Cisco Unified Communications Manager Cisco IP 전화회의 전화기 8832 관리 설명서

초판: 2017년 9월 15일

최종 변경: 2023년 6월 16일

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

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 명시적이거나 묵시적인 보증도 하지 않습니다. 제품의 활용 분야나 용도에 대한 책임은 온전히 사용자 본인에게 있습니다.

동봉한 제품에 대한 소프트웨어 라이센스 및 제한된 보증은 제품과 함께 제공된 정보 패킷의 내용을 따르며 여기에 인용된 내용은 참조입니다. 소프트웨어 라이센스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

클래스 A 장치의 FCC 규정 준수에 관한 정보: 이 장비는 테스트를 거쳐 FCC 규정 15부에 의거하여 클래스 A 디지털 장치 제한 규정을 준수함이 확인되었습니다. 이러한 제한은 장비가 상업 환경에서 작동될 때 유해한 전파 혼선으로부터 적정한 수준의 보호를 제공하기 위해 고안되었습니다. 이 장비는 무선 주파수 에너지를 생성, 사용 및 방사하므로 지침에 따라 설치하여 사용하지 않을 경우 무선 통신에서 유해한 전파 혼선을 일으킬 수 있습니다. 주거 지역에서 이 장비의 작동은 유해한 전파 혼선을 야기할 가능성이 있으며, 그 경우에 사용자는 자비로 전파 혼선을 시정해야 합니다.

클래스 B 장치의 FCC 규정 준수에 관한 정보: 이 장비는 테스트를 거쳐 FCC 규정 15부에 의거하여 클래스 B 디지털 장치 제한 규정을 준수함이 확인되었습니다. 이러한 제한은 주거용 설치 시 유해한 전파 혼선으로부터 적정한 수준의 보호를 제공하기 위해 고안되었습니다. 이 장비는 무선 주파수 에너지를 생성, 사용 및 방사하므로 지침에 따라 설치하여 사용하지 않을 경우 무선 통신에서 유해한 전파 혼선을 일으킬 수 있습니다. 특정한 설치에서 전파 혼선이 발생하지 않는다는 보장은 없습니다. 본 장비를 켜거나 끌 때 라디오 또는 TV 수신에 전파 혼선을 일으키는 경우, 다음 중 하나 이상의 조치를 수행하여 전파 혼선을 해결해 보십시오.

- 수신 안테나의 방향을 조정하거나 다시 설치합니다.
- 장비와 수신기 사이의 간격을 늘립니다.
- 장비를 수신기가 연결된 회로와 다른 회로의 콘센트에 연결합니다.
- 구매처 또는 전문 라디오/TV 기사에게 지원을 요청합니다.

Cisco에서 승인하지 않은 방식으로 이 제품을 수정하면 FCC 승인이 무효화되고 제품 작동 권한을 상실할 수 있습니다.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 University of California, Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright ⓒ 1981, Regents of the University of California.

여기에 언급된 기타 모든 보증에도 불구하고 이러한 공급자의 모든 문서 및 소프트웨어는 모든 결함이 포함된 "있는 그대로" 제공됩니다. CISCO 및 위에서 언급한 공급자는 상품성, 특정 목적에의 적합성 및 비침해에 대한 보증을 포함하되 이에 제한되지 않으며 거래 과정, 사용 또는 거래 관행으로부터 발생되는 모든 명시적이거나 묵시적인 보증을 부인합니다.

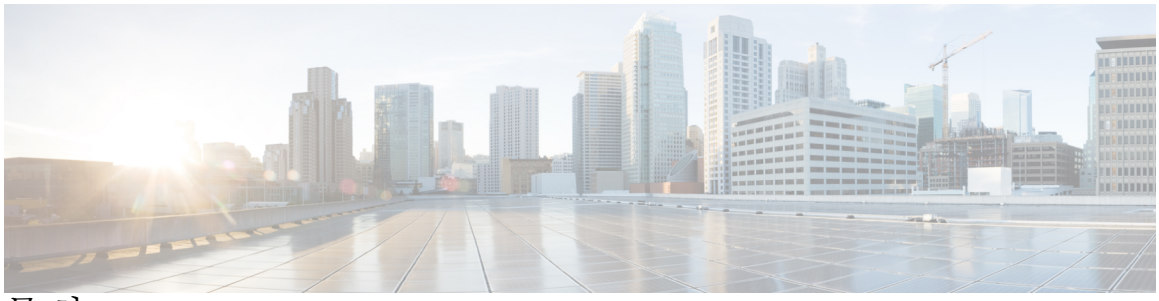
CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 인터넷 프로토콜(IP) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예, 명령 디스플레이 출력, 네트워크 토폴로지 다이어그램 및 기타 그림은 설명을 위한 목적으로만 표시됩니다. 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

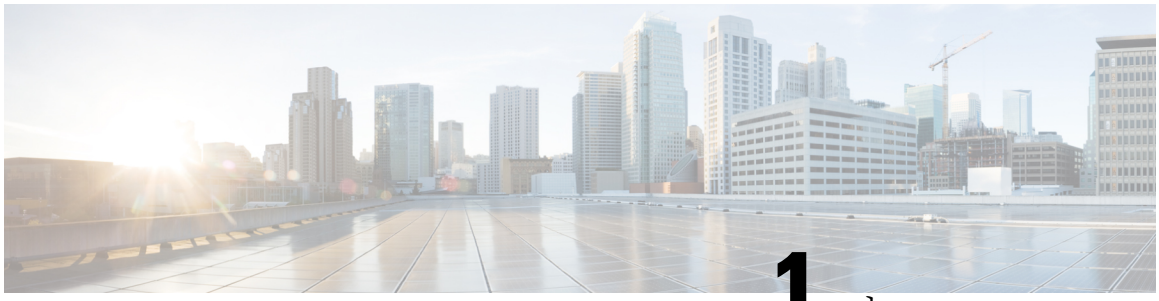
모든 인쇄된 사본 및 이 문서의 중복된 소프트 복사본은 제어 대상이 아닌 것으로 간주됩니다. 최신 버전에 대한 현재 온라인 버전을 참조하십시오.

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다. 각 지사의 주소 및 전화번호는 Cisco 웹사이트(www.cisco.com/go/office)에서 확인하십시오.

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)



목 차



1 장

신규 및 변경된 정보

펌웨어 릴리스 14.2(1)에 대한 새 정보 및 변경된 정보

다음 정보는 각 펌웨어 릴리스 14.2(1)에 대한 새로운 기능 또는 변경된 기능입니다.

기능	신규 또는 변경
SRST에서 SIP OAuth 지원	전화기 네트워크의 보안 강화, 76 페이지

펌웨어 릴리스 14.1(1)에 대한 새 정보 및 변경된 정보

다음 정보는 각 펌웨어 릴리스 14.1(1)에 대한 새로운 기능 또는 변경된 기능입니다.

기능	신규 또는 변경
프록시 TFTP 지원을 위한 SIP OAuth	전화기 네트워크의 보안 강화, 76 페이지
전환 로드 없이 전화기 마이그레이션	전화기를 다중 플랫폼 전화기로 직접 마이그레이션, 97 페이지

펌웨어 릴리스 14.0(1)에 대한 새 정보 및 변경된 정보

표 *1:* 신규 및 변경된 정보

기능	신규 또는 변경
통화 지정 보류 모니터링 개선 기능	제품별 구성, 102 페이지
SIP OAuth 개선 기능	전화기 네트워크의 보안 강화, 76 페이지
MRA에 대한 OAuth 개선 기능	Expressway를 통한 모바일 및 Remote Access, 124 페이지
사용자 인터페이스 개선 기능	SRST(Survivable Remote Site Telephony), 67 페이지

펌웨어 릴리스 14.0부터 전화기는 DTLS 1.2를 지원합니다. DTLS 1.2에는 Cisco Adaptive Security Appliance (ASA) 릴리스 9.10 이상이 필요합니다. 사용자가 ASA에서 VPN 연결을 위한 최소 DTLS 버전을 구성합니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html의 *ASDM* 설명서 *3: Cisco ASA Series VPN ASDM* 구성 가이드를 참조하십시오.

펌웨어 릴리스 12.8(1)에 대한 새 정보 및 변경된 정보

다음 정보는 펌웨어 릴리스 12.8(1)에 대한 새로운 정보이거나 변경된 정보입니다.

기능	새 내용 또는 변경된 내용
전화기 데이터 마이그레이션	사용자의 전화기 모델 변경, 54 페이지
웹 액세스 필드에 대한 정보 추가	제품별 구성, 102 페이지

펌웨어 릴리스 12.7(1)에 관한 새 정보 및 변경된 정보

펌웨어 릴리스 12.7(1)용 사용 관리 업데이트가 필요하지 않음

펌웨어 릴리스 12.6(1)에 대한 새 정보 및 변경된 정보

펌웨어 릴리스 12.6(1)용 사용 관리 업데이트가 필요하지 않음

펌웨어 릴리스 12.5(1)SR3에 대한 새 정보 및 변경된 정보

모든 Cisco Unified Communications Manager 릴리스를 지원하도록 Cisco Unified Communications Manager 설명서에 대한 모든 참조가 업데이트되었습니다.

표 *2:* 펌웨어 릴리스 *12.5(1)SR3*용 *Cisco IP* 전화기 *8832* 관리 설명서 개정

개정	업데이트된 섹션
활성화 코드 온보딩 및 모바일 및 Remote Access 지원	활성화 코드 온보딩 및 모바일 및 Remote Access, 29 페이지
Cisco Unified Communications Manager에서 문제 보고 도구 사용을 지원합니다.	Cisco Unified Communications Manager에서 전화 문제 보고서 만들기, 176 페이지

펌웨어 릴리스 12.5(1)SR2에 대한 새 정보 및 변경된 정보

펌웨어 릴리스 12.5(1)SR2용 사용 관리 업데이트가 필요하지 않음

펌웨어 릴리스 12.5(1)SR2는 펌웨어 릴리스 12.5(1) 및 펌웨어 12.5(1) SR1을 대체합니다. 펌웨어 릴리스 12.5(1) 및 펌웨어 릴리스 12.5(1)SR1은 펌웨어 릴리스 12.5(1)SR2를 위해 보류되었습니다.

펌웨어 릴리스 12.5(1)SR1에 대한 새 정보 및 변경된 정보

다음 표에서는 펌웨어 릴리스 12.5(1)를 지원하기 위한 *Cisco Unified Communications Manager*용 *Cisco IP* 전화회의 전화기 *8832* 관리 설명서의 변경 사항을 나열합니다.

표 *3:* 펌웨어 릴리스 *12.5(1)SR1*용 *Cisco IP* 전화회의 전화기 *8832* 관리 설명서 개정

개정	신규 또는 업데이트된 섹션
Elliptic Curve에 대한 지원	지원 보안 기능, 77 페이지

펌웨어 릴리스 12.5(1)에 대한 새 정보 및 변경된 정보

다음 표에서는 펌웨어 릴리스 12.5(1)를 지원하기 위한 *Cisco Unified Communications Manager*용 *Cisco IP* 전화회의 전화기 *8832* 관리 설명서의 변경 사항을 나열합니다.

표 4: 펌웨어 릴리스 12.5(1)용 Cisco IP 전화회의 전화기 8832 관리 설명서 개정

개정	신규 또는 업데이트된 섹션
Cisco Unified Communications Manager Express에서 귓속말 페이지 지원	Cisco Unified Communications Manager Express 상호 작용, 23 페이지
TLS 암호화 비활성화에 대한 지원	제품별 구성, 102 페이지
Inter-Digit 타이머 T.302 향상을 위한 Enbloc 전화걸기를 지원합니다.	제품별 구성, 102 페이지

펌웨어 릴리스 12.1(1)에 대한 새 정보 및 변경된 정보

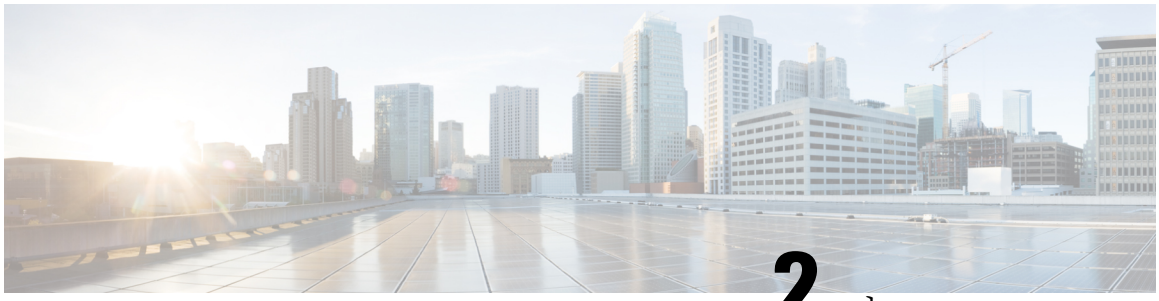
다음 표에서는 펌웨어 릴리스 12.1(1)을 지원하기 위한 *Cisco Unified Communications Manager*용 *Cisco IP* 전화회의 전화기 *8832* 관리 설명서의 변경 사항을 설명합니다.

