Cisco IP-Konferenztelefon 7832 – Administratorhandbuch für Cisco Unified Communications Manager

Erste Veröffentlichung: 30 August 2017

Letzte Änderung: 12 Juli 2021

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

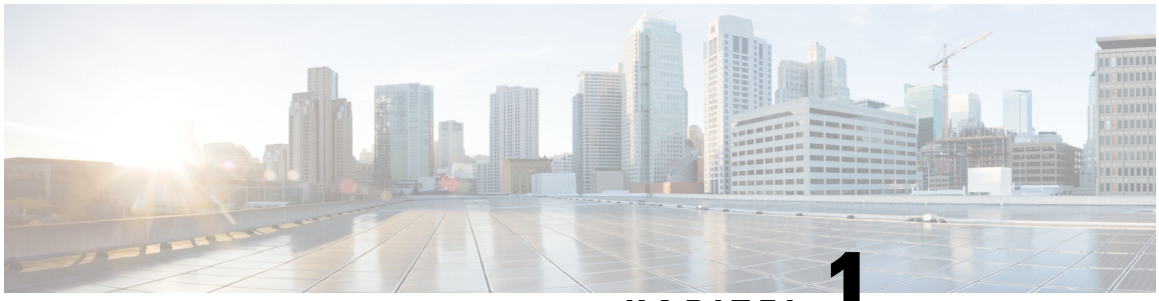
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

INHALTSVERZEICHNIS



KAPITEL 1

Neue und geänderte Informationen

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	Sicherheitsverbesserungen für Ihr Telefonnetzwerk, auf Seite 58
Telefonmigration ohne Übergangs-Firmware	Direkte Migration Ihres Telefons zu einem Multiplattform-Telefon, auf Seite 76

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

Tabelle 1: Neue und geänderte Informationen

Funktion	Neue oder geänderte Abschnitte
SIP-OAuth-Verbesserungen	Sicherheitsverbesserungen für Ihr Telefonnetzwerk, auf Seite 58
Verbesserungen der Benutzeroberfläche	SRST (Survivable Remote Site Telephony), auf Seite 49

Funktion	Neue oder geänderte Abschnitte
OAuth-Verbesserungen für MRA	Mobil- und Remote Access über Expressway, auf Seite 104

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-Version12.8(1)

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

Funktion	Neuer oder geänderter Inhalt
Telefondatenmigration	Telefonmodell eines Benutzers ändern, auf Seite 37
Weitere Informationen zum Feld „Webzugriff“ hinzugefügt	Produktspezifische Konfiguration, auf Seite 80

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

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

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

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

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

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

In der folgenden Tabelle werden die Änderungen für das *Cisco IP-Konferenztelefon 7832-Administratorhandbuch für Cisco Unified Communications Manager* zur Unterstützung von Firmware-Version 12.5(1)SR3 aufgeführt.

Tabelle 2: Überarbeitung des Cisco IP Phone 7832-Administratorhandbuchs für Firmware-Version 12.5(1)SR3

Überarbeitung	Neuer oder aktualisierter Abschnitt
Unterstützung für die Integration über Aktivierungscode mit mobilem und Remotezugriff	Aktivierungscode-Integration mit mobilem und Remotezugriff, auf Seite 27
Unterstützung für die Verwendung des Problemberichtstools über Cisco Unified Communications Manager	Telefonproblemberichte im Cisco Unified Communications Manager erstellen, auf Seite 164

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

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

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

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

In der folgenden Tabelle werden die Änderungen für das *Cisco IP-Konferenztelefon 7832-Administratorhandbuch für Cisco Unified Communications Manager* zur Unterstützung von Firmware-Version 12.5(1)SR1 aufgeführt.

Tabelle 3: Überarbeitung des Cisco IP-Konferenztelefons 7832-Administratorhandbuchs für Firmware-Version 12.5(1)SR1

Überarbeitung	Neuer oder aktualisierter Abschnitt
Unterstützung für elliptische Kurven	Unterstützte Sicherheitsfunktionen, auf Seite 59
Unterstützung für Medienpfade und Interactive Connectivity Establishment	Medienpfade und Interactive Connectivity Establishment, auf Seite 106
Unterstützung für das Integrieren des Aktivierungscodes	Aktivierungscode-Integration für lokale Telefone, auf Seite 26

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

In der folgenden Tabelle werden die Änderungen für das *Cisco IP-Konferenztelefon 7832-Administratorhandbuch für Cisco Unified Communications Manager* zur Unterstützung von Firmware-Version 12.5(1) aufgeführt.

Tabelle 4: Überarbeitung des Cisco IP-Konferenztelefons 7832-Administratorhandbuchs für Firmware-Version 12.5(1)

Überarbeitung	Neuer oder aktualisierter Abschnitt
Unterstützung für Whisper Paging auf Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express-Interaktion, auf Seite 20
Unterstützung für das Deaktivieren des TLS-Schlüssels	Produktspezifische Konfiguration, auf Seite 80
Unterstützung für Blockwahl für T.302-Erweiterung des Interdigit-Timers.	Produktspezifische Konfiguration, auf Seite 80

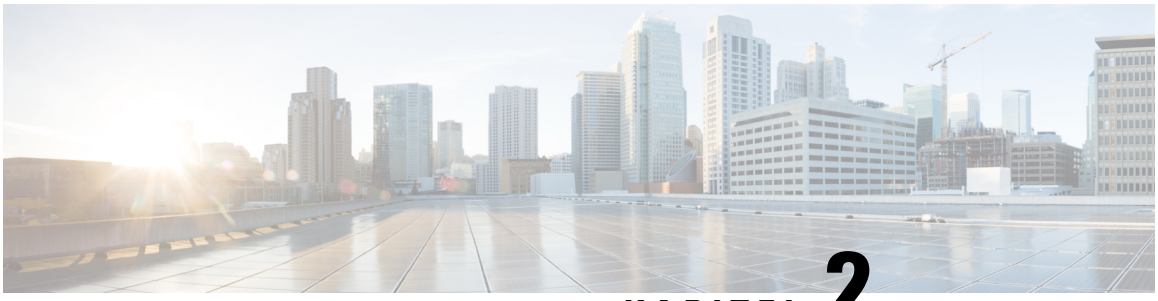
Neue und geänderte Informationen zur Firmware-Version 12.1(1)

In der folgenden Tabelle werden die Änderungen für das *Cisco IP-Konferenztelefon 7832-Administratorhandbuch für Cisco Unified Communications Manager* zur Unterstützung von Firmware-Version 12.1(1) aufgeführt.

Überarbeitung	Neuer oder aktualisierter Abschnitt
Unterstützung für Mobilzugriff und Remote Access über Expressway	• Mobil- und Remote Access über Expressway, auf Seite 104 • Bereitstellungsszenarien, auf Seite 105 • Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren, auf Seite 106
Unterstützung für das Aktivieren oder Deaktivieren von TLS 1.2 für den Webserverzugriff	Produktspezifische Konfiguration, auf Seite 80
Unterstützung für G722.2 AMR-WB-Audio-Codec	• Die Cisco IP-Konferenztelefon 7832, auf Seite 7 • Anrufstatistikfelder, auf Seite 126

TEIL I

Allgemeines zum Cisco IP-Konferenztelefon



KAPITEL 2

Cisco IP-Konferenztelefon – Hardware

Die Cisco IP-Konferenztelefon 7832

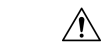
Cisco IP-Konferenztelefon 7832 verbessert die personenorientierte Kommunikation durch die Kombination von hervorragender (HD) Audio-Leistung und 360-Grad-Abdeckung für Konferenzräume und Chefbüros verschiedenster Größe. Es bietet ein audiophiles Sound-Erlebnis mit einem Zwei-Wege-Lautsprecher mit Wideband-Audio (G.722) für Freisprechen im Vollduplex-Betrieb. Das Cisco IP-Konferenztelefon 7832 ist eine einfache Lösung, die die Anforderungen der unterschiedlichsten Räume erfüllt.

Das Telefon hat empfindliche Mikrofone, die 360 Grad abdecken. Die Benutzer können normal sprechen und werden in einer Entfernung von bis zu 2,1 Metern klar gehört. Die Technologie des Telefons widersteht

Störungen von Mobiltelefonen und anderen drahtlosen Geräten, um eine klare Kommunikation ohne Ablenkungen sicherzustellen.

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.

Tasten und Hardware des Cisco IP-Telefon 7832

Die folgende Abbildung zeigt das Cisco IP-Konferenztelefon 7832.

Abbildung 1: Tasten und Funktionen des Cisco IP-Konferenztelefon 7832

In der folgenden Tabelle werden die Tasten auf dem Cisco IP-Konferenztelefon 7832 beschrieben.

1	**Stummschaltleiste**	Zum Ein- bzw. Ausschalten des Mikrofons. Wenn das Mikrofon stummgeschaltet ist, leuchtet die LED-Leiste rot.
2	LED-Leiste	Zeigt den Anrufstatus an: • Grün, leuchtend: Aktiver Anruf • Grün, blinkend: Eingehender Anruf • Grün, blinkend: Gehaltener Anruf • Rot, leuchtend: Stummgeschalteter Anruf
3	Softkeys	Zugriff auf Funktionen und Services.
4	Navigationsleiste und **Auswahltaste**	Zum Blättern durch Menüs, Markieren von Elementen und Auswählen des markierten Elements. Wenn das Telefon inaktiv ist, drücken Sie **Nach oben**, um auf die Anrufliste zuzugreifen. Drücken Sie **Nach unten**, um auf die Favoritenliste zuzugreifen.

5	**Lautstärke**-Taste	 Passen Sie die Lautstärke des Lautsprechermodus (abgehoben) und des Ruftons (aufgelegt) an. Wenn Sie die Lautstärke ändern, leuchtet die LED-Leiste weiß.

Softkeys des Konferenztelefons

Sie können auf die Funktionen Ihres Telefons über die Softkeys zugreifen. 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.

Die Softkeys an. Der Softkey ●● gibt an, dass weitere Softkey-Funktionen verfügbar sind.

Zugehöriges Dokumentationsmaterial

In den folgenden Abschnitten finden Sie zugehörige Informationen.

Dokumentation für das Cisco IP-Konferenztelefon 7832

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

Dokumentation Cisco Unified Communications Manager

Lesen Sie den *Cisco Unified Communications Manager Dokumentationsleitfaden* und andere Veröffentlichungen für Ihre Version von Cisco Unified Communications Manager auf der Seite mit Produkt-Support.

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.

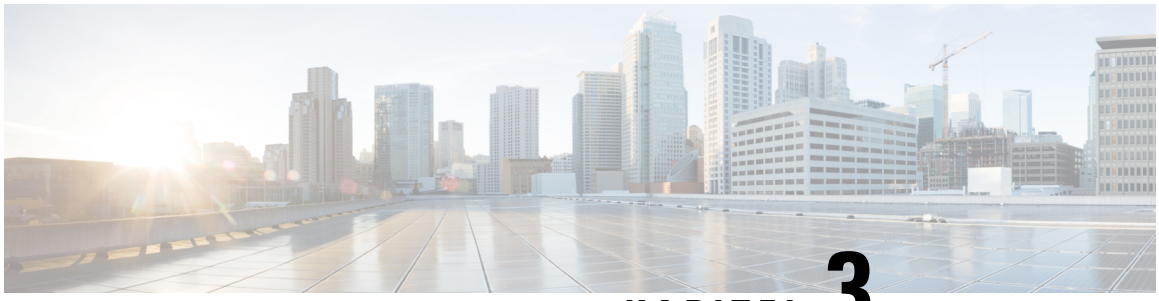
Begriffsunterschiede

In diesem Dokument umfasst der Begriff *Cisco IP Phone* das Cisco IP-Konferenztelefon 7832.

Die folgende Tabelle enthält einige der Begriffsunterschiede im *Benutzerhandbuch für das Cisco IP-Konferenztelefon 7832*, im *Administratorhandbuch für das Cisco IP-Konferenztelefon 7832 für Cisco Unified Communications Manager* und in der Dokumentation zu Cisco Unified Communications Manager.

Tabelle 5: Begriffsunterschiede

Benutzerhandbuch	Administratorhandbuch
Nachrichtenanzeigen	Briefkastenlampe (MWI)
Voicemail-System	Voicemail-System



KAPITEL 3

Technische Details

Physische und Umgebungsspezifikationen

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

Tabelle 6: Physische und Umgebungsspezifikationen

Spezifikation	Wert oder Bereich
Betriebstemperatur	0 °C bis 40 °C (32 °F bis 104 °F)
Relative Luftfeuchtigkeit beim Betrieb	10 % bis 90 % (nicht kondensierend)
Lagertemperatur	-10 °C bis 60 °C (14 °F bis 140 °F)
Höhe	226 mm (8,9 Zoll)
Breite	226 mm (8,9 Zoll)
Tiefe	54,4 mm (2,14 Zoll)
Gewicht	0,907 kg (2,0 lb.)

Spezifikation	Wert oder Bereich
Netzanschluss	• IEEE PoE Klasse 2. Das Telefon ist kompatibel mit den beiden Switch Blades nach IEEE 802.3af bzw. 802.3at und unterstützt CDP (Cisco Discovery Protocol) sowie (LLDP-PoE (Link Layer Discovery Protocol mit Power over Ethernet). • Wenn die verbundenen LAN-Switches PoE nicht unterstützen, wird ein zusätzlicher PoE-Power Injector benötigt, um den Wechselstrom aus der Steckdose für die PoE-Stromversorgung zu konvertieren.
Kabel	Kategorie 3/5/5e/6 für 10-Mbit/s-Kabel mit vier Paaren Kategorie 5/5e/6 für 100 Mbps Kabel mit 4 Paaren **Hinweis** Die Kabel haben 4 Drahtpaare für insgesamt 8 Leiter.
Abstandsanforderungen	Die Ethernet-Spezifikation setzt voraus, dass die maximale Kabellänge zwischen dem Konferenztelefon und dem Switch 100 Meter (330 Fuß) beträgt.

Weitere Informationen finden Sie im *Datenblatt für das Cisco IP-Konferenztelefon 7832*: http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7800-series/datasheet-listing.html

Kabelspezifikationen

- RJ-45-Buchse für die LAN 10/100BaseT-Verbindung.

Stromversorgung des Telefons

Cisco IP-Konferenztelefon kann folgende Stromquellen verwenden:

- Power over Ethernet (PoE)
- PoE-Midspan-Kabel und Cisco Power Cube 3 für Cisco IP-Konferenztelefon 7832
- Power Injector für Cisco IP-Telefone

Hinweis Das Midspan-Kabel ist derzeit nicht verfügbar.

Tabelle 7: Richtlinien zur Stromversorgung des Cisco IP-Konferenztelefon

Energietyp	Richtlinien
PoE-Energie: Wird von einem Switch über das Ethernet-Kabel am Telefon bereitgestellt.	Um den ununterbrochenen Betrieb des Telefons sicherzustellen, muss der Switch über eine Notstromversorgung verfügen. Stellen Sie sicher, dass die CatOS- oder IOS-Version, die auf dem Switch ausgeführt wird, Ihre beabsichtigte Telefonbereitstellung unterstützt. Informationen zur Betriebssystemversion finden Sie in der Dokumentation für den Switch.
Externe Stromversorgung: Über PoE Midspan-Kabel und Cisco Power Cube 3 für das Cisco IP-Konferenztelefon 7832.	Das Midspan-Kabel und der Power Cube versorgen das Ethernet-Kabel mit Strom. Wenn Sie ein Telefon installieren, das über den Midspan-Adapter betrieben wird, schließen Sie den Adapter an die Stromversorgung an, bevor Sie das Ethernet-Kabel mit dem Telefon verbinden. Wenn Sie ein Telefon entfernen, das den Midspan-Adapter verwendet, trennen Sie das Ethernet-Kabel vom Telefon, bevor Sie den Adapter von der Stromversorgung trennen.
Externe Stromversorgung: Erfolgt über den Power Injector für Cisco IP-Telefone.	Der Power Injector versorgt das Ethernet-Kabel mit Strom. Wenn Sie ein Telefon installieren, das über den Power Injector betrieben wird, verbinden Sie den Injector mit der Stromversorgung, bevor Sie das Ethernet-Kabel mit dem Telefon verbinden. Wenn Sie ein Telefon entfernen, das den Injector verwendet, trennen Sie das Ethernet-Kabel vom Telefon, bevor Sie den Injector von der Stromversorgung trennen.

Stromausfall

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

Senkung des Stromverbrauchs

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

Energiesparmodus

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

Power Save Plus (EnergyWise)

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

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

Verwandte Themen

Energiesparmodus für Cisco IP-Telefon planen, auf Seite 94
EnergyWise für das Cisco IP-Telefon planen, auf Seite 95

Unterstützte Netzwerkprotokolle

Cisco IP-Konferenztelefone unterstützen mehrere Protokolle nach Branchenstandard sowie Cisco-Netzwerkprotokolle, die für die Sprachkommunikation erforderlich sind. Die folgende Tabelle enthält eine Übersicht der Netzwerkprotokolle, die von den Telefonen unterstützt werden.

Tabelle 8: Auf Cisco IP Conference Phone unterstützte Netzwerkprotokolle

Netzwerkprotokoll	Zweck	Hinweis zur Verwendung
Bootstrap Protocol (BootP)	BootP ermöglicht einem Netzwerkgerät, wie dem Telefon, bestimmte Startinformationen zu erkennen, wie z. B. die IP-Adresse.	—
Cisco Discovery Protocol (CDP)	CDP ist ein Protokoll für die Geräteerkennung, das auf allen Geräten von Cisco ausgeführt wird. Ein Gerät kann CDP verwenden, um sich für andere Geräte anzukündigen und Informationen über diese Geräte im Netzwerk zu empfangen.	Das Telefon verwendet CDP, um Informationen, beispielsweise eine zusätzliche VLAN-ID, Details zur Energieverwaltung pro Port und QoS-Konfigurationsinformationen, mit dem Cisco Catalyst-Switch zu übertragen.

Netzwerkprotokoll	Zweck	Hinweis zur Verwendung
Dynamic Host Configuration Protocol (DHCP)	DHCP reserviert und weist IP-Adressen zu Netzwerkgeräten zu. 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.	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. 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 zur DHCP-Konfiguration finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager. **Hinweis** Wenn Sie die Option 150 nicht verwenden können, verwenden Sie die DHCP-Option 66.
Hypertext Transfer Protocol (HTTP)	HTTP ist das Standardprotokoll zum Übertragen von Informationen und Dokumenten im Internet.	Die Telefone nutzen HTTP für XML-Dienste, Bereitstellungen, Upgrades 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.	Für Webanwendungen, die HTTP und HTTPS unterstützen, sind zwei URLs konfiguriert. Telefone, die HTTPS unterstützen, wählen die HTTPS-URL. Ein Schloss-Symbol zeigt an, ob die Verbindung mit dem Service über HTTPS hergestellt wird.
IEEE 802.1X	Der IEEE 802.1X-Standard definiert ein Client-/Server-basiertes Zugriffssteuerungs- und Authentifizierungsprotokoll, das verhindert, dass sich nicht autorisierte Clients über öffentliche Ports mit einem LAN verbinden. Bis der Client authentifiziert ist, erlaubt die 802.1X-Zugriffssteuerung nur den EAPOL-Verkehr (Extensible Authentication Protocol over LAN) über den Port, mit dem der Client verbunden ist. Nach der erfolgreichen Authentifizierung kann der normale Verkehr über den Port weitergeleitet werden.	Das Telefon implementiert den IEEE 802.1X-Standard durch Unterstützung der folgenden Authentifizierungsmethoden: EAP-FAST und EAP-TLS. Wenn die 802.1X-Authentifizierung auf dem Telefon aktiviert ist, sollten Sie das Sprach-VLAN deaktivieren.

Netzwerkprotokoll	Zweck	Hinweis zur Verwendung
Internet Protocol (IP)	IP ist ein Messaging-Protokoll, das Pakete im Netzwerk verarbeitet und sendet.	Um mit IP zu kommunizieren, muss Geräten eine IP-Adresse, ein Subnetz und ein Gateway zugewiesen sein. IP-Adressen-, Subnetz- und Gateway-IDs werden automatisch zugewiesen, wenn Sie für das Telefon DHCP (Dynamic Host Configuration Protocol) nutzen. Wenn Sie DHCP nicht verwenden, müssen Sie diese Eigenschaften jedem Telefon manuell zuweisen. Die Telefone unterstützen IPv6-Adressen. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.
Link Layer Discovery Protocol (LLDP)	LLDP ist ein standardisiertes Netzwerkerkennungsprotokoll (ähnlich wie CDP), das auf einigen Geräten von Cisco und Drittanbietern unterstützt wird.	Das Telefon unterstützt LLDP auf dem PC-Port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED ist eine Erweiterung des LLDP-Standard, der für Sprachprodukte entwickelt wurde.	Das Telefon unterstützt LLDP-MED auf dem SW-Port, um u. a. folgende Informationen zu übertragen: • Sprach-VLAN-Konfiguration • Geräteerkennung • Energieverwaltung • Bestandsverwaltung 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.html
Real-Time Transport Protocol (RTP)	RTP ist ein Standardprotokoll für die Übermittlung von Echtzeit-Daten, beispielsweise interaktive Sprache und Videos, über Datennetzwerke.	Die Telefone verwenden das RTP-Protokoll zum Senden und Empfangen von Echtzeit-Sprachdatenverkehr an bzw. von anderen Telefonen und Gateways.
Real-Time Control Protocol (RTCP)	RTCP stellt zusammen mit RTP die QoS-Daten (beispielsweise Jitter, Latenz und Roundtrip-Verzögerung) auf RTP-Streams bereit.	RTCP ist standardmäßig aktiviert.

Netzwerkprotokoll	Zweck	Hinweis 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 abzubrechen.	Wie andere VoIP-Protokolle ist SIP ausgelegt, um die Signalisierungsfunktionen und Sitzungsverwaltung in einem Telefonienetzwerk zu verarbeiten. Die Signalisierung ermöglicht, dass Anrufinformationen netzwerkübergreifend übermittelt werden. Die Sitzungsverwaltung ermöglicht das Steuern der Attribute eines durchgehenden Anrufs. Cisco IP Phones unterstützen das SIP-Protokoll sowohl beim Betrieb im reinen IPv6-Modus und im reinen IPv4-Modus als auch im kombinierten IPv4-/IPv6-Modus.
Secure Real-Time Transfer Protocol (SRTP)	SRTP ist eine Erweiterung des RTP Audio-/Videoprofils und stellt die Integrität von RTP- und RTCP-Paketen über Authentifizierung, Integrität und Verschlüsselung der Medienpakete zwischen zwei Endpunkten sicher.	Die Telefone verwenden SRTP zur Medienverschlüsselung.
Transmission Control Protocol (TCP)	TCP ist ein verbindungsorientiertes Transportprotokoll.	Die Telefone 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.	Bei implementierter Sicherheit verwenden die Telefone das TLS-Protokoll für die sichere Registrierung mit dem Cisco Unified Communications Manager. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP ermöglicht die Dateiübertragung über das Netzwerk. Auf dem Telefon ermöglicht TFPT das Abrufen einer für den Telefontyp spezifischen Konfigurationsdatei.	TFTP erfordert einen TFTP-Server im Netzwerk, der vom DHCP-Server automatisch erkannt werden kann. Wenn ein Telefon einen anderen TFTP-Server, als den vom DHCP-Server angegebenen, verwenden soll, müssen Sie die IP-Adresse des TFTP-Servers über das Menü Netzwerkkonfiguration auf dem Telefon manuell 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.	Die Telefone senden und empfangen RTP-Streams, die UDP nutzen.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Cisco Unified Communications Manager-Interaktion

Cisco Unified Communications Manager ist ein offenes Anrufverarbeitungssystem, das dem Industriestandard entspricht. Die Cisco Unified Communications Manager-Software startet und bricht Anrufe zwischen Telefonen

ab, indem herkömmliche PBX-Funktionen im IP-Firmennetzwerk integriert werden. Cisco Unified Communications Manager verwaltet die Komponenten des Telefonie-Systems, beispielsweise die Telefone, die Gateways für den Zugriff und die für Funktionen erforderlichen Ressourcen, beispielsweise Konferenzanrufe und Routenplanung. Cisco Unified Communications Manager stellt auch Folgendes bereit:

- Firmware für Telefone
- Certificate Trust List-(CTL-) und Identity Trust List-(ITL-)Dateien, die TFTP- und HTTP-Dienste verwenden
- Telefonregistrierung
- Der Anruf wird beibehalten, damit eine Mediensitzung fortgesetzt wird, wenn das Signal zwischen 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 10

Cisco Unified Communications Manager Express-Interaktion

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

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

Die Telefone bieten keine Unterstützung für folgende Aktionen:

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

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

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

Interaktion mit dem Sprachnachrichtensystem

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

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

Sie müssen jedem Benutzer folgende Informationen zur Verfügung stellen:

- Wie der Zugriff auf das Konto des Sprachnachrichtensystems erfolgt.

