• Wenn Sie DHCP verwenden der DHCP-Server auf dem verweist.</li> <li>• Wenn Sie statische IP-Adresse Sie die Konfiguration des</li> </ul>
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 Communications Manager registriert
IP-Adresse freigegeben	Das Telefon ist konfiguriert, um die IP-Adresse freizugeben.	Das Telefon bleibt inaktiv, bis wird oder die DHCP-Adresse z

Nachricht	Beschreibung	Mögliche Erklärung und durchzuführen
ITL installiert	Die ITL-Datei ist auf dem Telefon installiert.	Keine. Diese Meldung ist nur für IP-Telefone bestimmt. Zuvor war keine ITL-Datei installiert.
Abgelehnte HW-Komp. laden	Die heruntergeladene Anwendung ist nicht mit der Telefonhardware kompatibel.	Dieses Problem tritt auf, wenn Sie eine Anwendung der Software, die Hardwareänderungen enthält, auf dem Telefon zu installieren.  Überprüfen Sie die Last-ID, die dem Telefon zugewiesen ist (wählen Sie <b>Gerät</b> > <b>Telefon</b> im Cisco Unified Communications Manager aus). Gehen Sie zurück zum Telefon, das die Last-ID zeigt, und wählen Sie das Telefon erneut ein.
Kein Standardrouter	DHCP oder die statische Konfiguration geben keinen Standardrouter an.	Wenn das Telefon eine statische IP-Adresse hat, überprüfen Sie, ob der Standardrouter konfiguriert ist.  Wenn Sie DHCP verwenden, hat der Standardrouter bereitgestellt. Überprüfen Sie die DHCP-Serverkonfiguration.
Keine DNS-Server-IP-Adresse	Es wurde zwar ein Name angegeben, jedoch wurde in DHCP bzw. der statischen IP-Konfiguration keine DNS-Serveradresse festgelegt.	Wenn das Telefon über eine statische IP-Adresse verfügt, überprüfen Sie, ob der DNS-Server konfiguriert ist.  Wenn Sie DHCP verwenden, hat der Standardrouter den 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. Überprüfen Sie die Vertrauensliste, die auf dem Telefon installiert wird nicht standardmäßig unterstützt.
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.	Wahrscheinlich wurden im Cisco Unified Communications Manager Änderungen an der Telefonkonfiguration vorgenommen, und es wurde „Überprüfen“ ausgewählt, sodass die Änderungen übernommen werden.
Fehler bei TFTP-Zugang	Der TFTP-Server verweist auf ein Verzeichnis, das nicht vorhanden ist.	Wenn Sie DHCP verwenden, stellen Sie sicher, dass der DHCP-Server auf den richtigen TFTP-Server zeigt.  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.

Nachricht	Beschreibung	Mögliche Erklärung und durch
TFTP-Zeitüberschreitung	Der TFTP-Server reagiert nicht.	Hohe Netzwerkauslastung: Das allein lösen, sobald sich die Ne verringert. Keine Netzwerkverbindung zw und dem Telefon: Überprüfen S TFTP-Server ist ausgefallen: Ü Konfiguration des TFTP-Server
Zeitüberschreitung	Supplicant versuchte eine 802.1X-Transaktion, aber die Zeit wurde überschritten, da kein Authentifikator vorhanden ist.	Bei der Authentifizierung tritt Zeitüberschreitung auf, wenn 8 konfiguriert ist.
Aktualisierung der Vertrauensliste fehlgeschlagen	Die Aktualisierung der CTL- und ITL-Datei ist fehlgeschlagen.	Auf dem Telefon sind CTL- und die neuen CTL- und ITL-Datei werden. Mögliche Fehlerursachen: <ul style="list-style-type: none"> <li>• Ein Netzwerkfehler ist au</li> <li>• Der TFTP-Server ist ausg</li> <li>• Der neue Sicherheitstoker CTL-Datei verwendet wur dass zum Signieren der IT sind in den aktuellen CTL Telefon noch nicht verfüg</li> <li>• Ein interner Telefonfehler</li> </ul> Mögliche Lösungen: <ul style="list-style-type: none"> <li>• Überprüfen Sie die Netz</li> <li>• Überprüfen Sie, ob der TH normal funktioniert.</li> <li>• Wenn der TVS-Server (Tr von Cisco Unified Comm unterstützt wird, überprüf aktiv ist und normal funkt</li> <li>• Überprüfen Sie, ob der Si TFTP-Server gültig sind.</li> </ul> Löschen Sie die CTL- und ITL Lösungen fehlschlagen. Setzen
Vertrauensliste aktualisiert	Die CTL-Datei, die ITL-Datei oder beide Dateien werden aktualisiert.	Keine. Diese Meldung ist nur f bestimmt.
Versionsfehler	Der Name der Telefonlastdatei ist ungültig.	Stellen Sie sicher, dass die Tele Namen hat.
XmlDefault.cnf.xml oder .cnf.xml übereinstimmend mit dem Gerätenamen des Telefons.	Name der Konfigurationsdatei.	Keine. Die Meldung zeigt den Konfigurationsdatei für das Te

**Verwandte Themen**


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

**Anzeigen des Netzwerk-Info-Bildschirms**

Verwenden Sie die Informationen auf dem Netzwerk-Info-Bildschirm, um Verbindungsprobleme auf einem Telefon zu beheben.

Eine Meldung wird auf dem Telefon angezeigt, wenn ein Benutzer Probleme bei der Verbindung mit einem Telefonnetzwerk hat.


**Prozedur**

- Schritt 1** Um das Statusmenü anzuzeigen, drücken Sie auf **Anwendungen** .
- Schritt 2** Wählen Sie **Verwaltereinstellungen > Status > Statusmeldungen**.
- Schritt 3** Wählen Sie **Netzwerkinfo.** aus.
- Schritt 4** Um die Netzwerk-Info zu schließen, drücken Sie auf **Beenden**.

**Bildschirm „Netzwerkstatistik“ anzeigen**

Auf dem Bildschirm „Netzwerkstatistik“ werden Informationen zur Telefon- und Netzwerkleistung angezeigt. Führen Sie die folgenden Schritte aus, um den Bildschirm „Netzwerkstatistik“ anzuzeigen:

**Prozedur**

- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Verwaltereinstellungen > Status > Netzwerkstatistik**.
- Schritt 3** Drücken Sie **Leeren**, um die Statistiken zu Rx-Frames, Tx-Frames und Rx-Broadcasts auf 0 zurückzusetzen.
- Schritt 4** Drücken Sie zum Schließen des Bildschirms „Netzwerkstatistik“ **Beenden**.

**Informationen der Ethernet-Statistik**

In der folgenden Tabelle werden die Informationen im Bildschirm „Ethernet-Statistik“ beschrieben.

*Tabelle 42: Informationen der Ethernet-Statistik*

Element	Beschreibung
Rx Frames	Anzahl der Pakete, die vom Telefon empfangen wurden.
Übertr. – Frames	Anzahl der Pakete, die vom Telefon gesendet wurden.
Rx Broadcasts	Anzahl der Broadcast-Pakete, die vom Telefon empfangen wurden.

Element	Beschreibung
Ursache für Neustart	Ursache für das letzte Zurücksetzen des Telefons. Einer der folgenden Werte wird angegeben: <ul style="list-style-type: none"> <li>• Initialisiert</li> <li>• TCP-Zeitüberschreitung</li> <li>• TCP-Verb. durch CM geschlossen</li> <li>• TCP-Bad-ACK</li> <li>• CM-reset-TCP</li> <li>• CM-aborted-TCP</li> <li>• CM-NAKed</li> <li>• KeepaliveTO</li> <li>• Failback</li> <li>• Telefontastenfeld</li> <li>• Telefon-IP-Neuzuweisung</li> <li>• Zurücksetzen-Zurücksetzen</li> <li>• Zurücksetzen-Neustart</li> <li>• Telefonregister-Zurückweisung</li> <li>• Last zurückgewiesen – HC</li> <li>• CM-ICMP-Ziel nicht erreichbar</li> <li>• Telefonabbruch</li> </ul>
Abgelaufene Zeit	Zeit, die seit dem letzten Neustart des Telefons verstrichen ist.
Port 1	Verbindungszustand und Verbindung des Netzwerk-Ports. <b>Auto 100 Mbit/s Vollduplex</b> bedeutet beispielsweise, dass sich der Netzwerk-Port in einem verbundenen Zustand befindet und automatisch eine Vollduplex-100-Mbit/s-Verbindung ausgehandelt hat.
Port 2	Verbindungszustand und Verbindung des PC-Ports.
DHCP-Status (IPv4 / IPv6)	<ul style="list-style-type: none"> <li>• Im reinen IPv4-Modus wird nur der DHCPv4-Status angezeigt, z. B. DHCP BOUND.</li> <li>• Im IPv6-Modus wird nur der DHCPv6-Status angezeigt, z. B. ROUTER ADVERTISE.</li> <li>• DHCPv6-Status-Informationen werden angezeigt.</li> </ul>

In den folgenden Tabellen werden die Meldungen beschrieben, die für DHCPv4- und DHCPv6-Status angezeigt werden.