개정	신규 또는 업데이트된 섹션
다음에 대한 지원: Cisco IP 전화회의 전화기 8832 PoE Injector	• 전화기 전원 요구 사항, 18 페이지 • 전화회의 전화기에 전원을 제공하는 방법, 33 페이지 • 전화회의 전화기 설치, 31 페이지
무선 마이크 지원	• Cisco IP 전화회의 전화기 8832, 9 페이지 • 무선 확장 마이크(8832만 해당), 13 페이지 • 유선 확장 마이크 설치, 36 페이지 • 무선 마이크 충전 거치대 설치, 37 페이지
데이지 체인 지원	• Cisco IP 전화회의 전화기 8832, 9 페이지 • 데이지 체인 모드, 31 페이지 • 데이지 체인 모드로 전화회의 전화기 설치, 38 페이지 • 데이지 체인 모드에서 하나의 전화기가 작동하지 않음, 175 페이지
다음에 대한 지원: Cisco IP 전화회의 전화기 8832 비 PoE 이더넷 인젝터	• 전화회의 전화기 설치, 31 페이지 • 전화회의 전화기에 전원을 제공하는 방법, 33 페이지

개정	신규 또는 업데이트된 섹션
Wi-Fi 지원	• 전화회의 전화기 설치, 31 페이지 • 전화회의 전화기에 전원을 제공하는 방법, 33 페이지 • 도메인 이름 필드 설정, 47 페이지 • 전화기에서 무선 LAN 활성화, 47 페이지 • Cisco Unified Communications Manager에서 무선 LAN 설정, 48 페이지 • 전화기에 무선 LAC 설정, 49 페이지 • WLAN 인증 시도 수 설정, 50 페이지 • WLAN 프롬프트 모드 활성화, 51 페이지 • Cisco Unified Communications Manager를 사용하여 Wi-Fi 프로파일 설정, 51 페이지 • Cisco Unified Communications Manager를 사용하여 Wi-Fi 그룹 설정, 53 페이지
Expressway를 통한 모바일 및 Remote Access 지원	• Expressway를 통한 모바일 및 Remote Access, 124 페이지 • 구축 시나리오, 126 페이지 • Expressway 로그인을 위해 사용자 자격 증명 영구 구성, 126 페이지
웹 서버 액세스를 위한 TLS 1.2 활성화 또는 비활성화 지원	제품별 구성, 102 페이지
G722.2 AMR-WB 오디오 코덱 지원	• Cisco IP 전화회의 전화기 8832, 9 페이지 • 통화 통계 필드, 146 페이지

I 부

Cisco IP 전화회의 전화기 정보



2 장

Cisco IP 전화회의 전화기 하드웨어

Cisco IP 전화회의 전화기 8832

Cisco IP Conference Phone 8832 및 8832NR은 직원 중심 커뮤니케이션을 향상시킵니다. HD(high definition) 오디오 성능과 360도 커버리지를 제공합니다. 양방향 광대역(G.722) 오디오 핸즈프리 스피커는 오디오 애호가를 만족시킬 사운드 경험을 선사합니다. 이 전화기는 다양한 공간적인 요구 사항을 해결할 수 있는 간단한 솔루션입니다.

그림 ***1: Cisco IP*** 전화회의 전화기 ***8832***

전화회의 전화기에는 적용 범위가 360인 고감도 마이크가 있습니다. 이 적용 범위를 사용하면 사용자가 일반 음성으로 말하면 최대 3m(10피트) 거리에서 명확하게 들을 수 있습니다. 또한 전화기는 휴대폰 및 기타 무선 장치의 간섭에 저항하는 기술을 갖추고 있어 방해를 받지 않고 선명한 통신을 전

달할 수 있습니다. 이 전화기는 사용자 기능에 액세스할 수 있는 컬러 화면과 소프트키 단추를 제공합니다. 기본 장치가 독립형인 경우 전화기는 6.1 x 6.1m(20 x 20피트)의 적용 범위를 제공하며 최대 10명이 사용할 수 있습니다.

2개의 유선 확장 마이크는 전화기와 함께 사용할 수 있습니다. 기본 장치에서 확장 마이크를 멀리 배치하면 대형 회의실의 경우 성능이 더 향상됩니다. 기본 장치와 확장 마이크가 있는 경우 전화회의 전화기는 6.1 x 10m(20 x 34피트)의 적용 범위를 제공하며 최대 22명이 사용할 수 있습니다.

또한 전화기는 두 무선 확장 마이크의 선택적 세트를 지원합니다. 기본 장치와 무선 확장 마이크가 있는 경우 전화회의 전화기는 6.1 x 12.2m(20 x 40피트)의 적용 범위를 제공하며 최대 26명이 사용할 수 있습니다. 20 x 40 피트의 방을 커버하려면 각 마이크를 베이스로부터 최대 10 피트의 거리에 배치하는 것이 좋습니다.

2개의 기본 장치를 연결하여 룸의 커버리지를 늘릴 수 있습니다. 이 구성에는 선택 사항인 데이지 체인 키트가 필요하며 2개의 확장 마이크(유선 또는 무선이지만 혼합된 조합은 지원하지 않음)를 지원할 수 있습니다. 데이지 체인 키트와 함께 유선 마이크를 사용하는 경우 구성은 최대 6.1 x 15.2m(20 x 50 피트)의 룸과 최대 38명을 위한 커버리지를 제공합니다. 데이지 체인 키트와 함께 유선 마이크를 사용하는 경우 구성은 최대 6.1 x 17.4m(20 x 57 피트)의 룸과 최대 42명을 위한 커버리지를 제공합니다.

Cisco IP 전화회의 전화기 8832NR (비 라디오) 버전은 Wi-Fi, 무선 확장 마이크 또는 Bluetooth를 지원하지 않습니다.

다른 장치와 마찬가지로 Cisco IP 전화기를 구성 및 관리해야 합니다. 이러한 전화기는 다음 코드를 인코딩 및 디코딩합니다.

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

주의 Cisco IP 전화기 가까이에서 휴대폰이나 GSM 폰 또는 양방향 라디오를 사용하면 간섭 현상이 발생할 수 있습니다. 자세한 내용은 방해 장치에 대한 제조사 문서를 참조하십시오.

Cisco IP 전화기는 착신 전환, 통화 호전화, 재다이얼, 단축 다이얼, 전화회의, 음성 메시징 시스템 액세스 같은 일반적인 텔레포니 기능을 제공합니다. 또한 그 밖의 다양한 기능도 제공합니다.

Cisco IP 전화기도 다른 네트워크 장치처럼 Cisco Unified Communications Manager 및 IP 네트워크에 속한 기타 항목에 액세스할 수 있도록 구성해줘야 합니다. DHCP를 사용하면 전화기에 구성할 수 있

는 설정이 적습니다. 그러나 네트워크 요구 사항이라면, IP 주소, TFTP 서버 및 서브넷 정보 같은 정보를 수동으로 구성할 수 있습니다.

Cisco IP 전화기는 향상된 기능을 제공하기 위해 IP 네트워크의 다른 서비스 및 장치와 상호 작용할 수 있습니다. 예를 들어 Cisco Unified Communications Manager와 회사의 LDAP3(Lightweight Directory Access Protocol 3) 표준 디렉터리를 통합하면, 사용자가 IP 전화기에서 바로 동료의 연락처 정보를 검색할 수 있습니다. 또한 사용자가 날씨, 주식, 그 날의 명언, 기타 웹 기반 정보 같은 정보에 액세스할 수 있도록 XML을 사용할 수도 있습니다.

마지막으로 Cisco IP 전화기는 네트워크 장치이기 때문에, 기기에서 직접 상세한 상태 정보를 확인할 수 있습니다. 그리고 이러한 정보는 사용자가 IP 전화기를 사용하면서 부딪칠 수 있는 여러 가지 문제를 해결하는 데 도움을 줄 수 있습니다. 뿐만 아니라 활성 통화 또는 전화기의 펌웨어 버전에 대한 통계치도 확인할 수 있습니다.

그리고 IP 텔레포니 네트워크가 작동하려면 Cisco IP 전화기와 Cisco Catalyst 스위치 같은 네트워크 장치를 연결해야 합니다. 그리고 전화를 걸고 받기 전에 먼저 Cisco Unified Communications Manager 시스템에 Cisco IP 전화기를 등록해야 합니다.

Cisco IP 전화회의 전화기 8832 단추 및 하드웨어

다음 그림은 Cisco IP 전화회의 전화기 8832를 나타냅니다.

그림 *2: Cisco IP* 전화회의 전화기 *8832* 단추 및 기능

다음 표에서는 Cisco IP 전화회의 전화기 8832의 단추에 대해 설명합니다.

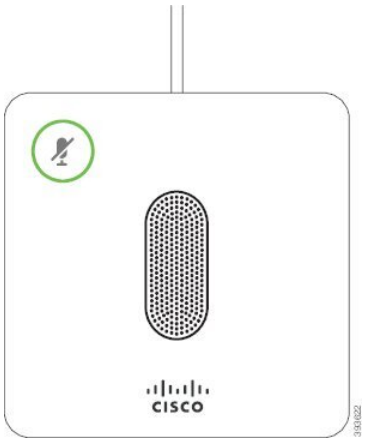
표 5: Cisco IP 전화회의 전화기 8832 버튼

1	LED 막대	다음과 같이 통화 상태를 나타냅니다. • 녹색, 켜짐—통화 중인 호 • 녹색, 깜박임—인입 호 • 녹색, 신호—보류된 통화 • 빨간색, 켜짐—음소거된 통화
2	확장 마이크 포트	유선 확장 마이크 케이블을 포트에 연결합니다.
3	음소거 막대	마이크를 켜거나 끕니다. 마이크를 음소거하면 LED 막대가 빨간색으로 켜집니다.
4	소프트키 버튼	기능 및 서비스에 액세스합니다.
5	탐색 막대 및 선택 단추	메뉴를 스크롤하고 항목을 강조 표시하며, 강조 표시한 항목을 선택합니다.
6	볼륨 버튼	스피커폰 볼륨(오프 훅)과 벨소리 장치 볼륨(온 훅)을 조절합니다. 볼륨을 변경할 때 LED 막대가 흰색으로 켜져 볼륨이 변하는 것을 보여줍니다.

유선 확장 마이크(8832만 해당)

Cisco IP Conference Phone 8832는 2개의 유선 확장 마이크를 지원하며 옵션 키트에서 사용할 수 있습니다. 대규모 회의실 또는 넓은 방에서는 확장 마이크를 사용하십시오. 최상의 결과를 얻으려면 마이크를 전화기에서 0.91m ~ 2.1m 사이의 거리를 두고 통화하는 것이 좋습니다.

그림 3: 유선 확장 마이크



통화할 때 음소거 단추 주변의 확장 마이크 LED가 녹색으로 켜집니다.

마이크를 음소거하면 LED가 빨간색으로 켜집니다. 음소거 단추를 누르면 전화기와 확장 마이크가 음소거됩니다.

관련 항목

유선 확장 마이크 설치, 35 페이지

무선 확장 마이크(8832만 해당)

Cisco IP Conference Phone 8832는 2개의 무선 확장 마이크를 지원하며 옵션 키트에 있는 충전 거치대와 함께 사용할 수 있습니다. 무선 마이크를 충전 거치대에 놓으면 거치대의 LED가 흰색으로 켜집니다.

그림 4: 무선 마이크

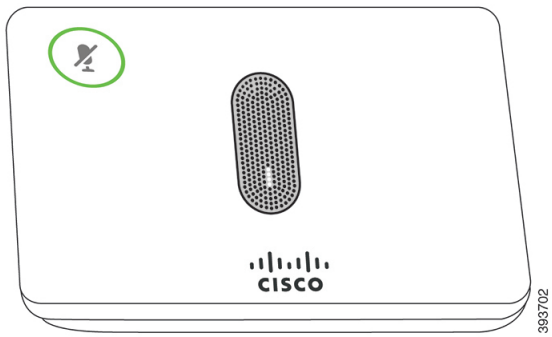
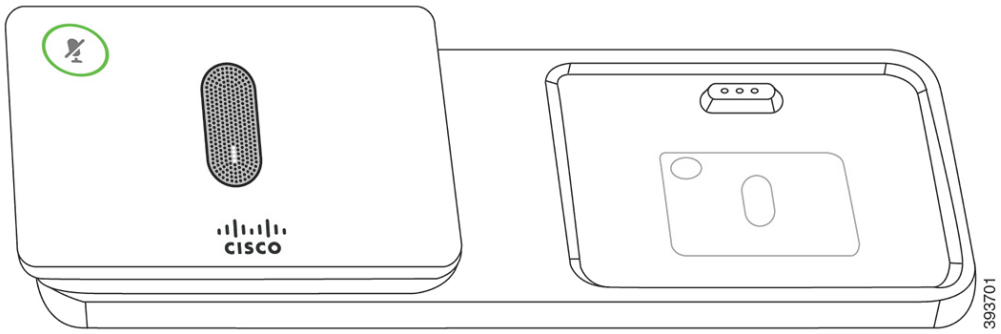


그림 5: 충전 거치대에 장착된 무선 마이크



전화회의 전화기로 통화할 때 음소거 단추 주변의 확장 마이크 LED가 녹색으로 켜집니다.

마이크를 음소거하면 LED가 빨간색으로 켜집니다. 음소거 단추를 누르면 전화기와 확장 마이크가 음소거됩니다.

전화기가 무선 마이크(예 : 무선 마이크 1)와 페어링되어 있고 무선 마이크를 충전기에 연결하는 경우 세부 정보 표시 소프트 키를 누르면 해당 마이크의 충전 레벨이 표시됩니다.

전화기가 무선 마이크와 페어링되어 있고 유선 마이크를 연결하면 무선 마이크가 페어링 해제되고 전화기가 유선 마이크와 페어링됩니다. 유선 마이크가 연결되었다는 알림이 전화기 화면에 나타납니다.

관련 항목

유선 확장 마이크 설치, 36 페이지
무선 마이크 충전 거치대 설치, 37 페이지

관련 설명서

관련 정보는 다음 섹션을 참조하십시오.

Cisco IP 전화회의 전화기 8832 설명서

Cisco IP 전화기 7800 시리즈에 대한 제품 지원 페이지에서 해당 언어, 전화 모델 및 통화 제어 시스템 관련 문서를 찾아보십시오.

Cisco Unified Communications Manager 설명서

Cisco Unified Communications Manager 설명서 및 사용 중인 Cisco Unified Communications Manager 릴리스와 관련된 기타 게시물을 확인하십시오. 다음 문서 URL에서 찾을 수 있습니다.

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

Cisco Unified Communications Manager Express 설명서

사용 언어, 전화기 모델 및 Cisco Unified Communications Manager Express 릴리스와 관련된 게시물을 참조하십시오. 다음 문서 URL에서 찾을 수 있습니다.

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

Cisco Hosted Collaboration 서비스 설명서

Cisco Hosted Collaboration Solution 설명서 및 사용 중인 Cisco Hosted Collaboration Solution 릴리스와 관련된 기타 게시물을 확인하십시오. 다음 URL에서 찾을 수 있습니다.

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

Cisco Business Edition 4000 설명서

Cisco Business Edition 4000 설명서 및 사용 중인 Cisco Business Edition 4000 릴리스와 관련된 기타 게시물을 확인하십시오. 다음 URL에서 찾을 수 있습니다.