  Stellen Sie sicher, dass die Taste „Nachrichten“ auf dem Cisco IP-Telefon in Cisco Unified Communications Manager konfiguriert wurde.

- Wie das Initialkennwort für den Zugriff auf das Sprachnachrichtensystem lautet.

  Konfigurieren Sie für das Sprachnachrichtensystem ein Standardkennwort für alle Benutzer.

- Wie das Telefon anzeigt, dass Sprachnachrichten vorhanden sind.

  Verwenden Sie Cisco Unified Communications Manager, um eine Nachrichtenanzeigemethode (MWI) einzurichten.

Konfigurationsdateien für Telefone

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

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

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

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

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

Verhalten des Telefons bei Netzwerküberlastung

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

- Verwaltungsaufgaben, beispielsweise die Überprüfung von internen Anschlüssen oder der Sicherheit
- Netzwerkangriffe, beispielsweise ein Denial-of-Service-Angriff

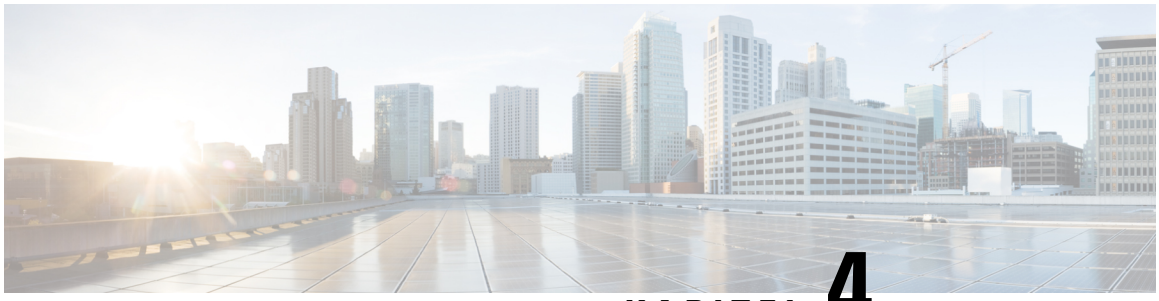
Application Programming Interface

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

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

TEIL II

Installation des Telefons



KAPITEL 4

Cisco IP-Konferenztelefon – Installation

Netzwerkkonfiguration überprüfen

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

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

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 10

Aktivierungscode-Integration für lokale Telefone

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

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

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

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

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

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

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

Vorhandene Telefone zurücksetzen, nachdem Sie für die Integration des Aktivierungscodes konfiguriert wurden. Sie werden erst registriert, wenn der Aktivierungscode eingegeben und der MIC des Telefons verifiziert

wurde. Informieren Sie die aktuellen Benutzer darüber, dass Sie zur Integration des Aktivierungscodes wechseln, bevor Sie diese Methode implementieren.

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

Aktivierungscode-Integration mit mobilem und Remotezugriff

Sie können die Aktivierungscode-Integration mit mobilem und Remotezugriff bei der Bereitstellung von Cisco IP-Telefons 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 Aktivierungscodes 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 Aktivierungcode-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 automatischer 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 ein TAPS-Verzeichnisnummer und folgenden 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 automatischen 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**.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Installation des Konferenztelefons

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

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

Vorbereitungen

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

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

Prozedur

Schritt 1 Wählen Sie die Stromquelle für das Telefon aus:

- Power over Ethernet (PoE)
- Power Injector für das Cisco Unified IP-Telefon

Weitere Informationen finden Sie unter Ihr Konferenztelefon mit Energie versorgen , auf Seite 30.

Schritt 2 Schließen Sie das Telefon am Switch an.

- Wenn Sie PoE verwenden, schließen Sie das Ethernet-Kabel an den LAN-Port und das andere Ende an das Telefon an.
- Wenn Sie den Power Injector für das Cisco Unified IP-Telefon verwenden, schließen Sie den Injector mit einem Ethernet-Kabel an den LAN-Port an. Verbinden Sie das Netzkabel mit dem Injector und

schließen Sie das Kabel an die Steckdose an. Verwenden Sie ein weiteres Ethernet-Kabel, um den Injector mit dem Konferenztelefon zu verbinden.

Jedes Telefon wird mit einem Ethernet-Kabel geliefert.

Schritt 3 Überwachen Sie den Startprozess des Telefons. Dieser Schritt stellt sicher, dass das Telefon richtig konfiguriert ist.

Schritt 4 Wenn Sie die automatische Registrierung nicht verwenden, konfigurieren Sie die Sicherheitseinstellungen auf dem Telefon manuell.

Siehe Konfigurieren der Sicherheitseinstellungen, auf Seite 67.

Schritt 5 Lassen Sie zu, dass das Telefon auf das aktuelle Firmware-Image aktualisiert wird, das auf Ihrem Cisco Unified Communications Manager gespeichert ist.

Schritt 6 Tätigen Sie mit dem Telefon Anrufe, um sicherzustellen, dass das Telefon richtig funktioniert.

Schritt 7 Informieren Sie die Benutzer über die Verwendung der Telefone und die Konfiguration der Telefonoptionen. Dieser Schritt stellt sicher, dass die Benutzer hinreichend informiert sind, um ihr Cisco IP-Telefon richtig zu nutzen.

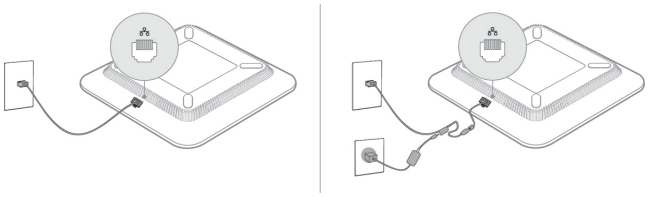
Ihr Konferenztelefon mit Energie versorgen

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

- PoE (Power over Ethernet) des Netzwerks
- Power Injector für Cisco IP-Telefone.
- Ein PoE-Netzkabel und Power Cube 3

Die folgende Abbildung zeigt die PoE- und nicht-PoE-fähigen Kabeloptionen.

Abbildung 2: Energieoptionen für das Konferenztelefon



Telefone über Menüs konfigurieren

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

Das Telefon umfasst die folgenden Konfigurationsmenüs:

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

- IPv6-Konfiguration: Dieses Untermenü enthält weitere Netzwerkoptionen.

- Sicherheitsoptionen: Enthält Optionen zum Anzeigen und Konfigurieren verschiedener Sicherheitseinstellungen.

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

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

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

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

Prozedur

Schritt 1 Drücken Sie **Anwendungen** .

Schritt 2 Drücken Sie **Einstellungen**.

Schritt 3 Wählen Sie **Administratoreinstellungen** aus.

Schritt 4 Geben Sie gegebenenfalls das Kennwort ein und klicken Sie auf **Anmelden**.

Schritt 5 Wählen Sie **Netzwerk-Setup** oder **Sicherheits-Setup** aus.

Schritt 6 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 7 Um ein Untermenü anzuzeigen, wiederholen Sie Schritt 5.

Schritt 8 Um das Menü zu schließen, drücken Sie **Zurück**.

Verwandte Themen

Konferenztelefon neu starten oder zurücksetzen, auf Seite 147
Netzwerkeinstellungen konfigurieren, auf Seite 33
Konfigurieren der Sicherheitseinstellungen, auf Seite 67

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 auf dem Telefon

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

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

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

Verwandte Themen

Konferenztelefon neu starten oder zurücksetzen, auf Seite 147
Anwenden eines Telefonkennworts, auf Seite 32

Netzwerkeinstellungen konfigurieren

Prozedur

Schritt 1 Drücken Sie **Einstellungen**.

Schritt 2 Wählen Sie **Administratoreinstellungen** > **Netzwerk-Setup**.

Schritt 3 Legen Sie die Felder fest, wie in Felder für das Netzwerk-Setup, auf Seite 33 beschrieben.
Nachdem Sie die Felder festgelegt haben, müssen Sie das Telefon möglicherweise neu starten.

Felder für das Netzwerk-Setup

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

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

Tabelle 9: Menü „Netzwerk-Setup“

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

Eintrag	Typ	Standard	Beschreibung
SW-Portkonfiguration	Autom. aushandeln 10 Halb 10 Voll 100 Halb 100 Voll	Autom. aushandeln	Geschwindigkeit und Duplex-Status des Switch-Ports: • 10 Halb = 10-BaseT/Halbduplex • 10 Voll = 10-BaseT/Vollduplex • 100 Halb = 100-BaseT/Halbduplex • 100 Voll = 100-BaseT/Vollduplex
LLDP-MED: SW-Port	Deaktiviert Aktiviert	Aktiviert	Gibt an, ob LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) auf dem Switch-Port aktiviert ist.

Tabelle 10: IPv4-Setup (Untermenü)

Eintrag	Typ	Standard	Beschreibung
DHCP	Deaktiviert Aktiviert	Aktiviert	Aktiviert oder deaktiviert die Verwendung von DHCP.
IP-Adresse			IP-Adresse (IPv4) des Telefons Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
Subnetzmaske			Die vom Telefon verwendete Subnetzmaske. Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
Standardrouter 1			Der vom Telefon verwendete Standardrouter. Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
DNS-Server 1			Vom Telefon verwendeter primärer DNS-Server (Domain Name System) (DNS-Server 1) Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
Alternativer TFTP-Server	Nein Ja	Nein	Gibt an, ob das Telefon einen alternativen TFTP-Server verwendet.

Eintrag	Typ	Standard	Beschreibung
TFTP-Server 1			Der vom Telefon verwendete primäre TFTP-Server (Trivial File Transfer Protocol). Wenn die Option „Alternativer TFTP-Server“ auf „Ein“ gesetzt ist, müssen Sie für die Option „TFTP-Server 1“ einen Wert ungleich null eingeben. Wenn weder der primäre TFTP-Server noch der Backup-TFTP-Server in der CTL- oder ITL-Datei auf dem Telefon aufgeführt ist, müssen Sie die Datei entsperren, bevor Sie Änderungen an der Option „TFTP-Server 1“ speichern können. In diesem Fall löscht das Telefon die Datei, wenn Sie Änderungen an der Option „TFTP-Server 1“ speichern. Von der Adresse des neuen TFTP-Servers 1 wird eine neue CTL- oder ITL-Datei heruntergeladen. Weitere Informationen finden Sie in den Hinweisen zu TFTP nach der letzten Tabelle.
TFTP Server 2			Vom Telefon verwendeter sekundärer TFTP-Server. Wenn weder der primäre TFTP-Server noch der Backup-TFTP-Server in der CTL- oder ITL-Datei auf dem Telefon aufgeführt ist, müssen Sie die Datei entsperren, bevor Sie Änderungen an der Option „TFTP-Server 2“ speichern können. In diesem Fall löscht das Telefon die Datei, wenn Sie Änderungen an der Option „TFTP-Server 2“ speichern. Von der Adresse des neuen TFTP-Servers 2 wird eine neue CTL- oder ITL-Datei heruntergeladen. Weitere Informationen finden Sie im Abschnitt mit Hinweisen zu TFTP nach der letzten Tabelle.
DHCP-Adressfreigabe	Nein Ja	Nein	

Tabelle 11: IPv6-Setup (Untermenü)

Eintrag	Typ	Standard	Beschreibung
DHCPv6 aktiviert	Deaktiviert Aktiviert	Aktiviert	Aktiviert oder deaktiviert die Verwendung von IPv6 DHCP.
IPv6-Adresse			Die IPv6-Adresse des Telefons. Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
Länge des IPv6-Präfixes			Länge der IPv6-Adresse. Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
IPv6 - Standardrouter 1			Standard-IPv6-Router. Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
IPv6 – DNS-Server 1			Primärer IPv6-DNS-Server Deaktivieren Sie DHCP, um dieses Feld ändern zu können.
IPv6 – Alternativer TFTP-Server	Nein Ja	Nein	Gibt an, ob das Telefon einen alternativen IPv6-TFTP-Server verwendet.
IPv6 – TFTP-Server 1			Der vom Telefon verwendete primäre IPv6-TFTP-Server. Weitere Informationen finden Sie im Abschnitt mit Hinweisen zu TFTP nach dieser Tabelle.
IPv6 – TFTP-Server 2			Der vom Telefon verwendete sekundäre IPv6-TFTP-Server. Weitere Informationen finden Sie im Abschnitt mit Hinweisen zu TFTP nach dieser Tabelle.
IPv6-Adresse freigegeben	Nein Ja	Nein	

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

- IP-Adressierungsmodus
- IP-Adressierungsmodus – Signalisierungsvoreinstellung

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

Weitere Informationen zu IPv6 finden Sie unter:

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

Hinweise zu TFTP

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

1. Manuell zugewiesene IPv4-TFTP-Server
2. Manuell zugewiesene IPv6-TFTP-Server
3. Durch DHCP zugewiesene TFTP-Server
4. Durch DHCPv6 zugewiesene TFTP-Server

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

Telefonstart überprüfen

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

Prozedur

Schließen Sie das Telefon an eine Stromquelle an.

Wenn der Hauptbildschirm angezeigt wird, wurde es ordnungsgemäß gestartet.

Telefonmodell eines Benutzers ändern

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

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

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

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

Das Telefon wird nach der Konfiguration neu gestartet.

Vorbereitungen

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

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

Prozedur

Schritt 1 Schalten Sie das alte Telefon aus.

Schritt 2 Schalten Sie das neue Telefon ein.

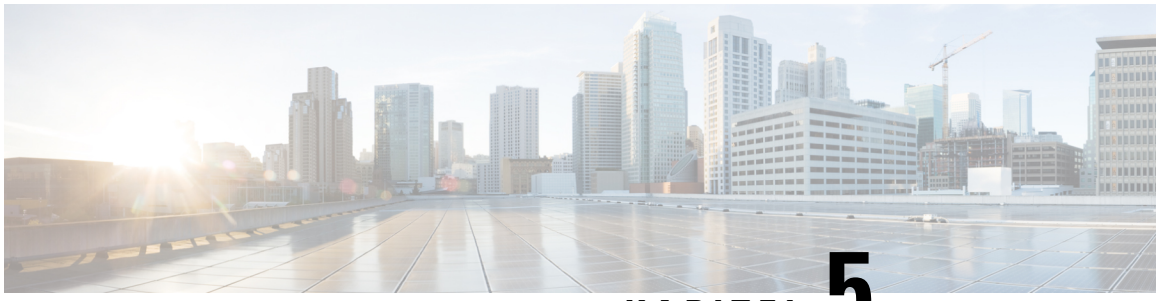
Schritt 3 Wählen Sie auf dem neuen Telefon **Vorhandenes Telefon ersetzen** aus.

Schritt 4 Geben Sie den Hauptanschluss des alten Telefons ein.

Schritt 5 Wenn dem alten Telefon eine PIN zugewiesen wurde, geben Sie diese PIN ein.

Schritt 6 Drücken Sie **Senden**.

Schritt 7 Wenn für den Benutzer mehrere Geräte vorhanden sind, wählen Sie das zu ersetzende Gerät aus, und drücken Sie **Weiter**.



KAPITEL 5

Cisco Unified Communications Manager – Telefoninstallation

Cisco IP-Konferenztelefon einrichten

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

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

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

Prozedur

Schritt 1 Stellen Sie die folgenden Telefoninformationen zusammen:

- Telefonmodell
- MAC-Adresse: Siehe Die MAC-Adresse des Telefons bestimmen, auf Seite 44
- Physischer Standort des Telefons
- Name oder Benutzer-ID des Telefonbenutzers
- Gerätepool

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

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

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

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

Schritt 3 Definieren Sie die Gerätepools. Wählen Sie **System** > **Gerätepool** aus.

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

Schritt 4 Definieren Sie das allgemeine Telefonprofil. Wählen Sie **Gerät** > **Geräteeinstellungen** > **Allgemeines Telefonprofil** aus.

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

Schritt 5 Definieren Sie einen Anrufsuchraum. Klicken Sie in der Cisco Unified Communications Manager-Verwaltung auf **Anrufumleitung** > **Steuerungsklasse** > **Anrufsuchraum**.

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

Schritt 6 Konfigurieren Sie ein Sicherheitsprofil für den Gerätetyp und das Protokoll. Wählen Sie **System** > **Sicherheit** > **Telefonsicherheitsprofil** aus.

Schritt 7 Konfigurieren Sie das Telefon. Wählen Sie **Gerät** > **Telefon**.

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

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

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

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

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

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

d) Aktivieren Sie im Bereich Anschlussinformationen das Kontrollkästchen Anschlussmobilität aktivieren, wenn das Telefon die Cisco Anschlussmobilität unterstützt.

e) Klicken Sie auf **Speichern**.

Schritt 8 Wählen Sie **Gerät** > **Geräteeinstellungen** > **SIP-Profil** aus, um SIP-Parameter zu konfigurieren.

Schritt 9 Wählen Sie **Gerät** > **Telefon** aus, um Verzeichnisnummern (Leitungen) auf dem Telefon zu konfigurieren, indem Sie die erforderlichen Felder im Fenster Verzeichnisnummernkonfiguration ausfüllen.

a) Suchen Sie das Telefon.

b) Klicken Sie im Fenster „Telefonkonfiguration“ auf „Leitung 1“ im linken Fensterbereich.

Konferenztelefone haben nur eine Leitung.

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

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

d) Wählen Sie in der Dropdown-Liste „Routenpartition“ die Partition aus, zu der die Verzeichnisnummer gehört. Wenn Sie den Zugriff auf die Verzeichnisnummer einschränken möchten, wählen Sie <Keine> für die Partition aus.

e) Wählen Sie in der Dropdown-Liste „Anrufsuchraum“ den geeigneten Anrufsuchraum aus. Der ausgewählte Wert wird für alle Geräte übernommen, die diese Verzeichnisnummer verwenden.

f) Wählen Sie in den Einstellungen für die Anrufweiterleitung und Anrufübernahme die Elemente (beispielsweise Alle weiterleiten oder Bei besetzt intern weiterleiten) und die Ziele aus, an die Anrufe gesendet werden.

Beispiel:

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

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

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

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

Beispiel:

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

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

h) Wählen Sie **Speichern** aus.

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

Schritt 10 (optional) Weisen Sie dem Benutzer ein Telefon zu. Klicken Sie auf **Benutzer zuweisen** unten im Fenster „Telefonkonfiguration“, um einen Benutzer zur Leitung zuzuweisen, die konfiguriert wird.

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

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

c) Wählen Sie **Speichern** aus.

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

Schritt 11 (optional) Weisen Sie dem Benutzer ein Gerät zu:

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

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

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

Schritt 12 Passen Sie die Softkey-Vorlagen an. Wählen Sie **Gerät** > **Geräteeinstellungen** > **Softkey-Vorlage** aus.

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

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

Schritt 13 Konfigurieren Sie die Cisco IP Phone-Services und weisen Sie Services zu. Wählen Sie **Gerät** > **Geräteeinstellungen** > **Telefonservices** aus.

Stellt IP-Telefonservices für das Telefon bereit.

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

Schritt 14 (optional) Fügen Sie Benutzerinformationen zum globalen Verzeichnis für Cisco Unified Communications Manager hinzu. Wählen Sie **Benutzerverwaltung** > **Benutzer** aus, klicken Sie auf **Neu hinzufügen** und konfigurieren Sie die erforderlichen Felder. Erforderliche Felder sind mit einem Sternchen (*) markiert.

Hinweis Wenn Ihr Unternehmen ein LDAP-Verzeichnis (Lightweight Directory Access Protocol) zum Speichern der Benutzerinformationen verwendet, können Sie Cisco Unified Communications für die Verwendung des vorhandenen LDAP-Verzeichnisses konfigurieren (siehe Konfiguration des Firmenverzeichnisses, auf Seite 111). Nachdem die Option Synchronisierung vom LDAP-Server aktivieren ausgewählt wurde, können Sie keine weiteren Benutzer über die Cisco Unified Communications Manager-Verwaltung hinzufügen.

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

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

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

Schritt 15 (optional) Weisen Sie einen Benutzer einer Benutzergruppe zu. Wählen Sie **Benutzerverwaltung** > **Benutzereinstellungen** > **Zugriffssteuerungsgruppe** aus.

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

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

Verwandte Themen

Cisco IP-Konferenztelefon – Funktionen und Einrichtung, auf Seite 75
Produktspezifische Konfiguration, auf Seite 80
Dokumentation Cisco Unified Communications Manager, auf Seite 10
Softkey-Vorlagen konfigurieren, auf Seite 76

Die MAC-Adresse des Telefons bestimmen

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

Prozedur

Führen Sie einen der folgenden Schritte aus:

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

Methoden zum Hinzufügen von Telefonen

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

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

Bevor Sie Telefone einzeln oder mit dem BAT hinzufügen, benötigen Sie die MAC-Adresse des Telefons. Weitere Informationen finden Sie unter Die MAC-Adresse des Telefons bestimmen, auf Seite 44.

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

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Einzelne Telefone hinzufügen

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

Prozedur

Schritt 1 Wählen Sie **Gerät** > **Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.

Schritt 2 Klicken Sie auf **Neu hinzufügen**.

Schritt 3 Wählen Sie den Telefontyp aus.

Schritt 4 Wählen Sie **Weiter** aus.

Schritt 5 Vervollständigen Sie die Informationen über das Telefon, einschließlich die MAC-Adresse.

Die vollständigen Anweisungen und weitere Informationen zu Cisco Unified Communications Manager finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Schritt 6 Wählen Sie **Speichern** aus.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

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 10

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 47.

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 10

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 nicht, dass die Benutzer-ID geändert wird, nachdem sie erstellt wurde. 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.

Benutzern Telefone zuweisen

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

Prozedur

Schritt 1 Wählen Sie **Benutzerverwaltung** > **Endbenutzer** in der Cisco Unified Communications Manager-Verwaltung aus.

Das Fenster Benutzer suchen und auflisten wird angezeigt.

Schritt 2 Geben Sie die Suchkriterien ein und klicken Sie auf **Suchen**.

Schritt 3 Wählen Sie in der angezeigten Eintragsliste den Link für den Benutzer aus.

Schritt 4 Wählen Sie **Gerätezuordnung** aus.

Das Fenster Benutzergerätezuordnung wird geöffnet.

Schritt 5 Geben Sie die Suchkriterien ein und klicken Sie auf **Suchen**.

Schritt 6 Wählen Sie das Gerät aus, das Sie dem Benutzer zuweisen möchten, indem Sie das Kontrollkästchen links neben dem Gerät aktivieren.

Schritt 7 Wählen Sie **Auswahl/Änderungen speichern** aus, um dem Benutzer das Gerät zuzuweisen.

Schritt 8 Wählen Sie in der Dropdown-Liste Ähnliche Links in der oberen rechten Fensterecke die Option **Zurück zum Benutzer** aus und klicken Sie auf **Los**.

Das Fenster Benutzerkonfiguration wird angezeigt und die zugewiesenen Geräte, die Sie ausgewählt haben, werden unter Gesteuerte Geräte aufgelistet.

Schritt 9 Wählen Sie **Auswahl/Änderungen speichern** aus.