**Tabelle 43: Meldungen der DHCPv4-Ethernet-Statistik**

DHCPv4-Status	Beschreibung
CDP INIT	CDP ist nicht gebunden, oder WLAN ist außer Betrieb
DHCP BOUND	DHCPv4 ist gebunden
DHCP DISABLED	DHCPv4 ist deaktiviert

DHCPv4-Status	Beschreibung
DHCP INIT	DHCPv4 ist initialisiert
DHCP INVALID	DHCPv4 ist ungültig; dies ist der Anfangsstatus
DHCP RENEWING	DHCPv4 wird erneuert
DHCP REBINDING	DHCPv4 wird neu gebunden
DHCP REBOOT	DHCPv4 wird initialisiert/neu gestartet
DHCP REQUESTING	Anforderung durch DHCPv4
DHCP RESYNC	DHCPv4-Neusynchronisierung
DHCP WAITING COLDBOOT TIMEOUT	DHCPv4 wird gestartet
DHCP UNRECOGNIZED	Nicht erkannter DHCPv4-Status
DISABLED DUPLICATE IP	Doppelte IPv4-Adresse
DHCP TIMEOUT	DHCPv4-Zeitüberschreitung
IPV4 STACK TURNED OFF	Telefon befindet sich im reinen IPv6-Modus, und der IPv4-Stapel ist deaktiviert
ILLEGAL IPV4 STATE	Unzulässiger IPv4-Status, darf nicht auftreten

Tabelle 44: Meldungen der DHCPv6-Ethernet-Statistik

DHCPv6-Status	Beschreibung
CDP INIT	CDP wird initialisiert
DHCP6 BOUND	DHCPv6 ist gebunden
DHCP6 DISABLED	DHCPv6 ist deaktiviert
DHCP6 RENEW	DHCPv6 wird erneuert
DHCP6 REBIND	DHCPv6 wird neu gebunden
DHCP6 INIT	DHCPv6 wird initialisiert
DHCP6 SOLICIT	DHCPv6 sendet Anfrage
DHCP6 REQUEST	Anforderung durch DHCPv6
DHCP6 RELEASING	DHCPv6 wird freigegeben
DHCP6 RELEASED	DHCPv6 ist freigegeben
DHCP6 DISABLING	DHCPv6 wird deaktiviert
DHCP6 DECLINING	DHCPv6 wird abgelehnt




DHCPv6-Status	Beschreibung
DHCP6 DECLINED	DHCPv6 wurde abgelehnt
DHCP6 INFOREQ	DHCPv6 führt INFOREQ aus
DHCP6 INFOREQ DONE	DHCPv6 hat INFOREQ abgeschlossen
DHCP6 INVALID	DHCPv6 ist ungültig; dies ist der Anfangsstatus
DISABLED DUPLICATE IPV6	DHCP6 ist deaktiviert – doppelte IPv6 erkannt
DHCP6 DECLINED DUPLICATE IP	DHCP6 wurde abgelehnt – doppelte IPv6 erkannt
ROUTER ADVERTISE., (DUPLICATE IP)	Doppelte automatisch konfigurierte IPv6-Adresse
DHCP6 WAITING COLDBOOT TIMEOUT	DHCPv6 wird gestartet
DHCP6 TIMEOUT USING RESTORED VAL	DHCPv6-Zeitüberschreitung, im Flash-Speicher gespeicherter Wert wird verwendet
DHCP6 TIMEOUT CANNOT RESTORE	DHCPv6-Zeitüberschreitung, und es ist keine Sicherung im Flash-Speicher vorhanden
IPV6 STACK TURNED OFF	Telefon befindet sich im reinen IPv4-Modus, und der IPv6-Stapel ist deaktiviert
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY	IPv6-Adresse stammt nicht vom Router oder DHCPv6-Server
ILLEGAL IPV6 STATE	Unzulässiger IPv6-Status, darf nicht auftreten

## Bildschirm „Wireless-Statistik“ anzeigen

Diese Vorgehensweise gilt nur für das Cisco schnurlos IP-Telefon 8861.

Führen Sie die folgenden Schritte aus, um den Bildschirm „Wireless-Statistik“ anzuzeigen:

### Prozedur

- 
- Schritt 1** Drücken Sie **Anwendungen** .
  - Schritt 2** Wählen Sie **Verwaltungseinstellungen > Status > Wireless-Statistik**.
  - Schritt 3** Drücken Sie **Leeren**, um die Wireless-Statistik auf 0 zurückzusetzen.
  - Schritt 4** Drücken Sie zum Schließen des Bildschirms „Wireless-Statistik“ **Beenden**.
-

## WLAN-Statistik

In der folgenden Tabelle wird die WLAN-Statistik auf dem Telefon beschrieben.

**Tabelle 45: WLAN-Statistik auf dem Cisco Unified IP-Telefon**

Element	Beschreibung
Gesendete Bytes	Anzahl der Bytes, die vom Telefon übertragen wurden.
Empfangene Bytes	Anzahl der Bytes, die vom Telefon empfangen wurden.
Gesendete Pakete	Anzahl der Pakete, die vom Telefon übertragen wurden.
Empfangene Pakete	Anzahl der Pakete, die vom Telefon empfangen wurden.
Verlorene ausgehende Pakete	Die Anzahl der Pakete, die während der Übertragung verloren gegangen sind.
Verlorene eingehende Pakete	Die Anzahl der Pakete, die während des Empfangs verloren gegangen sind.
Fehler bei gesendeten Paketen	Die Anzahl fehlerhafter Pakete, die vom Telefon gesendet wurden.
Fehler bei empfangenen Paketen	Die Anzahl fehlerhafter Pakete, die vom Telefon empfangen wurden.
Übertr. – Frames	Die Anzahl erfolgreich übertragener MSDU.
Gesendet – Multicast-Frames	Die Anzahl erfolgreich übertragener Multicast-MSDU.
Gesendet – Neuversuch	Die Anzahl von MSDU, die nach einem oder mehreren Neuversuchen erfolgreich übertragen wurden.
Gesendet – mehrere Neuversuche	Die Anzahl von Multicast-MSDU, die nach einem oder mehreren Neuversuchen erfolgreich übertragen wurden.
Senden fehlgeschlagen	Die Anzahl der MSDU, die nicht erfolgreich übertragen wurden, weil die Anzahl der Sendeveruche das Limit für Neuversuche überschritten hat.
Erfolgreiche Sendeanforderung	Dieser Zähler vergrößert sich, wenn als Antwort auf eine RTS eine CTS empfangen wird.
Fehlgeschlagene Sendeanforderung	Dieser Zähler vergrößert sich, wenn als Antwort auf eine RTS keine CTS empfangen wird.
Fehler bei Bestätigung	Dieser Zähler vergrößert sich, wenn eine erwartete ACK nicht empfangen wird.
Empfangene doppelte Frames	Die Anzahl der empfangenen Frames, die laut dem Feld „Abfolgekontrolle“ Duplikate sind.
Empfangene fragmentierte Pakete	Die Anzahl der erfolgreich empfangenen MPDU vom Typ „Daten“ oder „Management“.
Roaming-Anzahl	Die Anzahl erfolgreicher Roaming-Vorgänge.

## Die Anrufstatistik anzeigen


Sie können auf den Bildschirm Anrufstatistik auf dem Telefon zugreifen, um Zähler, Statistiken und die Sprachqualitätsmetrik des letzten Anrufs anzuzeigen.



**Hinweis** Sie können die Anrufstatistik auch in einem Webbrowser anzeigen, um auf die Webseite Streaming-Statistik zuzugreifen. Diese Webseite enthält zusätzliche RTCP-Statistiken, die auf dem Telefon nicht verfügbar sind.

Ein Anruf kann mehrere Voicestreams verwenden, aber nur für den letzten Voicestream werden Daten aufgezeichnet. Ein Voicestream ist ein Paketstream zwischen zwei Endpunkten. Wenn ein Endpunkt gehalten wird, wird der Voicestream angehalten, auch wenn der Anruf noch verbunden ist. Wenn der Anruf fortgesetzt wird, beginnt ein neuer Voicepaketstream und die neuen Anrufrufen überschreiben die vorherigen Anrufrufen.

### Prozedur

- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Verwaltereinstellungen > Status > Anrufstatistik**.
- Schritt 3** Drücken Sie zum Verlassen des Bildschirms „Anrufstatistik“ auf **Beenden**.

### Anrufstatistikfelder

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

**Tabelle 46: Elemente der Anrufstatistik für das Cisco Unified-Telefon**

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>• G722.2 AMR-WB</li> <li>• G.711 mu-law</li> <li>• G.711 A-law</li> <li>• iLBC</li> <li>• Opus</li> <li>• iSAC</li> </ul>

Element	Beschreibung
Sender – Codec	<p>Typ des übertragenen Sprachstreams (RTP-Audiostreaming vom Codec):</p> <ul style="list-style-type: none"> <li>• G.729</li> <li>• G.722</li> <li>• G722.2 AMR-WB</li> <li>• G.711 mu-law</li> <li>• G.711 A-law</li> <li>• iLBC.</li> <li>• Opus</li> <li>• iSAC</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.
Empfänger – Pakete	<p>Anzahl der RTP-Sprachpakete, die empfangen wurden, seit der Voicestream geöffnet wurde.</p> <p><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.</p>
Sender – Pakete	<p>Anzahl der RTP-Sprachpakete, die gesendet wurden, seit der Voicestream geöffnet wurde.</p> <p><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.</p>
Durchschn. 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, in Millisekunden, der bemerkt wurde, seit der empfangene Voicestream geöffnet wurde.
Empfänger – Verworfen	<p>Anzahl der RTP-Pakete im eingehenden Voicestream, die verworfen wurden (ungültige Pakete, zu spät usw.).</p> <p><b>Hinweis</b> Das Telefon verwirft Comfort Noise-Pakete des Nutzlasttyps 19, die von den Cisco Gateways generiert werden, da diese den Zähler erhöhen.</p>

Element	Beschreibung
Empfänger – Verlorene Pakete	Fehlende RTP-Pakete (während Übertagung verloren).
<b>Sprachqualitätsmetrik</b>	
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.
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).
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.