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

설명서, 지원 및 보안 지침

설명서 가져오기, 지원 받기, 문서 피드백 제공하기, 보안 가이드라인 확인하기 및 권장되는 별칭과 일반적인 Cisco문서에 대한 자세한 내용은 다음 사이트에서 월간으로 발행되는 *What's New in Cisco Product Documentation(Cisco* 제품의 새로운 기능 설명서*)*를 참조하십시오. 여기에는 모든 신규 및 개정판 Cisco 기술 설명서가 정리되어 있습니다.

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

What's New in Cisco Product Documentation RSS(Really Simple Syndication) 피드에 가입하여 reader 애플리케이션을 통해 내용이 데스크톱으로 직접 전달되도록 설정하십시오. RSS 피드는 무료 서비스이며 Cisco는 현재 RSS 버전 2.0을 지원합니다.

Cisco 제품 보안 개요

이 제품은 암호화 기능을 포함하고 있으며 수입, 수출, 운송 및 사용을 규제하는 미국 및 현지 법규의 적용을 받습니다. Cisco 암호화 제품을 제공하는 것은 제3자에게 이 암호화의 수입, 수출, 유통 또는 사용 권한을 부여하는 것을 의미하는 것이 아닙니다. 수입자, 수출자, 유통업자 및 사용자는 미국과 현지 법규를 준수할 책임이 있습니다. 이 제품을 사용하면 해당 법률 및 규정을 준수하기로 동의하는 것입니다. 미국 및 현지 법규를 준수할 수 없는 경우 이 제품을 즉시 반품하십시오.

미국 수출 규정과 관련한 자세한 내용은 웹 사이트(https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear)를 참조하십시오.

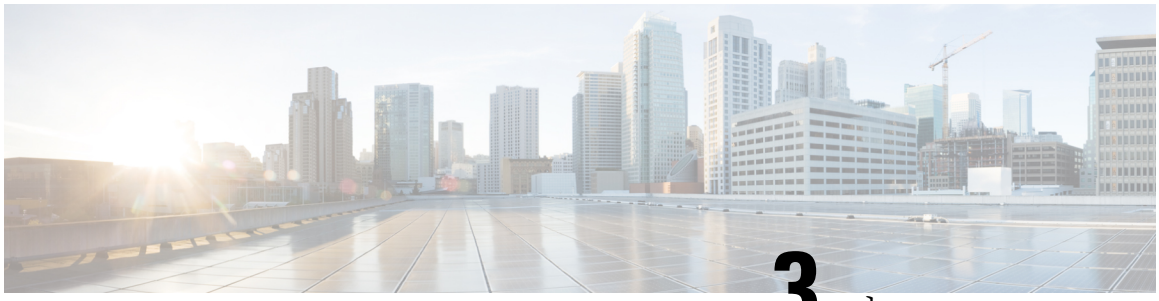
용어 차이

이 문서에서 용어 *Cisco IP* 전화기는 Cisco IP 전화회의 전화기 8832를 포함합니다.

다음 표에서는 *Cisco IP* 전화회의 전화기 *8832* 사용 설명서, *Cisco Unified Communications Manager*용 *Cisco IP* 전화회의 전화기 *8832* 관리 설명서 및 Cisco Unified Communications Manager 문서에 나타난 몇 가지 용어 차이에 관해 설명합니다.

표 ***6:*** 용어 차이

사용 설명서	관리 가이드
메시지 표시기	MWI(메시지 대기 중 표시기)
음성 메일 시스템	음성 메시징 시스템



3 장

기술 세부사항

물리적 및 운영 환경 사양

다음 표에는 전화회의 전화기의 물리적 운영 환경 명세가 정리되어 있습니다.

표 *7:* 물리적 운영 사양

사양	값 또는 범위
작동 온도	0°~40°C(32°~104°F)
작동 상대 습도	10%~90%(비응결)
보관 온도	-10°~60°C(14°~140°F)
높이	278mm(10.9인치)
폭	278mm(10.9인치)
깊이	61.3mm(2.4인치)
무게	1852g(4.07 lb.)

사양	값 또는 범위
전원	PoE 인젝터를 통한 IEEE PoE 클래스 3. IEEE 802.3af 및 802.3at 스 Layer Discovery Protocol - Power over Ethernet)를 모두 지원합니다 다른 옵션에는 연결된 LAN 스위치가 PoE를 지원하지 않는 경우 화회의 전화기 8832 전원 어댑터가 필요합니다.
보안 기능	보안 부팅
케이블	USB-C
거리 요구 사항	이더넷 사양은 각 전화회의 전화기와 스위치 사이의 최대 케이블

자세한 내용은 *Cisco IP* 전화회의 전화기 *8832* 데이터 시트: https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html를 참조하십시오.

전화기 전원 요구 사항

Cisco IP Conference Phone 8832는 다음과 같은 전원을 사용할 수 있습니다.

- 다음을 사용한 PoE(Power over Ethernet) 구축: Cisco IP 전화회의 전화기 8832 PoE Injector
- 다음을 사용한 비 PoE 이더넷 구축: Cisco IP 전화회의 전화기 8832 비 PoE 이더넷 인젝터
- Cisco IP 전화회의 전화기 8832 전원 어댑터를 통한 Wi-Fi 구축

표 ***8: Cisco IP*** 전화회의 전화기 전원 지침

전원 유형	지침
PoE 전원 - 전화기에 연결된 USB-C 케이블을 통해 Cisco IP 전화회의 전화기 8832 PoE Injector 또는 Cisco IP 전화회의 전화기 8832 이더넷 인젝터에서 공급됩니다.	Cisco IP 전화회의 전화기 8832 PoE Injector 또는 Cisco IP 전화회의 전화기 8832 이더넷 인젝터을 사용 중인 경우 전화기의 무중단 작동을 보장하려면 스위치에 백업 전원 공급장치가 있는지 확인하십시오. 스위치에서 실행되는 CatOS 또는 IOS 버전이 원하는 전화기 배포를 지원하는지 확인하십시오. 운영 체제 버전용 스위치에 관한 정보는 설명서를 참조하십시오. PoE에서 전원이 공급되는 전화기를 설치할 때는 USB-C 케이블을 전화기에 연결하기 전에 인젝터를 LAN에 연결합니다. PoE를 사용하는 전화기를 제거할 때는 어댑터에서 전원을 제거하기 전에 전화기에서 USB-C 케이블을 분리합니다.

전원 유형	지침
외부 전원 • 다음을 사용한 비 PoE 이더넷 구축: Cisco IP 전화회의 전화기 8832 비 PoE 이더넷 인젝터 • Cisco IP 전화회의 전화기 8832 전원 어댑터를 통한 Wi-Fi 구축 • Cisco IP 전화회의 전화기 8832 이더넷 인젝터 및 Cisco IP 전화회의 전화기 8832 전원 어댑터를 통한 비 PoE 이더넷 구축	외부 전원에서 전원이 공급되는 전화기를 설치할 때는 USB-C 케이블을 전화기에 연결하기 전에 인젝터를 전원과 이더넷에 연결합니다. 외부 전원을 사용하는 전화기를 제거할 때는 어댑터에서 전원을 제거하기 전에 전화기에서 USB-C 케이블을 분리합니다.

정전

전화를 통해 긴급 서비스에 액세스하려면 전화에 전원이 공급되어야 합니다. 정전이 발생할 경우 전력이 복원될 때까지 서비스 또는 긴급 통화 서비스 전화 걸기 기능이 작동하지 않습니다. 전원 공급이 안되거나 중단되는 경우 서비스 또는 긴급 통화 서비스 전화 걸기 기능을 사용하려면 장비를 재설정하거나 재구성해야 할 수 있습니다.

전력 소비 감소

절전 또는 EnergyWise(절전 플러스) 모드를 사용하면 Cisco IP 전화기에서 소비하는 에너지량을 줄일 수 있습니다.

절전

절전 모드에서 화면의 백라이트는 전화기가 사용 중이 아니면 켜지지 않습니다. 전화기는 예약된 기간 동안 또는 사용자가 임의 버튼을 누를 때까지 절전 모드에 남아 있습니다.

절전 플러스**(EnergyWise)**

Cisco IP 전화기는 Cisco EnergyWise(절전 플러스) 모드를 지원합니다. 네트워크에 EW(EnergyWise) 컨트롤러가 포함되어 있다면(예: EnergyWise 기능이 있는 Cisco 스위치가 활성화됨), 이 전화기는 전력 소비량을 더욱 줄이도록 일정에 맞춰 대기(절전) 및 활성화(작동)로 구성할 수 있습니다.

각 전화기에 [EnergyWise] 설정을 활성화 또는 비활성화하도록 설정합니다. [EnergyWise]가 활성화되어 있으면 대기(절전) 및 활성화(작동) 시간과 기타 매개변수를 구성합니다. 이러한 매개변수는 전화기 구성 XML 파일 항목으로 전화기에 전송됩니다.

관련 항목

Cisco IP 전화기의 절전 일정, 115 페이지

Cisco IP 전화기에서 EnergyWise 예약, 116 페이지

네트워크 프로토콜

Cisco IP Conference Phone 8832는 음성 통신에 필요한 몇 개의 업계 표준과 Cisco 네트워크 프로토콜을 지원합니다. 다음 표에는 전화기에서 지원하는 네트워크 프로토콜에 대한 개요가 나와 있습니다.

표 ***9: Cisco IP*** 전화회의 전화기에서 지원하는 네트워크 프로토콜

네트워크 프로토콜	목적	사용 참고 사항
BootP(Bootstrap Protocol)	BootP는 전화기 같은 네트워크 장치를 활성화하여 IP 주소와 같은 특정 시작 정보를 확인합니다.	—
CDP (Cisco 탐색 프로토콜)	CDP는 모든 Cisco 제조 장비에서 실행되는 장치 검색 프로토콜입니다. 장치는 CDP를 사용하여 해당 장치의 존재 여부를 다른 장치에 알리고 네트워크에 있는 다른 장치에 대한 정보를 수신할 수 있습니다.	전화기는 CDP를 사용해 Cisco Catalyst 스위치와 구성 정보 같은 정보를 주고 받을 수 있습니다.
DHCP(Dynamic Host Configuration Protocol)	DHCP는 네트워크 장치에 IP 주소를 역동적으로 할당합니다. DHCP를 사용하면 네트워크에 IP 전화기를 연결하고, 수동으로 IP 주소를 할당하거나 추가 네트워크 매개변수를 구성하지 않고도 전화기를 작동시킬 수 있습니다.	DHCP는 기본값으로 활성화됩니다. 비활성화된 TFTP 서버를 수동으로 구성해야 합니다. DHCP 사용자 정의 옵션 150을 사용할 것을 권합 지원되는 DHCP 구성에 관한 자세한 내용은 해당 참고 옵션 150을 사용할 수 없다면, DHCP
HTTP(Hypertext Transfer Protocol)	HTTP는 인터넷 및 웹 상에서 정보 교환 및 문서 이동을 위해 사용하는 표준 프로토콜입니다.	전화기는 XML 서비스, 프로비저닝, 업그레이드
HTTPS(Hypertext Transfer Protocol Secure)	HTTPS(Hypertext Transfer Protocol Secure)는 HTTP(Hypertext Transfer Protocol)와 SSL/TLS 프로토콜의 조합으로 서버에 암호화 및 보안 식별 기능을 제공합니다.	HTTP와 HTTPS가 모두 지원되는 웹 애플리케이 URL을 선택합니다. 서비스에 대한 연결이 HTTPS를 통해 이루어지
IEEE 802.1X	IEEE 802.1X 표준은 클라이언트 서버 기반 액세스 제어 및 개방형 액세스 포트를 통한 LAN 연결에서 인증받지 못한 클라이언트를 제한하는 인증 프로토콜을 정의합니다. 클라이언트가 인증될 때까지, 802.1X 액세스 제어는 클라이언트가 연결된 포트를 통해 오직 EAPOL(Extensible Authentication Protocol over LAN) 트래픽만 허용합니다. 인증에 성공하면 정상적인 트래픽은 포트를 통과할 수 있습니다.	전화기는 EAP-FAST 및 EAP-TLS라는 인증 방식 전화기에서 802.1X 인증이 활성화되면, 음성 VL

네트워크 프로토콜	목적	사용 참고 사항
IP(Internet Protocol)	IP는 네트워크를 통해 패킷을 처리하고 전송하는 메시징 프로토콜입니다.	IP로 통신하기 위해서는 네트워크 장치에 IP IP 주소, 서브넷 및 게이트웨이 ID는 전화기에 으로 할당됩니다. DHCP를 사용하지 않는다면 전화기는 IPv6 주소를 지원합니다. 자세한 내 시오.
LLDP(Link Layer Discovery Protocol)	LLDP는 일부 Cisco 및 타사 장치에서 지원되는 표준화된 네트워크 검색 프로토콜(CDP와 유사)입니다.	전화기는 PC 포트에서 LLDP를 지원합니다.
LLDP-MED(Link Layer Discovery Protocol-Media Endpoint Devices)	LLDP-MED는 음성 제품을 위해 개발된 LLDP 확장 표준입니다.	전화기는 다음과 같은 정보를 주고받기 위해 • 음성 VLAN 구성 • 장치 검색 • 전력 관리 • 재고 관리 LLDP-MED 지원에 대한 자세한 내용은 다음 https://www.cisco.com/en/US/tech/tk652/tk701/
RTP(Real-Time Transport Protocol)	RTP는 데이터 네트워크상에서 대화형 음성 및 비디오 같은 실시간 데이터를 전송하기 위한 표준 프로토콜입니다.	전화기는 RTP 프로토콜을 사용해 기타 전화기
RTCP(Real-Time Control Protocol)	RTCP는 RTP와 함께 작동하여 RTP 스트림에 대한 QoS 데이터(예: 지터, 대기 시간 및 왕복 지연) 를 제공합니다.	RTCP는 기본적으로 활성화됩니다.
SDP(Session Description Protocol)	SDP는 두 엔드포인트 간 연결 중 사용할 수 있는 매개 변수를 판별하는 SIP 프로토콜의 부분입니다. 전화회의는 전화회의의 모든 엔드포인트가 지원하는 SDP 기능만을 사용하여 설정됩니다.	코덱 유형, DTMF 탐지 및 통신 소음과 같은 S 는 Media Gateway에 의해 전역으로 구성됩니 성을 허용할 수 있습니다.
SIP(Session Initiation Protocol)	SIP는 IP를 통해 멀티미디어 전화 회의를 진행할 때 사용하는 인터넷 IETF(Engineering Task Force) 표준입니다. SIP는 2개 이상의 엔드포인트 간에 통화를 연결, 유지, 종료할 때 사용할 수 있는 ASCII 기반의 애플리케이션 레이어 프로토콜(RFC 3261 정의 내용)입니다.	다른 VoIP 프로토콜처럼 SIP도 패킷 텔레포니 다. 시그널링을 통해 통화 정보는 네트워크 장 니다.
SRTP(Secure Real-Time Transfer protocol)	SRTP는 RTP(Real-Time Protocol) 음성/비디오 프로파일이 확장된 것으로, 두 엔드포인트를 이동하는 미디어 패킷의 인증, 무결성 및 암호화를 제공하여 RTP와 RTCP(Real-Time Control Protocol) 패킷의 무결성을 보장합니다.	전화기는 미디어 암호화를 위해 SRTP를 사용
TCP(Transmission Control Protocol)	TCP는 연결 지향형 전송 프로토콜입니다.	전화기는 TCP를 사용하여 Cisco Unified Com