SRST (Survivable Remote Site Telephony)

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

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

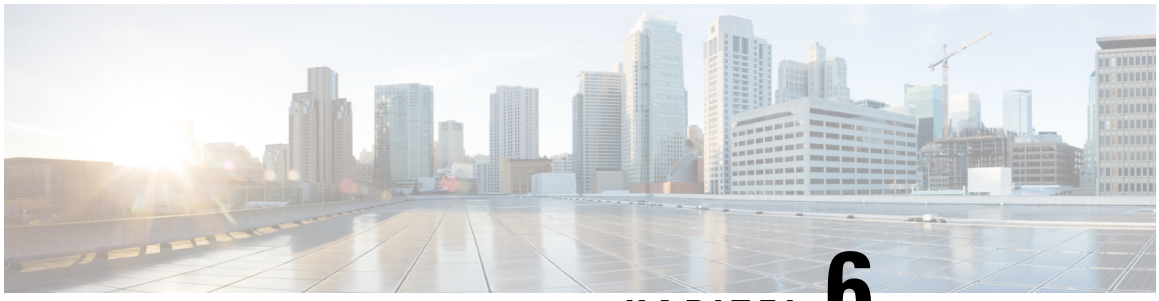
In der folgenden Tabelle ist die Verfügbarkeit der Funktionen während eines Failovers angegeben.

Tabelle 12: Unterstützte SRST-Funktionen

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

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

Funktion	Unterstützt	Hinweise
Mobilität	Nein	Der Softkey wird nicht angezeigt.
Privatfunktion	Nein	Der Softkey wird nicht angezeigt.
Rückruf	Nein	Der Softkey Rückruf wird nicht angezeigt.
Service-URL	Ja	Die programmierbare Leitungstaste mit der zugewiesenen Dienst-URL wird nicht angezeigt.



KAPITEL 6

Verwaltung des Selbstservice-Portals

Übersicht des Selbstservice-Portals

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 Selbstservice-Portal zugreifen kann, müssen Sie in der Cisco Unified Communications Manager-Verwaltung den Benutzer zu einer Standardbenutzergruppe in Cisco Unified Communications Manager 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 10

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 **Benutzerverwaltung** > **Endbenutzer** in der Cisco Unified Communications Manager-Verwaltung 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

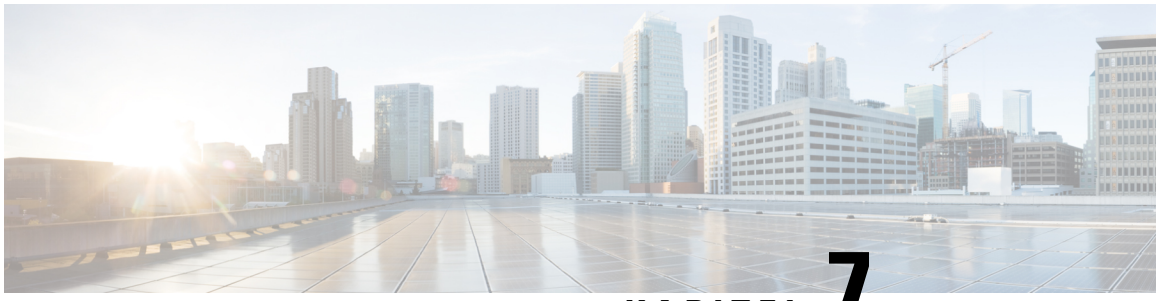
Hinweis Die Einstellungen gelten für alle Seiten des Selbstservice-Portals an Ihrem Standort.

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

Administration des Telefons



KAPITEL 7

Cisco IP-Konferenztelefon – Sicherheit

Übersicht der Sicherheit des Cisco IP-Telefon

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

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

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

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

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

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

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

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

Das Cisco IP-Konferenztelefon 7832 entspricht dem FIPS (Federal Information Processing Standard). Um ordnungsgemäß zu funktionieren, ist für den FIPS-Modus eine RSA-Schlüssellänge von mindestens 2048 Bit erforderlich. Wenn das RSA-Serverzertifikat nicht 2048 Bit oder mehr umfasst, wird das Telefon nicht beim Cisco Unified Communications Manager registriert und die Meldung `Telefon konnte nicht registriert werden erscheint. Die Größe des Zertifikatsschlüssels ist nicht FIPS-konform.` wird auf dem Telefon angezeigt.

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

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

Verwandte Themen

Einrichten eines LSC (Locally Significant Certificate), auf Seite 68
Dokumentation Cisco Unified Communications Manager, auf Seite 10

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 ManagerVersion 14.0 (1) SU1 oder höher und Cisco IP-Telefon-Firmware Version 14.1 (1) unterstützt. Proxy-TFTP und OAuth für Proxy-TFTP werden für Mobile Remote Access (MRA) nicht unterstützt.

Weitere Informationen zur Sicherheit finden Sie unter:

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

- *Sicherheitshandbuch für Cisco Unified Communications Manager*(https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)

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

Unterstützte Sicherheitsfunktionen

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

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

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

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

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

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

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

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

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

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

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

Die folgende Tabelle enthält eine Übersicht der Sicherheitsfunktionen, die von Cisco IP-Konferenztelefon 7832 unterstützt werden. Weitere Informationen zu diesen Funktionen und zur Sicherheit von Cisco Unified Communications Manager und Cisco IP-Telefon finden Sie in der Dokumentation zu Ihrer Version von Cisco Unified Communications Manager.

Tabelle 13: Überblick der Sicherheitsfunktionen

Funktion	Beschreibung
Imageauthentifizierung	Signierte Binärdateien (mit der Erweiterung SBN) verhindern Manipulationen des Firmware-Images, bevor es auf ein Telefon geladen wird. Wenn das Image manipuliert wurde, kann das Telefon nicht authentifiziert werden und das Image wird abgelehnt.
Installation des Zertifikats am Kundenstandort	Für jedes Telefon ist zur Geräteauthentifizierung ein eindeutiges Zertifikat erforderlich. Die Telefone enthalten ein MIC (Manufacturing Installed Certificate), aber für zusätzliche Sicherheit können Sie in Cisco Unified Communications Manager Administration angeben, dass ein Zertifikat über die CAPF (Certificate Authority Proxy Function) installiert werden muss. Sie können ein LSC (Locally Significant Certificate) auch über das Menü Sicherheitskonfiguration auf dem Telefon installieren.
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. Cisco Unified Communications Manager registriert Telefone nur, wenn diese von Cisco Unified Communications Manager authentifiziert werden können.

Funktion	Beschreibung
Dateiauthentifizierung	Überprüft digital signierte Dateien, die das Telefon herunterlädt. Das Telefon überprüft die Signatur, um sicherzustellen, dass die Datei, nachdem sie erstellt wurde, 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.
Signalisierungsauthentifizierung	Verwendet das TLS-Protokoll, um sicherzustellen, dass die Signalpakete während der Übermittlung nicht manipuliert wurden.
MIC (Manufacturing Installed Certificate)	Auf jedem Telefon ist ein eindeutiges, vom Hersteller installiertes Zertifikat (Manufacturing Installed Certificate, MIC) vorhanden, das für die Geräteauthentifizierung verwendet wird. Das MIC ist ein permanenter Identitätsnachweis für das Telefon und ermöglicht Cisco Unified Communications Manager, das Telefon zu authentifizieren.
Sichere SRST-Referenz	Nachdem Sie eine SRST-Referenz für die Sicherheit konfiguriert und die abhängigen Geräte in der Cisco Unified Communications Manager-Verwaltung zurückgesetzt haben, fügt der TFTP-Server das SRST-Zertifikat zur Datei cnf.xml hinzu und sendet diese Datei an das Telefon. Ein sicheres Telefon verwendet eine TLS-Verbindung, um mit dem SRST-fähigen Router zu kommunizieren.
Medienverschlüsselung	Verwendet SRTP, um sicherzustellen, dass die Medienstreams zwischen den unterstützten Geräten sicher sind und die Daten nur von den vorgesehenen Geräten empfangen und gelesen werden können. 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.
Sicherheitsprofile	Definiert, ob das Telefon nicht sicher, authentifiziert oder verschlüsselt ist.

Funktion	Beschreibung
Verschlüsselte Konfigurationsdateien	Ermöglicht Ihnen, den Datenschutz für Telefonkonfigurationsdateien sicherzustellen.
Die Webserverfunktionalität für ein Telefon deaktivieren	Sie können den Zugriff auf eine Telefon-Webseite verhindern, auf der verschiedene Statistiken für ein Telefon angezeigt werden.
Telefonhärtung	Weitere Sicherheitsoptionen, die in der Cisco Unified Communications Manager-Verwaltung festgelegt werden: • Zugriff auf die Webseiten für ein Telefon deaktivieren **Hinweis** Sie können die aktuellen Einstellungen für die Optionen „GARP aktiviert“ und „Sprach-VLAN aktiviert“ im Telefonkonfigurationsmenü anzeigen.
802.1X-Authentifizierung	Das Telefon kann die 802.1X-Authentifizierung verwenden, um den Zugriff auf das Netzwerk anzufordern und zu erhalten.
AES 256-Verschlüsselung	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 neuen Schlüssel: • Für TLS-Verbindungen: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • Für sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM Weitere Informationen finden Sie in der Dokumentation zu Cisco Unified Communications Manager.

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 VOS-Produkte (Voice Operating System) ab der Version 11.5 von Cisco Unified Communications Manager.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

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

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

- Geschütztes Gerät: Um den Status eines sicheren Telefons in „Geschützt“ zu ändern, aktivieren Sie das Kontrollkästchen „Geschütztes Gerät“ im Fenster „Telefonkonfiguration“ in Cisco Unified Communications Manager Administration (**Gerät** > **Telefon**).
- Sicherheitssignal ausgeben: Damit das geschützte Telefon ein Signal ausgibt, das angibt, ob der Anruf sicher oder nicht sicher ist, legen Sie die Einstellung Sicherheitssignal ausgeben auf True fest. Die Einstellung Sicherheitssignal ausgeben ist standardmäßig auf False festgelegt. Sie legen diese Option in der Cisco Unified Communications Manager-Verwaltung fest (**System** > **Serviceparameter**). Wählen Sie den Server und anschließend den Unified Communications Manager-Service aus. Wählen Sie im

Fenster Serviceparameterkonfiguration die Option unter Funktion - Sicherheitssignal aus. Der Standardwert ist False.

Sichere 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 14: 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 `Sicherheitsstufe nicht erfüllt, Anruf abgelehnt.`

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

Sichere Anruf-ID

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

Ein sicherer Anruf wird mit diesem Prozess initiiert:

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

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

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

Geschützte Telefone spielen unter folgenden Umständen einen Signalton ab:

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

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

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 Paramater zu bestimmen, beispielsweise die VLAN-Zuweisung und Inline-Energieanforderungen.

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

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

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

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

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Die aktuellen Sicherheitsfunktionen auf dem Telefon anzeigen

Weitere Informationen zu den Sicherheitsfunktionen und zur Sicherheit von Cisco Unified Communications Manager und des Cisco IP-Telefon, finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Prozedur

Schritt 1 Wählen Sie **Einstellungen** aus.

Schritt 2 Wählen Sie **Administratoreinstellungen** > **Sicherheitskonfiguration** aus.

Die meisten Sicherheitsfunktionen sind nur verfügbar, wenn eine Zertifikatvertrauensliste (CTL) auf dem Telefon installiert ist.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Sicherheitsprofile anzeigen

Alle Cisco IP-Telefons, die Cisco Unified Communications Manager unterstützen, verwenden ein Sicherheitsprofil, das definiert, ob das Telefon nicht geschützt, authentifiziert oder verschlüsselt ist. Weitere Informationen zum Konfigurieren des Sicherheitsprofils und das Übernehmen des Profils auf dem Telefon 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 **System** > **Sicherheit** > **Telefonsicherheitsprofil** aus.

Schritt 2 Überprüfen Sie die Einstellung „Sicherheitsmodus“.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Konfigurieren der Sicherheitseinstellungen

Prozedur

Schritt 1 Drücken Sie **Einstellungen**.

Schritt 2 Wählen Sie **Administratoreinstellungen** > **Sicherheitskonfiguration** aus.

Schritt 3 Legen Sie die Felder fest.
Nachdem Sie die Felder festgelegt haben, müssen Sie das Telefon möglicherweise neu starten.

Sicherheitskonfigurationsfelder

Das Menü „Sicherheits-Setup“ enthält Felder und Untermenüs für Vertrauenslisten und 802.1X-Authentifizierung.

Tabelle 15: Menü „Sicherheits-Setup“

Eintrag	Typ	Standard	Beschreibung
Sicherheitsmodus			Nur lesen
LSC			Siehe Einrichten eines LSC (Locally Significant Certificate), auf Seite 68.

Eintrag	Typ	Standard	Beschreibung
Vertrauensliste	Menü		Siehe die Tabelle „Untermenü Vertrauensliste“.
802.1x-Authentifiz.	Menü		Siehe die Tabelle „Untermenü 802.1X-Authentifizierung“.

Tabelle 16: Untermenü Vertrauensliste

Eintrag	Typ	Standard	Beschreibung
CTL-Datei	Menü		Zeigt eine Liste von CTL-Dateien an
ITL-Datei	Menü		Zeigt eine Liste von ITL-Dateien an
Konfiguration (signiert)	Menü		Siehe die Tabelle „Untermenü Konfiguration.“

Tabelle 17: Untermenü Konfiguration

Eintrag	Typ	Standard	Beschreibung
SRST-Router			Zeigt die IP-Adresse von SRST an.

Tabelle 18: Untermenü 802.1X-Authentifizierung

Eintrag	Typ	Standard	Beschreibung
Geräteauthentifizierung	Deaktiviert Aktiviert	Deaktiviert	
Transaktionsstatus	Untermenü		Siehe die Tabelle „Untermenü Transaktionsstatus“.

Tabelle 19: Untermenü Transaktionsstatus

Eintrag	Typ	Standard	Beschreibung
Transaktionsstatus	Getrennt Verbunden		
Protokolle			Liste von Protokollen.

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 auf dem Telefon **Einstellungen** aus.

Schritt 4 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 5 Wählen Sie **LSC** aus und drücken Sie **Auswählen** oder **Aktualisieren**.

Das Telefon fordert eine Authentifizierungszeichenfolge an.

Schritt 6 Geben Sie die Authentifizierungscode ein und drücken Sie **Senden**.

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

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

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

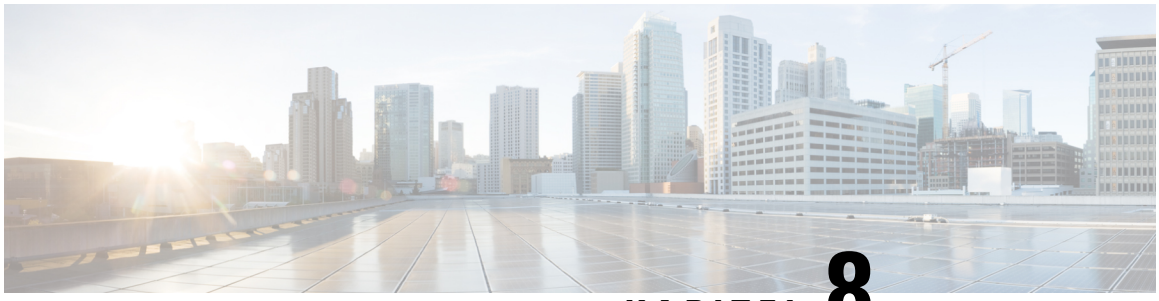
Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

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**.
Schritt 6	Starten Sie das Telefon neu.



KAPITEL 8

Cisco IP-Konferenztelefon – Anpassung

Individuelle Ruftöne

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

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

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

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Einen benutzerdefinierten Rufton konfigurieren

Prozedur

Schritt 1 Erstellen Sie für jeden benutzerdefinierten Rufton eine PCM-Datei (ein Rufton pro Datei).

Stellen Sie sicher, dass die PCM-Dateien die Formatrichtlinien einhalten, die im Abschnitt Formate benutzerdefinierter Ruftondateien aufgeführt sind.

Schritt 2 Laden Sie die neuen PCM-Dateien, die Sie erstellt haben, auf den Cisco TFTP-Server für jeden Cisco Unified Communications Manager im Cluster hoch.

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

Schritt 3 Bearbeiten Sie die Datei Ringlist-wb in einem Text-Editor.

Weitere Informationen zum Formatieren dieser Datei und eine Ringlist-wb-Beispieldatei finden Sie im Abschnitt „Formate benutzerdefinierter Ruftondateien“.

Schritt 4 Speichern Sie die Änderungen und schließen Sie die Datei Ringlist-wb.

Schritt 5 So speichern Sie die neue Ringlist.wb-Datei zwischen:

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

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Dateiformate für benutzerdefinierte Ruftöne

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

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

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

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

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

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

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

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

```
   </Ring>
</CiscoIPPhoneRingList>
```

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

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

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

Den Wählton anpassen

Sie können die Telefone so konfigurieren, das 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.

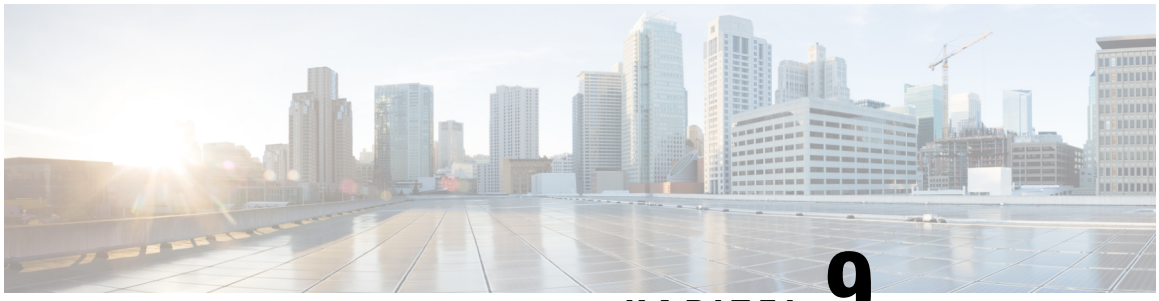
Schritt 4 Navigieren Sie zum Bereich „Clusterweite Parameter“.

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

Cisco IP-Konferenztelefon – Funktionen und Einrichtung

Benutzersupport für Cisco IP-Telefon

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

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

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

Die Webseite sollte die folgenden Informationen enthalten:

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

Direkte Migration Ihres Telefons zu einem Multiplattform-Telefon

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

Weitere Informationen hierzu finden Sie unter https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html

Softkey-Vorlagen konfigurieren

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

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

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

Prozedur

Schritt 1 Melden Sie sich als Administrator bei Cisco Unified Communications Manager Administration an.

Schritt 2 Wählen Sie **Gerät** > **Geräteeinstellungen** > **Softkey-Vorlage** aus.

Schritt 3 Klicken Sie auf **Suchen**.

Schritt 4 Wählen Sie eine der folgenden Optionen aus:

- Cisco Unified Communications Manager 11.5 und frühere Versionen: **Standardbenutzer**
- Cisco Unified Communications Manager 12.0 und neuere Versionen: **Personal Conference User (Benutzer persönliche Konferenz)** oder **Public Conference User (Benutzer öffentliche Konferenz)**.

Schritt 5 Klicken Sie auf **Kopieren**.

Schritt 6 Ändern Sie den Namen der Vorlage.

Beispiel: 7832 Konferenzraumvorlage.

Schritt 7 Klicken Sie auf **Speichern**.

Schritt 8 Navigieren Sie über das Menü oben rechts zur Seite **Softkey-Layout konfigurieren**.

Schritt 9 Legen Sie für jeden Anrufstatus fest, welche Funktionen angezeigt werden sollen.

Schritt 10 Klicken Sie auf **Speichern**.

Schritt 11 Kehren Sie über das Menü oben rechts zurück zum Bildschirm **Suchen/Liste**.

Die neue Vorlage wird in der Vorlagenliste angezeigt.

Schritt 12 Wählen Sie **Gerät** > **Telefon**.

Schritt 13 Suchen Sie das Telefon, dem Sie die neue Vorlage zuweisen möchten, und wählen Sie es aus.

Schritt 14 Wählen Sie im Feld **Softkey-Vorlage** die neue Softkey-Vorlage aus.

Schritt 15 Klicken Sie auf **Speichern** und **Konfiguration übernehmen**.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Telefonservices für Benutzer konfigurieren

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

Bevor ein Benutzer auf einen Service zugreifen kann:

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

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

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

Prozedur

Schritt 1 Wählen Sie in Cisco Unified Communications Manager-Verwaltung **Gerät** > **Geräteeinstellungen** > **Telefondienste** aus.

Schritt 2 Stellen Sie sicher, dass die Benutzer auf Self-Service-Portal für Cisco Unified Communications zugreifen können, damit sie die konfigurierten Dienste auswählen und abonnieren können.

Siehe Übersicht des Selbstservice-Portals, auf Seite 53 für eine Übersicht der Informationen, die Sie an die Benutzer weitergeben müssen.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Telefonfunktion – Konfiguration

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

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

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

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

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

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

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

Verwandte Themen

Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren, auf Seite 106

Einrichten von Telefonfunktionen für alle Telefone

Prozedur

Schritt 1	Melden Sie sich als Administrator bei 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.