## Fenster „Aktueller Zugangspunkt“ anzeigen

Im Fenster „Aktueller Zugangspunkt“ werden Statistiken zum Access Point angezeigt, der vom Cisco IP-Telefon 8861 für die kabellose Kommunikation verwendet wird.

### Prozedur

- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Verwaltereinstellungen > Status > Aktueller Zugangspunkt**.
- Schritt 3** Drücken Sie zum Schließen des Bildschirms „Aktueller Zugangspunkt“ **Beenden**.

### Felder für „Aktueller Zugangspunkt“

In der folgenden Tabelle werden die Felder im Dialogfeld „Aktueller Zugangspunkt“ beschrieben.

*Tabelle 47: Elemente in „Aktueller Zugangspunkt“*

Element	Beschreibung
AP-Name	Name des Access Points, wenn dieser CCX-kompatibel ist; andernfalls wird hier die MAC-Adresse angezeigt.
MAC-Adresse	MAC-Adresse des Access Points.

Element	Beschreibung
Frequenz	Die letzte Frequenz, auf der dieser Access Point beobachtet wurde.
Aktueller Kanal	Der letzte Kanal, bei dem dieser Access Point beobachtet wurde.
Letzter RSSI	Der letzte RSSI, in dem dieser Access Point beobachtet wurde.
Beacon-Intervall	Anzahl der Zeiteinheiten zwischen Beacons. Eine Zeiteinheit umfasst 1,024 ms.
Funktion	Dieses Feld enthält eine Reihe von untergeordneten Feldern, in denen angeforderte bzw. angebotene optionale Funktionen angegeben werden.
Basisraten	Vom Access Point geforderte Datenraten sowie der Access Point, bei dem die Station betriebsfähig sein muss.
Optionale Raten	Vom Access Point unterstützte Datenraten und die Access Points, mit denen der Betrieb der Station möglich ist.
Unterstützte VHT-Raten (Empf.)	Vom Access Point empfangenes VHT (Empf.)-MCS-Set.
Unterstützte VHT-Raten (Übertr.)	Vom Access Point empfangenes VHT (Übertr.)-MCS-Set.
Unterstützte HT MCS	Vom Access Point empfangenes HT-MCS-Set.
DTIM-Zeitraum	Jedes n-te Beacon ist ein DTIM-Zeitraum. Nach jedem DTIM-Beacon sendet der Access Point Broadcast- oder Multicast-Pakete, die für Geräte im Energiesparmodus in die Warteschlange gestellt sind.
Ländercode	Ein zweistelliger Ländercode. Wenn das Länder-Informationselement im Beacon nicht vorhanden ist, werden möglicherweise keine Länderinformationen angezeigt.
Kanäle	Eine Liste der unterstützten Kanäle (aus der Länder-Informationseinheit).
Leistungsbeschränkung	Die Energiemenge, um die die maximale Stromzufuhr zum Übertragen vom Geltungsbereich-Limit aus reduziert werden sollte.
Leistungsgrenze	Maximale Übertragungsleistung in dBm, die für den betreffenden Kanal zulässig ist.
Kanalnutzung	Der prozentuale Anteil an Zeit, normalisiert auf 255, in der der Access Point erkannt hat, dass das Medium besetzt war, entsprechend dem physischen oder virtuellen CS-Mechanismus (CS: Carrier Sense, Trägerprüfung).
Anzahl Stationen	Die Gesamtanzahl der Stationen, die diesem Access Point derzeit zugeordnet sind.
Zugangskapazität	Eine Ganzzahl ohne Vorzeichen, die die verbleibende Medienzeit angibt, die durch explizite Zugangssteuerung verfügbar ist, in Einheiten von 32 Mikrosekunden pro Sekunde.  Beim Wert 0 wird dieses Informationselement vom Access Point nicht unterstützt, und die Kapazität ist unbekannt.

Element	Beschreibung
WMM unterstützt	Unterstützung für WLAN-Multimedia-Erweiterungen.
Unterstützung für UAPSD	Der Access Point unterstützt Unscheduled Automatic Power Save Delivery (U-APSD). Möglicherweise nur verfügbar, wenn WMM unterstützt wird. Diese Funktion ist grundlegend wichtig für die Gesprächszeit und zum Erreichen einer maximalen Anrufrichte auf dem Wireless IP-Telefon.
Proxy-ARP	CCX-kompatibler Access Point unterstützt das Beantworten von IP ARP-Anforderungen im Auftrag der zugeordneten Station. Diese Funktion ist grundlegend wichtig für die Standby-Zeit auf dem Wireless IP-Telefon.
CCX-Version	Wenn der Access Point CCX-kompatibel ist, wird in diesem Feld die CCX-Version angezeigt.
Best Effort	Enthält Informationen zur Best Effort-Warteschlange.
Hintergrund	Enthält Informationen zur Hintergrund-Warteschlange.
Video	Enthält Informationen zur Video-Warteschlange.
Voice	Enthält Informationen zur Gesprächs-Warteschlange.

## Webseite für Cisco IP-Telefon

Jedes Cisco IP-Telefon hat eine Webseite, auf der verschiedene Informationen über das Telefon angezeigt werden, einschließlich:

- Geräteinformationen: Zeigt Geräteeinstellungen und zugehörige Informationen für das Telefon an.
- Netzwerk-Setup: Zeigt Informationen zum Netzwerk-Setup und zu weiteren Telefoneinstellungen an.
- Netzwerkstatistik: Zeigt Hyperlinks an, über die Informationen zum Netzwerkverkehr abrufbar sind.
- Geräteprotokolle: Zeigt Hyperlinks an, über die Informationen zur Unterstützung bei der Fehlerbehebung abrufbar sind.
- Streaming-Statistik: Zeigt Hyperlinks an, über die eine Vielzahl von Streaming-Statistiken aufgerufen werden kann.
- System: Zeigt einen Hyperlink an, über den das Telefon neu gestartet werden kann.

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.

## Webseite für Telefon öffnen

Führen Sie zum Zugreifen auf die Webseite eines Telefons folgende Schritte durch:




**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 sich beim Cisco Unified Communications Manager registrieren, wird die IP-Adresse im Fenster **Telefone suchen und auflisten** sowie oben im Fenster **Telefonkonfiguration** angezeigt.
- Drücken Sie auf dem Cisco IP-Telefon **Anwendungen** , wählen Sie **Verwaltereinstellungen > Netzwerk-Setup > Ethernet-Setup > IPv4-Setup**, und führen Sie dann einen Bildlauf zum IP-Adressfeld durch.

#### 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\_Adresse**

## Geräteinformationen

Im Bereich „Geräteinformationen“ auf der Telefon-Webseite werden Geräteeinstellungen und zugehörige Informationen für das Telefon angezeigt. Diese Elemente werden in der folgenden Tabelle beschrieben.



**Hinweis** Einige Elemente in der folgenden Tabelle sind nicht für alle Telefonmodelle relevant.

Rufen Sie zum Anzeigen des Bereichs **Geräteinformationen** die Telefon-Webseite entsprechend der Beschreibung in [Webseite für Telefon öffnen, auf Seite 239](#) auf, und klicken Sie dort auf den Hyperlink **Geräteinformationen**.

**Tabelle 48: Elemente in den Geräteinformationen**

Element	Beschreibung
Servicemodus	Der Servicemodus für das Telefon.
Servicename	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.



Element	Beschreibung
Anwendungs-Software-ID	Firmware-Version der Anwendung, die auf dem Telefon ausgeführt wird.
Boot-Software-ID	Boot-Firmware-Version.
Version	ID der Firmware, die auf dem Telefon ausgeführt wird.
Erweiterungsmodul 1	Kennung für das erste Erweiterungsmodul, sofern zutreffend. Gilt für Cisco IP-Telefon 8851, 8851NR, 8861, 8865 und 8865NR.
Erweiterungsmodul 2	Kennung für das zweite Erweiterungsmodul, sofern zutreffend. Gilt für Cisco IP-Telefon 8851, 8851NR, 8861, 8865 und 8865NR.
Erweiterungsmodul 3	Kennung für das dritte Erweiterungsmodul, sofern zutreffend. Gilt für Cisco IP-Telefon 8851, 8851NR, 8861, 8865 und 8865NR.
Hardware-Revision	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.
UDI	<p>Zeigt die folgenden Cisco UDI-Informationen (Unique Device Identifier) über das Telefon an:</p> <ul style="list-style-type: none"> <li>• Gerätetyp – Gibt den Hardwaretyp an. Beispielsweise das Telefondisplay für alle Telefonmodelle.</li> <li>• Gerätebeschreibung – Zeigt den Namen des Telefons für den angegebenen Modelltyp an.</li> <li>• Produkt-ID – Gibt das Telefonmodell an.</li> <li>• Versions-ID (VID): Gibt die Hauptversionsnummer der Hardware an.</li> <li>• Seriennummer – Zeigt die eindeutige Seriennummer des Telefons an.</li> </ul>
Erweiterungsmodul-UDI	<p>Cisco Unique Device Identifier (UDI, eindeutige Geräteerkennung) des Erweiterungsmoduls.</p> <p>Gilt für Cisco IP-Telefon 8851, 8851NR, 8861, 8865 und 8865NR.</p>