네트워크 프로토콜	목적	사용 참고 사항
TLS(Transport Layer Security)	TLS는 통신 보안 및 인증을 위한 표준 프로토콜입니다.	보안이 시행될 때, 전화기는 Cisco Unified Commu 자세한 내용은 해당 Cisco Unified Communicatio
TFTP(Trivial File Transfer Protocol)	TFTP를 사용하면 네트워크상에서 파일을 전송할 수 있습니다. 전화기에서 TFTP는 전화기 유형에 맞는 구성 파일을 확보할 수 있게 해줍니다.	TFTP는 네트워크에 TFTP 서버를 요구하고, 이는 가 지정한 것이 아닌 다른 TFTP 서버를 사용하려 수동으로 할당해야 합니다. 자세한 내용은 해당 Cisco Unified Communicatio
사용자 데이터그램 프로토콜	UDP는 데이터 패킷 전달을 위한 연결 메시징 프로토콜입니다.	UDP는 RTP 스트림에만 사용됩니다. 전화기에서

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

Cisco Unified Communications Manager 상호 작용

Cisco Unified Communications Manager는 개방형의 업계 표준 통화 처리 시스템입니다. Cisco Unified Communications Manager 소프트웨어는 여러 전화기 사이에서 통화를 설정하고 분류하며, 기존 PBX 기능과 회사 IP 네트워크를 통합합니다. Cisco Unified Communications Manager는 전화기와 같은 텔레포니 시스템 구성 요소와 액세스 게이트웨이, 그리고 전화회의 및 경로 플랜 같은 기능에 필요한 리소스를 관리합니다. Cisco Unified Communications Manager는 다음과 같은 내용도 제공합니다.

- 전화기용 펌웨어
- TFTP 및 HTTP 서비스를 사용하는 CTL(Certificate Trust List) 및 ITL(Identity Trust List) 파일
- 전화기 등록
- 통화 보호, 기본 Communications Manager와 전화기 사이에 시그널링이 사라져도 미디어 세션을 유지할 수 있음

이 장에서 설명한 대로 전화기와 작동하도록 Cisco Unified Communications Manager를 구성하는 것에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

참고 구성하려는 전화기 모델이 Cisco Unified Communications Manager Administration의 [전화 유형] 드롭다운 목록에 나타나지 않으면 Cisco.com에서 보유 중인 Cisco Unified Communications Manager 버전에 맞는 최신 장치 패키지를 설치하십시오.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

Cisco Unified Communications Manager Express 상호 작용

전화기에서 Cisco Unified Communications Manager Express(Unified CME)를 사용하면 전화기는 CME 모드로 바뀌어야 합니다.

사용자가 전화회의 기능을 시작하면, 태그를 통해 전화기는 로컬 또는 네트워크 하드웨어 컨퍼런스 브리지를 사용할 수 있습니다.

전화기에서는 다음과 같은 작업을 지원하지 않습니다.

- 호전환 - 연결된 통화 호전환 시나리오에서만 지원됩니다.
- 전화회의 - 연결된 통화 호전환 시나리오에서만 지원됩니다.
- 통화참가 - [전화회의] 버튼이나 훅플래시 액세스를 통해서만 지원됩니다.
- 보류 - [보류] 버튼을 사용하여 지원됩니다.
- 참여 및 병합 - 지원되지 않습니다.
- 호연결 - 지원되지 않습니다.
- 선택 - 지원되지 않습니다.

사용자는 다른 회선에서는 전화회의와 호전환 통화를 실행할 수 없습니다.

Unified CME는 귓속말 페이징이라고도 하는 인터콤 전화를 지원합니다. 하지만 통화 중 전화기에 의해 페이지가 거부됩니다.

음성 메시징 시스템 상호 작용

Cisco Unified Communications Manager를 사용하면 Cisco Unity Connection 음성 메시징 시스템을 포함하여 다른 음성 메시징 시스템과 통합할 수 있습니다. 다양한 시스템과 통합할 수 있으므로, 특정 시스템을 사용하는 방법에 대한 정보를 사용자에게 제공해야 합니다.

사용자가 음성 메일로 전환하는 기능을 사용하려면 *xxxxx 전화 걸기 패턴을 설정하고 음성 메일로 모두 착신 전환으로 구성합니다. 자세한 내용은 Cisco Unified Communications Manager 문서를 참조하십시오.

각 사용자에게 다음 정보를 제공합니다.

- 음성 메시징 시스템 계정에 액세스하는 방법.

  Cisco Unified Communications Manager를 사용하여 Cisco IP 전화기에 [메시지] 버튼을 구성했는지 확인하십시오.

- 음성 메시징 시스템에 액세스하기 위한 초기 암호.

  모든 사용자에 대한 기본 음성 메시징 시스템 암호를 구성합니다.

- 전화기가 음성 메시지를 대기 중임을 나타내는 방법.

Cisco Unified Communications Manager를 사용하여 MWI(Message Waiting Indicator) 방법을 설정합니다.

전화기 구성 파일

전화기에 대한 구성 파일은 TFTP 서버에 저장되고 Cisco Unified Communications Manager에 연결하기 위한 매개변수를 정의합니다. 일반적으로 전화기를 재설정해야 하는 변경 사항을 Cisco Unified Communications Manager에서 작성할 때 자동으로 전화기 구성 파일에 변경 사항이 작성됩니다.

또한 구성 파일은 전화기를 로드하는 이미지가 실행 중이어야 하는 정보를 포함합니다. 이 이미지 로드가 현재 전화기에 로드된 이미지와 다를 경우 전화기는 TFTP 서버에 연결하여 필수 로드 파일을 요청합니다.

Cisco 통합 커뮤니케이션 매니저 관리에서 보안 관련 설정을 구성할 경우 전화기 구성 파일은 중요 정보를 포함합니다. 구성 파일의 프라이버시를 보장하려면 암호화에 대한 설정을 구성해야 합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오. 전화기는 재설정되고 Cisco Unified Communications Manager에 등록할 때마다 구성 파일을 요청합니다.

다음 조건이 있을 때 전화기는 TFTP 서버에서 XmlDefault.cnf.xml이라는 기본 구성 파일에 액세스합니다.

- 에서 자동 등록을 활성화했습니다. Cisco Unified Communications Manager
- 전화기가 Cisco Unified Communications Manager 데이터베이스에 추가되지 않았습니다.
- 전화기가 처음 등록되는 중입니다.

네트워크 혼잡 시 전화기 동작

네트워크 성능을 저하시키는 것이라면 무엇이나 전화기 오디오에 영향을 미칠 수 있고, 어떤 경우에는 통화가 끊어지게 만들 수도 있습니다. 네트워크 저하의 근원에는 다음과 같은 활동이 포함되며 이에 국한되는 것은 아닙니다.

- 관리자 작업(예: 내부 포트 스캔 또는 보안 스캔)
- 네트워크에 발생한 공격(예: DoS(서비스 거부) 공격 등)

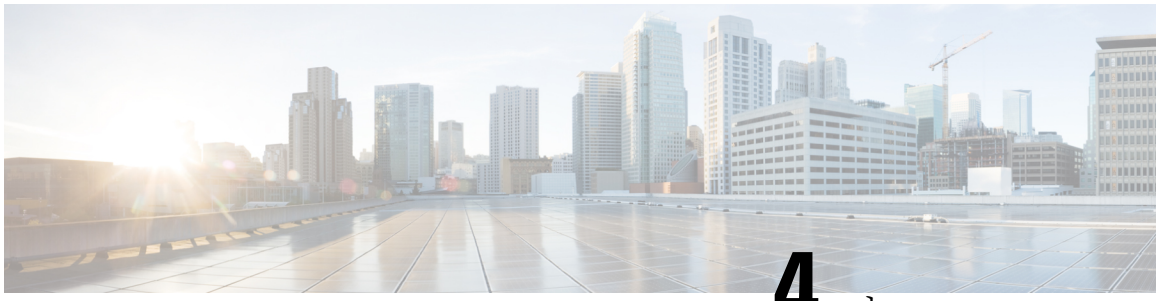
애플리케이션 프로그래밍 인터페이스

Cisco는 타사 애플리케이션 개발자가 Cisco를 통해 테스트하고 인증한 타사 애플리케이션의 전화 API 활용을 지원합니다. 인증되지 않은 애플리케이션 상호 작용과 관련된 전화기 문제는 제3자가 해결해야 하며 Cisco는 이를 해결하지 않습니다.

Cisco 인증 타사 애플리케이션/솔루션의 지원 모델은 Cisco Solution Partner Program 웹 사이트를 참조하십시오.

II 부

Cisco IP 전화회의 전화기 설치



4 장

전화 설치

네트워크 설정 확인

IP 전화 통신 시스템을 배포할 때 시스템 관리자와 네트워크 관리자는 네트워크가 IP 전화 통신 서비스에 대해 준비할 수 있도록 몇 가지 초기 구성 작업을 수행해야 합니다. Cisco IP 텔레포니 네트워크 설정 및 구성용 체크리스트와 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

전화기가 네트워크에서 엔드포인트로 제대로 작동하려면, 네트워크에서 특정 요구 사항을 충족해야 합니다. 한 가지 요구 사항은 적절한 대역폭입니다. 전화기를 사용하려면 Cisco Unified Communications Manager에 등록할 때 권장하는 32 kbps 보다 더 많은 대역폭이 필요합니다. QoS 대역폭을 구성할 때 더 높은 대역폭 요구 사항을 고려하십시오. 자세한 내용은 *Cisco Collaboration System 12.x SRND(*솔루션 참조 네트워크 설계*)* 이상(https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html)을 참조하십시오.

참고 전화기는 Cisco Unified Communications Manager의 날짜와 시간을 표시합니다. 전화기에 표시된 시간은 Cisco Unified Communications Manager 시간과 최대 10초까지 차이가 날 수 있습니다.

프로시저

단계 1 다음 요구 사항을 충족하도록 VoIP 네트워크를 구성합니다.

- VoIP는 라우터와 게이트웨이에 구성됩니다.
- Cisco Unified Communications Manager 는 네트워크에 설치된 다음, 통화 처리를 수행하도록 구성됩니다.

단계 2 다음 중 하나를 지원하도록 네트워크를 설정합니다.

- DHCP 지원
- IP 주소, 게이트웨이 및 서브넷 마스크 수동 지정

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

온-프레미스 전화기에 대한 활성화 코드 온보딩

활성화 코드 온보딩을 사용하면 자동 등록 없이 새 전화기를 빠르게 설정할 수 있습니다. 이 방법을 사용하면 다음 중 하나를 사용하여 전화기 온보딩 프로세스를 제어할 수 있습니다.

- Cisco Unified Communications BAT(Bulk Administration Tool)
- Cisco Unified Communications Manager 관리 인터페이스
- Administrative XML 웹 서비스(AXL)

전화 구성 페이지의 장치 정보 섹션에서 이 기능을 활성화합니다. 이 기능을 단일 온프레미스 전화에 적용하려면 온보딩을 위해 활성화 코드 필요를 선택합니다.

전화기를 등록하려면 사용자가 활성화 코드를 입력해야 합니다. 활성화 코드 온보딩은 개별 전화기, 전화기 그룹 또는 전체 네트워크에 적용될 수 있습니다.

이 방법을 사용하면 16자리 활성화 코드만 입력하기 때문에 전화기를 쉽게 온보딩할 수 있습니다. 수동으로 입력하거나 전화기에 비디오 카메라가 있는 경우 QR 코드로 입력됩니다. 안전한 방법을 사용하여 이 정보를 사용자에게 제공하는 것이 좋습니다. 그러나 사용자가 전화기에 할당된 경우 이 정보는 셀프 케어 포털에서 이용할 수 있습니다. 사용자가 포털에서 코드에 액세스하면 감사 로그가 기록됩니다.

활성화 코드는 한 번만 사용할 수 있으며, 기본적으로 1주일 후에 만료됩니다. 코드가 만료되면 사용자에게 새 코드를 제공해야 합니다.

MIC(Manufacturing Installed Certificate) 및 활성화 코드가 확인될 때까지 전화기를 등록할 수 없기 때문에 이 방법을 사용하면 네트워크를 안전하게 유지할 수 있습니다. 이 방법은 TAPS(자동 등록된 전화기 지원) 또는 자동 등록을 위한 도구를 사용하지 않기 때문에 대량의 온보드 전화기에도 편리한 방법입니다. 온보딩 비율은 초당 1대의 전화기 또는 시간당 약 3600대의 전화기입니다. 전화기는 Cisco

Unified Communications Manager 관리, 관리 XML 웹 서비스(AXL) 또는 BAT를 사용하여 추가할 수 있습니다.

활성화 코드 온보딩이 구성된 후 기존 전화기는 재설정됩니다. 활성화 코드가 입력되고 전화기 MIC가 확인될 때까지는 등록되지 않습니다. 활성화 코드 온보딩을 구현하기 전에 현재 사용자에게 이를 알리십시오.

자세한 내용은 *Cisco Unified Communications Manager* 및 *IM and Presence* 서비스용 관리 가이드, 릴리스 *12.0(1)* 이상을 참조하십시오.