Verwandte Themen

Produktspezifische Konfiguration, auf Seite 80

Einrichten von Telefonfunktionen für eine Telefongruppe

Prozedur

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

Verwandte Themen

Produktspezifische Konfiguration, auf Seite 80

Einrichten von Telefonfunktionen für ein einzelnes Telefon

Prozedur

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

Verwandte Themen

Produktspezifische Konfiguration, auf Seite 80

Produktspezifische Konfiguration

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

Tabelle 20: Felder im Bereich „Produktspezifische Konfiguration“

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Zugriff auf Einstellungen	Deaktiviert Aktiviert Eingeschränkt	Aktiviert	Aktiviert, deaktiviert oder schränkt den Zugriff auf die lokalen Konfigurationseinstellungen im Menü „Einstellungen“ ein. Mit beschränktem Zugriff kann auf die Voreinstellungen und die Statusmenüs zugegriffen werden. Bei deaktiviertem Zugriff kann auf das Statusmenü zugegriffen werden.
ARP unnötig	Deaktiviert Aktiviert	Deaktiviert	Aktiviert oder deaktiviert die Möglichkeit des Telefons, MAC-Adressen von Gratuitous ARP-Paketen zu erkennen. Diese Funktion ist erforderlich, um Sprach-Streams zu überwachen oder aufzuzeichnen.
Webzugriff	Deaktiviert Aktiviert	Deaktiviert	Aktiviert oder deaktiviert den Zugriff auf die Webseiten des Telefons über einen Webbrowser. **Vorsicht** Wenn Sie dieses Feld aktivieren, legen Sie möglicherweise vertrauliche Daten über das Telefon offen.
TLS 1.0 und TLS 1.1 für Webzugriff deaktivieren	Deaktiviert Aktiviert	Deaktiviert	Steuert die Verwendung von TLS 1.2 für eine Webserververbindung. • Deaktiviert: Ein für TLS 1.0, TLS 1.1 oder TLS 1.2 konfiguriertes Telefon kann als HTTPS-Server fungieren. • Aktiviert: Nur ein für TLS 1.2 konfiguriertes Telefon kann als HTTPS-Server fungieren.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Enbloc-Wählen	Deaktiviert Aktiviert	Deaktiviert	Steuert die Wählmethode. • Deaktiviert: Der Cisco Unified Communications Manager wartet, bis der Interdigit-Timer abläuft, wenn eine Überschneidung beim Rufnummernplan oder beim Routenmuster vorliegt. • 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. Berechtigungscodes (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.
Hintergrundbeleuchtung nicht aktiv – Tage	Tage der Woche		Definiert die Tage, an denen sich die Hintergrundbeleuchtung nicht automatisch zur im Feld „Hintergrundbeleuchtung eingeschaltet - Uhrzeit“ angegebenen Uhrzeit einschaltet. 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. Siehe Energiesparmodus für Cisco IP-Telefon planen, auf Seite 94.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Hintergrundbeleuchtung eingeschaltet – Uhrzeit	hh:mm	07:30	Definiert die Uhrzeit, an der sich die Hintergrundbeleuchtung jeden Tag automatisch einschaltet (außer an den im Feld „Hintergrundbeleuchtung nicht aktiv – Tage“ angegebenen Tagen). Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (0:00 ist Mitternacht). Um die Hintergrundbeleuchtung beispielsweise um 7:00 Uhr einzuschalten, geben Sie 07:00 ein. Um die Hintergrundbeleuchtung um 14:00 Uhr einzuschalten, geben Sie 14:00 ein. Wenn in dieses Feld nichts eingegeben wird, schaltet sich die Hintergrundbeleuchtung automatisch um 00:00 Uhr ein. Siehe Energiesparmodus für Cisco IP-Telefon planen, auf Seite 94.
Hintergrundbeleuchtung aktiv – Dauer	hh:mm	10:30	Definiert den Zeitraum, über den die Hintergrundbeleuchtung eingeschaltet bleibt, nachdem sie sich zu der im Feld „Hintergrundbeleuchtung eingeschaltet – Uhrzeit“ angegebenen Uhrzeit eingeschaltet hat. Damit die Hintergrundbeleuchtung nach der automatischen Aktivierung beispielsweise vier Stunden und 30 Minuten lang aktiviert bleibt, geben Sie 04:30 ein. Wenn in dieses Feld nichts eingegeben wird, schaltet sich der Bildschirm am Tagesende (00:00 Uhr) ab. Wenn im Feld „Hintergrundbeleuchtung eingeschaltet - Uhrzeit“ der Wert „00:00“ eingetragen und im Feld „Hintergrundbeleuchtung eingeschaltet – Dauer“ kein Wert (oder „24:00“) vorhanden ist, wird die Hintergrundbeleuchtung nicht ausgeschaltet. Siehe Energiesparmodus für Cisco IP-Telefon planen, auf Seite 94.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Hintergrundbeleuchtung – Leerlauf-Zeitlimit	hh:mm	1:00	Definiert den Zeitraum, über den das Telefon inaktiv gewesen sein muss, bevor sich die Hintergrundbeleuchtung abschaltet. Trifft nur zu, wenn die Hintergrundbeleuchtung wie geplant ausgeschaltet und vom Benutzer eingeschaltet wurde (durch das Drücken einer Taste oder das Abheben des Hörers). Wenn die Hintergrundbeleuchtung beispielsweise ausgeschaltet werden soll, wenn das Telefon nach dem Einschalten der Hintergrundbeleuchtung durch einen Benutzer 1 Stunde und 30 Minuten lang inaktiv war, geben Sie 01:30 ein. Siehe Energiesparmodus für Cisco IP-Telefon planen, auf Seite 94.
Hintergrundbeleuchtung ein bei eingehendem Anruf	Deaktiviert Aktiviert	Aktiviert	Schaltet die Hintergrundbeleuchtung ein, wenn ein Anruf eingeht.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Power Save Plus aktivieren	Tage der Woche		Definiert die Tage, an denen das Telefon deaktiviert werden soll. 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. Wenn das Feld „Power Save Plus aktivieren“ aktiv ist, erhalten Sie eine Warnmeldung aufgrund von Sicherheitsbedenken (E911-Meldung). **Vorsicht** 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. 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. Siehe EnergyWise für das Cisco IP-Telefon planen, auf Seite 95.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Telefon einschalten – Uhrzeit	hh:mm	00:00	Legt fest, wann das Telefon an den Tagen, die im Feld Power Save Plus aktivieren ausgewählt sind, automatisch eingeschaltet wird. Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (00:00 ist Mitternacht). Um das Telefon beispielsweise um 07:00 Uhr automatisch einzuschalten, geben Sie 07:00 ein. Um das Telefon um 14:00 Uhr einzuschalten, geben Sie 14:00 ein. Der Standardwert ist leer, das heißt 00:00. 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. Siehe EnergyWise für das Cisco IP-Telefon planen, auf Seite 95.
Telefon ausschalten – Uhrzeit	hh:mm	24:00	Definiert die Tageszeit, zu der das Telefon an den im Feld „Power Save Plus aktivieren“ ausgewählten Tagen deaktiviert wird. Wenn die Felder den gleichen Wert enthalten, wird das Telefon nicht ausgeschaltet. Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (00:00 ist Mitternacht). Um das Telefon beispielsweise um 07:00 Uhr auszuschalten, geben Sie 07:00 ein. Um das Telefon um 14:00 Uhr auszuschalten, geben Sie 14:00 ein. Der Standardwert ist leer, das heißt 00:00. 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. Siehe EnergyWise für das Cisco IP-Telefon planen, auf Seite 95.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Telefon ausschalten - Leerlauf-Timeout	mm	60	Gibt den Zeitraum an, für den das Telefon inaktiv gewesen sein muss, bevor es sich deaktiviert. Der Timeout tritt unter folgenden Bedingungen auf: • Wenn das Telefon, wie geplant, in den Power Save Plus-Modus gewechselt ist und eingeschaltet wurde, da der Benutzer die Taste „Auswahl“ gedrückt hat. • Wenn das Telefon vom angeschlossenen Switch wieder eingeschaltet wurde. • Wenn die Ausschaltzeit des Telefons erreicht wird, aber das Telefon verwendet wird. Siehe EnergyWise für das Cisco IP-Telefon planen, auf Seite 95.
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. Siehe EnergyWise für das Cisco IP-Telefon planen, auf Seite 95.
EnergyWise-Domäne	Bis zu 127 Zeichen		Ermittelt die EnergyWise-Domäne, in der sich das Telefon befindet. Siehe EnergyWise für das Cisco IP-Telefon planen, auf Seite 95.
EnergyWise-Secret	Bis zu 127 Zeichen		Ermittelt das Kennwort der Sicherheitsabfrage, das in der Kommunikation mit den Endgeräten in der EnergyWise-Domäne verwendet wird. Siehe EnergyWise für das Cisco IP-Telefon planen, auf Seite 95.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
EnergyWise-Überschreibung zulassen	Kontrollkästchen	Deaktiviert	Bestimmt, ob die Controller-Richtlinie der EnergyWise-Domäne aktualisierte Energiepegeldaten an die Telefone senden darf. Es gelten die folgenden Bedingungen: • Im Feld Power Save Plus aktivieren muss mindestens ein Tag ausgewählt werden. • Die Einstellungen in der Cisco Unified Communications Manager-Verwaltung werden planmäßig übernommen, auch wenn EnergyWise eine Überschreibung sendet. 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. • Wenn EnergyWise das Telefon anweist, sich um 20:00 Uhr auszuschalten, bleibt diese Anweisung bis zur festgelegten Einschaltzeit um 6:00 Uhr in Kraft. • Um 6 Uhr schaltet sich das Telefon ein und empfängt wieder die Energiepegeländerungen aus den Einstellungen in Cisco Unified Communications Manager Administration. • Um den Energiepegel auf dem Telefon erneut zu ändern, muss EnergyWise einen neuen Befehl ausgeben. 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. Siehe EnergyWise für das Cisco IP-Telefon planen, auf Seite 95.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Richtlinie für Zusammenführung und direkte Übergabe	Nur gleiche Leitung aktivieren Nur gleiche Leitung aktivieren	Nur gleiche Leitung aktivieren	Steuert die Möglichkeit eines Benutzers, Anrufen beitreten und diese zu übergeben. • Nur gleiche Leitung aktivieren: Benutzer können einen Anruf auf der aktuellen Leitung an einen Anruf auf derselben Leitung übergeben oder diesem beitreten. • Nur gleiche Leitung deaktivieren: Benutzer können keine Anrufe auf derselben Leitung übergeben oder diesen beitreten. Die Beitritts- und Übergabefunktionen sind deaktiviert, und der Benutzer kann diese Funktionen nicht verwenden.
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.
Aufzeichnungstondauer	Ganzzahl 1 bis 3000 Millisekunden		Steuert die Dauer des Aufzeichnungstons.
'Weiter'-Softkey-Zeitgeber	Ganzzahl 0,5 bis 30 Sekunden	5	Steuert, wie lange eine Zeile mit sekundären Softkeys angezeigt wird, bevor das Telefon wieder die anfängliche Gruppe von Softkeys anzeigt. Mit der Eingabe von „0“ wird der Timer deaktiviert.
Protokollserver	Zeichenfolge mit bis zu 256 Zeichen		Identifiziert den IPv4-Syslog-Server für die Debug-Ausgabe des Telefons. Das Format für die Adresse lautet: `address:<port>@@base=<0-7>;pfs=<0-1>` Siehe Debuginformationen über Cisco Unified Communications Manager verwalten, auf Seite 168.
Remote-Protokoll	Deaktiviert Aktiviert	Deaktiviert	Steuert die Möglichkeit, Protokolle an den Syslog-Server zu senden. Siehe Debuginformationen über Cisco Unified Communications Manager verwalten, auf Seite 168.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Protokollprofil	Standard Voreinstellung Telefonie SIP UI Netzwerk Medien Update Zubehörteil Sicherheit EnergyWise MobileRemoteAccess	Voreinstellung	Gibt das vordefinierte Protokollierungsprofil an. • Standard – Standard-Protokollierungsebene bei der Fehlersuche • Voreinstellung – Überschreibt nicht die lokale Einstellung für die Fehlersuchprotokollierung des Telefons. • Telefonie – Protokolliert Informationen zu den Funktionen für Telefonie oder Anrufe. • SIP – Protokolliert Informationen zu den SIP-Signalen. • UI – Protokolliert Informationen zur Benutzeroberfläche des Telefons. • Netzwerk – Protokolliert Informationen zum Netzwerk. • Medien – Protokolliert Mediendaten. • Upgrade – Protokolliert Upgrade-Informationen. • Zubehör – Protokolliert Zubehör-Informationen. • Sicherheit – Protokolliert Sicherheitsinformationen. • EnergyWise – Protokolliert Energiesparinformationen. • MobileRemoteAccess – Protokolliert Informationen zum Mobile und Remote Access über Expressway. Siehe Debuginformationen über Cisco Unified Communications Manager verwalten, auf Seite 168.
IPv6 – Protokollserver	Zeichenfolge mit bis zu 256 Zeichen		Identifiziert den IPv6-Syslog-Server für die Debug-Ausgabe des Telefons. Siehe Debuginformationen über Cisco Unified Communications Manager verwalten, auf Seite 168.
Cisco Discovery Protocol (CDP): Switchport	Deaktiviert Aktiviert	Aktiviert	Steuert das CDP (Cisco Discovery Protocol) auf dem Telefon.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Link Layer Discovery Protocol – Media Endpoint Discover (LLDP-MED): Switchport	Deaktiviert Aktiviert	Aktiviert	Aktiviert LLDP-MED für den SW-Port.
LLDP Asset-ID	Zeichenfolge mit bis zu 32 Zeichen		Identifiziert die Asset-ID, die dem Telefon für die Bestandsverwaltung zugewiesen wird.
Energy Efficient Ethernet(EEE): Switch-Port	Deaktiviert Aktiviert	Deaktiviert	Steuert EEE für den Switch-Port.
LLDP-Leistungspriorität	Unbekannt Niedrig Hoch Kritisch	Unbekannt	Weist dem Switch eine Energiepriorität des Telefons zu, damit der Switch die entsprechende Leistung für die Telefone bereitstellen kann.
802.1x-Authentifizierung	Vom Benutzer gesteuert Deaktiviert Aktiviert	Vom Benutzer gesteuert	Gibt den Status der 802.1x-Authentifizierungsfunktion an. • Vom Benutzer gesteuert – Der Benutzer kann die 802.1x-Authentifizierung auf dem Telefon konfigurieren. • Deaktiviert: 802.1x-Authentifizierung wird nicht verwendet. • Aktiviert – 802.1x-Authentifizierung wird verwendet, und Sie konfigurieren die Authentifizierung für die Telefone.
Remotekonfiguration für Switchport	Deaktiviert Autom. aushandeln 10 Halb 10 Voll 100 Halb 100 Voll	Deaktiviert	Ermöglicht es Ihnen, die Geschwindigkeit und Duplex-Funktion für den SW-Port des Telefons remote zu konfigurieren. Dies verbessert die Leistung für große Bereitstellungen mit bestimmten Porteinstellungen. Wenn die SW-Ports in Cisco Unified Communications Manager für die Remote-Portkonfiguration konfiguriert sind, können die Daten auf dem Telefon nicht geändert werden.
SSH-Zugriff	Deaktiviert Aktiviert	Deaktiviert	Steuert den Zugriff auf den SSH-Daemon über Port 22. Wenn Sie Port 22 offen lassen, ist das Telefon anfällig für DoS-Angriffe (Denial of Service).

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Ruftonbereich	Standard Japan	Standard	Steuert das Ruftonmuster.
TLS-Fortsetzungs-Timer	Ganzzahl 0 bis 3600 Sekunden	3370	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	Legt fest, ob das Anrufprotokoll von einer gemeinsam genutzten Leitung aufgezeichnet wird.
Minimale Ruftonlautstärke	0 – Stumm 1 – 15	0 – Stumm	Steuert die minimale Ruftonlautstärke für das Telefon.
Peer-Firmware-Freigabe	Deaktiviert Aktiviert	Aktiviert	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. Peer-Firmware-Freigabe: • Beschränkt Überlastungen bei TFTP-Übertragungen an zentrale Remote-TFTP-Server. • Firmware-Updates müssen nicht mehr manuell gesteuert werden. • Reduziert die Ausfallzeiten der Telefone während Updates, wenn zahlreiche Telefone gleichzeitig zurückgesetzt werden. • Unterstützt Firmware-Updates bei Bereitstellungen in Niederlassungen oder an Remotestandorten, die über WAN-Links mit beschränkter Bandbreite laufen.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Software-Server	Zeichenfolge mit bis zu 256 Zeichen		Identifiziert den alternativen IPv4-Server, den das Telefon verwendet, um Firmware und Updates abzurufen.
IPv6 – Lastserver	Zeichenfolge mit bis zu 256 Zeichen		Identifiziert den alternativen IPv6-Server, den das Telefon verwendet, um Firmware und Updates abzurufen.
Unified CM-Verbindungsfehler erkennen	Normal Verzögert	Normal	Legt die Empfindlichkeit des Telefons für die Erkennung eines Verbindungsfehlers mit Cisco Unified Communications Manager (Unified CM) fest. Dies ist der erste Schritt vor dem Gerätefailover auf einen Sicherungs-Unified CM/SRST. Zulässig sind die Werte „Normal“ (Unified CM-Verbindungsfehler werden in der Standardsystemgeschwindigkeit erkannt) und „Verzögert“ (Unified CM-Verbindungsfehler werden etwa viermal langsamer erkannt als bei der Einstellung „Normal“) Für eine schnellere Erkennung eines Unified CM-Verbindungsfehlers wählen Sie „Normal“ aus. Wenn Sie den Failover etwas verzögern möchten, um zu versuchen, die Verbindung wiederherzustellen, wählen Sie „Verzögert“ aus. Der genaue Zeitunterschied zwischen Normal und Verzögert hängt von mehreren Faktoren ab, die sich ständig ändern.
ID für spezielle Anforderung	Zeichenfolge		Steuert benutzerdefinierte Funktionen von ES-Lasten (Engineering Special).
HTTPS-Server	HTTP und HTTPS aktiviert Nur HTTPS	HTTP und HTTPS aktiviert	Steuert die Art der Kommunikation mit dem Telefon. Wenn Sie „Nur HTTPS“ auswählen, ist die Telefonkommunikation besser geschützt.

Feldname	Feldtyp oder Auswahlmöglichkeiten	Standard	Beschreibung
Dauerhafte Benutzeranmeldedaten für die Expressway-Anmeldung	Deaktiviert Aktiviert	Deaktiviert	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). Wenn Sie die Benutzeranmeldung vereinfachen möchten, können Sie dieses Feld aktivieren, damit die Expressway-Anmeldedaten beibehalten werden. Der Benutzer muss dann die Anmeldeinformationen nur beim ersten Mal eingeben. Im Anschluss (wenn das Telefon an einem externen Standort eingeschaltet wird) werden die Anmeldeinformationen auf dem Anmeldebildschirm vorab ausgefüllt. Weitere Informationen hierzu finden Sie unter Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren, auf Seite 106.
Upload-URL für Kundensupport	Zeichenfolge mit bis zu 256 Zeichen		Stellt die URL für das Tool für Problemberichte (PRT) bereit. Wenn Sie Geräte mit Mobil- und Remote-Zugriff über Expressway bereitstellen, müssen Sie zudem die PRT-Serveradresse der Liste der zulässigen HTTP-Server auf dem Expressway-Server hinzufügen. Weitere Informationen hierzu finden Sie unter Permanente Benutzerinformationen für die Expressway-Anmeldung konfigurieren, auf Seite 106.
TLS-Schlüssel deaktivieren	Siehe Transport Layer Security-Schlüssel deaktivieren, auf Seite 93.	Kein	Deaktiviert den ausgewählten TLS-Schlüssel. Deaktivieren Sie mehr als eine Verschlüsselungs-Suite, indem Sie die **Strg**-Taste auf Ihrer Computertastatur auswählen und gedrückt halten.

Transport Layer Security-Schlüssel deaktivieren

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

"Keine" ist die Standardeinstellung.

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

- Kein

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

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

Energiesparmodus für Cisco IP-Telefon planen

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

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

Mit den folgenden Aktionen können Sie das Display jederzeit einschalten:

- Drücken Sie die eine beliebige Taste auf dem Telefon.

  Das Telefon schaltet das Display ein und führt die der Taste zugeordnete Aktion aus.

- Nehmen Sie den Hörer ab.

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

Prozedur

Schritt 1 Wählen Sie **Gerät** > **Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.

Schritt 2 Suchen Sie das Telefon, das Sie konfigurieren müssen.

Schritt 3 Navigieren Sie zum produktspezifischen Konfigurationsbereich, und legen Sie die folgenden Felder fest:

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

Tabelle 21: 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 **07:00** ein. Um das Display um 14.00 Uhr (1400) einzuschalten, geben Sie **14:00 ein**. 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 *Stunden:Minuten* ein. Um das Display beispielsweise für vier Stunden und 30 Minuten zu aktivieren, nachdem es automatisch aktiviert wurde, geben Sie **04:30** ein. Wenn das Feld leer ist, wird das Telefon am Ende des Tages (0:00) ausgeschaltet. **Hinweis** Wenn der Zeitpunkt zum Einschalten des Displays auf 0:00 festgelegt ist und die Zeitdauer leer (oder 24:00) ist, bleibt das Display eingeschaltet.
Display-Leerlaufzeitüberschreitung	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). Geben Sie den Wert in diesem Feld im Format *Stunden:Minuten* ein. 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. Der Standardwert ist 01:00.

Schritt 4 Wählen Sie **Speichern** aus.

Schritt 5 Wählen Sie **Konfiguration übernehmen**.

Schritt 6 Starten Sie das Telefon neu.

EnergyWise für das Cisco IP-Telefon planen

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

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

Wenn EnergyWise aktiviert und der Zeitpunkt für das Ausschalten festgelegt ist, sendet das Telefon eine Anforderung an den Switch, damit es zum konfigurierten Zeitpunkt aktiviert wird. Der Switch akzeptiert oder lehnt die Anforderung ab. Wenn der Switch die Anforderung ablehnt oder nicht antwortet, wird das Telefon nicht ausgeschaltet. Wenn der Switch die Anforderung akzeptiert, wird das inaktive Telefon ausgeschaltet und der Stromverbrauch wird auf einen angegebenen Pegel reduziert. Ein aktives Telefon legt einen Leerlauf-Timer fest und schaltet sich aus, nachdem der Timer abgelaufen ist.

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

Prozedur

Schritt 1 Wählen Sie **Gerät** > **Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.

Schritt 2 Suchen Sie das Telefon, das Sie konfigurieren müssen.

Schritt 3 Navigieren Sie zum produktspezifischen Konfigurationsbereich und legen Sie die folgenden Felder fest.

- Power Save Plus aktivieren
- Telefon einschalten – Uhrzeit
- Telefon ausschalten – Uhrzeit
- Telefon ausschalten – Leerlauf-Timeout
- Signalton aktivieren
- EnergyWise-Domäne
- EnergyWise-Secret
- EnergyWise-Überschreibung zulassen

Tabelle 22: EnergyWise-Konfigurationsfelder

Feld	Beschreibung
Power Save Plus aktivieren	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. Standardmäßig sind keine Tage ausgewählt. Wenn „Power Save Plus aktivieren“ ausgewählt ist, wird eine Warnung bezüglich Notfällen angezeigt. **Vorsicht** 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. **Hinweis** 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.
Telefon einschalten – Uhrzeit	Legt fest, wann das Telefon an den Tagen, die im Feld Power Save Plus aktivieren ausgewählt sind, automatisch eingeschaltet wird. Geben Sie die Uhrzeit in diesem Feld im 24-Stunden-Format an (00:00 ist Mitternacht). Um das Telefon beispielsweise um 07:00 Uhr automatisch einzuschalten, geben Sie 07:00 ein. Um das Telefon um 14:00 Uhr einzuschalten, geben Sie 14:00 ein. Der Standardwert ist leer, das heißt 00:00. **Hinweis** 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.
Telefon ausschalten – Uhrzeit	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). Um das Telefon beispielsweise um 07:00 Uhr auszuschalten, geben Sie 07:00 ein. Um das Telefon um 14:00 Uhr auszuschalten, geben Sie 14:00 ein. Der Standardwert ist leer, das heißt 00:00. **Hinweis** 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.

Feld	Beschreibung
Telefon ausschalten – Leerlauf-Timeout	Die Länge der Zeitdauer, die das Telefon inaktiv sein muss, bevor es ausgeschaltet wird. Der Timeout tritt unter folgenden Bedingungen auf: • Wenn das Telefon, wie geplant, in den Power Save Plus-Modus gewechselt ist und eingeschaltet wurde, da der Benutzer die Taste **Auswahl** gedrückt hat. • Wenn das Telefon vom angeschlossenen Switch wieder eingeschaltet wurde. • Wenn die Ausschaltzeit des Telefons erreicht wird, aber das Telefon verwendet wird. Das Feld hat einen Bereich von 20 und 1440 Minuten. Der Standardwert ist 60 Minuten.
Signalton aktivieren	Wenn diese Option aktiviert ist, gibt das Telefon 10 Minuten vor der angegebenen Ausschaltzeit einen Signalton aus. 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: • Zehn Minuten vor dem Ausschalten wird der Rufton viermal wiedergegeben. • Sieben Minuten vor dem Ausschalten wird der Rufton viermal wiedergegeben. • Vier Minuten vor dem Ausschalten wird der Rufton viermal wiedergegeben. • 30 Sekunden vor dem Ausschalten wird der Rufton 15 Mal wiedergegeben oder so lange, bis sich das Telefon ausschaltet. Dieses Kontrollkästchen ist nur relevant, wenn im Listenfeld Power Save Plus aktivieren mindestens ein Tag ausgewählt ist.
EnergyWise-Domäne	Die EnergyWise-Domäne, in der sich das Telefon befindet. Dieses Feld darf maximal 127 Zeichen enthalten.
EnergyWise-Secret	Das Sicherheitskennwort, das verwendet wird, um mit den Endpunkten in der EnergyWise-Domäne zu kommunizieren. Dieses Feld darf maximal 127 Zeichen enthalten.

Feld	Beschreibung
EnergyWise-Überschreibung zulassen	Dieses Kontrollkästchen legt fest, ob die EnergyWise-Domänencontrollerrichtlinie Energiepegelaktualisierungen an die Telefone senden kann. Es gelten die folgenden Bedingungen: • Im Feld Power Save Plus aktivieren muss mindestens ein Tag ausgewählt werden. • Die Einstellungen in der Cisco Unified Communications Manager-Verwaltung werden planmäßig übernommen, auch wenn EnergyWise eine Überschreibung sendet. 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. • Wenn EnergyWise das Telefon anweist, sich um 20:00 Uhr auszuschalten, bleibt diese Anweisung bis zur festgelegten Einschaltzeit um 6:00 Uhr in Kraft. • Um 6:00 Uhr schaltet sich das Telefon ein und empfängt die Energiepegelaktualisierungen basierend auf den Einstellungen in der Unified Communications Manager-Verwaltung. • Um den Energiepegel auf dem Telefon erneut zu ändern, muss EnergyWise einen neuen Befehl ausgeben. **Hinweis** 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.

Schritt 4 Wählen Sie **Speichern** aus.

Schritt 5 Wählen Sie **Konfiguration übernehmen**.

Schritt 6 Starten Sie das Telefon neu.