Element	Beschreibung
Name des Headsets	<p>Zeigt den Namen des angeschlossenen Cisco-Headsets in der linken Spalte an. Die rechte Spalte enthält folgende Informationen:</p> <ul style="list-style-type: none"> <li>• Port – Zeigt an, wie das Headset mit dem Telefon verbunden ist. <ul style="list-style-type: none"> <li>• USB</li> <li>• AUX</li> </ul> </li> <li>• Version – Zeigt die Firmware-Version des Headsets an.</li> <li>• Funkbereich – Zeigt die für den DECT-Funk konfigurierte Stärke an. Gilt nur für Cisco-Headset 560 Serie.</li> <li>• Bandbreite – Zeigt an, ob das Headset Breitband oder Schmalband verwendet. Gilt nur für Cisco-Headset 560 Serie.</li> <li>• Bluetooth – Zeigt an, ob Bluetooth aktiviert oder deaktiviert ist. Gilt nur für Cisco-Headset 560 Serie.</li> <li>• Konferenz – Zeigt an, ob die Konferenzfunktion aktiviert oder deaktiviert ist. Gilt nur für Cisco-Headset 560 Serie.</li> <li>• Firmware-Quelle – zeigt die zulässige Firmware-Upgrademethode an: <ul style="list-style-type: none"> <li>• Nur auf UCM beschränken</li> <li>• Von UCM oder Cisco Cloud zulassen</li> </ul> </li> </ul> <p>Gilt nur für Cisco-Headset 560 Serie.</p>
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 nicht verwendeten Speichers auf dem Telefon
Java-Heap - Freier Speicherplatz	Menge des freien internen Java-Heap-Speichers
Java-Pool - Freier Speicherplatz	Menge des freien internen Java-Pool-Speichers
FIPS-Modus aktiviert	Gibt an, ob der FIPS-Modus (Federal Information Processing Standard) aktiviert ist.

## Netzwerkconfiguration

Im Bereich „Netzwerk-Setup“ auf der Telefon-Webseite werden Informationen zum Netzwerk-Setup sowie Informationen zu anderen Telefoneinstellungen angezeigt. Diese Elemente werden in der folgenden Tabelle beschrieben.

Sie können viele dieser Elemente im Menü Netzwerkconfiguration auf dem Cisco IP-Telefon anzeigen und festlegen.



**Hinweis** Einige Elemente in der folgenden Tabelle sind nicht für alle Telefonmodelle relevant.

Rufen Sie zum Anzeigen des Bereichs **Netzwerk-Setup** die Telefon-Webseite entsprechend der Beschreibung in [Webseite für Telefon öffnen, auf Seite 239](#) auf, und klicken Sie dort auf den Hyperlink **Netzwerk-Setup**.

**Tabelle 49: Elemente der Netzwerkconfiguration**

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.
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	IP-Adresse (IPv4) des Telefons.
Subnetzmaske	Die vom Telefon verwendete Subnetzmaske.
Standardrouter	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-Adresse freigegeben	Gibt die Einstellung der Option „DHCP-Adresse freigegeben“ im Menü „Netzwerkconfiguration“ des Telefons 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.

Element	Beschreibung
CUCM-Server 1 – 5	<p>Hostnamen oder IP-Adressen der Cisco Unified Communications Manager-Server, mit denen ein 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 – Cisco Unified Communications Manager-Server, von dem das Telefon derzeit Anrufverarbeitungsdienste empfängt</li> <li>• Bereitschaft – Cisco Unified Communications Manager-Server, zu dem das Telefon wechselt, wenn der aktuelle Server nicht mehr verfügbar ist</li> <li>• Leer – Derzeit keine 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 Cisco Unified Communications Manager wird in der Serverliste immer zuletzt angezeigt, auch wenn er 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.
Verzeichnis-URL	URL des Servers, von dem das Telefon Verzeichnisinformationen abrufen kann.
Nachrichten-URL	URL des Servers, von dem das Telefon Nachrichtenservices erhält.
Service-URL	URL des Servers, von dem das Telefon Cisco Unified IP-Telefon-Dienste 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.
Leerlauf-URL – Zeit	Anzahl der Sekunden, die das Telefon inaktiv und kein Menü geöffnet ist, bevor der XML-Service in der URL angegeben ist, aktiviert wird.
Proxyserver-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-Port-Setup	<p>Geschwindigkeit und Duplex-Status des Switch-Ports:</p> <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>

Element	Beschreibung
PC-Port-Setup	Geschwindigkeit und Duplex-Status des PC-Ports. Hierbei gilt Folgendes: <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>
PC-Port deaktiviert	Gibt an, ob der PC-Port am Telefon aktiviert oder deaktiviert ist.
Benutzersprache	Das dem Telefonbenutzer zugeordnete Gebietsschema. Detaillierte Informationen, um die Tastatur zu unterstützen, einschließlich Sprache, Schriftart, Datum- und Uhrzeitformat sowie Textinput für die Tastatur zur alphanumerischen Tastatur.
Netzwerkgebietsschema	Das dem Telefonbenutzer zugeordnete Netzwerkgebietsschema. Detaillierte Informationen, um das Telefon an einem bestimmten Standort zu unterstützen, einschließlich Definitionen der verwendeten Töne und Kadenzen.
Gebietsschema-Version	Version des Benutzergebietsschemas, das auf dem Telefon geladen ist.
Netz.Gebietsschema-Ver.	Version des Netzwerkgebietsschemas, das auf dem Telefon geladen ist.
Lautsprecher aktiviert	Gibt an, ob der Lautsprecher des Telefons aktiviert ist.
GARP aktiviert	Gibt an, ob das Telefon MAC-Adressen von Gratuitous ARP-Antworten lernt.
An PC-Port weiterleiten	Gibt an, ob das Telefon Pakete, die über den Netzwerk-Port gesendet und empfangen werden, über den Access-Port weiterleitet.
Videofunktion aktiviert	Gibt an, ob das Telefon an Videoanrufen teilnehmen kann, wenn es mit einer entsprechend angeschlossen Kamera verbunden ist.
Sprach-VLAN aktiviert	Gibt an, ob das Telefon einem Gerät, das am PC-Port angeschlossen ist, den Zugriff auf das Sprach-VLAN erlaubt.
PC-VLAN aktiviert	VLAN, das 802.1P/Q-Tags von Paketen, die an den PC gesendet werden, identifiziert und weiterleitet.
Autom. Leitungsauswahl aktiviert	Gibt an, ob das Telefon automatisch eine Leitung auswählt, wenn der Hörer abgenommen wird.
DSCP-Protokoll-Steuerung	DSCP IP-Klassifizierung für Anrufsteuerungssignale.
DSCP für Konfiguration	DSCP IP-Klassifizierung zur Weitergabe von Telefonkonfigurationen.
DSCP für Dienste	DSCP IP-Klassifizierung für telefonbasierte Services.
Sicherheitsmodus (unsicher)	Der für das Telefon festgelegte Sicherheitsmodus.
Webzugriff aktiviert	Gibt an, ob der Webzugriff für das Telefon aktiviert (Ja) oder deaktiviert (Nein) ist.

Element	Beschreibung
SSH-Zugriff aktiviert	Gibt an, ob der SSH-Port aktiviert oder deaktiviert wurde.
CDP: SW-Port	Gibt an, ob die CDP-Unterstützung auf dem Switch-Port verfügbar ist (standardmäßig aktiviert). Aktivieren Sie CDP auf dem Switch-Port für die VLAN-Zuweisung für das Telefon, Stromausfall, QoS-Verwaltung und 802.1x-Sicherheit. Aktivieren Sie CDP, wenn das Telefon mit einem Cisco Switch verbunden ist. 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 nicht-Cisco-Switch verbunden ist. Die aktuellen CDP-Werte für den PC- und Switch-Port werden im Menü „Einstellungen“ angezeigt.
CDP: PC-Port	Gibt an, ob die CDP auf dem Switch-Port unterstützt wird (standardmäßig aktiviert). Wenn CDP in Cisco Unified Communications Manager deaktiviert ist, wird eine Warnung angezeigt, dass CVTA nicht funktioniert, wenn CDP auf dem PC-Port deaktiviert ist. Die aktuellen CDP-Werte des PC- und Switch-Ports werden im Menü Einstellungen angezeigt.
LLDP-MED: SW-Port	Gibt an, ob LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) auf dem Switch-Port aktiviert ist.
LLDP-MED: PC-Port	Gibt an, ob LLDP-MED auf dem PC-Port aktiviert ist.
LLDP-Leistungspriorität	Energiepriorität des Telefons auf dem Switch, damit der Switch die entsprechende Leistung für die Telefone bereitstellen kann. Die Einstellungen umfassen folgende Optionen: <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	Asset-ID, die dem Telefon für das Bestandsmanagement zugewiesen ist.
CTL-Datei	MD5-Hash der CTL-Datei.
ITL-Datei	Die ITL-Datei enthält die Initial Trust List.
ITL-Signatur	MD5-Hash der ITL-Datei.
CAPF-Server	CPF-Server wird verwendet.
TVS	Die Hauptkomponente von Security by Default. Mit TVS (Trust Verification Services) können Unified IP-Telefone Anwendungsserver, beispielsweise EM-Services, Verzeichnis und MIDX, bei der Herstellung einer HTTPS-Verbindung authentifizieren.
TFTP-Server	Der Name des TFTP-Servers, der vom Telefon verwendet wird.
TFTP-Server	Der Name des TFTP-Servers, der vom Telefon verwendet wird.
Automatische Portsynchronisierung	Gibt an, ob das Telefon die Port-Geschwindigkeit automatisch synchronisiert, um Paketverluste zu vermeiden.