활성화 코드 온보딩 및 모바일 및 Remote Access

원격 사용자를 위해 Cisco IP 전화기를 구축할 때 활성화 코드 온보딩을 모바일 및 Remote Access와 함께 사용할 수 있습니다. 이 기능은 자동 등록이 필요하지 않을 때 오프-프레미스 전화기를 구축하는 안전한 방법입니다. 하지만 온-프레미스 환경에서는 자동 등록을 통해, 오프-프레미스에서는 활성화 코드로 전화기를 구성할 수 있습니다. 이 기능은 온-프레미스 전화기의 활성화 코드 온보딩과 유사하지만 오프-프레미스 전화기에도 활성화 코드를 사용할 수 있습니다.

모바일 및 Remote Access에 활성화 코드를 사용하려면 Cisco Unified Communications Manager 12.5(1)SU1 이상 및 Cisco Expressway X12.5 이상이 필요합니다. 스마트 라이센스도 활성화해야 합니다.

이 기능은 Cisco Unified Communications Manager 관리에서 사용할 수 있지만 다음 사항에 유의하십시오.

- 전화 구성 페이지의 장치 정보 섹션에서 이 기능을 활성화합니다.
- 이 기능을 단일 온프레미스 전화기에만 적용하려면 온보딩을 위해 활성화 코드 필요를 선택합니다.
- 단일 오프-프레미스 전화기에 대해 활성화 온보딩을 사용하려면 **MRA**를 통한 활성화 코드 허용 및 온보딩을 위해 활성화 코드 필요를 선택합니다. 전화기가 오프-프레미스에 있는 경우 모바일 및 Remote Access 모드로 변경되고 Expressway를 사용합니다. 전화기를 Expressway에 연결할 수 없는 경우 오프-프레미스가 될 때까지 등록되지 않습니다.

자세한 내용은 다음 문서를 참조하십시오.

- *Cisco Unified Communications Manager* 및 *IM and Presence* 서비스용 관리 가이드, 릴리스 *12.0(1)*
- Cisco Expressway X12.5 이상의 경우 *Cisco Expressway*를 통한 모바일 및 *Remote Access*

전화기 자동 등록 활성화

Cisco IP 전화기는 Cisco Unified Communications Manager에 통화 처리를 요구합니다. Cisco Unified Communications Manager가 전화기를 관리하고 통화를 제대로 라우팅하고 처리하도록 적절하게 설정되어 있는지 확인하려면, Cisco Unified Communications Manager Administration의 상황에 맞는 도움말이나 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

Cisco IP 전화기를 설치하려면 먼저 Cisco Unified Communications Manager 데이터베이스에 전화기를 추가하는 방식을 선택해야 합니다.

전화기를 설치하기 전에 자동 등록을 활성화하면 다음과 같은 이점이 있습니다.

- 전화기에서 MAC 주소를 수집하지 않고도 전화기를 추가할 수 있습니다.
- 실제로 IP 텔레포니 네트워크에 전화기를 연결할 때 Cisco Unified Communications Manager 데이터베이스에 자동으로 Cisco IP 전화기를 추가할 수 있습니다. 자동 등록 중에는 Cisco Unified Communications Manager가 다음으로 사용 가능한 순차적 디렉터리 번호를 전화기에 할당합니다.
- Cisco Unified Communications Manager 데이터베이스에 신속하게 전화기를 입력하고, Cisco Unified Communications Manager에서 디렉터리 번호 같은 설정을 수정할 수 있습니다.
- 자동 등록된 전화기를 새 위치로 이동하고 디렉터리 번호에 영향을 미치지 않으면서 다양한 장치 풀에 이를 할당할 수 있습니다.

자동 등록은 기본적으로 비활성화됩니다. 자동 등록 사용을 원치 않을 때도 있습니다. 예를 들어 전화기에 특정 디렉터리 번호를 할당하고자 한다거나 Cisco Unified Communications Manager와 보안 연결을 사용하려는 경우가 이에 해당합니다. 자동 등록 활성화에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오. Cisco CTL 클라이언트를 통해 클러스터를 혼합 모드로 구성하는 경우에는 자동 등록이 자동으로 비활성화되지만 다시 활성화할 수 있습니다. Cisco CTL 클라이언트를 통해 클러스터를 비보안 모드로 구성하는 경우, 자동 등록은 자동으로 활성화되지 않습니다.

먼저 전화기에서 MAC 주소를 수집하지 않고도 TAPS(Tool for AutoRegistered Phones Support)와 자동 등록으로 전화기를 추가할 수 있습니다.

TAPS는 BAT(Bulk Administration Tool)와 함께 작동하여 더미 MAC 주소로 이미 Cisco Unified Communications Manager 데이터베이스에 추가되어 있는 전화기의 배치를 업데이트합니다. TAPS를 사용하여 MAC 주소를 업데이트하고 전화기의 사전 정의된 구성을 다운로드합니다.

Cisco에서는 자동 등록과 TAPS를 사용하여 100개 이하의 전화기만 네트워크에 추가할 것을 권장합니다. 네트워크에 100개 이상의 전화기를 추가하려면 BAT(Bulk Administration Tool)를 사용하십시오.

TAPS를 구현하려면, 관리자나 최종 사용자가 TAPS 디렉터리 번호로 전화를 걸어 음성 지시 사항을 따릅니다. 프로세스가 완료되면, 전화기에 디렉터리 번호와 기타 설정이 지정되고 Cisco Unified Communications Manager Administration에서 정확한 MAC 주소로 전화기가 업데이트됩니다.

네트워크에 Cisco IP 전화기를 연결하기 전에 자동 등록이 활성화되고 Cisco Unified Communications Manager Administration에 제대로 구성되어 있는지 확인합니다. 자동 등록 활성화 및 구성에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

TAPS가 작동하려면 Cisco Unified Communications Manager Administration에 자동 등록이 활성화되어 있어야 합니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 시스템 > **Cisco Unified CM**을 클릭합니다.

단계 2 찾기를 클릭하여 필요한 서버를 선택합니다.

단계 3 자동 등록 정보에서 이러한 필드를 구성합니다.

- 범용 장치 템플릿
- 범용 회선 템플릿
- 시작 디렉터리 번호
- 끝 디렉터리 번호

단계 4 이 Cisco Unified Communications Manager에서 자동 등록 비활성화됨 확인란을 선택 취소합니다.

단계 5 저장을 클릭합니다.

단계 6 구성 적용을 클릭합니다.

데이지 체인 모드

데이지 체인 키트에 제공된 스마트 어댑터 및 USB-C 케이블을 사용하여 회의전화 전화기를 연결하여 룸의 오디오 서비스 지역을 확장할 수 있습니다.

데이지 체인 모드에서 두 장치는 전원 어댑터에 연결된 스마트 어댑터를 통해 전원을 공급 받습니다. 장치당 하나의 외부 마이크만 사용할 수 있습니다. 장치에 유선 마이크 한쌍을 사용하거나 무선 마이크 한쌍을 사용할 수 있지만 마이크의 혼합된 조합은 사용할 수 없습니다. 유선 마이크가 장치 중 하나에 연결되면 동일한 장치에 연결된 모든 무선 마이크의 페어링이 해제됩니다. 활성 통화가 있을 때마다 두 장치의 전화기 화면에 있는 LED 및 메뉴 옵션이 동기화됩니다.

관련 항목

데이지 체인 모드로 전화회의 전화기 설치, 38 페이지
데이지 체인 모드에서 하나의 전화기가 작동하지 않음, 175 페이지

전화회의 전화기 설치

전화기를 네트워크에 연결한 후, 전화기 시작 프로세스가 시작되고 전화기가 Cisco Unified Communications Manager에 등록합니다. DHCP 서비스를 비활성화한 경우 전화기에 네트워크 설정을 구성해야 합니다.

자동 등록을 사용하는 경우에는 전화기와 사용자 연결, 버튼 테이블 변경이나 디렉터리 번호 같이 전화기에 대한 특정 구성 정보를 업데이트해야 합니다.

전화기를 연결한 후에 전화기에 새 펌웨어 로드를 설치해야 하는지 확인합니다.

전화회의 전화기를 데이지 체인 모드에서 사용하는 경우 데이지 체인 모드로 전화회의 전화기 설치, 38 페이지의 내용을 참조하십시오.

시작하기 전에

최신 펌웨어 버전이 Cisco Unified Communications Manager에 설치되었는지 확인합니다. 여기서 장치 패키지가 업데이트되었는지 확인합니다.

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

프로시저

단계 **1** 전화기의 전원 공급지를 선택합니다.

- 다음을 사용한 PoE(Power over Ethernet) 구축: Cisco IP 전화회의 전화기 8832 PoE Injector
- 다음을 사용한 비 PoE 이더넷 구축: Cisco IP 전화회의 전화기 8832 비 PoE 이더넷 인젝터
- Cisco IP 전화회의 전화기 8832 전원 어댑터를 통한 Wi-Fi 구축

자세한 정보는 전화회의 전화기에 전원을 제공하는 방법, 33 페이지를 참조하십시오.

단계 **2** 전화기를 스위치에 연결합니다.

- PoE를 사용하는 경우:
  1. 이더넷 케이블을 LAN 포트에 꽂습니다.
  2. 이더넷 케이블의 다른 쪽 끝을 Cisco IP 전화회의 전화기 8832 PoE Injector 또는 Cisco IP 전화회의 전화기 8832 이더넷 인젝터에 꽂습니다.
  3. USB-C 케이블을 사용하여 인젝터를 전화회의 전화기에 연결합니다.
- PoE를 사용하지 않는 경우:
  1. Cisco IP 전화회의 전화기 8832 이더넷 인젝터을 사용하는 경우 전원 어댑터를 전기 콘센트에 꽂습니다.
  2. USB-C 케이블을 사용하여 전원 어댑터를 이더넷 인젝터에 연결합니다.

     또는

     Cisco IP 전화회의 전화기 8832 비 PoE 이더넷 인젝터을 사용하는 경우 전원 어댑터를 전기 콘센트에 꽂습니다.
  3. 이더넷 케이블을 비 PoE 이더넷 인젝터 또는 이더넷 인젝터에 꽂습니다.
  4. 이더넷 케이블을 LAN 포트에 꽂습니다.
  5. USB-C 케이블을 사용하여 비 PoE 이더넷 인젝터 또는 이더넷 인젝터를 전화회의 전화기에 연결합니다.
- Wi-Fi를 사용하는 경우:
  1. Cisco IP 전화회의 전화기 8832 전원 어댑터를 전기 콘센트에 꽂습니다.

2. USB-C 케이블을 사용하여 전원 어댑터를 전화회의 전화기에 연결합니다.

   참고 전원 어댑터 대신 비 PoE 이더넷 인젝터를 사용하여 전화기의 전원을 켤 수 있습니다. 그러나 LAN 케이블의 플러그를 빼야 합니다. 이 전화기는 이더넷 연결이 불가능할 때만 Wi-Fi에 연결됩니다.

단계 **3** 전화기 시작 프로세스를 모니터링합니다. 이 단계는 전화기가 제대로 구성되었는지를 확인합니다.

단계 **4** 자동 등록을 사용하지 않는 경우 전화기에서 수동으로 보안 설정을 구성합니다.

단계 **5** 전화기에서 Cisco Unified Communications Manager에 저장되어 있는 최신 펌웨어 이미지를 업그레이드할 수 있습니다.

단계 **6** 전화기로 전화를 걸어 전화기와 기능이 정확하게 작동하는지 확인합니다.

단계 **7** 사용자에게 전화기 사용법과 전화기 옵션 구성 방법에 관한 정보를 제공합니다. 이 단계에서는 사용자에게 Cisco 전화기를 잘 사용하기 위한 적절한 정보가 있는지 확인합니다.

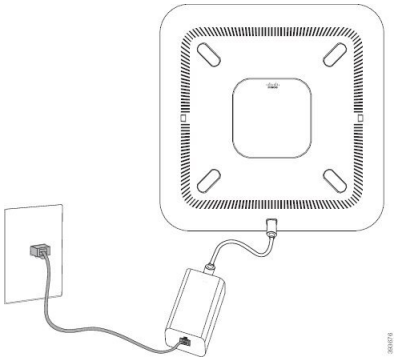
전화회의 전화기에 전원을 제공하는 방법

전화회의 전화기를 사용하려면 다음 전원 중 하나가 필요합니다.

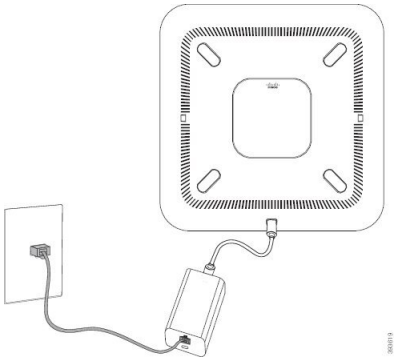
- PoE(Power over Ethernet)
  - 북미
    - Cisco IP 전화회의 전화기 8832 PoE Injector
    - Cisco IP 전화회의 전화기 8832 이더넷 인젝터
  - 북미 이외의 지역 -Cisco IP 전화회의 전화기 8832 PoE Injector
- 비 PoE 이더넷
  - 북미
    - Cisco IP 전화회의 전화기 8832 비 PoE 이더넷 인젝터
    - Cisco IP 전화회의 전화기 8832 이더넷 인젝터 Cisco IP 전화회의 전화기 8832 전원 어댑터를 전기 콘센트에 연결.
  - 북미 이외의 지역 -Cisco IP 전화회의 전화기 8832 비 PoE 이더넷 인젝터
- WiFi - 전기 콘센트에 연결된 Cisco IP 전화회의 전화기 8832 전원 어댑터를 사용합니다.

그림 ***6:*** 전화회의 전화기 ***PoE*** 전원 옵션

다음 그림은 두 가지 PoE 전원 옵션을 보여줍니다.