Bitte nicht stören“ (Ruhefunktion) einrichten

Wenn „Nicht stören“ aktiviert ist, leuchtet die Lichtleiste auf dem Konferenztelefon rot.

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

Prozedur

Schritt 1 Wählen Sie **Gerät** > **Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.

Schritt 2 Suchen Sie das gewünschte Telefon.

Schritt 3 Legen Sie die folgenden Parameter fest:

- DND: Mit diesem Kontrollkästchen können Sie DND auf dem Telefon aktivieren.
- DND-Option: Rufton aus, Anruf ablehnen oder Allgemeine Telefonprofileinstellungen verwenden.
- DND-Benachrichtigung für eingehenden Anruf: Wählen Sie den Typ der Benachrichtigung für eingehende Anrufe aus, wenn DND aktiviert ist.

Hinweis Dieser Parameter befindet sich in den Fenstern „Allgemeines Telefonprofil“ und „Telefonkonfiguration“. Der Wert im Fenster „Telefonkonfiguration“ hat Vorrang.

Schritt 4 Wählen Sie **Speichern** aus.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

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 10

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.

Vom Gerät aufgerufene Aufzeichnung aktivieren

Konfigurieren Sie die vom Gerät aufgerufene Aufzeichnung in der Cisco Unified Communications Manager-Verwaltung. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Prozedur

Schritt 1 Legen Sie den Parameter Integrierte IP-Telefonbrücke auf **Ein** fest.

Schritt 2 Legen Sie auf der Seite Leitungskonfiguration die Aufzeichnungsoption auf **Selektive Anrufaufzeichnung aktiviert** fest und wählen Sie das passende Aufzeichnungsprofil aus.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

UCR 2008-Konfiguration

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

Tabelle 23: UCR 2008-Parameterpfad

Parameter	Verwaltungspfad
FIPS-Modus	**Gerät** > **Geräteeinstellungen** > **Allgemeines Telefonprofil**
	System > **Firmentelefonkonfiguration**
	Gerät > **Telefone**
SSH-Zugriff	**Gerät** > **Telefon**
	Gerät > **Geräteeinstellungen** > **Allgemeines Telefonprofil**
Webzugriff	**Gerät** > **Telefon**
	System > **Firmentelefonkonfiguration**
	Gerät > **Geräteeinstellungen** > **Allgemeines Telefonprofil**
System > **Firmentelefonkonfiguration**	
IP-Adressierungsmodus	**Gerät** > **Geräteeinstellungen** > **Allgemeine Gerätekonfiguration**
Bevorzugter IP-Adressierungsmodus für die Signalisierung	**Gerät** > **Geräteeinstellungen** > **Allgemeine Gerätekonfiguration**

UCR 2008 in der allgemeinen Gerätekonfiguration konfigurieren

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

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

Prozedur

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

UCR 2008 im allgemeinen Telefonprofil konfigurieren

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

- FIPS-Modus
- SSH-Zugriff
- Webzugriff

Prozedur

Schritt 1	Wählen Sie **Gerät** > **Geräteeinstellungen** > **Allgemeines Telefonprofil** in der Cisco Unified Communications Manager-Verwaltung aus.
Schritt 2	Legen Sie den FIPS-Modusparameter auf **Aktiviert** fest.
Schritt 3	Legen Sie den SSH-Zugriffsparameter auf **Deaktiviert** fest.
Schritt 4	Legen Sie den Webzugriffsparameter auf **Deaktiviert** fest.
Schritt 5	Legen Sie den 80-Bit SRTCP-Parameter auf **Aktiviert** fest.
Schritt 6	Wählen Sie **Speichern** aus.

UCR 2008 in der Firmentelefonkonfiguration konfigurieren

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

- FIPS-Modus
- Webzugriff

Prozedur

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

Schritt 4 Wählen Sie **Speichern** aus.

UCR 2008 auf dem Telefon konfigurieren

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

- FIPS-Modus
- SSH-Zugriff
- Webzugriff

Prozedur

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

Mobil- und Remote Access über Expressway

Mobil- und Remote Access über Expressway(MRA) ermöglicht Remotebenutzern, sich einfach und sicher mit dem Firmennetzwerk zu verbinden, ohne einen VPN-Clienttunnel verwenden zu müssen. Expressway verwendet TLS (Transport Layer Security), um den Netzwerkverkehr zu schützen. Damit ein Telefon ein Expressway-Zertifikat authentifizieren und eine TLS-Sitzung einrichten kann, muss das Expressway-Zertifikat von einer öffentlichen Zertifizierungsstelle, der die Telefon-Firmware vertraut, signiert sein. Es ist nicht möglich, andere CA-Zertifikate auf Telefonen für die Authentifizierung eines Expressway-Zertifikats zu installieren oder anderen Zertifikaten zu vertrauen.

Die Liste der CA-Zertifikate, die in der Telefon-Firmware eingebettet sind, ist unter http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-technical-reference-list.html verfügbar.

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

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

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

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

- *Mobil- und Remote-Zugriff über Cisco Expressway – Bereitstellungshandbuch*

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

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

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

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

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

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

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

Bereitstellungsszenarien

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

Szenario	Aktionen
Vor Ort meldet sich der Benutzer am Unternehmensnetzwerk an, nachdem Mobil- und Remote Access über Expressway bereitgestellt wurde.	Das Firmennetzwerk wird erkannt und das Telefon wird wie üblich mit Cisco Unified Communications Manager registriert.

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

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)

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 78
Produktspezifische Konfiguration, auf Seite 80

Tool zur Problemmeldung

Die Benutzer senden Problemberichte mit dem Tool für Problemberichte (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 Problembericht zu erstellen, greifen die Benutzer auf das Tool für Problemberichte 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 (mehrteilige 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

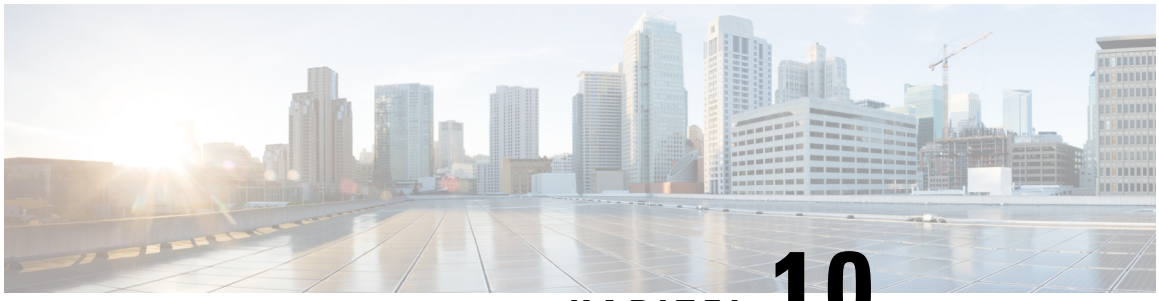
Schritt 1 Wählen Sie **Gerät** > **Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.

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.



KAPITEL 10

Konfiguration des Firmenverzeichnisses und persönlichen Verzeichnisses

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

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

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

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Konfiguration des persönlichen Verzeichnisses

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

Das persönliche Verzeichnis umfasst folgende Features:

- Persönliches Adressbuch (PAB)
- Kurzwahl

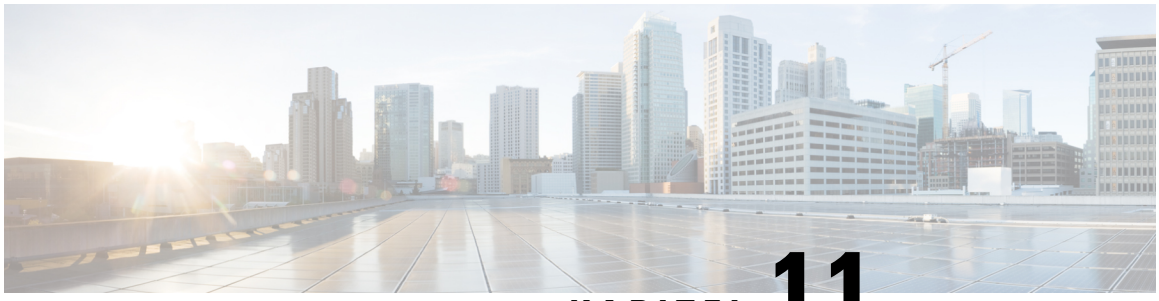
Die Benutzer können mit folgenden Methoden auf die Funktionen des persönlichen Verzeichnisses zugreifen:

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

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

TEIL IV

Telefonfehlerbehebung



KAPITEL 11

Telefonsysteme überwachen

Übersicht der Telefonsystemüberwachung

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

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

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

Verwandte Themen

Fehlerbehebung, auf Seite 151

Cisco IP-Telefon-Status

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

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

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

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

Fenster „Telefoninformationen anzeigen“

Prozedur

Schritt 1 Drücken Sie **Einstellungen** > **Telefoninfo**.

Schritt 2 Um das Menü zu verlassen, drücken Sie **Beenden**.

Statusmenü anzeigen

Prozedur

Schritt 1 Drücken Sie **Einstellungen** > **Status**.

Schritt 2 Um das Menü zu verlassen, drücken Sie **Zurück**.

Das Fenster „Statusmeldungen“ anzeigen

Prozedur

Schritt 1 Drücken Sie **Einstellungen** > **Status** > **Statusmeldungen**.

Schritt 2 Um das Menü zu verlassen, drücken Sie **Zurück**.

Statusmeldungen

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

Tabelle 24: Statusmeldungen auf Cisco IP-Telefon

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

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
TFTP-Größenfehler	Die Konfigurationsdatei ist zu groß für das Dateisystem auf dem Telefon.	Schalten Sie das Telefon aus und wieder ein.
ROM-Prüfsummenfehler	Die heruntergeladene Softwaredatei ist beschädigt.	Beziehen Sie eine neue Kopie der Telefon-Firmware und speichern Sie diese im TFTPPath-Verzeichnis. Sie sollten Dateien nur in dieses Verzeichnis kopieren, wenn die TFTP-Serversoftware deaktiviert ist, da die Dateien ansonsten beschädigt werden können.
Doppelte IP	Ein anderes Gerät verwendet die IP-Adresse, die dem Telefon zugewiesen ist.	Wenn das Telefon eine statische IP-Adresse hat, stellen Sie sicher, dass keine doppelte IP-Adresse zugewiesen wurde. 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 Informationszwecke bestimmt.

Fehler beim Aktualisieren des Gebietsschemas	Mindestens eine Lokalisierungsdatei konnte nicht im TFTP-Pfadverzeichnis gefunden werden oder ist ungültig. Das Gebietsschema wurde geändert.	Überprüfen Sie von der Administrationsebene des Cisco Unified-Betriebssystems aus, ob in den Unterverzeichnissen der TFTP-Dateiverwaltung folgende Dateien vorhanden sind:
		• Im Unterverzeichnis, das den gleichen Namen wie das Netzwerkgebietsschema hat:
		  • tones.xml
		• Mit dem gleichen Namen wie das Benutzergebietsschema im Unterverzeichnis gespeichert:
		  • glyphs.xml
		  • dictionary.xml
		  • kate.xml

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
Datei nicht gefunden <Cfg File>	Die auf dem Namen basierende und Standardkonfigurationsdatei wurde nicht auf dem TFTP-Server gefunden.	Die Konfigurationsdatei für ein Telefon wird erstellt, wenn das Telefon zur Cisco Unified Communications Manager-Datenbank hinzugefügt wird. Wenn das Telefon nicht in der Cisco Unified Communications Manager-Datenbank vorhanden ist, generiert der TFTP-Server eine **CFG-Datei nicht gefunden**-Antwort. • Das Telefon ist nicht mit Cisco Unified Communications Manager registriert. Sie müssen das Telefon manuell zu Cisco Unified Communications Manager hinzufügen, wenn Sie die automatische Registrierung von Telefonen nicht zulassen. • Wenn Sie DHCP verwenden, stellen Sie sicher, dass der DHCP-Server auf den richtigen TFTP-Server verweist. • Wenn Sie statische IP-Adressen verwenden, überprüfen Sie die Konfiguration des TFTP-Servers.
Datei nicht gefunden <CTLFile.tlv>	Diese Meldung wird auf dem Telefon angezeigt, wenn sich der Cisco Unified Communications Manager-Cluster nicht im sicheren Modus befindet.	Keine Auswirkung. Das Telefon kann sich mit Cisco Unified Communications Manager registrieren.
IP-Adresse freigegeben	Das Telefon ist konfiguriert, um die IP-Adresse freizugeben.	Das Telefon bleibt inaktiv, bis es aus- und eingeschaltet wird oder die DHCP-Adresse zurückgesetzt wird.
IPv4 DHCP-Zeitüberschreitung	Der IPv4 DHCP-Server reagiert nicht.	Netzwerk ist ausgelastet: Die Fehler sollten sich selbst beheben, wenn die Netzwerklast reduziert wird. Keine Netzwerkverbindung zwischen dem IPv4 DHCP-Server und dem Telefon: Überprüfen Sie die Netzwerkverbindung. IPv4 DHCP-Server ist ausgefallen: Überprüfen Sie die Konfiguration des IPv4 DHCP-Servers. Fehler treten erneut auf: Weisen Sie eine statische IPv4-Adresse zu.

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
IPv6 DHCP-Zeitüberschreitung	Der IPv6 DHCP-Server reagiert nicht.	Netzwerk ist ausgelastet: Die Fehler sollten sich selbst beheben, wenn die Netzwerklast reduziert wird. Keine Netzwerkverbindung zwischen dem IPv6 DHCP-Server und dem Telefon: Überprüfen Sie die Netzwerkverbindung. IPv6 DHCP-Server ist ausgefallen: Überprüfen Sie die Konfiguration des IPv6 DHCP-Servers. Fehler treten erneut auf: Weisen Sie eine statische IPv6-Adresse zu.
IPv4 DNS-Zeitüberschreitung	Der IPv4 DNS-Server reagiert nicht.	Netzwerk ist ausgelastet: Die Fehler sollten sich selbst beheben, wenn die Netzwerklast reduziert wird. Keine Netzwerkverbindung zwischen dem IPv4 DNS-Server und dem Telefon: Überprüfen Sie die Netzwerkverbindung. IPv4 DNS-Server ist ausgefallen: Überprüfen Sie die Konfiguration des IPv4 DNS-Servers.
IPv6 DNS-Zeitüberschreitung	Der IPv6 DNS-Server reagiert nicht.	Netzwerk ist ausgelastet: Die Fehler sollten sich selbst beheben, wenn die Netzwerklast reduziert wird. Keine Netzwerkverbindung zwischen dem IPv6 DNS-Server und dem Telefon: Überprüfen Sie die Netzwerkverbindung. IPv6 DNS-Server ist ausgefallen: Überprüfen Sie die Konfiguration des IPv6 DNS-Servers.
Unbekannter DNS IPv4-Host	IPv4 DNS konnte den Namen des TFTP-Servers oder von Cisco Unified Communications Manager nicht auflösen.	Überprüfen Sie, ob die Hostnamen des TFTP-Servers oder von Cisco Unified Communications Manager richtig in IPv4 DNS konfiguriert sind. Verwenden Sie IPv4-Adressen anstatt Hostnamen.
Unbekannter DNS IPv6-Host	IPv6 DNS konnte den Namen des TFTP-Servers oder von Cisco Unified Communications Manager nicht auflösen.	Überprüfen Sie, ob die Hostnamen des TFTP-Servers oder von Cisco Unified Communications Manager richtig in IPv6 DNS konfiguriert sind. Verwenden Sie IPv6-Adressen anstatt Hostnamen.

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
Last zurückgewiesen – HC	Die heruntergeladene Anwendung ist nicht mit der Telefonhardware kompatibel.	Dieses Problem kann auftreten, wenn Sie versucht haben, auf dem Telefon eine Softwareversion zu installieren, die keine Veränderungen der Hardware des Telefons unterstützt. Überprüfen Sie die Last-ID, die dem Telefon zugewiesen ist (wählen Sie **Gerät** > **Telefon** in Cisco Unified Communications Manager aus). Geben Sie die auf dem Telefon angezeigt Last 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 DHCP-Server keinen Standardrouter bereitgestellt. Überprüfen Sie die DHCP-Serverkonfiguration.
Kein IPv4 DNS-Server	Ein Name wurde angegeben, aber DHCP oder die statische IP-Konfiguration geben keine IPv4 DNS-Serveradresse an.	Wenn das Telefon eine statische IP-Adresse hat, überprüfen Sie, ob der IPv4 DNS-Server konfiguriert ist. Wenn Sie DHCP verwenden, hat der DHCP-Server keinen IPv4 DNS-Server bereitgestellt. Überprüfen Sie die DHCP-Serverkonfiguration.
Kein IPv6 DNS-Server	Ein Name wurde angegeben, aber DHCP oder die statische IP-Konfiguration geben keine IPv6 DNS-Serveradresse an.	Wenn das Telefon eine statische IP-Adresse hat, überprüfen Sie, ob der IPv6 DNS-Server konfiguriert ist. Wenn Sie DHCP verwenden, hat der DHCP-Server keinen IPv6 DNS-Server bereitgestellt. Überprüfen Sie die DHCP-Serverkonfiguration.
Keine Vertrauensliste installiert	Die CTL- oder ITL-Datei ist nicht auf dem Telefon installiert.	Die Vertrauensliste ist nicht in Cisco Unified Communications Manager konfiguriert und die Sicherheit wird nicht standardmäßig unterstützt. Die Vertrauensliste ist nicht konfiguriert. Weitere Informationen zu Vertrauenslisten finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
Telefon konnte nicht registriert werden. Die Größe des Zertifikatsschlüssels ist nicht FIPS-konform.	FIPS erfordert, dass das RSA-Serverzertifikat 2048 Bit oder mehr umfasst.	Aktualisieren Sie das Zertifikat.
Neustart von Cisco Unified Communications Manager angefordert	Das Telefon wird aufgrund einer Anforderung von Cisco Unified Communications Manager neu gestartet.	In Cisco Unified Communications Manager wurden möglicherweise Konfigurationsänderungen am Telefon vorgenommen und **Konfiguration übernehmen** wurde gedrückt, um die Änderungen zu übernehmen.
TFTP-Zugriffsfehler	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 verweist. Wenn Sie statische IP-Adressen verwenden, überprüfen Sie die Konfiguration des TFTP-Servers.
TFTP-Fehler	Das Telefon erkennt einen Fehlercode vom TFTP-Server nicht.	Kontaktieren Sie das Cisco TAC.
TFTP-Zeitüberschreitung	Der TFTP-Server reagiert nicht.	Netzwerk ist ausgelastet: Die Fehler sollten sich selbst beheben, wenn die Netzwerklast reduziert wird. Keine Netzwerkverbindung zwischen dem TFTP-Server und dem Telefon: Überprüfen Sie die Netzwerkverbindung. TFTP-Server ist ausgefallen: Überprüfen Sie die Konfiguration des TFTP-Servers.
Zeitüberschreitung	Supplicant versuchte eine 802.1X-Transaktion, aber die Zeit wurde überschritten, da kein Authentifikator vorhanden ist.	Bei der Authentifizierung tritt normalerweise eine Zeitüberschreitung auf, wenn 802.1X nicht auf dem Switch konfiguriert ist.

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
Aktualisierung der Vertrauensliste fehlgeschlagen	Die Aktualisierung der CTL- und ITL-Datei ist fehlgeschlagen.	Auf dem Telefon sind CTL- und ITL-Dateien installiert und die neuen CTL- und ITL-Dateien konnten nicht aktualisiert werden. Mögliche Fehlerursachen: • Ein Netzwerkfehler ist aufgetreten. • Der TFTP-Server ist ausgefallen. • Der neue Sicherheitstoken, der zum Signieren der CTL-Datei verwendet wurde, und das TFTP-Zertifikat, dass zum Signieren der ITL-Datei verwendet wurde, sind in den aktuellen CTL- und ITL-Dateien auf dem Telefon noch nicht verfügbar. • Ein interner Telefonfehler ist aufgetreten. Mögliche Lösungen: • Überprüfen Sie die Netzwerkverbindung. • Überprüfen Sie, ob der TFTP-Server aktiv ist und normal funktioniert. • Wenn der TVS-Server (Transactional Vsam Services) von Cisco Unified Communications Manager nicht unterstützt wird, überprüfen Sie, ob der TVS-Server aktiv ist und normal funktioniert. • Überprüfen Sie, ob der Sicherheitstoken und der TFTP-Server gültig sind. Löschen Sie die CTL- und ITL-Datei manuell, wenn diese Lösungen fehlschlagen. Setzen Sie das Telefon zurück. Weitere Informationen zu Vertrauenslisten finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.
Vertrauensliste aktualisiert	Die CTL-Datei, die ITL-Datei oder beide Dateien werden aktualisiert.	Keine. Diese Meldung ist nur für Informationszwecke bestimmt. Weitere Informationen zu Vertrauenslisten finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Nachricht	Beschreibung	Mögliche Erklärung und Aktion
Versionsfehler	Der Name der Telefonlastdatei ist ungültig.	Stellen Sie sicher, dass die Telefonlastdatei den richtigen Namen hat.
XmlDefault.cnf.xml oder .cnf.xml übereinstimmend mit dem Gerätenamen des Telefons.	Name der Konfigurationsdatei.	Keine. Die Meldung zeigt den Namen der Konfigurationsdatei für das Telefon an.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager, auf Seite 10

Das Fenster „Netzwerkstatistik“ anzeigen

Prozedur

Schritt 1 Drücken Sie **Einstellungen** > **Status** > **Netzwerkstatistik**.

Schritt 2 Um das Menü zu verlassen, drücken Sie **Zurück**.

Netzwerkstatistikfelder

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

Tabelle 25: Netzwerkstatistikfelder

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

Element	Beschreibung
CDP Nachbar-Port	ID eines Geräts, das mit diesem Port verbunden ist und vom CDP-Protokoll erkannt wird.
Ursache des Neustarts: Einer dieser Werte: • Zurücksetzen der Hardware (Power-On-Reset) • Zurücksetzen der Software (Speichercontroller wird ebenfalls zurückgesetzt) • Zurücksetzen der Software (Speichercontroller wird nicht zurückgesetzt) • Watchdog zurücksetzen • Initialisiert • Unbekannt	Ursache des letzten Zurücksetzens des Telefons
Port 1	Linkstatus und Verbindung des Netzwerk-Ports (z. B. bedeutet **`100 Full`**, dass der PC-Port verbunden ist und automatisch eine Vollduplex-100-Mbit/s-Verbindung ausgehandelt hat)
IPv4	Informationen zum DHCP-Status. Dies schließt die folgenden Statusangaben ein: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • DISABLED DUPLICATE IP • SET DHCP COLDBOOT • SET DHCP DISABLED • SET DHCP FAST

Element	Beschreibung
IPv6	Informationen zum DHCP-Status. Dies schließt die folgenden Statusangaben ein: • CDP INIT • DHCP6 BOUND • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DISABLED DUPLICATE IPV6 • DHCP6 DECLINED DUPLICATE IP • ROUTER ADVERTISE • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT CANNOT RESTORE • IPV6 STACK TURNED OFF • ROUTER ADVERTISE • ROUTER ADVERTISE • UNRECOGNIZED MANAGED BY • ILLEGAL IPV6 STATE

Das Fenster „Anrufstatistik“ anzeigen

Prozedur

Schritt 1 Drücken Sie **Einstellungen** > **Status** > **Anrufstatistiken**.

Schritt 2 Um das Menü zu verlassen, drücken Sie **Zurück** .