Element	Beschreibung
Switch-Port – Remote-Konfiguration	Gibt an, ob der SW-Port ferngesteuert wird.
PC-Port – Remote-Konfiguration	Gibt an, ob der PC-Port ferngesteuert wird.
IP-Adressierungsmodus	Identifiziert den Adressierungsmodus: <ul style="list-style-type: none"> <li>• Nur IPv4</li> <li>• IPv4 und IPv6</li> <li>• Nur IPv6</li> </ul>
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 sind.
Bevorzugter IP-Modus für Medien	
Automatische IPv6-Konfiguration	Gibt an, dass für das Gerät für das Medium eine IPv4-Adresse verwendet, um die Verbindung mit Cisco Unified Communications Manager herzustellen.
Schutz doppelt vorhandener IPv6-Adressen	
IPv6 – Nachrichtenumlenkung akzeptieren	Gibt an, ob das Telefon umgeleitete Nachrichten vom Router akzeptiert, der für die Zieladresse verwendet wird.
IPv6 – Antwort auf Multicast-Echo-Anforderung	Gibt an, dass das Telefon eine Echo-Antwort auf eine Echo-Anforderung sendet, die an eine IPv6-Adresse gesendet wurde.
IPv6 – Software-Server	Wird verwendet, um die Installationsdauer für Updates der Telefon-Firmware zu optimieren, indem Bilder lokal gespeichert werden, sodass es nicht erforderlich ist, bei Telefon-Upgrade den WAN-Link zu verwenden.
IPv6 – Protokollserver	
IPv6 – CAPF-Server	Gibt die IP-Adresse und den Port des Remotecomputers für die Protokollierung an, an dem das Telefon die Protokollnachrichten sendet.
DHCPv6	Gibt die Methode an, die das Telefon zum Abrufen der reinen IPv6-Adresse verwendet.  Wenn DHCPv6 aktiviert ist, ruft das Telefon die IPv6-Adresse entweder vom DHCPv6-Server oder durch SLAAC per Router-Advertisement vom IPv6-fähigen Router ab. Und wenn DHCPv6 nicht aktiviert ist, besitzt das Telefon keine zustandsbehaftete (vom DHCPv6-Server) oder zustandslose (SLAAC) IPv6-Adresse.  <b>Hinweis</b> Im Gegensatz zu DHCPv4 kann das Telefon trotz deaktiviertem DHCPv6 im Netzwerk eine SLAAC-Adresse generieren, wenn die automatische Konfiguration aktiviert ist.

Element	Beschreibung
IPv6-Adresse	Zeigt die aktuelle reine IPv6-Adresse des Telefons an. Zwei Adressformate werden unterstützt: <ul style="list-style-type: none"> <li>• Acht durch Doppelpunkte getrennte Gruppen von Hexadezimalziffern X:X:X:X:X:X:X:X</li> <li>• Komprimiertes Format zur Zusammenfassung einer Reihe von fortlaufenden Nullgruppen in einer einzigen Gruppe, die durch einen doppelten Doppelpunkt dargestellt wird.</li> </ul>
IPv6 – Präfixlänge	Zeigt die aktuelle Länge des reinen IPv6-Präfixes für das Subnetz an.
IPv6 – Standardrouter	Zeigt den IPv6-Standardrouter an, der vom Telefon verwendet wird.
IPv6 – DNS-Server 1 – 2	Zeigt den primären und sekundären DNSv6-Server an, die vom Telefon verwendet werden.
IPv6 – Alternativer TFTP-Server	Wird angezeigt, wenn ein alternativer IPv6-TFTP-Server verwendet wird.
IPv6 – TFTP-Server 1 – 2	Zeigt den primären und sekundären IPv6-TFTP-Server an, die vom Telefon verwendet werden.
IPv6-Adresse freigegeben	Wird angezeigt, wenn der Benutzer die IPv6-bezogenen Informationen zur Verfügung gestellt hat.
EnergyWise-Energiepegel	Der Energiepegel, der verwendet wird, wenn sich das Telefon im Schlafmodus befindet.
EnergyWise-Domäne	Die EnergyWise-Domäne, in der sich das Telefon befindet.
DF_BIT	Gibt die DF-Bit-Einstellung für Pakete an.

## Netzwerkstatistik

Über die folgenden Hyperlinks zu Netzwerkstatistiken auf der Telefon-Webseite können Sie auf Informationen zum Netzwerkverkehr auf dem Telefon zugreifen:

- **Ethernet-Informationen:** Zeigt Informationen zum Ethernet-Datenverkehr an.
- **Zugriff:** Zeigt Informationen zum Netzwerkverkehr am PC-Port des Telefons an.
- **Netzwerk:** Zeigt Informationen zum Netzwerkverkehr am Netzwerk-Port des Telefons an.

Wenn Sie einen Bereich der Netzwerkstatistik anzeigen möchten, rufen Sie die Webseite für das Telefon auf, und klicken Sie auf einen der Hyperlinks **Ethernet-Informationen**, **Zugriff** oder **Netzwerk**.

### Webseite mit Ethernet-Informationen

In der folgenden Tabelle werden die Daten auf der Webseite für Ethernet-Informationen beschrieben.

*Tabelle 50: 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.



Element	Beschreibung
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.

**Webseiten „Zugriff“ und „Netzwerk“**

In der folgenden Tabelle werden die Informationen auf den Webseiten „Zugriff“ und „Netzwerk“ erläutert.

**Table 51: Felder unter „Zugriff“ und „Netzwerk“**

Element	Beschreibung
Rx totalPkt	Gesamtanzahl der Pakete, die das Telefon empfangen hat.
Übertr. – CRC-Fehler	Gesamtanzahl der Pakete, die empfangen wurden, während CRC fehlgeschlagen ist.
Übertr. – Zuordnungsfehler	Gesamtanzahl der Pakete zwischen 64 und 1522 Bytes, die empfangen wurden und eine ungültige FCS (Frame Check Sequence) haben.
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.
Übertr. – Kurz, fehlerhaft	Gesamtanzahl der empfangenen FCS-Fehlerpakete oder Ausrichtungsfehlerpakete, die kleiner als 64 Byte sind.
Übertr. – Kurz, fehlerfrei	Gesamtanzahl der gültigen empfangenen Pakete, die kleiner als 64 Bytes sind.
Übertr. – Lang, fehlerfrei	Gesamtanzahl der gültigen empfangenen Pakete, die größer als 1522 Byte sind.
Übertr. – Lang, fehlerhaft	Gesamtanzahl der empfangenen FCS-Fehlerpakete oder Ausrichtungsfehlerpakete, die größer als 1522 Byte sind.
Übertr. – Größe 64	Gesamtanzahl der empfangenen Paket, einschließlich ungültiger Pakete, die zwischen 0 und 64 Byte groß sind.

Element	Beschreibung
Übertr. – Größe 65–127	Gesamtanzahl der empfangenen Paket, einschließlich ungültiger Pakete, die zwischen 65 und 127 Byte groß sind.
Übertr. – Größe 128–255	Gesamtanzahl der empfangenen Paket, einschließlich ungültiger Pakete, die zwischen 128 und 255 Byte groß sind.
Übertr. – Größe 256–511	Gesamtanzahl der empfangenen Paket, einschließlich ungültiger Pakete, die zwischen 256 und 511 Byte groß sind.
Übertr. – Größe 512–1023	Gesamtanzahl der empfangenen Paket, einschließlich ungültiger Pakete, die zwischen 512 und 1023 Byte groß sind.
Übertr. – Größe 1024–1518	Gesamtanzahl der empfangenen Paket, einschließlich ungültiger Pakete, die zwischen 1024 und 1518 Byte groß sind.
Rx tokenDrop	Gesamtanzahl der Pakete, die aufgrund unzureichender Ressourcen verworfen wurden (beispielsweise FIFO-Überlauf).
Übertr. – Übermäßig verzögert	Gesamtanzahl der Pakete, deren Übermittlung aufgrund eines ausgelasteten Mediums verzögert wurde.
Übertr. – Späte Kollision	Anzahl der Konflikte nach 512 Bits, nachdem die Paketübermittlung gestartet wurde.
Tx totalGoodPkt	Gesamtanzahl der gültigen Pakete (Multicast, Broadcast und Unicast), die das Telefon empfangen hat.
Übertr. – Kollisionen	Gesamtanzahl der Konflikte, die während der Übermittlung eines Pakets aufgetreten sind.
Übertr. – Zu lang	Gesamtanzahl der Pakete, die nicht übermittelt wurden, da 16 Übermittlungsversuche für ein Paket ausgeführt wurden.
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.