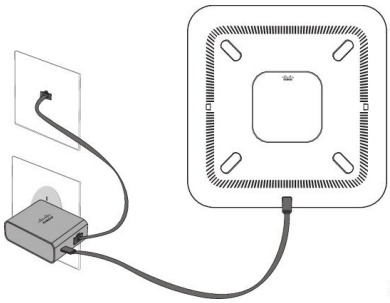
Cisco IP 전화회의 전화기 8832 PoE Injector PoE 전원 옵션 사용



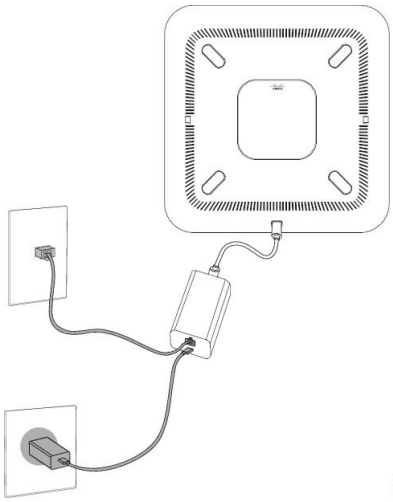
Cisco IP 전화회의 전화기 8832 이더넷 인젝터 PoE 전원 옵션 사용

그림 **7:** 전화회의 전화기 이더넷 전원 옵션

다음 그림은 두 가지 이더넷 전원 옵션을 보여줍니다.



Cisco IP 전화회의 전화기 8832 비 PoE 이더넷 인젝터 이더넷 전원 옵션 사용



Cisco IP 전화회의 전화기 8832 이더넷 인젝터 이더넷 전원 옵션 사용

그림 ***8: Wi-Fi*** 네트워크에 연결된 경우 전화회의 전화기 전원 옵션

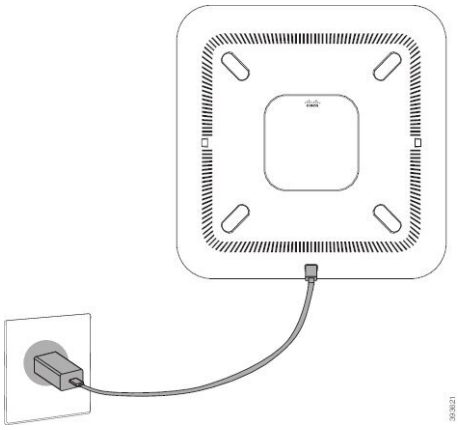
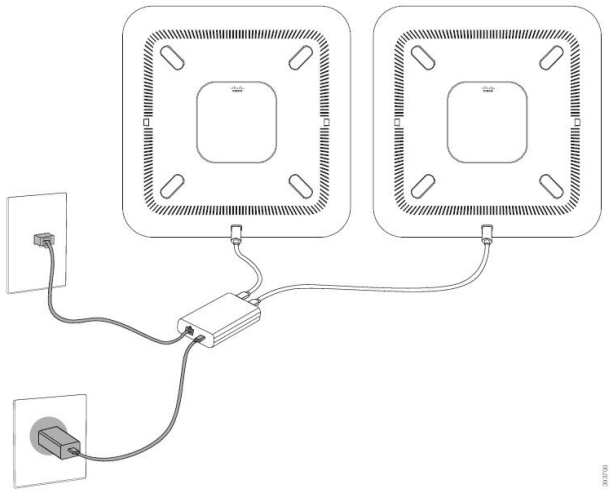


그림 ***9:*** 데이지 체인 모드의 전화회의 전화기 전원 옵션

다음 그림은 전화기가 데이지 체인 모드로 연결되었을 때의 전원 옵션을 보여줍니다.



유선 확장 마이크 설치

전화기는 2개의 유선 확장 마이크가 있는 옵션 키트를 지원합니다. 마이크는 전화기에서 최대 2.13m(7피트)까지 마이크를 확장할 수 있습니다. 최상의 결과를 얻으려면 마이크를 전화기에서 0.91m ~ 2.1m 사이의 거리를 두고 통화하십시오.

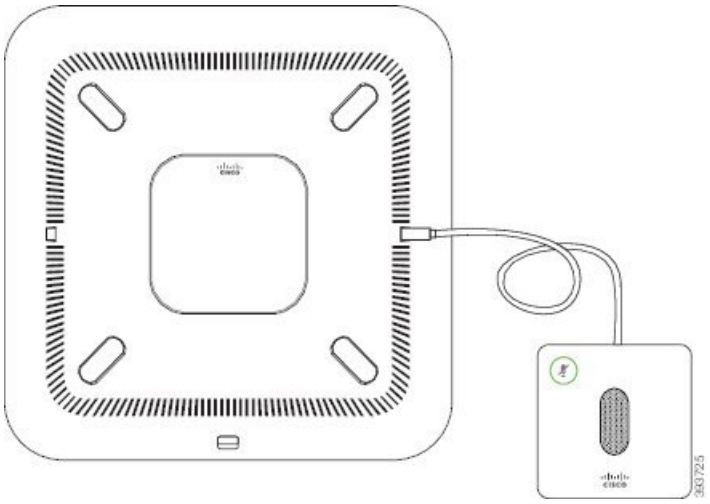
프로시저

단계 **1** 마이크 케이블의 끝을 전화기의 측면 포트에 꽂습니다.

단계 **2** 원하는 위치로 마이크 케이블을 확장합니다.

다음 그림은 유선 확장 마이크의 설치를 보여줍니다.

그림 *10:* 유선 확장 마이크 설치



유선 확장 마이크 설치

전화회의 전화기에서는 두 개의 무선 확장 마이크 옵션을 제공합니다.

참고 2개의 유선 마이크 또는 2개의 무선 마이크를 전화기와 함께 사용해야 하지만 혼합된 조합은 사용하지 않아야 합니다.

전화기로 통화할 때 확장 마이크의 LED가 녹색으로 켜집니다. 확장 마이크를 음소거하려면 음소거 키를 누릅니다. 마이크를 음소거하면 LED가 빨간색으로 켜집니다. 마이크의 배터리가 부족하면 배터리 표시 LED가 빠르게 깜박입니다.

시작하기 전에

무선 확장 마이크를 설치하기 전에 먼저 유선 확장 마이크 연결을 끊습니다. 두 유선 및 무선 확장 마이크를 동시에 사용할 수 없습니다.

프로시저

단계 **1** 마이크 놓으려는 테이블 표면 위치에 테이블 장착 판을 놓습니다.

단계 **2** 테이블 장착판 맨 아래에 있는 양면 테이프의 접착제를 제거합니다. 테이블 장착판을 테이블 표면에 접착합니다.

단계 **3** 테이블 장착판에 마이크를 연결합니다. 마이크를 제자리에 고정시켜 주는 자석이 포함되어 있습니다.

필요하면 마이크와 부착된 테이블 장착판을 테이블 표면의 다른 위치로 이동할 수 있습니다. 장치를 보호하기 위해 이동할 때 주의하십시오.

관련 항목

무선 확장 마이크(8832만 해당), 13 페이지
무선 마이크 충전 거치대 설치, 37 페이지

무선 마이크 충전 거치대 설치

충전 거치대를 사용하여 무선 마이크 배터리를 충전합니다.

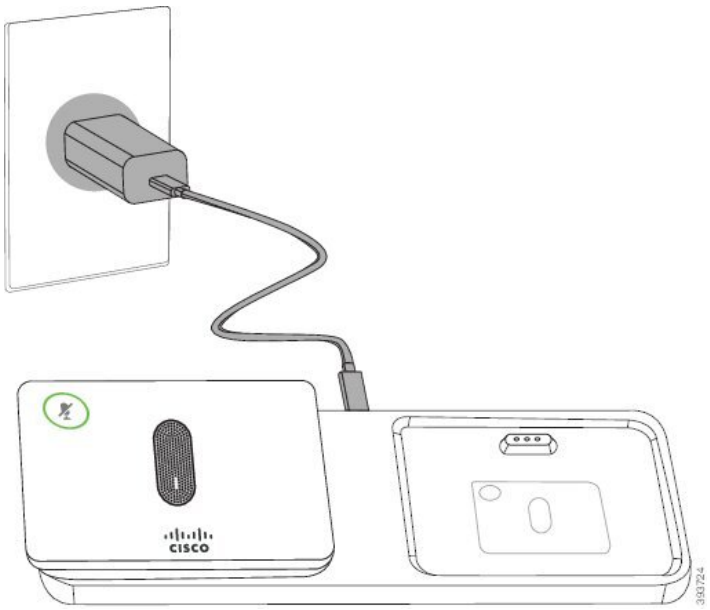
프로시저

단계 **1** 충전 거치대 전원 어댑터를 전기 콘센트에 꽂습니다.

단계 **2** USB-C 케이블의 한쪽 끝을 충전 거치대에 연결하고 다른 쪽 끝을 전원 어댑터에 연결합니다.

다음 그림은 무선 마이크 충전 거치대의 설치를 보여줍니다.

그림 ***11:*** 무선 마이크 충전 거치대 설치



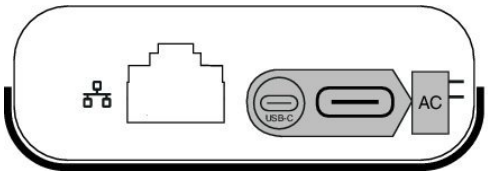
관련 항목

무선 확장 마이크(8832만 해당), 13 페이지
유선 확장 마이크 설치, 36 페이지

데이지 체인 모드로 전화회의 전화기 설치

데이지 체인 키트에는 스마트 어댑터, 짧은 LAN 케이블, 길고 두꺼운 USB-C 케이블 2개 및 더 짧고 더 얇은 USB-C 케이블이 포함되어 있습니다. 데이지 체인 모드에서 전화회의 전화기는 전기 콘센트의 외부 전원이 필요합니다. 스마트 어댑터를 사용하여 전화기를 서로 연결해야 합니다. 긴 USB-C 케이블은 전화기에 연결되고 짧은 케이블은 전원 어댑터에 연결됩니다. 전원 어댑터 및 LAN 포트를 스마트 어댑터에 연결할 때는 다음 그림을 참조하십시오.

그림 ***12:*** 스마트 어댑터 전원 포트 및 ***LAN*** 포트



장치당 하나의 마이크만 사용할 수 있습니다.

참고 2개의 유선 마이크 또는 2개의 무선 마이크를 전화기와 함께 사용해야 하지만 혼합된 조합은 사용하지 않아야 합니다.

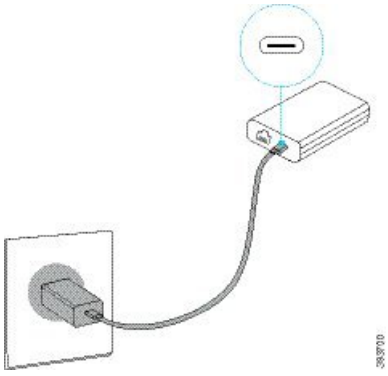
전원 어댑터용 USB-C 케이블은 전화기에 연결된 USB-C 케이블보다 얇습니다.

프로시저

단계 **1** 전원 어댑터를 전기 콘센트에 꽂습니다.

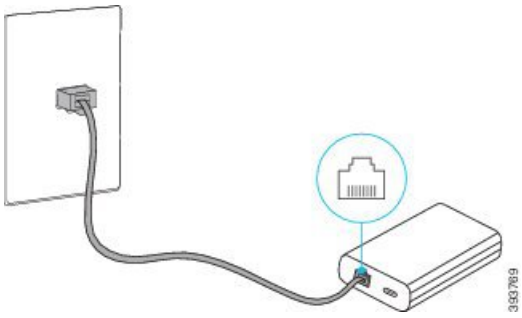
단계 **2** 전원 어댑터에서 짧고 얇은 USB-C 케이블을 스마트 어댑터에 연결합니다.

그림 ***13:*** 전원 콘센트에 연결된 스마트 어댑터 ***USB*** 포트



단계 **3** 필수: 이더넷 케이블을 스마트 어댑터 및 LAN 포트에 연결합니다.

그림 ***14:*** 벽면 콘센트의 ***LAN*** 포트에 연결된 스마트 어댑터 ***LAN*** 포트

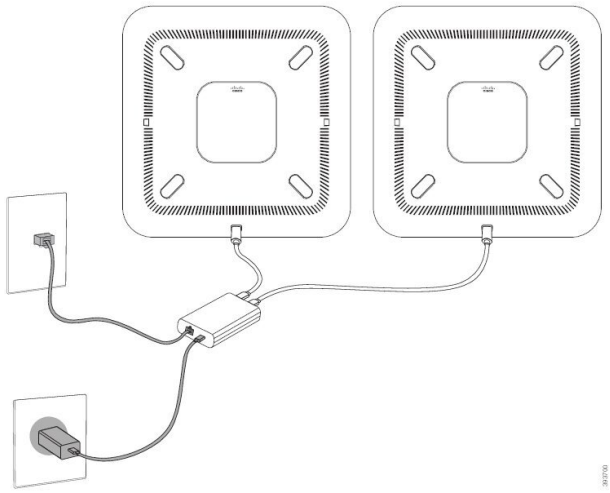


단계 **4** 더 길고 두꺼운 USB-C 케이블을 사용하여 첫 번째 전화기를 스마트 어댑터에 연결합니다.

단계 **5** USB-C 케이블을 사용하여 두 번째 전화기를 스마트 어댑터에 연결합니다.

다음 그림은 데이지 체인 모드에서 전화회의 전화기의 설치를 보여줍니다.

그림 ***15:*** 데이지 체인 모드로 전화회의 전화기 설치



관련 항목

데이지 체인 모드, 31 페이지
데이지 체인 모드에서 하나의 전화기가 작동하지 않음, 175 페이지

백업 이미지에서 전화회의 전화기 재부팅

Cisco IP 전화회의 전화기 8832에는 기본 이미지가 손상되었을 때 전화기를 복구할 수 있는 보조 백업 이미지가 있습니다.

백업 이미지에서 전화기를 재부팅하려면 다음 절차를 수행하십시오.

프로시저

단계 **1** 전화회의 전화기에 전원을 연결하는 동안 * 키를 누릅니다.
단계 **2** LED 막대가 녹색으로 켜졌다가 꺼지면 * 키에서 손을 뗍니다.
단계 **3** 전화회의 전화기가 백업 이미지로 재부팅됩니다.

설정 메뉴에서 전화기 설정

전화기에는 사용자가 전화기를 사용하기 전에 수정해야 할 수도 있는 여러 가지 구성 가능한 네트워크 설정이 있습니다. 이러한 설정은 전화기 메뉴에서 액세스하고, 일부는 변경도 가능합니다.