Anrufstatistikfelder

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

Tabelle 26: Anrufstatistikelemente

Element	Beschreibung
Empfänger – Codec	Typ des empfangenen Sprachstreams (RTP-Audiostreaming vom Codec): • G.729 • G.722 • G. 722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS • iSAC
Sender – Codec	Typ des übertragenen Sprachstreams (RTP-Audiostreaming vom Codec): • G.729 • G.722 • G. 722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS • iSAC

Element	Beschreibung
Empfänger – Größe	Größe der Sprachpakete (in Millisekunden) im empfangenem Voicestream (RTP-Streaming-Audio).
Sender – Größe	Größe der Sprachpakete (in Millisekunden) im gesendeten Voicestream.
Rcvr Packets (Empfänger - Pakete)	Anzahl der RTP-Sprachpakete, die empfangen wurden, seit der Voicestream geöffnet wurde. **Hinweis** Diese Anzahl ist nicht unbedingt mit der Anzahl der RTP-Sprachpakete identisch, die seit Beginn des Anrufs empfangen wurden, da der Anruf möglicherweise gehalten wurde.
Sender – Pakete	Anzahl der RTP-Sprachpakete, die gesendet wurden, seit der Voicestream geöffnet wurde. **Hinweis** Diese Anzahl ist nicht unbedingt mit der Anzahl der RTP-Sprachpakete identisch, die seit Beginn des Anrufs gesendet wurden, da der Anruf möglicherweise gehalten wurde.
Avg Jitter (Durchschnittlicher Jitter)	Geschätzter, durchschnittlicher RTP-Paket-Jitter (dynamische Verzögerung eines Pakets bei der Übertragung im Netzwerk), in Millisekunden, der bemerkt wurde, seit der empfangene Voicestream geöffnet wurde.
Max Jitter (Maximaler Jitter)	Maximaler Jitter, in Millisekunden, der bemerkt wurde, seit der empfangene Voicestream geöffnet wurde.
Empfänger – Verworfen	Anzahl der RTP-Pakete im eingehenden Voicestream, die verworfen wurden (ungültige Pakete, zu spät usw.). **Hinweis** Das Telefon verwirft Comfort Noise-Pakete des Nutzlasttyps 19, die von den Cisco Gateways generiert werden, da diese den Zähler erhöhen.
Rcvr Lost Packets (Empfänger – Verlorene Pakete)	Fehlende RTP-Pakete (während Übertagung verloren).
Sprachqualitätsmetrik	
Cumulative Conceal Ratio (Verdeckung - kumulierte Rate)	Gesamtanzahl der Verdeckungsrahmen dividiert durch die Gesamtanzahl der Sprachrahmen, die ab Beginn des Voicestreams empfangen wurden.

Element	Beschreibung
Verdeckung (Intervallrate)	Verhältnis der Verdeckungsrahmen zu den Sprachrahmen im vorherigen 3-Sekundenintervall aktiver Sprache. Wenn VAD (Voice Activity Detection) verwendet wird, ist möglicherweise ein längeres Intervall erforderlich, um drei Sekunden der aktiven Sprache zu sammeln.
Max Conceal Ratio (Verdeckung - Maximalrate)	Höchstes Intervall der Verdeckungsrate ab Beginn des Voicestreams.
Verdeckung Sekunden	Anzahl der Sekunden mit Verdeckungsereignissen (verlorene Rahmen) ab Beginn des Voicestreams (einschließlich schwerwiegende Verdeckung).
Severely Conceal Seconds (Verdeckung (schwerwiegend) Sekunden)	Anzahl der Sekunden mit mehr als fünf Prozent Verdeckungsereignissen (verlorene Rahmen) ab Beginn des Voicestreams.
Latenz	Geschätzte Netzwerklatenz in Millisekunden. Mittelwert der Round-Trip-Verzögerung, der gemessen wird, wenn RTCP-Empfängerberichtsblöcke empfangen werden.

Webseite für Cisco IP-Telefon

Jedes Cisco IP-Telefon hat eine Webseite, auf der verschiedene Informationen über das Telefon angezeigt werden, einschließlich:

- Geräteinformationen: Zeigt die Geräteeinstellungen und zugehörige Informationen für das Telefon an.
- Netzwerkkonfiguration: Zeigt Informationen über die Netzwerkkonfiguration und andere Telefoneinstellungen an.
- Netzwerkstatistik: Zeigt Links zu Informationen über den Netzwerkverkehr an.
- Geräteprotokolle: Zeigt Links zu Informationen für die Problembehandlung an.
- Streaming-Statistik: Zeigt Links zu verschiedenen Streaming-Statistiken an.

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

Sie können viele dieser Informationen auch direkt vom Telefon abrufen.

Auf die Webseite des Telefons zugreifen

Hinweis Wenn Sie nicht auf die Webseite zugreifen können, ist diese möglicherweise standardmäßig deaktiviert.

Prozedur

Schritt 1 Ermitteln Sie die IP-Adresse des Cisco IP-Telefon mit einer dieser Methoden:

a) Suchen Sie das Telefon in der Cisco Unified Communications Manager-Verwaltung, indem Sie **Gerät** > **Telefon** auswählen. Für Telefone, die bei Cisco Unified Communications Manager registriert sind, wird die IP-Adresse im Fenster „Telefone suchen und auflisten“ sowie oben im Fenster „Telefonkonfiguration“ angezeigt.

b) Drücken Sie auf dem Telefon **Einstellungen** > **Verwaltereinstellungen** > **Netzwerk-Setup** > **IPv4-Setup**, und blättern Sie zum IP-Adressfeld.

Schritt 2 Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein, wobei *IP-Adresse* für die jeweilige IP-Adresse des Cisco IP-Telefon steht:

http://<IP_address>

Webseite mit Geräteinformationen

Unter Geräteinformationen auf der Telefon-Webseite werden die Geräteeinstellungen und zugehörige Informationen für das Telefon angezeigt. Diese Elemente werden in der folgenden Tabelle beschrieben.

Um die Geräteinformationen anzuzeigen, öffnen Sie die Webseite für das Telefon und klicken Sie auf den Link **Geräteinformationen**.

Tabelle 27: Felder der Webseite mit Geräteinformationen

Feld	Beschreibung
Servicemodus	Der Servicemodus für das Telefon.
Servicedomäne	Die Domäne für den Service.
Servicestatus	Der aktuelle Status des Service.
MAC-Adresse	Die MAC-Adresse (Media Access Control) des Telefons.
Hostname	Eindeutiger, unveränderlicher Name, der dem Telefon gemäß der MAC-Adresse automatisch zugewiesen wird.
Telefon-DN	Verzeichnisnummer, die dem Telefon zugewiesen ist.
Anwendungs-ID	Identifiziert die Anwendungsversion.
Boot-Software-ID	Gibt die Version der Boot-Software an.

Feld	Beschreibung
Version	ID der Firmware, die auf dem Telefon ausgeführt wird.
Hardwarerevision	Nebenversionswert der Telefonhardware.
Seriennummer	Die Seriennummer des Telefons.
Modellnummer	Die Modellnummer des Telefons.
Wartende Nachricht vorhanden	Zeigt an, ob eine Voicemail auf der primären Leitung des Telefons wartet.
UDI	Zeigt die folgenden Cisco UDI-Informationen (Unique Device Identifier) über das Telefon an: • Hardwaretyp • Name des Telefonmodells • Produktbezeichner • Versions-ID (VID): Gibt die Hauptversionsnummer der Hardware an. • Seriennummer
Zeit	Zeit für die Datum/Zeit-Gruppe, zu der das Telefon gehört. Diese Informationen kommen vom Cisco Unified Communications Manager.
Zeitzone	Zeitzone für die Datum/Zeit-Gruppe, zu der das Telefon gehört. Diese Informationen kommen vom Cisco Unified Communications Manager.
Datum	Datum für die Datum/Zeit-Gruppe, zu der das Telefon gehört. Diese Informationen kommen vom Cisco Unified Communications Manager.
System – Freier Speicherplatz	Menge des verfügbaren Systemspeichers.
Java-Heap – Freier Speicher	Der für den Java-Heap verfügbare Speicher.
Java-Pool – Freier Speicher	Der für den Java-Pool verfügbare Speicher.
FIPS-Modus aktiviert	Zeigt an, ob der FIPS-Modus (Federal Information Processing Standard) aktiviert ist.

Webseite „Netzwerk-Setup“

Im entsprechenden Bereich auf einer Telefon-Webseite werden Informationen zur Netzwerkkonfiguration und zu anderen Telefoneinstellungen angezeigt. Diese Elemente werden in der folgenden Tabelle beschrieben.

Sie können viele dieser Elemente im Menü Netzwerkkonfiguration auf dem Cisco IP-Telefon anzeigen und festlegen.

Um die Netzwerkkonfiguration anzuzeigen, öffnen Sie die Webseite für das Telefon und klicken Sie auf den Link **Netzwerkkonfiguration**.

Tabelle 28: Elemente der Netzwerkkonfiguration

Element	Beschreibung
MAC-Adresse	Die MAC-Adresse (Media Access Control) des Telefons.
Hostname	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) abruft.
DHCP	Gibt an, ob das Telefon DHCP verwendet.
IP-Adresse	Die IP-Adresse (Internet Protocol) des Telefons.
Subnetzmaske	Die vom Telefon verwendete Subnetzmaske.
Standardrouter 1	Der vom Telefon verwendete Standardrouter.
DNS-Server 1–3	Der primäre DNS-Server (DNS Server 1) und optionale DNS-Backupserver (DNS-Server 2 und 3), die das Telefon verwendet.
Alternativer TFTP-Server	Gibt an, ob das Telefon einen alternativen TFTP-Server verwendet.
TFTP-Server 1	Der vom Telefon verwendete primäre TFTP-Server (Trivial File Transfer Protocol).
TFTP Server 2	Der TFTP-Backupserver (Trivial File Transfer Protocol), den das Telefon verwendet.
DHCP-Adressfreigabe	Gibt die Einstellung der Option DHCP-Adressfreigabe an.
VLAN-ID (Betrieb)	Das VLAN (Virtual Local Area Network), das auf einem Cisco Catalyst-Switch konfiguriert ist, in dem das Telefon ein Mitglied ist.
VLAN-ID (Verwaltung)	Zusätzliches VLAN, in dem das Telefon ein Mitglied ist.

Element	Beschreibung
Unified CM 1-5	Hostnamen oder IP-Adressen der Cisco Unified Communications Manager-Server, mit denen sich das Telefon registrieren kann, in der Reihenfolge ihrer Priorität. Ein Element kann auch die IP-Adresse eines verfügbaren SRST-Routers anzeigen, der eingeschränkte Funktionen von Cisco Unified Communications Manager bereitstellt. Für einen verfügbaren Server zeigt ein Element die IP-Adresse des Cisco Unified Communications Manager-Servers und eine der folgenden Statusangaben an: • Aktiv: Der Cisco Unified Communications Manager-Server, der derzeit die Anrufverarbeitungsservices für das Telefon bereitstellt. • Standby: Der Cisco Unified Communications Manager-Server, zu dem das Telefon wechselt, wenn der aktuelle Server nicht mehr verfügbar ist. • Leer: Keine aktuelle Verbindung mit diesem Cisco Unified Communications Manager-Server. Ein Eintrag kann auch die SRST-Bezeichnung (Survivable Remote Site Telephony) enthalten, die einen SRST-Router angibt, der Cisco Unified Communications Manager-Funktionen in eingeschränktem Umfang bereitstellt. Dieser Router übernimmt die Steuerung der Anrufverarbeitung, wenn alle anderen 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.
Informations-URL	Die URL des Hilfetextes, der auf dem Telefon angezeigt wird.
Verzeichnis-URL	URL des Servers, von dem das Telefon Verzeichnisinformationen abruft.
Nachrichten-URL	URL des Servers, von dem das Telefon Nachrichtenservices erhält.
Service-URL	URL des Servers, von dem das Telefon Cisco IP-Telefon-Services erhält.

Element	Beschreibung
Leerlauf-URL	URL, die das Telefon anzeigt, wenn es für die im Feld URL-Leerlaufzeit angegebene Zeitdauer inaktiv und kein Menü geöffnet ist.
URL-Leerlaufzeit	Anzahl der Sekunden, die das Telefon inaktiv und kein Menü geöffnet ist, bevor der XML-Service, der in der URL angegeben ist, aktiviert wird.
Proxy-Server-URL	URL des Proxy-Servers, der HTTP-Anforderungen für HTTP-Telefonclients an nicht lokale Hostadressen sendet und Antworten vom nicht lokalen Host an den HTTP-Telefonclient weitergibt.
Authentifizierungs-URL	Die URL, die das Telefon verwendet, um Anforderungen an den Telefonwebserver zu überprüfen.
SW-Portkonfiguration	Geschwindigkeit und Duplex-Status des Switch-Ports: • A = Automatisch aushandeln • 10H = 10-BaseT/Halbduplex • 10F = 10-BaseT/Vollduplex • 100H = 100-BaseT/Halbduplex • 100F = 100-BaseT/Vollduplex • 1000F = 1000-BaseT/Vollduplex • Kein Link= Keine Verbindung zum Switch-Port
Benutzergebietsschema	Das dem Telefonbenutzer zugeordnete Gebietsschema. Detaillierte Informationen, um den Benutzer zu unterstützen, einschließlich Sprache, Schriftart, Datum- und Uhrzeitformat sowie Textinformationen zur alphanumerischen Tastatur.
Netzwerkgebietsschema	Das dem Telefonbenutzer zugeordnete Netzwerkgebietsschema. Detaillierter Informationen, um das Telefon an einem bestimmten Standort zu unterstützen, einschließlich Definitionen der vom Telefon verwendeten Töne und Kadenzen.
Version des Benutzergebietsschemas	Version des Benutzergebietsschemas, das auf dem Telefon geladen ist.
Version des Netzwerkgebietsschemas	Version des Netzwerkgebietsschemas, das auf dem Telefon geladen ist.
Lautsprecher aktiviert	Gibt an, ob der Lautsprecher des Telefons aktiviert ist.

Element	Beschreibung
Mithören	Gibt an, ob die Funktion zum Mithören auf dem Telefon aktiviert ist. Mithören ermöglicht es Ihnen, über den Hörer sprechen und den Ton über den Lautsprecher ausgeben.
GARP aktiviert	Gibt an, ob das Telefon MAC-Adressen von Gratuitous ARP-Antworten lernt.
Automatische Leitungsauswahl aktiviert	Gibt an, ob das Telefon den Anruf-Fokus auf die eingehenden Anrufe aller Leitungen wechselt.
DSCP für Anrufsteuerung	DSCP IP-Klassifizierung für Anrufsteuerungssignale.
DSCP für Konfiguration	DSCP IP-Klassifizierung zur Weitergabe von Telefonkonfigurationen.
DSCP für Services	DSCP IP-Klassifizierung für telefonbasierte Services.
Sicherheitsmodus	Der für das Telefon festgelegte Sicherheitsmodus.
Webzugriff aktiviert	Gibt an, ob der Webzugriff für das Telefon aktiviert (Ja) oder deaktiviert (Nein) ist.
SSH-Zugriff aktiviert	Gibt an, ob das Telefon die SSH-Verbindungen akzeptiert oder blockiert.
CDP: SW-Port	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, Stromaushandlung, 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.
LLDP-MED: SW-Port	Gibt an, ob LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) auf dem Switch-Port aktiviert ist.

Element	Beschreibung
LLDP-Leistungspriorität	Kündigt die Energiepriorität des Telefons auf dem Switch an, damit der Switch die entsprechende Leistung für die Telefone bereitstellen kann. Die Einstellungen umfassen folgende Optionen: • Unbekannt: Dies ist der Standardwert. • Niedrig • Hoch • Kritisch
LLDP Asset-ID	Identifiziert die Asset-ID, die dem Telefon für die Bestandsverwaltung zugewiesen wird.
CTL-Datei	Identifiziert die CTL-Datei.
ITL-Datei	Die ITL-Datei enthält die Initial Trust List.
ITL-Signatur	Verbessert die Sicherheit mit einem sicheren Hash-Algorithmus (SHA-1) in der CTL- und ITL-Datei.
CAPF-Server	Der Name des CAPF-Servers, der vom Telefon verwendet wird.
TVS	Die Hauptkomponente von Security by Default. Mit TVS (Trust Verification Services) können Cisco Unified IP-Telefone Anwendungsserver, beispielsweise EM-Services, Verzeichnis und MIDlet, bei der Herstellung einer HTTPS-Verbindung authentifizieren.
TFTP-Server	Der Name des TFTP-Servers, der vom Telefon verwendet wird.
Automatische Portsynchronisierung	Synchronisiert die Ports in einer langsameren Geschwindigkeit, um Paketverlust zu verhindern.
Remotekonfiguration für Switchport	Ermöglicht dem Administrator, die Geschwindigkeit und Funktionalität des Cisco Desktop Collaboration Experience-Ports unter Verwendung der Cisco Unified Communications Manager-Verwaltung zu konfigurieren.
IP-Adressierungsmodus	Zeigt den IP-Adressierungsmodus an, der auf dem Telefon verfügbar ist.
Bevorzugter IP-Modus	Gibt die IP-Adressenversion an, die das Telefon bei der Signalisierung mit Cisco Unified Communications Manager verwendet, wenn sowohl IPv4 als auch IPv6 auf dem Telefon verfügbar sind.

Element	Beschreibung
Bevorzugter IP-Modus für Medien	Gibt an, dass für das Gerät für das Medium eine IPv4-Adresse verwendet, um die Verbindung mit Cisco Unified Communications Manager herzustellen.
Automatisch IPv6-Konfiguration	Zeigt an, ob die automatisch Konfiguration auf dem Telefon aktiviert oder deaktiviert ist.
IPv6 – DAD (Erkennung doppelter Adressen)	Überprüft die Eindeutigkeit neuer IPv6-Unicastadressen, bevor die Adressen den Schnittstellen zugewiesen werden.
IPv6 – Nachrichtenumleitung akzeptieren	Gibt an, ob das Telefon umgeleitete Nachrichten vom Router akzeptiert, der für die Zielnummer verwendet wird.
IPv6 – Antwort auf Multicast-Echo-Anforderung	Gibt an, ob das Telefon eine Echo-Antwort auf eine Echo-Anforderung an eine IPv6-Adresse sendet.
IPv6 – Lastserver	Wird verwendet, um die Installationsdauer für Updates der Telefon-Firmware zu optimieren und das WAN zu entlasten, indem Bilder lokal gespeichert werden, sodass es nicht erforderlich ist, bei jedem Telefon-Upgrade den WAN-Link zu verwenden.
IPv6 - Protokollserver	Gibt die IP-Adresse und den Port des Remotecomputers für die Protokollierung an, an den das Telefon die Protokollnachrichten sendet.
IPv6 - CAPF-Server	Allgemeiner Name (im Cisco Unified Communications Manager-Zertifikat) des CAPF-Servers, der vom Telefon verwendet wird.
DHCPv6	DHCP (Dynamic Host Configuration Protocol) weist einem Gerät automatisch eine IPv6-Adresse zu, wenn es mit dem Netzwerk verbunden wird. Cisco Unified IP-Telefone aktivieren DHCP standardmäßig.
IPv6-Adresse	Zeigt die aktuelle IPv6-Adresse des Telefons an oder ermöglicht dem Benutzer, eine neue IPv6-Adresse einzugeben.
Länge des IPv6-Präfixes	Zeigt die aktuelle Länge des Präfixes für das Subnetz an oder ermöglicht dem Benutzer, eine neue Länge einzugeben.
IPv6 – Standardrouter 1	Zeigt den Standardrouter an, der vom Telefon verwendet wird, oder ermöglicht dem Benutzer, eine neuen IPv6-Standardrouter einzugeben.
IPv6 – DNS-Server 1	Zeigt den primären DNSv6-Server an, der vom Telefon verwendet wird, oder ermöglicht dem Benutzer, einen neuen Server festzulegen.

Element	Beschreibung
IPv6 – DNS-Server 2	Zeigt den sekundären DNSv6-Server an, der vom Telefon verwendet wird, oder ermöglicht dem Benutzer, einen neuen Server festzulegen.
IPv6 – Alternativer TFTP-Server	Ermöglicht dem Benutzer einen alternativen (sekundären) IPv6 TFTP-Server zu verwenden.
IPv6 – TFTP-Server 1	Zeigt den primären IPv6 TFTP-Server an, der vom Telefon verwendet wird, oder ermöglicht dem Benutzer, einen neuen Server festzulegen.
IPv6 – TFTP-Server 2	Zeigt den sekundären IPv6 TFTP-Server an, der vom Telefon verwendet wird, wenn der primäre Server nicht verfügbar ist, oder ermöglicht dem Benutzer, einen neuen Server festzulegen.
IPv6-Adresse freigegeben	Ermöglicht dem Benutzer IPv6-bezogene Informationen freizugeben.
Energywise-Energiepegel	Eine Messung der von den Geräten in einem EnergyWise-Netzwerk verbrauchten Energie.
EnergyWise-Domäne	Eine administrative Gerätegruppe für die Energieüberwachung und Steuerung.

Webseite mit Ethernet-Informationen

In der folgenden Tabelle wird der Inhalt der Webseite mit den Ethernet-Informationen beschrieben.

Tabelle 29: Ethernet-Informationselemente

Element	Beschreibung
Übertr. – Frames	Gesamtanzahl der Pakete, die das Telefon gesendet hat.
Tx Broadcast	Gesamtanzahl der Broadcast-Pakete, die das Telefon gesendet hat.
Tx multicast	Gesamtanzahl der Multicast-Pakete, die das Telefon gesendet hat.
Tx unicast	Gesamtanzahl der Unicast-Pakete, die das Telefon gesendet hat.
Rx Frames	Gesamtanzahl der Pakete, die das Telefon empfangen hat.
Rx broadcast	Gesamtanzahl der Broadcast-Pakete, die das Telefon empfangen hat.

Element	Beschreibung
Rx multicast	Gesamtanzahl der Multicast-Pakete, die das Telefon empfangen hat.
Rx unicast	Gesamtanzahl der Unicast-Pakete, die das Telefon empfangen hat.
Rx PacketNoDes	Gesamtanzahl der Shed-Pakete, die vom DMA-Deskriptor (Direct Memory Access) verursacht werden.

Netzwerk-Webseiten

In der folgenden Tabelle werden die Informationen auf den Netzwerkbereich-Webseiten erläutert.

Hinweis Wenn Sie unter „Netzwerkstatistik“ auf den Link **Netzwerk** klicken, wird eine Seite mit dem Titel „Port-Informationen“ angezeigt.

Tabelle 30: Elemente des Netzwerkbereichs

Element	Beschreibung
Rx totalPkt	Gesamtanzahl der Pakete, die das Telefon empfangen hat.
Rx multicast	Gesamtanzahl der Multicast-Pakete, die das Telefon empfangen hat.
Rx broadcast	Gesamtanzahl der Broadcast-Pakete, die das Telefon empfangen hat.
Rx unicast	Gesamtanzahl der Unicast-Pakete, die das Telefon empfangen hat.
Rx tokenDrop	Gesamtanzahl der Pakete, die aufgrund unzureichender Ressourcen verworfen wurden (beispielsweise FIFO-Überlauf).
Tx totalGoodPkt	Gesamtanzahl der gültigen Pakete (Multicast, Broadcast und Unicast), die das Telefon empfangen hat.
Tx broadcast	Gesamtanzahl der Broad-Pakete, die das Telefon gesendet hat.
Tx multicast	Gesamtanzahl der Multicast-Pakete, die das Telefon gesendet hat.

Element	Beschreibung
LLDP FramesOutTotal	Gesamtanzahl der LLDP-Rahmen, die das Telefon gesendet hat.
LLDP AgeoutsTotal	Gesamtanzahl der LLDP-Rahmen, die die Zeit um Cache überschritten haben.
LLDP FramesDiscardedTotal	Gesamtanzahl der LLDP-Rahmen, die verworfen wurden, da die erforderlichen TLVs fehlen, unzulässig sind oder zu lange Zeichenfolgen enthalten.
LLDP FramesInErrorsTotal	Gesamtanzahl der LLDP-Rahmen, die mit mindestens einem erkennbaren Fehler empfangen wurden.
LLDP FramesInTotal	Gesamtanzahl der LLDP-Rahmen, die das Telefon empfangen hat.
LLDP TLVDiscardedTotal	Gesamtanzahl der LLDP TLVs, die verworfen werden.
LLDP TLVUnrecognizedTotal	Gesamtanzahl der LLDP TLVs, die auf dem Telefon nicht erkannt werden.
CDP Nachbargeräte-ID	ID eines Geräts, das mit diesem Port verbunden ist, der von CDP erkannt wurde.
CDP Nachbar-IP-Adresse	IP-Adresse des Nachbargeräts, das von CDP erkannt wurde.
CDP Nachbar-IPv6-Adresse	IPv6-Adresse des Nachbargeräts, das von CDP erkannt wurde.
CDP Nachbar-Port	Nachbargeräteport, mit dem das Telefon verbunden ist, der von CDP erkannt wurde.
LLDP Nachbargeräte-ID	ID eines mit diesem Port verbundenen Geräts, das von LLDP erkannt wurde.
LLDP Nachbar-IP-Adresse	IP-Adresse des Nachbargeräts, das von LLDP erkannt wurde.
LLDP Nachbar-IPv6-Adresse	IPv6-Adresse des Nachbargeräts, das von CDP erkannt wurde.
LLDP Nachbar-Port	Nachbargeräteport, mit dem das Telefon verbunden ist, der von LLDP erkannt wurde.
Port-Informationen	Geschwindigkeits- und Duplex-Informationen.