Element	Beschreibung
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-IPv6-Adresse	IP-Adresse des Nachbargeräts, das vom CDP-Protokoll erkannt wurde.
CDP Nachbar-Port	Nachbar-Geräteport, mit dem das Telefon verbunden ist, der vom CDP-Protokoll erkannt wurde.
LLDP Nachbargeräte-ID	ID eines mit diesem Port verbundenen Geräts, das vom LLDP-Protokoll erkannt wurde.
LLDP Nachbar-IPv6-Adresse	IP-Adresse des Nachbargeräts, das vom LLDP-Protokoll erkannt wurde.
LLDP Nachbar-Port	Nachbar-Geräteport, mit dem das Telefon verbunden ist, der vom LLDP-Protokoll erkannt wurde.
Port-Informationen	Geschwindigkeits- und Duplex-Informationen.

## Geräteprotokolle

Über die folgenden Geräteprotokoll-Hyperlinks auf der Telefon-Webseite 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:** Hier werden die zehn letzten Statusmeldungen angezeigt, die vom Telefon seit dem letzten Einschalten generiert wurden. Auf dem Bildschirm Statusmeldungen auf dem Telefon werden diese Informationen ebenfalls angezeigt.
- **Fehlersuchanzeige:** Hier werden Debug-Meldungen angezeigt, die für Cisco TAC hilfreich sein können, wenn Sie Unterstützung bei der Fehlerbehebung anfordern.

## Streaming-Statistik

Ein Cisco Unified IP-Telefon kann an bzw. von bis zu drei Geräten gleichzeitig Informationen per Streaming übertragen. 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.

In der folgenden Tabelle werden die Elemente im Bereich Streaming-Statistik beschrieben.

**Tabelle 52: Elemente im Bereich Streaming-Statistik**

Element	Beschreibung
Remote-Adresse	IP-Adresse und UDP-Port des Ziel des Streams.

Element	Beschreibung
Lokale Adresse	IP-Adresse und UPD-Port des Telefons.
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.
Senderberichte gesendet (siehe Hinweis)	Wie oft der RTCP-Senderbericht gesendet wurde.
Empfängerbericht gesendet um (siehe Hinweis)	Interner Zeitstempel, der angibt, wann der letzte RTCP-Senderbericht gesendet wurde.
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 die Anzahl der verzögerten und doppelten Pakete umfasst. Der Wert ist 0, wenn die Verbindung auf den Sendemodus festgelegt ist.
Durchschn. 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.
Empfängerberichte gesendet (siehe Hinweis)	Wie oft die RTCP-Empfängerberichte gesendet wurden.
Empfängerbericht gesendet um (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.

Element	Beschreibung
Empfänger – Oktette	Gesamtanzahl der Nutzlast-Oktette, die das Telefon in RTP-Datenpaketen empfängt, die 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 im Sendemodus festgelegt ist.
MOS LQK	Dieser Ergebniswert ist eine objektive Schätzung des Mean Opinion Score (MOS) für die Hörqualität (LQK), der von Stufe 1 (schlecht) bis Stufe 5 (exzellent) reicht. Dieser Ergebniswert basiert auf hörbaren Verdeckungsereignissen, die aufgrund von Loss of Frame innerhalb vorhergehenden 8-sekündigen Audio-Stream-Intervalls aufgetreten sind. Weitere Informationen hierzu finden Sie unter <a href="#">Überwachung der Sprachqualität, auf Seite 282</a> .  <b>Hinweis</b> Der Ergebniswert für MOS LQK kann je nach dem vom Cisco Unified Communications Manager verwendeten Codec-Typen unterschiedlich ausfallen.
Durchschnitt: MOS LQK	Durchschnittlicher MOS LQK-Wert des gesamten Audio-Streams.
Min MOS LQK (Minimalwert: MOS LQK)	Niedrigster MOS LQK-Wert seit Beginn des Audio-Streams.
Max MOS LQK (Maximalwert: MOS LQK)	Grundsätzlicher oder höchster MOS LQK-Wert seit Beginn des Audio-Streams. Bei normalen Bedingungen ohne Loss of Frame führen die folgenden Codecs zu den maximalen MOS LQK-Werten: <ul style="list-style-type: none"> <li>• G.711: 4,5.</li> <li>• G.729 A/AB: 3,7.</li> </ul>
MOS-LQK-Version	Version des Cisco Algorithmus, der zur Berechnung der MOS LQK-Werte verwendet wird.
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.
Verdeckung (Maximalrate)	Höchstes Intervall der Verdeckungsrate ab Beginn des Voicestreams.
Verdeckung in Sekunden	Anzahl der Sekunden mit Verdeckungsereignissen (verlorene Rahmen) ab Beginn des Voicestreams (einschließlich schwerwiegende Verdeckung).
Verdeckung (schwerwiegend) in Sek.	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 Wert des unmittelbaren Jitters in Millisekunden.
Sender – Größe	RTP-Paketgröße in Millisekunden für den übermittelten Stream.

Element	Beschreibung
Senderberichte empfangen (siehe Hinweis)	Wie oft die RTCP-Senderberichte empfangen wurden.
Senderbericht empfangen um (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.
Empfängerberichte empfangen (siehe Hinweis)	Wie oft die RTCP-Empfängerberichte empfangen wurden.
Empfängerbericht empfangen um (siehe Hinweis)	Zeitpunkt, an dem zuletzt ein RTCP-Empfängerbericht empfangen wurde.
Empfänger verschlüsselt	Gibt an, ob der Empfänger eine Verschlüsselung verwendet.
Sender verschlüsselt	Gibt an, ob der Sender eine Verschlüsselung verwendet.
Sender – Frames	Anzahl der gesendeten Frames.
Sender - Teilweise Frames	Anzahl der teilweise gesendeten Frames.
Sender – I-Frames	Anzahl der gesendeten I-Frames. I-Frames werden bei der Videoübertragung verwendet.
Sender-IDR-Frames	Anzahl der gesendeten IDR-Frames (Instantaneous Decoder Refresh). IDR-Frames werden bei der Videoübertragung verwendet.
Sender – Bildfrequenz	Die Frequenz, mit der der Sender Frames sendet.
Sender – Bandbreite	Bandbreite für den Sender.
Sender – Auflösung	Die Videoauflösung des Senders.
Empfänger – Frames	Anzahl der empfangenen Frames.
Empfänger - Teilweise Frames	Anzahl der teilweise empfangenen Frames.
Empfänger – I-Frames	Anzahl der empfangenen I-Frames.
Empfänger-IDR-Frames	Anzahl der empfangenen IDR-Frames.
Empfänger – IFrames-Anforderung	Anzahl der angeforderten und empfangenen IDR-Frames.
Empfänger – Bildfrequenz	Die Frequenz, mit der der Empfänger Frames empfängt.
Empfänger - Frames verloren	Anzahl der Frames, die nicht empfangen wurden.
Empfänger - Framefehler	Anzahl der Frames, die nicht empfangen wurden.

Element	Beschreibung
Empfänger – Bandbreite	Die Bandbreite des Empfängers.
Empfänger – Auflösung	Die Videoauflösung des Empfängers.
Domäne	Domäne, in der sich das Telefon befindet.
Sender - Zusammenführungen	Anzahl der Beitritte des Senders.
Empfänger - Zusammenführungen	Anzahl der Beitritte des Empfängers.
Byte	Anzahl der „Bye“-Frames.
Sender - Startzeit	Uhrzeit, zu der der Sender begonnen hat.
Empfänger - Startzeit	Uhrzeit, zu der der Empfänger begonnen hat.
Zeilenstatus	Gibt an, ob auf dem Telefon ein Streaming durchgeführt wird.
Sender - Tool	Typ der Audiocodierung, der für den Stream verwendet wird.
Sender - Berichte	RTCP-Senderberichte
Sender - Berichtszeit	Letzter Zeitpunkt, zu dem ein RTCP-Senderbericht gesendet wurde.
Empfänger - Jitter	Maximaler Jitter des Streams
Empfänger - Tool	Typ der Audiocodierung, der für den Stream verwendet wird.
Empfänger - Berichte	Anzahl der Zugriffe auf diesen Streaming-Statistikbericht auf der Webseite.
Empfänger - Berichtszeit	Interner Zeitstempel, der angibt, wann dieser Streaming-Statistikbericht generiert wurde.
Ist Video	Gibt an, ob der Anruf ein Videoanruf oder ein Audioanruf war.
Anruf-ID	Anrufkennung
Gruppen-ID	Kennung der Gruppe, in der sich das Telefon befindet.



**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 Anruffsitzungen 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 „ModelInfo“

Der folgende XML-Code ist ein Beispiel für die Ausgabe des Befehls „ModelInfo“.