전화기에는 다음과 같은 설정 메뉴가 있습니다.

- 네트워크 설정: 다양한 네트워크 설정의 확인 및 구성을 위한 옵션을 제공합니다.
  - IPv4 설정: 이 하위 메뉴는 추가 네트워크 옵션을 제공합니다.
  - IPv6 설정: 이 하위 메뉴는 추가 네트워크 옵션을 제공합니다.
- 보안 설정: 다양한 보안 설정의 확인 및 구성을 위한 옵션을 제공합니다.

참고 전화기에서 [설정] 메뉴 또는 이 메뉴의 옵션에 액세스할 수 있는지 여부를 제어할 수 있습니다. Cisco 통합 커뮤니케이션 매니저 관리 전화기 설정 창에서 설정 액세스 필드를 사용하여 액세스를 제어합니다. 설정 액세스 필드는 다음과 같은 값을 허용합니다.

- 활성화됨: [설정] 메뉴에 대한 액세스를 허용합니다.
- 비활성화됨: [설정] 메뉴에서 대부분 항목에 대한 액세스를 금지합니다. 사용자는 설정 > 상태에 계속 액세스할 수 있습니다.
- 제한: [사용자 환경 설정] 및 상태 메뉴 항목에 대한 액세스를 허용하고, 볼륨 변경 사항 저장을 허용합니다. [설정] 메뉴의 기타 옵션에 대한 액세스를 차단합니다.

[관리자 설정] 메뉴 옵션에 액세스할 수 없다면 설정 액세스 필드를 선택합니다.

전화기의 표시 전용 설정은 Cisco 통합 커뮤니케이션 매니저 관리에서 구성합니다.

프로시저

단계 **1** 설정을 누릅니다.
단계 **2** 관리 설정을 선택합니다.
단계 **3** 필요할 경우 암호를 입력하고, 로그인을 클릭합니다.

단계 4 네트워크 설정 또는 보안 설정을 선택합니다.

단계 5 원하는 메뉴를 표시하려면 다음 중 한 작업을 수행합니다.

- 탐색 화살표를 사용해 원하는 메뉴를 선택한 다음 선택을 누릅니다.
- 전화기의 키패드를 사용해 메뉴에 해당하는 번호를 입력합니다.

단계 6 하위 메뉴를 표시하려면 단계 5를 반복합니다.

단계 7 메뉴를 종료하려면 돌아가기를 누릅니다.

관련 항목

전화회의 전화기를 다시 시작 또는 재설정, 183 페이지
네트워크 설정 구성, 42 페이지
보안 설정 구성

전화기 암호 적용

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 [일반 전화기 프로파일 구성] 창을 탐색합니다(장치 > 장치 설정 > 일반 전화기 프로파일).

단계 2 [로컬 전화 잠금 해제 암호] 옵션에 암호를 입력합니다.

단계 3 전화기에서 사용하는 일반 전화기 프로파일에 암호가 적용됩니다.

전화기의 텍스트 및 메뉴 항목

옵션 설정 값을 편집할 때는 다음 지침을 따르십시오.

- 탐색 패드의 화살표를 사용하여 편집하려는 필드를 강조 표시합니다. 탐색 패드에서 선택을 눌러 필드를 활성화합니다. 필드가 활성화되면 값을 입력할 수 있습니다.
- 키패드의 키를 사용해 숫자와 문자를 입력합니다.
- 키패드를 사용해 문자를 입력하려면 해당 번호 키를 사용해야 합니다. 특정 문자를 표시하려면 해당 키를 1번 이상 누릅니다. 예를 들어, “a”의 경우 **2** 키를 한 번, “b”의 경우 두 번, “c”의 경우 세 번 빠르게 누릅니다. 일시 중지한 후 커서가 자동으로 이동하면 다음 문자를 입력할 수 있습니다.
- 실수했다면 소프트키를 누릅니다. 그럼 소프트키가 커서 왼쪽의 문자를 삭제합니다.
- 적용을 누르기 전에 되돌리기를 누르면 변경한 내용이 모두 지워집니다.
- 점을 입력하려면(예: IP 주소), 키패드의 *를 누릅니다.
- IPv6 주소를 위해 콜론을 입력하려면 키패드의 *를 누릅니다.

참고 Cisco IP 전화기에서는 필요할 경우 몇 가지 방법으로 옵션 설정을 재설정하거나 복원할 수 있습니다.

네트워크 설정 구성

프로시저

단계 **1** 설정을 누릅니다.

단계 **2** 관리자 설정 > 네트워크 설정 > 이더넷 설정을 선택합니다.

단계 **3** 네트워크 설정 필드, 42 페이지에 설명된 대로 필드를 설정합니다.
필드를 설정하면 전화기를 재부팅해야 할 수 있습니다.

네트워크 설정 필드

[네트워크 설정] 메뉴는 IPv4 및 IPv6에 대한 필드 및 하위 메뉴를 포함합니다.

일부 필드를 변경하려면 DHCP를 해제해야 합니다.

표 ***10:*** 네트워크 설정 메뉴

항목	유형	기본값	설명
IPv4 설정	메뉴		“IPv4 설정 하위 메뉴” 테이블을 참조하십시오. 이 옵션은 모드 또는 이중 스택 모드일 때만 표시됩니다.
IPv6 설정	메뉴		“IPv6 설정 하위 메뉴” 테이블을 참조하십시오.
호스트 이름	문자열		전화기의 호스트 이름입니다. DHCP를 사용하는 경우 이 이름이 자동으로 할당됩니다.
도메인 이름	문자열		전화기가 위치한 DNS(Domain Name System) 도메인의 이름입니다. 이 필드를 변경하려면 DHCP를 해제합니다.

항목	유형	기본값	설명
사용 가능한 VLAN ID			전화기가 속해 있는 Cisco Catalyst 스위치에 구성된 사용 가능한 VLAN(Virtual Local Area Network)입니다.
관리자 VLAN ID			전화기가 속해 있는 보조 LAN입니다.
SW 포트 설정	자동 협상 10 반이중 10 전이중 100 반이중 100 전이중	자동 협상	스위치 포트의 속도 및 전이중/반이중: • 10 Half = 10-BaseT/반이중 • 10 Full = 10-BaseT/전이중 • 100 Half = 100-BaseT/반이중 • 100 Full = 100-BaseT/전이중
LLDP-MED: SW 포트	비활성화됨 활성화됨	활성화됨	스위치 포트에 LLDP-MED(Link Layer Discovery Protocol Media Endpoint Discovery)가 활성화되어 있는지를 알려줍니다.

표 ***11: IPv4*** 설정 하위 메뉴

항목	유형	기본값	설명
DHCP	비활성화됨 활성화됨	활성화됨	DHCP 사용을 활성화 또는 비활성화합니다.
IP 주소			전화기의 IPv4(인터넷 프로토콜 버전 4) 주소입니다. 이 필드를 변경하려면 DHCP를 해제합니다.
서브넷 마스크			전화기가 사용하는 서브넷 마스크입니다. 이 필드를 변경하려면 DHCP를 해제합니다.
기본 라우터 1			전화기가 사용하는 기본 라우터입니다. 이 필드를 변경하려면 DHCP를 해제합니다.

항목	유형	기본값	설명
DNS 서버 1			전화기가 사용하는 기본 DNS(Domain Name System) 서버(DNS Server 1)입니다. 이 필드를 변경하려면 DHCP를 해제합니다.
DNS 서버 2			전화기가 사용하는 기본 DNS(Domain Name System) 서버(DNS Server 2)입니다.
DNS 서버 3			전화기가 사용하는 기본 DNS(Domain Name System) 서버(DNS Server 3)입니다.
대체 TFTP	아니요 예	아니요	전화기에서 대체 TFTP 서버를 사용하는지 알려줍니다.
TFTP 서버 1			전화기에서 사용하는 기본 TFTP(Trivial File Transfer Protocol) 서버입니다. 대체 TFTP 옵션을 켜기로 설정하면 TFTP 서버 1 옵션에 대해 0이 아닌 값을 입력해야 합니다. 기본 TFTP 서버 또는 백업 TFTP 서버가 전화기의 CTL 또는 ITL 파일에 나열되어 있지 않은 경우 TFTP 서버 1 옵션에 변경 사항을 저장하려면 파일을 잠금 해제해야 합니다. 이 경우, TFTP 서버 1 옵션에 변경 사항을 저장할 때 전화기는 해당 파일을 삭제합니다. 새 CTL 또는 ITL 파일이 새 TFTP 서버 1 주소에서 다운로드됩니다. 최종 테이블 다음의 TFTP 노트를 참조하십시오.

항목	유형	기본값	설명
TFTP 서버 2			전화기에서 사용하는 보조 TFTP 서버. 기본 TFTP 서버 또는 백업 TFTP 서버가 전화기의 CTL 또는 ITL 파일에 나열되어 있지 않은 경우 TFTP 서버 2 옵션에 변경 사항을 저장하려면 파일을 잠금 해제해야 합니다. 이 경우, TFTP 서버 2 옵션에 변경 사항을 저장할 때 전화기는 해당 파일을 삭제합니다. 새 CTL 또는 ITL 파일이 새 TFTP 서버 2 주소에서 다운로드됩니다. 최종 테이블 다음의 TFTP 노트 섹션을 참조하십시오.
DHCP 주소 해제됨	아니요 예	아니요	

표 ***12: IPv6***설정 하위 메뉴

항목	유형	기본값	설명
DHCPv6 활성화됨	비활성화됨 활성화됨	활성화됨	IPv6 DHCP 사용을 활성화 또는 비활성화합니다.
IPv6 주소			전화기의 IPv6 주소입니다. 이 필드를 변경하려면 DHCP를 해제합니다.
IPv6 접두사 길이			IPv6 주소의 길이입니다. 이 필드를 변경하려면 DHCP를 해제합니다.
IPv6 기본 라우터 1			기본 IPv6 라우터입니다. 이 필드를 변경하려면 DHCP를 해제합니다.
IPv6 DNS 서버 1			기본 IPv6 DNS 서버 이 필드를 변경하려면 DHCP를 해제합니다.

항목	유형	기본값	설명
IPv6 대체 TFTP	아니요 예	아니요	전화기에서 대체 IPv6 TFTP 서버를 사용하는지 알려줍니다.
IPv6 TFTP 서버 1			전화기에서 사용하는 기본 IPv6 TFTP 서버입니다. 이 테이블 다음의 TFTP 노트 섹션을 참조하십시오.
IPv6 TFTP 서버 2			전화기에서 사용하는 보조 IPv6 TFTP 서버입니다. 이 테이블 다음의 TFTP 노트 섹션을 참조하십시오.
IPv6 주소 해제됨	아니요 예	아니요	

IPv6 설정 옵션을 장치에 구성하려면 Cisco Unified Communication Administration에서 IPv6를 활성화하고 구성해야 합니다. 다음 장치 구성 필드가 IPv6 구성에 적용됩니다.

- IP 주소 지정 모드
- 신호 처리용 IP 주소 지정 모드 기본 설정

IPv6가 Unified 클러스터에서 활성화된 경우 IP 주소 지정 모드의 기본 설정은 IPv4 및 IPv6(이중 스택)입니다. 이 주소 지정 모드에서 전화기는 IPv4 주소 하나와 IPv6 주소 하나를 획득하고 사용합니다. 이것은 미디어의 필요에 따라 IPv4 및 IPv6 주소를 사용할 수 있습니다. 전화기는 통화 제어 신호를 처리하기 위해 IPv4 또는 IPv6 주소를 사용합니다.

IPv6에 대한 자세한 내용은 다음을 참조하십시오.

- *Cisco Unified Communications Manager* 기능 및 서비스 설명서의 "일반 장치 구성", "Cisco Unified Communications 장치에서 IPv6 지원" 장.
- *IPv6 Deployment Guide for Cisco Collaboration Systems* 릴리스 *12.0*은 여기에 있습니다.https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

TFTP 참고

전화기가 TFTP 서버를 찾을 때 전화기는 프로토콜과 관계없이, 수동으로 할당된 TFTP 서버에 우선순위를 부여합니다. 구성에 IPv6 및 IPv4 TFTP 서버가 모두 포함되어 있는 경우 전화기는 수동으로 할당된 IPv6 TFTP 서버 및 IPv4 TFTP 서버에 우선 순위를 부여하여 TFTP 서버를 찾는 순서에 우선순위를 지정합니다. 전화기는 다음 순서로 TFTP 서버를 찾습니다.

1. 수동으로 할당된 IPv4 TFTP 서버

2. 수동으로 할당된 IPv6 서버
3. DHCP 할당 TFTP 서버
4. DHCPv6 할당 TFTP 서버

CTL 및 ITL 파일에 대한 자세한 내용은 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.

도메인 이름 필드 설정

프로시저

단계 **1** [DHCP 활성화] 옵션을 아니요로 설정합니다.
단계 **2** [도메인 이름] 옵션으로 스크롤하여 선택을 누르고 새 도메인 이름을 입력합니다.
단계 **3** 적용을 누릅니다.

전화기에서 무선 **LAN** 활성화

무선 LAN이 배포되는 위치에서 Wi-Fi 서비스 지역이 음성 패킷을 전송하기에 적합함을 확인하십시오.

빠른 보안 로밍 방법은 Wi-Fi 사용자에게 권장합니다. 802.11r (FT)를 사용하는 것이 좋습니다.

전체 구성 정보는 다음 위치에 있는 *Cisco IP* 전화기 *8832 Wireless LAN* 배포 안내서를 참조하십시오.

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

Cisco IP 전화기 *8832 Wireless LAN* 배포 안내서는 다음 구성 정보를 포함합니다.

- 무선 네트워크 구성
- Cisco Unified Communications Manager Administration의 무선 네트워크 구성
- Cisco IP Phone의 무선 네트워크 구성

시작하기 전에

Wi-Fi가 전화기에서 활성화되고 이더넷 케이블이 분리되었는지 확인합니다.

프로시저

단계 **1** 애플리케이션을 활성화하려면 설정을 누릅니다.
단계 **2** 관리 설정 > 네트워크 설정 > **Wi-Fi** 클라이언트 설정 > 무선으로 이동합니다.

단계 **3** 켜기를 누릅니다.