Webseiten für Konsolenprotokolle, Speicherauszüge, Statusmeldungen und Fehlersuchanzeige

Über die Hyperlinks „Konsolenprotokolle“, „Speicherauszüge“, „Statusmeldungen“ und „Fehlersuchanzeige“ unter der Überschrift „Geräteprotokolle“ können Sie auf Informationen zugreifen, die Sie beim Überwachen des Telefons und bei der Fehlerbehebung unterstützen.

- Konsolenprotokolle: Hier finden sich Hyperlinks zu den einzelnen Protokolldateien. Konsolenprotokolldateien enthalten Debug- und Fehlermeldungen, die das Telefon empfangen hat.
- Speicherauszüge: Hier finden sich Hyperlinks zu einzelnen Dumpdateien. Die Speicherauszugdateien enthalten Daten von einem Telefonabsturz.
- Statusmeldungen: Zeigt die 10 letzten Statusmeldungen an, die das Telefon seit dem letzten Start generiert hat. Sie können diese Informationen auch dem Fenster „Statusmeldungen“ auf dem Telefon entnehmen.
- Fehlersuchanzeige: Hier werden Debug-Meldungen angezeigt, die für Cisco TAC hilfreich sein können, wenn Sie Unterstützung bei der Fehlerbehebung anfordern.

Webseite „Streaming-Statistik“

Ein Cisco IP-Telefon kann Informationen gleichzeitig zu oder von drei Geräten streamen. Ein Telefon streamt Informationen, wenn ein Anruf aktiv ist oder ein Service ausgeführt wird, der Audio oder Daten sendet bzw. empfängt.

Die Streaming-Statistikbereiche auf einer Telefon-Webseite enthalten Informationen über die Streams.

Um die Streaming-Statistik anzuzeigen, öffnen Sie die Webseite für das Telefon und klicken Sie auf den Hyperlink **Stream**.

In der folgenden Tabelle werden die Elemente im Bereich Streaming-Statistik beschrieben.

Tabelle 31: Streaming-Statistikfelder

Element	Beschreibung
Remoteadresse	IP-Adresse und UDP-Port des Ziel des Streams.
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.
Hostname	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.

Element	Beschreibung
Sender - Oktette	Gesamtanzahl der Nutzlast-Oktette, die das Telefon in RTP-Datenpaketen gesendet hat, seit die Verbindung hergestellt wurde. Der Wert ist 0, wenn die Verbindung auf den Empfangsmodus festgelegt ist.
Sender – Codec	Typ der Audiocodierung für den gesendeten Stream.
Sender – Gesendete Berichte (siehe Hinweis)	Wie oft der RTCP-Senderbericht gesendet wurde.
Sender – Sendezeit Bericht (siehe Hinweis)	Interner Zeitstempel, der angibt, wann der letzte RTCP-Senderbericht gesendet wurde.
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 alle verzögerten und doppelten Pakete umfasst. Der Wert ist 0, wenn die Verbindung auf den Sendemodus festgelegt ist.
Durchschnittlicher Jitter	Schätzung der mittleren Abweichung der Zwischenankunftszeit der RTP-Datenpakete in Millisekunden. Der Wert ist 0, wenn die Verbindung auf den Sendemodus festgelegt ist.
Empfänger - Codec	Typ der für den Streaming-Empfang verwendeten Audiocodierung.
Empfänger – Gesendete Berichte (siehe Hinweis)	Wie oft die RTCP-Empfängerberichte gesendet wurden.
Empfänger – Sendezeit Bericht (siehe Hinweis)	Interner Zeitstempel, der angibt, wann der RTCP-Empfängerbericht gesendet wurde.
Empfänger – Pakete	Gesamtanzahl der RTP-Datenpakete, die das Telefon empfangen hat, seit die Verbindung hergestellt wurde. Umfasst Pakete, die von verschiedenen Quellen empfangen wurden, wenn der Anruf ein Multicast-Anruf ist. Der Wert ist 0, wenn die Verbindung auf den Sendemodus festgelegt ist.

Element	Beschreibung
Empfänger – Oktette	Gesamtanzahl der Nutzlast-Oktette, die das Telefon in RTP-Datenpaketen empfangen hat, seit die Verbindung hergestellt wurde. Umfasst Pakete, die von verschiedenen Quellen empfangen wurden, wenn der Anruf ein Multicast-Anruf ist. Der Wert ist 0, wenn die Verbindung auf den Sendemodus festgelegt ist.
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)	Höchstes Intervall der Verdeckungsrate ab Beginn des Voicestreams.
Verdeckung Sekunden	Anzahl der Sekunden mit Verdeckungsereignissen (verlorene Rahmen) ab Beginn des Voicestreams (einschließlich schwerwiegende Verdeckung).
Severely Conceal Seconds (Verdeckung (schwerwiegend) Sekunden)	Anzahl der Sekunden mit mehr als fünf Prozent Verdeckungsereignissen (verlorene Rahmen, ab Beginn des Voicestreams.
Latenz (siehe Hinweis)	Geschätzte Netzwerklatenz in Millisekunden. Mittelwert der Round-Trip-Verzögerung, der gemessen wird, wenn RTCP-Empfängerberichtsblöcke empfangen werden.
Maximaler Jitter	Maximaler Wert des unmittelbaren Jitters in Millisekunden.
Sender-Größe	RTP-Paketgröße in Millisekunden für den übermittelten Stream.
Sender - Empfangene Berichte (siehe Hinweis)	Wie oft die RTCP-Senderberichte empfangen wurden.
Sender - Empfangszeit Bericht (siehe Hinweis)	Letzter Zeitpunkt, zu dem ein RTCP-Senderbericht empfangen wurde.
Empfänger – Größe	RTP-Paketgröße in Millisekunden für den empfangenen Stream.

Element	Beschreibung
Empfänger – Verworfen	RTP-Pakete, die vom Netzwerk empfangen, aber von den Jitter-Puffern verworfen wurden.
Empfänger - Empfangene Berichte (siehe Hinweis)	Wie oft die RTCP-Empfängerberichte empfangen wurden.
Empfänger - Empfangszeit Bericht (siehe Hinweis)	Zeitpunkt, an dem zuletzt ein RTCP-Empfängerbericht empfangen wurde.

Hinweis Wenn das RTP-Steuerungsprotokoll deaktiviert ist, werden für dieses Feld keine Daten erzeugt. In diesem Fall wird der Wert 0 angezeigt.

Informationen im XML-Format vom Telefon anfordern

Für die Fehlerbehebung können Sie Informationen vom Telefon anfordern. Die Informationen werden im XML-Format ausgegeben. Folgende Informationen stehen zur Verfügung:

- CallInfo: Informationen zu Anrufsitzungen für eine bestimmte Leitung.
- LineInfo: Informationen zur Leitungskonfiguration für das Telefon.
- ModeInfo: Informationen zum Telefonmodus.

Vorbereitungen

Zum Abrufen der Informationen muss der Webzugriff aktiviert sein.

Das Telefon muss einem Benutzer zugeordnet sein.

Prozedur

Schritt 1 Geben Sie für Anrufinformationen die folgende URL in einen Browser ein: **`http://<IP-Adresse des Telefons>/CGI/Java/CallInfo<x>`**

Dabei ist

- <*IP-Adresse des Telefons*> 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://<IP-Adresse des Telefons>/CGI/Java/LineInfo`**

Dabei ist

- <*IP-Adresse des Telefons*> die IP-Adresse des Telefons.

Der Befehl gibt ein XML-Dokument zurück.

Schritt 3 Geben Sie für Modusinformationen die folgende URL in einen Browser ein: **`http://<IP-Adresse des Telefons>/CGI/Java/ModeInfo`**

Dabei ist

- <*IP-Adresse des Telefons*> die IP-Adresse des Telefons.

Der Befehl gibt ein XML-Dokument zurück.

Beispielausgabe für „CallInfo“

Der folgende XML-Code ist ein Beispiel für die Ausgabe des Befehls „CallInfo“.

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneCallLineInfo>
  <Prompt/>
  <Notify/>
  <Status/>
  <LineDirNum>1030</LineDirNum>
  <LineState>CONNECTED</LineState>
  <CiscoIPPhoneCallInfo>
     <CallState>CONNECTED</CallState>
     <CallType>INBOUND</CallType>
     <CallingPartyName/>
     <CallingPartyDirNum>9700</CallingPartyDirNum>
     <CalledPartyName/>
     <CalledPartyDirNum>1030</CalledPartyDirNum>
     <HuntPilotName/>
     <CallReference>30303060</CallReference>
     <CallDuration>12835</CallDuration>
     <CallStatus>null</CallStatus>
     <CallSecurity>UNAUTHENTICATED</CallSecurity>
     <CallPrecedence>ROUTINE</CallPrecedence>
     <FeatureList/>
   </CiscoIPPhoneCallInfo>
   <VisibleFeatureList>
     <Feature Position="1" Enabled="true" Label="End Call"/>
     <Feature Position="2" Enabled="true" Label="Show Detail"/>
   </VisibleFeatureList>
</CiscoIPPhoneCallLineInfo>
```

Beispielausgabe für „LineInfo“

Der folgende XML-Code ist ein Beispiel für die Ausgabe des Befehls „LineInfo“.

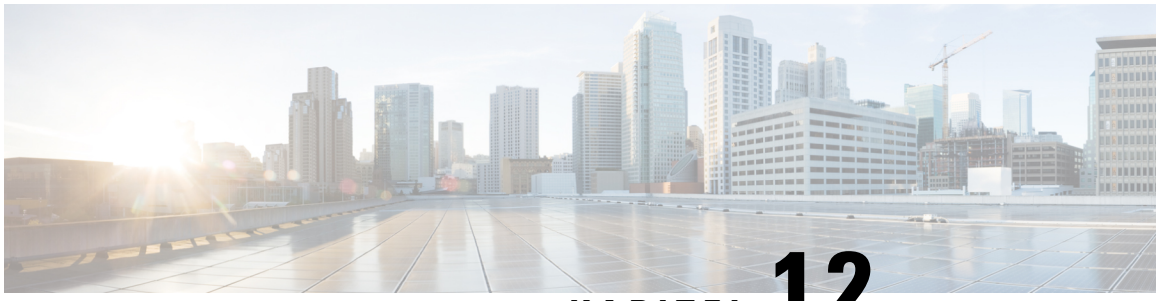
```
<CiscoIPPhoneLineInfo>
   <Prompt/>
   <Notify/>
   <Status>null</Status>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1028</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
```

```
      <RingerName>Chirp1</RingerName>
      <LineLabel/>
      <LineIconState>ONHOOK</LineIconState>
    </CiscoIPPhoneLines>
    <CiscoIPPhoneLines>
      <LineType>9</LineType>
      <lineDirNum>1029</lineDirNum>
      <MessageWaiting>NO</MessageWaiting>  <RingerName>Chirp1</RingerName>
      <LineLabel/>
      <LineIconState>ONHOOK</LineIconState>
    </CiscoIPPhoneLines>
    <CiscoIPPhoneLines>
      <LineType>9</LineType>
      <lineDirNum>1030</lineDirNum>
      <MessageWaiting>NO</MessageWaiting>
      <RingerName>Chirp1</RingerName>
      <LineLabel/>
      <LineIconState>CONNECTED</LineIconState>
    </CiscoIPPhoneLines>
    <CiscoIPPhoneLines>
      <LineType>2</LineType>
      <lineDirNum>9700</lineDirNum>
      <MessageWaiting>NO</MessageWaiting>
      <LineLabel>SD9700</LineLabel>
      <LineIconState>ON</LineIconState>
  </CiscoIPPhoneLines>
</CiscoIPPhoneLineInfo>
```

Beispielausgabe für „ModeInfo“

Der folgende XML-Code ist ein Beispiel für die Ausgabe des Befehls „ModeInfo“.

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
   <PlaneTitle>Applications</PlaneTitle>
   <PlaneFieldCount>12</PlaneFieldCount>
   <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
   <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
   <Prompt></Prompt>
   <Notify></Notify>
   <Status></Status>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Call History</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Preferences</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   ...
</CiscoIPPhoneModeInfo>
```



KAPITEL 12

Wartung

Konferenztelefon neu starten oder zurücksetzen

Sie können ein Telefon einfach zurücksetzen, um es nach einem Fehler wiederherzustellen. Zudem ist es möglich, die Konfigurations- und Sicherheitseinstellungen auf die werksseitigen Standardeinstellungen zurückzusetzen.

Konferenztelefon neu starten

Wenn Sie das Telefon neu starten, gehen alle Änderungen an Benutzer- und Netzwerk-Setup, die nicht im Flash-Speicher im Telefon gespeichert wurden, verloren.

Prozedur

Drücken Sie **Einstellungen** > **Verwaltereinstellungen** > **Einstellungen zurücksetzen** > **Gerät zurücksetzen**.

Die Einstellungen des Konferenztelefons über das Telefonmenü zurücksetzen

Prozedur

Schritt 1 Drücken Sie **Einstellungen**.

Schritt 2 Wählen Sie **Verwaltereinstellungen** > **Einstellungen zurücksetzen** aus.

Schritt 3 Wählen Sie die Art der Zurücksetzung aus.

- **Alle**: Stellt die Werkseinstellungen wieder her.
- **Gerät zurücksetzen**: Setzt das Gerät zurück. Die vorhandenen Einstellungen werden nicht geändert.
- **Netzwerk**: Setzt die Netzwerkkonfiguration auf die Standardeinstellungen zurück.

- **Servicemodus**: Löscht den aktuellen Servicemodus, deaktiviert das VPN und startet das Telefon neu.
- **Sicherheit**: Setzt die Sicherheitskonfiguration auf die Standardeinstellungen zurück. Bei Auswahl dieser Option wird die CTL-Datei gelöscht.

Schritt 4 Drücken Sie **Zurücksetzen** oder **Abbrechen**.

Konferenztelefon über das Tastenfeld auf die Werkseinstellungen zurücksetzen

Wenn Sie das Telefon über das Tastenfeld zurücksetzen, werden die Werkseinstellungen wiederhergestellt.

Prozedur

Schritt 1 Stecken Sie das Telefon aus:

- Wenn Sie PoE verwenden, stecken Sie das LAN-Kabel aus.
- Wenn Sie den Power Cube verwenden, stecken Sie ihn aus.

Schritt 2 Warten Sie 5 Sekunden lang.

Schritt 3 Halten Sie **#** gedrückt und schließen Sie das Telefon wieder an.

Schritt 4 Wenn das Telefon gestartet wird, leuchtet die LED-Leiste auf. Sobald sich die LED-Leiste einschaltet, drücken Sie nacheinander **123456789*0#**.

Nachdem Sie diese Tasten gedrückt haben, durchläuft das Telefon den Prozess zum Zurücksetzen auf die Werkseinstellungen.

Wenn Sie die Tasten nicht in der richtigen Reihenfolge drücken, wird das Telefon normal gestartet.

Vorsicht Schalten Sie das Telefon nicht aus, bis der Prozess abgeschlossen ist und der Hauptbildschirm angezeigt wird.

Überwachung der Sprachqualität

Um die Sprachqualität von Anrufen zu messen, die im Netzwerk gesendet und empfangen werden, verwenden die Cisco IP-Telefone diese Statistiken, 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 32: 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.	• Rauschen oder Verzerrung im Audiokanal, beispielsweise Echo oder Audiopegel. • Aufeinanderfolgende Anrufe, die mehrmals codiert/decodiert werden, beispielsweise Anrufe in einem Mobilfunknetz oder Callingcard-Netzwerk. • Akustische Probleme verursacht vom Lautsprecher, Mobiltelefon oder drahtlosen Headset. Überprüfen Sie die Paketübermittlung (TxCnt) und den Paketempfang (RxCnt), um sicherzustellen, dass die Sprachpakete gesendet werden.
Die MOS LQK-Anzahl verringert sich wesentlich	Netzwerkstörung durch Paketverlust und hohen Jitter: • Die durchschnittliche MOS LQK-Anzahl verringert sich und kann auf eine weitverbreitete und einheitliche Verminderung hinweisen. • Einzelne MOS LQK-Verminderungen können auf eine stoßweise Verminderung hinweisen. Überprüfen Sie die Verdeckungsrate und Sekunden der Verdeckung auf einen Hinweis auf Paketverlust und Jitter.

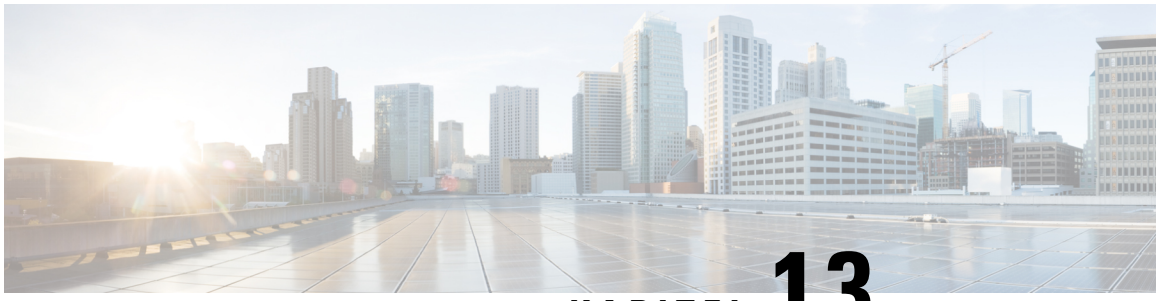
Metrikänderung	Bedingung
Die MOS LQK-Anzahl erhöht sich wesentlich	• Überprüfen Sie, ob das Telefon einen anderen als den erwarteten Codec verwendet (RxType und TxType). • Überprüfen Sie, ob sich die MOS LQK-Version geändert hat, nachdem eine Firmware aktualisiert wurde.

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 13

Fehlerbehebung

Allgemeine Informationen zur Fehlerbehebung

Die folgende Tabelle enthält allgemeine Informationen zur Problembehandlung für Cisco IP-Telefon.

Tabelle 33: Problembehandlung für Cisco IP-Telefone

Zusammenfassung	Erklärung
Länger dauernde Broadcast-Stürme verursachen, dass IP-Telefone zurückgesetzt werden und Anrufe nicht möglich sind.	Ein länger dauernder Broadcast-Sturm der Ebene 2 (mehrere Minuten) in einem Sprach-VLAN kann verursachen, dass IP-Telefone zurückgesetzt werden, ein aktiver Anruf getrennt wird und kein Anruf getätigt oder angenommen werden kann. Die Telefone können nicht verwendet werden, bis ein Broadcast-Sturm beendet ist.

Zusammenfassung	Erklärung
Eine Netzwerkverbindung vom Telefon auf eine Arbeitsstation verlegen	Wenn Sie Ihr Telefon über eine Netzwerkverbindung betreiben und das Netzwerkkabel ausstecken möchten, um es in einen Desktopcomputer einzustecken, müssen Sie vorsichtig vorgehen. **Vorsicht** Die Netzwerkkarte im Computer kann keine Energie über die Netzwerkverbindung empfangen. Wenn Energie über die Verbindung übertragen wird, kann die Netzkarte zerstört werden. Um eine Netzkarte zu schützen, warten Sie 10 Sekunden oder länger, nachdem Sie das Kabel aus dem Telefon ausgesteckt haben, bevor Sie das Kabel in einen 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.
Die Telefonkonfiguration ändern	Die Einstellungen für das Administratorkennwort sind standardmäßig gesperrt, um zu verhindern, dass die Benutzer Änderungen vornehmen, die die Netzwerkverbindung beeinträchtigen können. Sie müssen die Einstellungen für das Administratorkennwort entsperren, bevor Sie sie konfigurieren können. Weitere Informationen finden Sie unter Anwenden eines Telefonkennworts, auf Seite 32. **Hinweis** Wenn im allgemeinen Telefonprofil kein Administratorkennwort festgelegt ist, dann können die Benutzer die Netzwerkeinstellungen ändern.
Codec-Konflikt zwischen dem Telefon und einem anderen Gerät	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 oder ein Transcoder vorhanden ist, um den Service abzuwickeln. Weitere Informationen finden Sie unter Das Fenster „Anrufstatistik“ anzeigen, auf Seite 126.

Zusammenfassung	Erklärung
Sound-Sample-Konflikt zwischen dem Telefon und einem anderen Gerät	Die RxType- und TxType-Statistiken zeigen die Größe der Sprachpakete an, die in einer Konversation zwischen diesem Cisco IP-Telefon und anderen Geräten verwendet werden. Die Werte dieser Statistiken sollten übereinstimmen. Weitere Informationen finden Sie unter Das Fenster „Anrufstatistik“ anzeigen, auf Seite 126.
Loopback	Ein Loopback kann unter folgenden Bedingungen auftreten: • Die Option SW-Portkonfiguration auf dem Telefon ist auf 10 Halbduplex (10-BaseT/Halbduplex) festgelegt • Das Telefon wird über eine externe Stromversorgung betrieben. • Das Telefon ist ausgeschaltet (die Stromversorgung ist getrennt). In diesem Fall kann der Switch-Port auf dem Telefon deaktiviert werden und die folgende Meldung wird im Switch-Konsolenprotokoll angezeigt: HALF_DUX_COLLISION_EXCEED_THRESHOLD Um das Problem zu beheben, aktivieren Sie den Port erneut.

Startprobleme

Nachdem Sie ein Telefon im Netzwerk installiert und zu Cisco Unified Communications Manager hinzugefügt haben, sollte das Telefon, wie im entsprechenden Abschnitt beschrieben, gestartet werden.

Wenn das Telefon nicht richtig gestartet wird, lesen Sie die Informationen zur Fehlerbehebung in den folgenden Abschnitten.

Verwandte Themen

Telefonstart überprüfen, auf Seite 37

Cisco IP-Telefon wird nicht normal gestartet

Problem

Wenn Sie ein Cisco IP-Telefon in den Netzwerkport einstecken, durchläuft das Telefon den im entsprechenden Thema beschriebenen Startprozess nicht und auf dem Telefonbildschirm werden keine Informationen angezeigt.

Ursache

Die Ursache dafür, dass das Telefon den Startprozess nicht durchläuft, können defekte Kabel, schlechte Verbindungen, Netzwerkausfälle oder Funktionsstörungen des Telefons sein.

Lösung

Um festzustellen, ob das Telefon funktioniert, führen Sie die folgenden Aktionen aus, um andere potenzielle Probleme auszuschließen.

- Stellen Sie sicher, dass der Netzwerkport funktionsfähig ist:
  - Ersetzen Sie die Ethernet-Kabel durch Kabel, die nachweislich funktionieren.
  - Stecken Sie ein funktionierendes Cisco IP-Telefon von einem anderen Port aus und stecken Sie es in den Netzwerkport, um zu überprüfen, ob der Port aktiv ist.
  - Stecken Sie das Cisco IP-Telefon, das nicht gestartet wird, in einen anderen Netzwerkport ein, der nachweislich funktioniert.
  - Stecken Sie das Cisco IP-Telefon, das nicht gestartet wird, in den Port auf dem Switch, um die Patchpanel-Verbindung auszuschließen.
- Stellen Sie sicher, dass das Telefon mit Strom versorgt wird:
  - Wenn Sie eine externe Stromquelle verwenden, überprüfen Sie, ob die Steckdose funktioniert.
  - Für Inline-Strom verwenden Sie die externe Stromversorgung.
  - Wenn Sie die externe Stromversorgung verwenden, wechseln Sie zu einer Einheit, die funktioniert.
- Wenn das Telefon immer noch nicht richtig gestartet wird, schalten Sie das Telefon über das Sicherungs-Software-Image ein.
- Wenn das Telefon immer noch nicht richtig gestartet wird, setzen Sie es auf die Werkseinstellungen zurück.
- Wenn auf dem Display des Cisco IP-Telefon nach mindestens fünf Minuten keine Zeichen angezeigt werden, wenden Sie sich an den technischen Support von Cisco.