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
  <PlaneTitle>Applications</PlaneTitle>
  <PlaneFieldCount>12</PlaneFieldCount>
  <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
  <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
  <Prompt></Prompt>
  <Notify></Notify>
  <Status></Status>
  <CiscoIPPhoneFields>
    <FieldType>0</FieldType>
    <FieldAttr></FieldAttr>
    <fieldHelpIndex>0</fieldHelpIndex>
    <FieldName>Call History</FieldName>
    <FieldValue></FieldValue>
  </CiscoIPPhoneFields>
  <CiscoIPPhoneFields>
    <FieldType>0</FieldType>
    <FieldAttr></FieldAttr>
    <fieldHelpIndex>0</fieldHelpIndex>
    <FieldName>Preferences</FieldName>
    <FieldValue></FieldValue>
  </CiscoIPPhoneFields>
  ...
</CiscoIPPhoneModeInfo>
```



# KAPITEL 12

## Fehlerbehebung

- [Allgemeine Informationen zur Problembehandlung, auf Seite 259](#)
- [Startprobleme, auf Seite 260](#)
- [Probleme mit dem Zurücksetzen des Telefons, auf Seite 265](#)
- [Das Telefon kann sich nicht mit dem LAN verbinden, auf Seite 267](#)
- [Sicherheitsprobleme auf Cisco IP-Telefon, auf Seite 267](#)
- [Probleme bei Videoanrufen, auf Seite 269](#)
- [Allgemeine Anrufprobleme, auf Seite 270](#)
- [Fehlerbehebungsverfahren, auf Seite 271](#)
- [Debuginformationen von Cisco Unified Communications Manager, auf Seite 276](#)
- [Zusätzliche Informationen zur Problembehandlung, auf Seite 277](#)

## Allgemeine Informationen zur Problembehandlung

Die folgende Tabelle enthält allgemeine Informationen zur Problembehandlung für Cisco IP-Telefon.

**Tabelle 53: Fehlerbehebung beim Cisco IP-Telefon**

Zusammenfassung	Erklärung
Ein Cisco IP-Telefon mit einem anderen Cisco IP-Telefon verbinden	Cisco unterstützt die Verbindung eines IP-Telefons mit einem anderen über den PC-Port nicht. Jedes IP-Telefon sollte direkt mit einem Switch verbunden werden. Wenn Telefone in einer Leitung miteinander verbunden sind, funktionieren die Telefone nicht.
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. Die Telefone können nicht verwendet werden, bis ein Broadcast-Sturm beendet ist.

Zusammenfassung	Erklärung
Eine Netzwerkverbindung vom Telefon auf eine Arbeitsstation verlegen	<p>Wenn Sie Ihr Telefon über eine Netzwerkverbindung betreiben und das Netzwerk ausstecken möchten, um es in einen Desktopcomputer einzustecken, müssen Sie vorsichtig vorgehen.</p> <p><b>Vorsicht</b> Die Netzwerkkarte im Computer kann keine Energie über die Netzwerkverbindung empfangen. Wenn Energie über die Verbindung übertragen wird, kann die Netzwerkkarte zerstört werden. Um eine 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.</p>
Die Telefonkonfiguration ändern	<p>Die Netzwerkkonfigurationsoptionen sind standardmäßig gesperrt, damit die Benutzer keine Änderungen vornehmen können, die möglicherweise Auswirkungen auf andere Netzwerkverbindungen haben. Bevor Sie die Netzwerkkonfigurationsoptionen konfigurieren können, müssen Sie sie entsperren. Weitere Informationen hierzu finden Sie unter <a href="#">Anwenden eines Telefonkennworts</a>, auf Seite 50.</p> <p><b>Hinweis</b> Wenn das Administratorkennwort nicht im allgemeinen Telefonkennwort festgelegt ist, kann der 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 ein Transcoder vorhanden ist, um den Service abzuwickeln.</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.</p>
Loopback	<p>Ein Loopback kann unter folgenden Bedingungen auftreten:</p> <ul style="list-style-type: none"> <li>• Die Option „SW-Port-Konfiguration“ im Menü „Netzwerkkonfiguration“ des Telefons ist auf „10 Halb (10-BaseT/Halbduplex)“ eingestellt.</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> <p>HALF_DUX_COLLISION_EXCEED_THRESHOLD</p> <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

[Überprüfung des Telefons beim Starten](#), auf Seite 66

## 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, Netzerkausfälle 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

[Überprüfung des Telefons beim Starten](#), auf Seite 66

## 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 271](#).

## 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.

### Verwandte Themen

[Statusmeldungen anzeigen](#), auf Seite 225

## 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 272

## 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.

## 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.

## 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 275](#).

## 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.

## 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 73](#), 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 72](#).

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 263](#), 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.

## Telefon kann nicht registriert werden

### Problem

Auf dem Telefonbildschirm wird die Meldung „Geben Sie den Aktivierungscode oder die Servicedomäne ein“ angezeigt.

### Lösung

Eine TFTP-Adresse für das Telefon ist nicht vorhanden. Stellen Sie sicher, dass die Option 150 vom DHCP-Server bereitgestellt oder ein Alternativ-TFTP manuell konfiguriert wurde.



# 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.

## 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

Um zu überprüfen, ob ein Cisco IP-Telefon einen Befehl zum Zurücksetzen von Cisco Unified Communications Manager empfangen hat, drücken Sie **Anwendungen**  auf dem Telefon, und wählen Sie **Administratoreinstellungen > Status > Netzwerkstatistiken**.

- 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 273](#) 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.

## Probleme bei Videoanrufen

### Keine Videoübertragung zwischen zwei Cisco IP-Videotelefonen

**Problem**

Zwischen zwei Cisco IP-Videotelefonen erfolgt kein Video-Streaming.

**Lösung**

Stellen Sie sicher, dass kein Medienterminierungspunkt (MTP) im Anruffluss verwendet wird.

## Videowiedergabe stolpert oder es werden Frames ausgelassen

### Problem

Wenn ich einen Videoanruf tätige, wird das Video gepuffert, oder es werden Frames ausgelassen.

### Lösung

Die Qualität des Bildes hängt von der Bandbreite des Anrufs ab. Wenn Sie die Bitrate erhöhen, verbessert sich die Qualität des Videobildes. Allerdings werden dadurch zusätzliche Netzwerkressourcen benötigt. Verwenden Sie stets die für Ihren Videotyp am besten geeignete Bitrate. Videoanrufe mit 720p und 15 Frames pro Sekunde benötigen eine Bitrate von 790 Kbit/s oder mehr. Videoanrufe mit 720p und 30 Frames pro Sekunde benötigen eine Bitrate von 1360 Kbit/s oder mehr.

Weitere Informationen zur Bandbreite finden Sie im Abschnitt „Auflösung für Videoübertragung einrichten“ im Kapitel „Telefonfunktionen und Einrichtung“.

### Lösung

Bestätigen Sie, dass der Parameter „Maximale Sitzungsbitrate für Videoanrufe“ so konfiguriert ist, dass mindestens der minimale Video-Bitratensbereich verwendet wird. Navigieren Sie im Cisco Unified Communications Manager zu **System** > **Regionsinformationen** > **Region**.

## Videoanruf kann nicht übergeben werden

### Problem

Ich kann keine Videoanrufe von meinem Tischtelefon an mein Mobilgerät übergeben.

### Lösung

Cisco Unified Mobility kann nicht für Videoanrufe verwendet werden. Ein Videoanruf, der auf dem Tischtelefon empfangen wird, kann nicht auf einem Mobiltelefon angenommen werden.

## Kein Video während eines Konferenzgesprächs

### Problem

Videoanruf wird zu einem Audioanruf, wenn ich zwei oder mehr Teilnehmer zum Anruf hinzufüge.

Sie müssen eine Videokonferenzbrücke für spontane und MeetMe-Videokonferenzen verwenden.

## 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 Problebericht 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.
- 

## Erstellen eines Konsolenprotokolls auf Ihrem Telefon


Sie generieren ein Konsolenprotokoll, wenn Ihr Telefon nicht mit dem Netzwerk verbunden wird und Sie nicht auf das Probleberichtstool (PRT) zugreifen können.

### Vorbereitungen

Schließen Sie ein Konsolenkabel an den AUX-Anschluss an der Rückseite Ihres Telefons an.

### Prozedur


---

- Schritt 1** Drücken Sie auf Ihrem Telefon auf **Anwendungen** .
  - Schritt 2** Navigieren Sie zu **Administratoreinstellungen > AUX Port**.
  - Schritt 3** Wählen Sie **Konsolenprotokoll erfassen**, um Geräteprotokolle zu erfassen.
- 

## TFTP-Einstellungen überprüfen

### Prozedur

---

- Schritt 1** Drücken Sie auf dem Cisco IP-Telefon **Anwendungen** , wählen Sie **Administratoreinstellungen > Netzwerk-Setup > Ethernet-Setup > IPv4-Setup > TFTP-Server 1** aus.
- Schritt 2** Wenn Sie dem Telefon eine statische IP-Adresse zugewiesen haben, müssen Sie manuell einen Wert für die Option TFTP-Server 1 eingeben.
- Schritt 3** 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 4** 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 5** 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:
- a) Deaktivieren Sie DHCP.
  - b) Weisen Sie dem Telefon statische IP-Werte zu. Verwenden Sie die gleiche Standardroutereinstellungen wie für die anderen funktionierenden Telefone.