Verwandte Themen

Telefonstart überprüfen, auf Seite 37

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 kann nur richtig starten, wenn es mit dem Ethernet-Netzwerk verbunden und mit einem Cisco Unified Communications Manager-Server registriert ist.

Außerdem können Sicherheitsprobleme verhindern, dass das Telefon ordnungsgemäß gestartet wird. Weitere Informationen finden Sie unter Fehlerbehebungsverfahren, auf Seite 164.

Fehlermeldungen auf dem Telefon

Problem

Beim Starten des Telefons werden in Statusmeldungen Fehler gemeldet.

Lösung

Während das Telefon gestartet wird, können Sie auf Statusmeldungen zugreifen, die Informationen zur Ursache eines Problems anzeigen. Im Abschnitt „Fenster ‚Statusmeldungen' anzeigen" finden Sie Anweisungen für den Zugriff auf Statusmeldungen sowie eine Liste der potenziellen Fehler zusammen mit Erklärungen und Lösungen.

Verwandte Themen

Das Fenster „Statusmeldungen" anzeigen, auf Seite 116

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 164

Das Telefon kann sich nicht mit dem Server verbinden

Problem

Die Felder für IP-Adressen und Routing sind möglicherweise nicht richtig konfiguriert.

Lösung

Überprüfen Sie die IP-Adressen- und Routingeinstellungen auf dem Telefon. Wenn Sie DHCP verwenden, sollten diese Werte vom DHCP-Server bereitgestellt werden. Wenn Sie dem Telefon eine statische IP-Adresse zugewiesen haben, müssen Sie diese Werte manuell eingeben.

Verwandte Themen

DHCP-Einstellungen überprüfen, auf Seite 165

Das Telefon kann sich nicht über DNS verbinden

Problem

Die DNS-Einstellungen sind möglicherweise falsch.

Lösung

Wenn Sie DNS für den Zugriff auf den TFTP-Server oder Cisco Unified Communications Manager verwenden, müssen Sie einen DNS-Server angeben.

Verwandte Themen

Die DNS-Einstellungen überprüfen, auf Seite 167

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 finden Sie unter Service starten, auf Seite 167.

Die Konfigurationsdatei ist beschädigt

Problem

Wenn weiterhin Probleme mit einem bestimmten Telefon auftreten, die mit den anderen Vorschlägen in diesem Kapitel nicht behoben werden können, ist möglicherweise die Konfigurationsdatei beschädigt.

Lösung

Erstellen einer neuen Konfigurationsdatei für das Telefon.

Verwandte Themen

Erstellen einer neuen Konfigurationsdatei für das Telefon, auf Seite 166

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 44, 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 44.

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 156, falls Sie Hilfe benötigen.

Cisco IP-Telefon kann keine IP-Adresse abrufen

Problem

Wenn ein Telefon während des Starts keine IP-Adresse abrufen kann, befindet sich das Telefon möglicherweise nicht im gleichen Netzwerk oder VLAN wie der DHCP-Server oder der Switch-Port, mit dem das Telefon verbunden ist, ist deaktiviert.

Lösung

Stellen Sie sicher, dass das Netzwerk oder VLAN, mit dem das Telefon die Verbindung herstellt, auf den DHCP-Server zugreifen kann, und der Switch-Port aktiviert ist.

Probleme mit dem Zurücksetzen des Telefons

Wenn Benutzer melden, dass ihre Telefone während eines Anrufs oder im inaktiven Zustand zurückgesetzt werden, untersuchen Sie die Ursache. Wenn die Netzwerkverbindung und Cisco Unified Communications Manager-Verbindung stabil sind, sollte sich das Telefon nicht zurücksetzen.

Üblicherweise wird ein Telefon zurückgesetzt, wenn beim Verbinden mit dem Netzwerk oder Cisco Unified Communications Manager ein Problem auftritt.

Das Telefon wird aufgrund sporadischer Netzwerkausfälle zurückgesetzt

Problem

Das Netzwerk kann sporadisch ausfallen.

Lösung

Sporadische Netzwerkausfälle wirken sich unterschiedlich auf den Daten- und Sprachnachrichtenverkehr aus. Das Netzwerk ist möglicherweise sporadisch ausgefallen, ohne dass dies bemerkt wurde. In diesem Fall kann der Datenverkehr verloren gegangene Pakete erneut senden und sicherstellen, dass die Pakete empfangen und gesendet wurden. Beim Sprachdatenverkehr können verloren gegangene Pakete jedoch nicht erneut gesendet werden. Anstatt zu versuchen, über eine unterbrochene Netzwerkverbindung weiter zu übertragen, wird das Telefon zurückgesetzt und es wird versucht, die Netzwerkverbindung wiederherzustellen. Weitere Informationen zu bekannten Problemen im Sprachnetzwerk erhalten Sie vom Systemadministrator.

Das Telefon wird aufgrund von DHCP-Einstellungsfehlern zurückgesetzt

Problem

Die DHCP-Einstellungen sind möglicherweise falsch.

Lösung

Überprüfen Sie, ob das Telefon richtig für DHCP konfiguriert ist. Überprüfen Sie, ob der DHCP-Server richtig konfiguriert ist. Überprüfen Sie, die DHCP-Leasedauer. Wir empfehlen, eine Leasedauer von 8 Tagen festzulegen.

Verwandte Themen

DHCP-Einstellungen überprüfen, auf Seite 165

Das Telefon wird aufgrund einer falschen statischen IP-Adresse zurückgesetzt

Problem

Die statische IP-Adresse, die dem Telefon zugewiesen ist, ist möglicherweise ungültig.

Lösung

Wenn Sie dem Telefon eine statische IP-Adresse zuweisen, überprüfen Sie, ob Sie die richtigen Einstellungen eingegeben haben.

Das Telefon wird bei hoher Netzwerkauslastung zurückgesetzt

Problem

Wenn das Telefon bei einer hohen Netzwerkauslastung zurückgesetzt wird, ist wahrscheinlich kein Sprach-VLAN aktiviert.

Lösung

Wenn Sie die Telefone in einem separaten zusätzlichen VLAN isolieren, wird die Qualität des Sprachverkehrs verbessert.

Das Telefon wird absichtlich zurückgesetzt

Problem

Wenn Sie nicht der einzige Administrator mit Zugriff auf Cisco Unified Communications Manager sind, sollten Sie sicherstellen, dass kein anderer Administrator die Telefone absichtlich zurückgesetzt hat.

Lösung

Sie können prüfen, ob Cisco IP-Telefon einen Befehl zum Zurücksetzen von Cisco Unified Communications Manager empfangen hat; drücken Sie dazu **Einstellungen** auf dem Telefon, und wählen Sie **Administratoreinstellungen** > **Status** > **Netzwerkstatistik**.

- Wenn im Feld Grund für den Neustart `Zurücksetzen-Zurücksetzen` angezeigt wird, hat das Telefon den Befehl Zurücksetzen/Zurücksetzen von Cisco Unified Communications Manager empfangen.
- Wenn im Feld Grund für den Neustart `Zurücksetzen-Neustart` angezeigt wird, wurde das Telefon heruntergefahren, da es den Befehl Zurücksetzen/Neustart von Cisco Unified Communications Manager empfangen hat.

Das Telefon wird aufgrund von DNS-Problemen oder anderen Verbindungsproblemen zurückgesetzt

Problem

Das Telefon wird fortlaufend zurückgesetzt und Sie vermuten, dass ein DNS-Problem oder anderes Verbindungsproblem aufgetreten ist.

Lösung

Wenn das Telefon fortlaufend zurückgesetzt wird, beheben Sie DNS-Probleme oder andere Verbindungsprobleme, indem Sie das Verfahren in DNS-Probleme oder Verbindungsprobleme identifizieren, auf Seite 165 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 aktualisiert CTL-Datei signiert hat, ist in der CTL-Datei auf dem Telefon nicht vorhanden.

Lösung

Ändern Sie den Sicherheitstoken in der CTL-Datei und installieren Sie die neue Datei auf dem Telefon.

Die CTL-Datei wird authentifiziert, aber andere Konfigurationsdateien werden nicht authentifiziert

Problem

Das Telefon kann keine Konfigurationsdateien, außer der CTL-Datei, authentifizieren.

Ursache

Es ist ein ungültiger TFTP-Eintrag vorhanden oder die Konfigurationsdatei wurde möglicherweise nicht vom entsprechenden Zertifikat in der Vertrauensliste des Telefons signiert.

Lösung

Überprüfen Sie den TFTP-Eintrag und das Zertifikat in der Vertrauensliste.

Die ITL-Datei wird authentifiziert, aber andere Konfigurationsdateien werden nicht authentifiziert

Problem

Das Telefon kann keine Konfigurationsdateien, außer der ITL-Datei, authentifizieren.

Ursache

Die Konfigurationsdatei wurde möglicherweise nicht vom entsprechenden Zertifikat in der Vertrauensliste des Telefons signiert.

Lösung

Signieren Sie die Konfigurationsdatei erneut mit dem richtigen Zertifikat.

TFTP-Autorisierung fehlgeschlagen

Problem

Das Telefon meldet einen TFTP-Autorisierungsfehler.

Ursache

Die TFTP-Adresse des Telefons ist nicht in der CTL-Datei vorhanden.

Wenn Sie eine neue CTL-Datei mit einem neuen TFTP-Eintrag erstellt haben, enthält die CTL-Datei auf dem Telefon keinen Eintrag für den neuen TFTP-Server.

Lösung

Überprüfen Sie die Konfiguration der TFTP-Adresse in der CTL-Datei auf dem Telefon.

Das Telefon wird nicht registriert

Problem

Das Telefon wird nicht mit Cisco Unified Communications Manager registriert.

Ursache

Die CTL-Datei enthält nicht die richtigen Informationen für den Cisco Unified Communications Manager-Server.

Lösung

Ändern Sie die Cisco Unified Communications Manager-Serverinformationen in der CTL-Datei.

Signierte Konfigurationsdateien werden nicht angefordert

Problem

Das Telefon fordert keine signierten Konfigurationsdateien an.

Ursache

Die CTL-Datei enthält keine TFTP-Einträge mit Zertifikaten.

Lösung

Konfigurieren Sie TFTP-Einträge mit Zertifikaten in der CTL-Datei.

Audioprobleme

In den folgenden Abschnitten wird das Beheben von Audioproblemen beschrieben.

Kein Sprachpfad

Problem

Mindestens eine Person in einem Anruf hört nichts.

Lösung

Wenn mindestens eine Person bei einem Anruf keinen Ton empfängt, besteht keine IP-Verbindung zwischen den Telefonen. Überprüfen Sie die Konfiguration der Router und Switches, um sicherzustellen, dass die IP-Verbindung ordnungsgemäß konfiguriert ist.

Abgehackte Sprache

Problem

Ein Benutzer beschwert sich über die abgehackte Sprache in einem Anruf.

Ursache

Möglicherweise liegt ein Konflikt in der Jitter-Konfiguration vor.

Lösung

Überprüfen Sie die AvgJtr- und MaxJtr-Statistik. Eine große Abweichung zwischen diesen Statistiken weist auf ein Problem mit dem Jitter im Netzwerk oder zeitweise hohe Netzwerkaktivitäten hin.

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.

Telefonproblemberichte im Cisco Unified Communications Manager erstellen

Sie können einen Problembericht für die Telefone im Cisco Unified Communications Manager generieren. Diese Aktion führt zu denselben Informationen, die der Softkey "Problemberichtstool (PRT)" auf dem Telefon generiert.

Der Problembericht enthält Informationen über das Telefon und die Headsets.

Prozedur

Schritt 1 Wählen Sie **Gerät** > **Telefon** in der Cisco Unified CM Administration aus.

Schritt 2 Klicken Sie auf **Suchen**, und wählen Sie ein oder mehrere Cisco IP-Telefone aus.

Schritt 3 Klicken Sie auf **Generate PRT for Selected** (PRT für ausgewählte generieren), um PRT-Protokolle für die Headsets zu erfassen, die auf den ausgewählten Cisco IP-Telefonen verwendet werden.

TFTP-Einstellungen überprüfen

Prozedur

Schritt 1 Drücken Sie auf dem Telefon auf **Anwendungen** .

Schritt 2 Drücken Sie auf dem Telefon auf **Einstellungen**.

Schritt 3 Wählen Sie **Netzwerk-Setup** > **IPv4-Setup** aus.

Schritt 4 Überprüfen Sie das Feld „TFTP-Server 1“.

Wenn Sie dem Telefon eine statische IP-Adresse zugewiesen haben, müssen Sie manuell einen Wert für die Option TFTP-Server 1 eingeben.

Wenn Sie DHCP verwenden, ruft das Telefon die Adresse für den TFTP-Server vom DHCP-Server ab. Überprüfen Sie, ob die IP-Adresse in Option 150 konfiguriert ist.

Schritt 5 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 6 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

Die MAC-Adresse des Telefons bestimmen, auf Seite 44
Konferenztelefon neu starten oder zurücksetzen, auf Seite 147

DHCP-Einstellungen überprüfen

Prozedur

Schritt 1 Drücken Sie auf dem Telefon auf **Anwendungen**  .

Schritt 2 Drücken Sie auf dem Telefon auf **Einstellungen**.

Schritt 3 Wählen Sie **Netzwerk-Setup** > **IPv4-Setup** aus.

Schritt 4 Überprüfen Sie das Feld „DHCP-Server“.

Wenn Sie dem Telefon eine statische IP-Adresse zugewiesen haben, müssen Sie keinen Wert für den DHCP-Server eingeben. Wenn Sie einen DHCP-Server verwenden, muss diese Option jedoch einen Wert

enthalten. Wenn kein Wert gefunden wird, überprüfen Sie das IP-Routing und die VLAN-Konfiguration. Lesen Sie das Dokument *Troubleshooting Switch Port and Interface Problems* unter der folgenden URL:

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

Schritt 5 Überprüfen Sie die Felder „IP-Adresse“, „Subnetzmaske“ und „Standardrouter“.

Wenn Sie dem Telefon eine statische IP-Adresse zuweisen, müssen Sie manuell Einstellungen für diese Optionen eingeben.

Schritt 6 Wenn Sie DHCP verwenden, überprüfen Sie die IP-Adressen, die der DHCP-Server verteilt.

Lesen Sie das Dokument *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* unter der folgenden URL:

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

Erstellen einer neuen Konfigurationsdatei für das Telefon

Wenn Sie ein Telefon aus der Cisco Unified Communications Manager-Datenbank entfernen, wird die Konfigurationsdatei vom Cisco Unified Communications Manager TFTP-Server gelöscht. Die Verzeichnisnummer oder Nummern des Telefons verbleiben in der Cisco Unified Communications Manager-Datenbank. Diese Nummern werden als nicht zugewiesene DNs bezeichnet und können für andere Geräte verwendet werden. Wenn nicht zugewiesene DNs nicht von anderen Geräten verwendet werden, löschen Sie diese DNs aus der Cisco Unified Communications Manager-Datenbank. Sie können den Routenplanbericht verwenden, um nicht zugewiesene Referenznummern anzuzeigen und zu löschen. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Wenn Sie die Tasten in einer Telefontastenvorlage ändern oder einem Telefon eine andere Telefontastenvorlage zuordnen, kann auf dem Telefon möglicherweise nicht mehr auf Verzeichnisnummern zugegriffen werden. Die Verzeichnisnummern sind dem Telefon noch in der Cisco Unified Communications Manager-Datenbank zugewiesen, aber das Telefon hat keine Taste, mit der Anrufe angenommen werden können. Diese Verzeichnisnummern sollten vom Telefon entfernt und gelöscht werden.

Prozedur

Schritt 1 Wählen Sie in Cisco Unified Communications Manager **Gerät** > **Telefon** aus und klicken Sie auf **Suchen**, um das Telefon zu suchen, auf dem Probleme aufgetreten sind.

Schritt 2 Wählen Sie **Löschen** aus, um das Telefon aus der Cisco Unified Communications Manager-Datenbank zu entfernen.

Hinweis Wenn Sie ein Telefon aus der Cisco Unified Communications Manager-Datenbank entfernen, wird die Konfigurationsdatei vom Cisco Unified Communications Manager TFTP-Server gelöscht. Die Verzeichnisnummer oder Nummern des Telefons verbleiben in der Cisco Unified Communications Manager-Datenbank. Diese Nummern werden als nicht zugewiesene DNs bezeichnet und können für andere Geräte verwendet werden. Wenn nicht zugewiesene DNs nicht von anderen Geräten verwendet werden, löschen Sie diese DNs aus der Cisco Unified Communications Manager-Datenbank. Sie können den Routenplanbericht verwenden, um nicht zugewiesene Referenznummern anzuzeigen und zu löschen.

Schritt 3 Fügen Sie das Telefon wieder zur Cisco Unified Communications Manager-Datenbank hinzu.

Schritt 4 Schalten Sie das Telefon aus und wieder ein.

Verwandte Themen

Methoden zum Hinzufügen von Telefonen, auf Seite 44
Dokumentation Cisco Unified Communications Manager, auf Seite 10

Die DNS-Einstellungen überprüfen

Prozedur

Schritt 1 Drücken Sie auf dem Telefon auf **Anwendungen** .

Schritt 2 Drücken Sie auf dem Telefon auf **Einstellungen**.

Schritt 3 Wählen Sie **Netzwerk-Setup** > **IPv4-Setup** aus.

Schritt 4 Stellen Sie sicher, dass das Feld „DNS-Server 1“ ordnungsgemäß eingerichtet ist.

Schritt 5 Vergewissern Sie sich außerdem, dass im DNS-Server ein CNAME-Eintrag für den TFTP-Server und für das Cisco Unified Communications Manager-System festgelegt ist.

Sie müssen auch sicherstellen, dass DNS für Reverse-Lookups konfiguriert ist.

Service starten

Ein Service muss aktiviert werden, bevor er gestartet oder beendet werden kann.

Prozedur

Schritt 1 Wählen Sie **Cisco Unified Wartbarkeit** in der Dropdown-Liste „Navigation“ in der Cisco Unified Communications Manager-Verwaltung aus und klicken Sie auf **Los**.

Schritt 2 Wählen Sie **Tools** > **Control Center – Funktionsservices** aus.

Schritt 3 Wählen Sie den primären Cisco Unified Communications Manager-Server in der Dropdown-Liste „Server“ aus.

Im Fenster werden die Servicenamen für den ausgewählten Server, der Status der Services und das Servicefeld zum Starten und Beenden eines Services angezeigt.

Schritt 4 Wenn ein Service beendet wurde, klicken Sie auf das entsprechende Optionsfeld und anschließend auf **Starten**.

Das Servicestatussymbol ändert sich von einem Quadrat in einen Pfeil.

Debuginformationen über Cisco Unified Communications Manager verwalten

Wenn mit dem Telefon Probleme auftreten, die Sie nicht beheben können, kann Cisco TAC Ihnen Unterstützung bieten. Sie müssen das Debugging für das Telefon aktivieren, anschließend das Problem reproduzieren, und dann das Debugging wieder deaktivieren und die Protokolle zur Analyse an TCA senden.

Da beim Debugging detaillierte Informationen erfasst werden, kann es aufgrund der umfangreichen Datenübertragung dazu kommen, dass das Telefon langsamer reagiert. Nach dem Erfassen der Protokolle sollten Sie das Debugging deaktivieren, damit das Telefon wieder ordnungsgemäß funktioniert.

Die Fehlersuchinformationen können einen einstelligen Code enthalten, der den Schweregrad der Situation wiedergibt. Situationen werden wie folgt bewertet:

- 0 - Notfall
- 1 - Alarm
- 2 - Kritisch
- 3 - Fehler
- 4 - Warnung
- 5 - Benachrichtigung
- 6 – Informationen
- 7 – Debuggen

Wenden Sie sich an das Cisco TAC für weitere Informationen und Hilfe.

Prozedur

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

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

Schritt 2 Legen Sie die folgenden Parameter fest:

- Protokollprofil – Werte: Voreinstellung (Standard), Standard, Telefonie, SIP, UI, Netzwerk, Medien, Update, Zubehör, Sicherheit, EnergyWise, MobileRemoteAccess
- Remoteprotokoll – Werte: Deaktivieren (Standard), Aktivieren
- IPv6-Protokollserver oder Protokollserver – IP-Adresse (IPv4- oder IPv6-Adresse)

Hinweis Wenn der Protokollserver nicht erreicht werden kann, sendet das Telefon keine Debugmeldungen mehr.

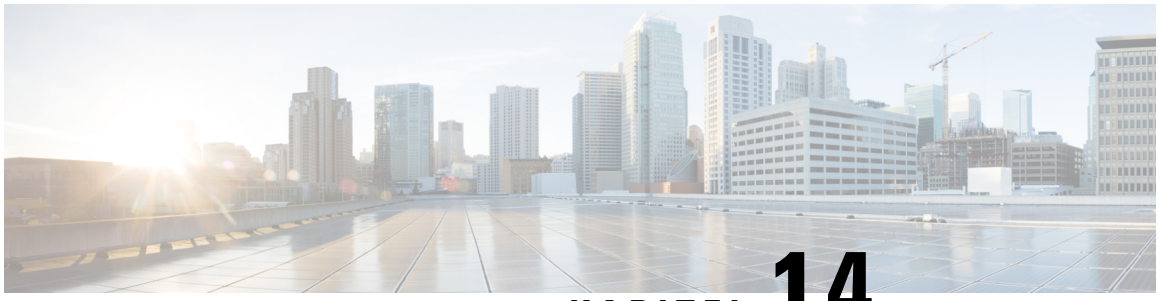
- Das Format der IPv4-Protokollserveradresse ist **`address:<port>@@base=<0-7>;pfs=<0-1>`**

- Das Format der IPv6-Protokollserveradresse ist **`[address]:<port>@@base=<0-7>;pfs=<0-1>`**
- Dabei gilt:
  - Die IPv4-Adresse wird mit Punkten (.) getrennt.
  - Die IPv6-Adresse wird mit Doppelpunkten (:) getrennt.

Zusätzliche Informationen zur Problembehandlung

Wenn Sie weitere Fragen zur Fehlerbehebung für Ihr Telefon haben, gehen Sie zur folgenden Cisco Website und navigieren Sie zum gewünschten Telefonmodell:

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



KAPITEL 14

Unterstützung von Benutzern in anderen Ländern

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 10

Internationaler Support für Anrufprotokollierung

Wenn Ihr Telefonsystem für die internationale Anrufprotokollierung (Anrufernormalisierung) konfiguriert ist, zeigen die Einträge für die Anrufprotokolle, die Wahlwiederholung oder das Anrufverzeichnis möglicherweise ein Pluszeichen (+) an, das die internationale Escapesequenz für Ihren Standort darstellt.

Abhängig von der Konfiguration Ihres Telefonsystems kann das Pluszeichen durch die richtige internationale Vorwahl ersetzt werden oder Sie müssen die Nummer vor dem Wählen bearbeiten, um das Pluszeichen durch die internationale Escapesequenz für Ihren Standort zu ersetzen. Obwohl im Anrufprotokoll oder Verzeichniseintrag die vollständige internationale Nummer des eingehenden Anrufs angezeigt wird, kann auf dem Telefondisplay die gekürzte lokale Version der Nummer ohne Landesvorwahl angezeigt werden.

Sprachbeschränkung

Für die folgenden asiatischen Gebietsschemata besteht keine lokalisierte KATE-Unterstützung (Keyboard Alphanumeric Text Entry):

- Chinesisch (China)
- Chinesisch (Hongkong)
- Chinesisch (Taiwan)
- Japanisch (Japan)
- Koreanisch (Korea, Republik)

Stattdessen wird der standardmäßige englische KATE (USA) für den Benutzer angezeigt.

Beispiel: Auf dem Telefonbildschirm wird Text in Koreanisch angezeigt, die Taste **2** auf dem Tastenfeld zeigt aber **a b c 2 A B C** an.