  - c) 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

[Standardmäßiges Zurücksetzen](#), auf Seite 279

[Die MAC-Adresse des Telefons bestimmen](#), auf Seite 72

## DHCP-Einstellungen überprüfen

### Prozedur

- 
- Schritt 1** Drücken Sie auf dem Telefon **Anwendungen** .
- Schritt 2** Wählen Sie **Wi-Fi** > **Netzwerk-Setup** > **IPv4-Setup** aus, und überprüfen Sie die folgenden Optionen:
- 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:
- [http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod\\_tech\\_notes\\_list.html](http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html)

- IP-Adresse, Subnetzmaske, Standardrouter: Wenn Sie dem Telefon eine statische IP-Adresse zugewiesen haben, müssen Sie die Einstellungen für diese Optionen manuell vornehmen.

**Schritt 3**

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:

[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a00800f0804.shtml](http://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

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

[Methoden zum Hinzufügen von Telefonen](#), auf Seite 73

## Ermitteln, ob bzw. welche 802.1X-Authentifizierungsprobleme bestehen

### Prozedur

---


- Schritt 1** Überprüfen Sie, dass Sie die erforderlichen Komponenten ordnungsgemäß konfiguriert haben.
- Schritt 2** Vergewissern Sie sich, dass das Shared Secret auf dem Telefon konfiguriert ist.
- Wenn das Shared Secret konfiguriert ist, überprüfen Sie, dass das gleiche Shared Secret auch auf dem Authentifizierungsserver vorhanden ist.
  - Wenn das Shared Secret auf dem Telefon nicht konfiguriert ist, geben Sie es dort ein, und achten Sie darauf, dass es mit dem Shared Secret auf dem Authentifizierungsserver übereinstimmt.
- 

## Die DNS-Einstellungen überprüfen

Um die DNS-Einstellungen zu überprüfen, führen Sie die folgenden Schritte aus:

### Prozedur

---

- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Administrator Einst.** > **Netzwerk-Setup** > **IPv4-Setup** > **DNS-Server 1**.
- Schritt 3** 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 Servicennamen 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, Wi-Fi, VPN, Energywise, MobileRemoteAccess

**Hinweis** Um die Unterstützung der Parameter auf mehreren Ebenen und in mehreren Bereichen zu implementieren, aktivieren Sie das Kontrollkästchen Protokollprofil.

- 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




- Standardmäßiges Zurücksetzen, auf Seite 279
- Netzwerkkonfiguration zurücksetzen, auf Seite 281
- Benutzer-Netzwerkkonfiguration zurücksetzen, auf Seite 281
- CTL-Datei entfernen, auf Seite 282
- Quality Report Tool, auf Seite 282
- Überwachung der Sprachqualität, auf Seite 282
- Reinigung des Cisco IP-Telefon, auf Seite 284

## Standardmäßiges Zurücksetzen

Mithilfe des standardmäßigen Zurücksetzens eines Cisco IP-Telefon kann das Telefon im Fall eines Fehlers wiederhergestellt werden, und es wird das Zurücksetzen auf bzw. Wiederherstellen von verschiedenen Konfigurations- und Sicherheitseinstellungen ermöglicht.

In der folgenden Tabelle sind die verschiedenen Methoden zum einfachen Zurücksetzen beschrieben. Sie können ein Telefon mit einem dieser Vorgänge zurücksetzen, nachdem das Telefon gestartet wurde. Wählen Sie den Vorgang aus, der für Ihre Situation passend ist.

**Tabelle 54: Methoden zum einfachen Zurücksetzen**

Vorgang	Aktion	Erklä
Telefon neu starten	Drücken Sie <b>Anwendungen</b>  . Navigieren Sie zu <b>Verwaltereinstellungen &gt; Einstellungen zurücksetzen &gt; Gerät zurücksetzen</b> .	Dara vom Einst
Einstellungen zurücksetzen	Drücken Sie zum Zurücksetzen der Einstellungen auf <b>Anwendungen</b>  , und wählen Sie dann <b>Administrator Einst. &gt; Einstellungen zurücksetzen &gt; Netzwerk</b> .	Dara Stanc
	Drücken Sie zum Zurücksetzen der CTL-Datei auf <b>Anwendungen</b>  , und wählen Sie dann <b>Administrator Einst. &gt; Einstellungen zurücksetzen &gt; Sicherheit</b> .	Dara

## Telefon über das Tastenfeld des Telefons auf die Werkseinstellungen zurücksetzen

Sie können das Telefon auf die Werkseinstellungen zurücksetzen. Durch das Zurücksetzen werden alle Parameter des Telefons gelöscht.

### Prozedur

---

- Schritt 1** Trennen Sie das Telefon durch einen der folgenden Schritte von der Stromzufuhr:
- Ziehen Sie den Netzstecker ab.
  - Ziehen Sie das LAN-Kabel ab.
- Schritt 2** Warten Sie 5 Sekunden lang.
- Schritt 3** Drücken und halten Sie # und schließen Sie das Telefon wieder an. Lassen Sie # erst los, wenn die Tasten für **Headset** und **Lautsprecher** leuchten.
- Hinweis** Bei einigen Hardwareversionen leuchtet zusammen mit den Tasten für **Headset** und **Lautsprecher** auch die Taste für **Stummschalten** auf, wenn Sie das Telefon wieder anschließen. Warten Sie in diesem Fall, bis alle Tasten ausgehen, und lassen Sie # erst dann los, wenn die Tasten für **Headset** und **Lautsprecher** wieder leuchten.
- Schritt 4** Geben Sie die folgende Tastenfolge ein:
- 123456789\*0#**
- Die Beleuchtung der Taste **Headset** erlischt, nachdem Sie die Taste **1** gedrückt haben. Nach dem Drücken der Tastenfolge leuchtet die Taste **Stummschaltung**.
- Vorsicht** Schalten Sie das Telefon nicht aus, bis der Prozess abgeschlossen ist und der Hauptbildschirm angezeigt wird.
- Das Telefon wird zurückgesetzt.
- 

## Alle Einstellungen über das Telefonmenü zurücksetzen

Führen Sie diese Aufgabe aus, wenn Sie die Einstellungen für die Benutzer- und Netzwerkkonfiguration auf die Standardwerte zurücksetzen möchten.

### Prozedur

---

- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Administrator Einst. > Einstellungen zurücksetzen > Alle Einstellungen**.
- Entsperren Sie gegebenenfalls die Telefonoptionen.
-



## Ihr Telefon über das Backup-Image neu starten

Ihr Cisco IP Phone 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** Trennen Sie die Stromversorgung.
  - Schritt 2** Halten Sie die Sternchentaste (\*) gedrückt.
  - Schritt 3** Schließen Sie die Stromversorgung wieder an. Drücken Sie weiterhin die Sternchentaste, bis die LED für Stummschaltung deaktiviert ist.
  - Schritt 4** Lassen Sie die Sternchentaste los.  
Das Telefon wird über das Backup-Image neu gestartet.
- 

## Netzwerkkonfiguration zurücksetzen

Hiermit werden die Netzwerkkonfigurationseinstellungen auf ihre Standardwerte zurückgesetzt, und das Telefon wird zurückgesetzt. Diese Methode bewirkt, dass DHCP die IP-Adresse des Telefons neu konfiguriert.

### Prozedur

---

- Schritt 1** Entsperren Sie ggf. im Menü „Administrator Einst.“ die Telefonoptionen.
  - Schritt 2** Wählen Sie **Einstellungen zurücksetzen** > **Netzwerk-Setup**.
- 

## Benutzer-Netzwerkkonfiguration zurücksetzen

Hiermit werden alle von Ihnen vorgenommenen, noch nicht in den Flash-Speicher geschriebenen Änderungen an der Benutzer- und Netzwerkkonfiguration auf die zuvor gespeicherten Einstellungen zurückgesetzt.

### Prozedur

---

- Schritt 1** Entsperren Sie ggf. im Menü „Administrator Einst.“ die Telefonoptionen.
  - Schritt 2** Wählen Sie **Einstellungen zurücksetzen** > **Gerät zurücksetzen**.
-

## CTL-Datei entfernen

Löscht nur die CTL-Datei vom Telefon.

### Prozedur

- 
- Schritt 1** Entsperren Sie ggf. im Menü „Administrator Einst.“ die Telefonoptionen.  
**Schritt 2** Wählen Sie **Einstellungen zurücksetzen** > **Sicherheitseinstellungen**.
- 

## Quality Report Tool

Das Tool für Qualitätsberichte (QRT) erstellt Berichte über die Sprachqualität und allgemeine Probleme mit dem Cisco IP-Telefon. Die QRT-Funktion wird als Komponente von Cisco Unified Communications Manager installiert.

Sie können die QRT-Funktion auf den Cisco IP-Telefon der Benutzer konfigurieren. Mit QRT können die Benutzer Anrufprobleme melden, indem sie Qualität melden drücken. Dieser Softkey oder die Taste ist nur verfügbar, wenn das Cisco IP-Telefon den Status Verbunden, Konferenz verbunden, Verbundene Übergabe oder Aufgelegt hat.

Wenn ein Benutzer Qualität melden drückt, werden die Problemkategorien aufgelistet. Der Benutzer wählt eine Problemkategorie aus und das Feedback wird in einer XML-Datei aufgezeichnet. Die tatsächlich protokollierten Informationen hängen von der Benutzerauswahl ab und davon, ob das Zielgerät ein Cisco IP-Telefon ist.

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

### Verwandte Themen

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

## 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 55: 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 285
- [Internationaler Support für Anrufprotokollierung](#), auf Seite 285
- [Sprachbeschränkung](#), auf Seite 286

## 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 xv

## 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 (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.

Die Eingabe für Chinesisch funktioniert ähnlich wie bei PCs und Mobilgeräten in Chinesisch. Das Sprachinstallationspaket für Chinesisch ist erforderlich, damit die Eingabe für Chinesisch funktioniert.

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.