Cisco Unified Communications Manager에서 무선 LAN 설정

Cisco Unified Communications Manager Administration에서 전화회의 전화기에 대해 "Wi-Fi"라는 매개변수를 활성화해야 합니다.

참고 Cisco Unified Communications Manager Administration의 [전화기 구성] 창에서(장치 > 전화기) MAC 주소를 구성할 때 유선 MAC 주소를 사용합니다. Cisco Unified Communications Manager 등록은 무선 MAC 주소를 사용하지 않습니다.

Cisco Unified Communications Manager Administration에서 다음 절차를 수행합니다.

프로시저

단계 **1** 특정 전화기에서 무선 LAN을 활성화하려면 다음 단계를 수행하십시오.

a) 장치 > 전화기를 선택합니다.
b) 필요한 전화기를 찾습니다.
c) [제품별 구성 레이아웃] 섹션에서 Wi-Fi 매개변수에 대한 활성화됨 설정을 선택합니다.
d) 일반 설정 무시 확인란을 선택합니다.

단계 **2** 전화기 그룹에 대해 무선 LAN을 활성화하려면

a) 장치 > 장치 설정 > 일반 전화기 프로파일을 선택합니다.
b) Wi-Fi 매개변수에 대한 활성화됨 설정을 선택합니다.

참고 이 단계의 구성이 제대로 작동하려면 1d 단계에서 설명한 일반 설정 무시 확인란의 선택을 취소합니다.

c) 일반 설정 무시 확인란을 선택합니다.
d) 장치 > 전화기를 사용해 일반 전화기 프로파일에 전화기를 연결합니다.

단계 **3** 네트워크의 모든 WLAN 기능 전화기에 대해 무선 LAN을 활성화하려면

a) 시스템 > 엔터프라이즈 전화기 구성을 선택합니다.
b) Wi-Fi 매개변수에 대한 활성화됨 설정을 선택합니다.

참고 이 단계의 구성이 제대로 작동하려면 1d 및 2c단계에서 설명한 일반 설정 무시 확인란의 선택을 취소합니다.

c) 일반 설정 무시 확인란을 선택합니다.

전화기에 무선 LAC 설정

Cisco IP 전화기를 WLAN에 연결하려면 해당 WLAN 설정으로 전화기에 대한 네트워크 프로파일을 구성해야 합니다. 전화기의 네트워크 설정 메뉴를 사용하여 **Wi-Fi** 클라이언트 설정 하위 메뉴에 액세스하고 WLAN 구성을 설정할 수 있습니다.

참고 Wi-Fi가 Cisco Unified Communications Manager에서 비활성화되었을 때는 **Wi-Fi** 클라이언트 설정 옵션이 네트워크 설정 메뉴에 나타나지 않습니다.

자세한 내용 http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html에서 *Cisco IP* 전화회의 전화기 *8832 WLAN* 배포 설명서를 참조하십시오.

시작하기 전에

Cisco Unified Communications Manager에서 무선 LAN을 구성합니다.

프로시저

단계 **1** 설정을 누릅니다.

단계 **2** 관리 설정 > 네트워크 설정 > **Wi-Fi** 클라이언트 설정을 선택합니다.

단계 **3** 다음 표에 설명된 대로 무선 구성을 설정합니다.

표 ***13: Wi-Fi*** 클라이언트 설정 메뉴 옵션

옵션	설명	변경
무선	Cisco IP 전화기의 무선 라디오를 켜거나 끕니다.	무선 옵션으로 스크롤하고 전환 용하여 켜기 또는 끄기로 설정을
네트워크 이름	네트워크 선택 창을 사용하여 무선 네트워크에 연결할 수 있습니다. 이 창에는 뒤로 및 기타의 두 소프트 키가 있습니다.	네트워크 선택 창에서 연결할 네 택합니다.
Wi-Fi 로그인 액세스	창에서 Wi-Fi 로그인 표시를 활성화합니다.	**Wi-Fi** 로그인 액세스 옵션으로 스 글 스위치를 사용하여 켜기와 끄 을 변경합니다.

옵션	설명	변경
IPv4 설정	IPv4 설정 구성 하위 메뉴에서 다음 작업을 수행할 수 있습니다. • 전화기에서 DHCP 서버가 할당하는 IP 주소를 사용할 수 있도록 설정하거나 설정을 해제합니다. • 수동으로 IP 주소, 서브넷 마스크, 기본 라우터, DNS 서버 및 대체 TFTP 서버를 설정합니다. IPv4 주소 필드에 대한 자세한 내용은 "IPv4 설정 하위 메뉴" 표를 참조하십시오.	**IPv4** 설정으로 스크롤하고 선택을
IPv6 설정	IPv6 설정 구성 하위 메뉴에서 다음 작업을 수행할 수 있습니다. • 사용자가 DHCPv6 서버에서 할당하거나 SLAAC에서 IPv6 사용 가능 라우터를 통해 획득하는 IPv6 주소를 사용할 수 있도록 설정하거나 설정을 해제합니다. • 수동으로 IPv6 주소, 접두사 길이, 기본 라우터, DNS 서버 및 대체 TFTP 서버를 설정합니다. IPv6 주소 필드에 대 한 자세한 내용은 "IPv6 설정 하위 메뉴" 표를 참조하십시오.	**IPv6** 설정으로 스크롤하고 선택을
MAC 주소	전화기의 고유한 MAC(Media Access Control) 주소입니다.	표시 전용입니다. 구성할 수 없습니
도메인 이름	전화기가 위치한 DNS(Domain Name System) 도메인의 이름입니다.	도메인 이름 필드 설정, 47 페이지 참

단계 **4** 저장을 눌러 변경 사항을 저장하거나 되돌리기를 눌러 변경 사항을 취소합니다.

WLAN 인증 시도 수 설정

인증 요청은 사용자 로그인 인증서의 확인입니다. Wi-Fi 네트워크에 참가한 전화기가 Wi-Fi 서버로 다시 연결을 시도할 때마다 발생합니다. 그런 예에는 Wi-Fi 세션 시간이 초과되거나 Wi-Fi 연결이 끊어졌다가 다시 연결되는 때가 포함됩니다.

Wi-Fi 전화기가 Wi-Fi 서버에 인증 요청을 보내는 횟수를 구성할 수 있습니다. 시도 기본 횟수는 2이지만 이 매개변수를 1에서 3까지 설정할 수 있습니다. 전화기가 인증에 실패하는 경우 사용자에게 다시 로그인하라는 메시지가 표시됩니다.

WLAN 인증 시도를 개별 전화기, 전화기의 풀 또는 네트워크에 있는 모든 Wi-Fi 전화기에 적용할 수 있습니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택하고 전화기를 찾습니다.

단계 **2** 제품별 구성 영역으로 이동하고 **WLAN** 인증 시도 필드를 설정합니다.

단계 **3** 저장을 선택합니다.

단계 **4** 구성 적용을 선택합니다.

단계 **5** 전화기를 다시 시작합니다.

WLAN 프롬프트 모드 활성화

사용자가 전화기의 전원이 켜질 때 또는 재설정할 때 Wi-Fi 네트워크에 로그인하도록 하려면 WLAN 프로파일 1 프롬프트 모드를 활성화합니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다.

단계 **2** 설정할 전화기를 검색합니다.

단계 **3** [제품별 구성 영역]으로 이동하고 **WLAN** 프로파일 **1** 프롬프트 모드 필드를 활성화로 설정합니다.

단계 **4** 저장을 선택합니다.

단계 **5** 구성 적용을 선택합니다.

단계 **6** 전화기를 다시 시작합니다.

Cisco Unified Communications Manager를 사용하여 Wi-Fi 프로파일 설정

Wi-Fi 프로파일을 구성한 다음 Wi-Fi를 지원하는 전화기에 해당 프로파일을 할당합니다. 프로파일에는 Wi-Fi를 사용하여 Cisco Unified Communications Manager에 연결하기 위한 전화기에 필요한 매개변수가 포함되어 있습니다. Wi-Fi를 만들고 사용할 때 개별 전화기에 대해 무선 네트워크를 구성할 필요가 없습니다.

Wi-Fi 프로파일은 Cisco Unified Communications Manager 10.5(2) 이상에서 지원됩니다. EAP-FAST, PEAP-GTC 및 PEAP-MSCHAPv2는 Cisco Unified Communications Manager 릴리스 10.0 이상에서 지원됩니다. EAP-TLS는 Cisco Unified Communications Manager 릴리스 11.0 이상에서 지원됩니다.

Wi-Fi 프로파일을 사용하면 사용자가 전화기에서 Wi-Fi 구성을 변경하는 것을 방지하거나 제한할 수 있습니다.

Wi-Fi 프로파일을 사용할 때는 키와 암호를 보호하기 위해 TFTP 암호화가 활성화된 보안 프로파일을 사용하는 것이 좋습니다.

EAP-FAST, PEAP-MSCHAPv2 또는 PEAP-GTC 인증을 사용하도록 전화기를 설정할 때는 개별 사용자 ID와 암호를 사용하여 전화기에 로그인해야 합니다.

전화기는 SCEP 또는 수동 설치 방법 중 하나만 설치할 수 있고 두 가지 방법 모두를 사용하여 설치할 수 없는 하나의 서버 인증서만을 지원합니다. 전화기가 인증서 설치의 TFTP 방법을 지원하지 않습니다.

프로시저

단계 **1** Cisco Unified Communications Administration에서 장치 > 장치 설정 > 무선 **LAN** 프로파일을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 무선 **LAN** 프로 파일 정보 섹션에서 매개변수를 설정합니다.

- 이름 - Wi-Fi 프로파일에 대한 고유한 이름을 입력합니다. 이 이름이 전화기에 표시됩니다.
- 설명 - 다른 Wi-Fi 프로파일과 이 프로파일을 구분하는 데 도움이 Wi-Fi 프로파일에 대한 설명을 입력합니다.
- 사용자 수정 가능 - 다음 옵션을 선택합니다.
  - 허용 - 사용자가 자신의 전화기 Wi-Fi 설정을 변경할 수 있음을 나타냅니다. 이 옵션은 기본적으로 선택되어 있습니다.
  - 허용 안 됨 - 사용자가 자신의 전화기에서 Wi-Fi 설정을 변경할 수 없음을 나타냅니다.
  - 제한됨 - 자신의 전화기에서 Wi-Fi 사용자 이름 및 암호를 변경할 수 있음을 나타냅니다. 하지만 사용자는 전화기에서 다른 Wi-Fi 설정을 변경할 수 없습니다.

단계 **4** 무선 설정 섹션에서 매개변수를 설정합니다.

- **SSID(**네트워크 이름**)** - 전화기를 연결할 수 있는 사용자 환경에서 사용할 수 있는 네트워크 이름을 입력합니다. 이 이름은 전화기에서 사용 가능한 네트워크 목록에 표시되며 전화기를 이 무선 네트워크에 연결할 수 있습니다.
- 주파수 대역 - 사용 가능한 옵션은 자동, 2.4GHz 및 5GHz입니다. 이 필드는 무선 연결이 사용하는 주파수 대역을 결정합니다. 자동을 선택하면 전화기는 5GHz 대역을 먼저 사용하려고 시도하고 5GHz를 사용할 수 없을 때만 2.4GHz 대역을 사용합니다.

단계 **5** 인증 설정 섹션에서 인증 방법을 EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP 및 없음 등의 인증 방법 중 하나로 설정합니다.

이 필드를 설정하고 나면 추가 설정해야 하는 필드가 표시될 수 있습니다.

- 사용자 인증서— EAP-TLS 인증에 필요합니다. 제조 설치됨 또는 사용자 설치됨을 선택합니다. SCEP에서 자동으로 또는 전화기의 관리 페이지에서 수동으로 전화기에 인증서를 설치해야 합니다.
- **PSK** 암호— PSK 인증에 필요합니다. 8- 63자의 ASCII 또는 64 HEX 문자 암호를 입력합니다.
- **WEP** 키— WEP 인증에 필요합니다. 40/102 또는 64/128 ASCII 또는 HEX WEP 키를 입력합니다.
  - 40/104 ASCII는 5자입니다.
  - 64/128 ASCII는 13자입니다.
  - 40/104 HEX는 10자입니다.
  - 64/128 HEX는 26자입니다.
- 공유 자격 증명 제공: EAP-FAST, PEAP-MSCHAPv2 및 PEAP-GTC 인증에 필요합니다.
  - 사용자가 사용자 이름과 암호를 관리하는 경우 사용자 이름 및 암호 필드는 비워 둡니다.
  - 모든 사용자가 동일한 사용자 이름 및 암호를 공유하는 경우 사용자 이름 및 암호 필드에 정보를 입력할 수 있습니다.
  - 암호 설명 필드에 설명을 입력합니다.

참고 각 사용자에게 고유한 사용자 이름과 암호를 할당하는 경우 각 사용자에 대한 프로파일을 생성해야 합니다.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

WLAN 프로파일 그룹을 장치 풀에 적용하거나(시스템 > 장치 풀) 전화기에 직접 적용합니다(장치 > 전화기).

Cisco Unified Communications Manager를 사용하여 Wi-Fi 그룹 설정

무선 LAN 프로파일 그룹을 만들고 이 그룹에 무선 LAN 프로파일을 추가할 수 있습니다. 그런 다음 전화기를 설정할 때 프로파일 그룹을 전화기에 할당할 수 있습니다.

프로시저

단계 **1** Cisco Unified Communications Administration에서 장치 > 장치 설정 > 무선 **LAN** 프로파일 그룹을 선택합니다.

시스템 > 장치 풀에서 무선 LAN 프로 파일 그룹을 정의할 수도 있습니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 무선 **LAN** 프로파일 그룹 정보 섹션에서 그룹 이름 및 설명을 입력합니다.

단계 **4** 이 무선 **LAN** 프로파일 그룹에 대한 프로파일 섹션에서 사용 가능한 프로파일 목록에서 사용 가능한 프로파일을 선택하고 선택한 프로파일을 선택한 프로파일 목록으로 이동합니다.

둘 이상의 무선 LAN 프로파일을 선택하면 전화기에서 첫 번째 무선 LAN 프로파일만 사용합니다.

단계 **5** 저장을 클릭합니다.

전화기 시작 확인

전화기에 전원이 연결되면, 전화기는 시작 진단 프로세스를 통해 자동으로 전원을 껐다 켭니다.

프로시저

전화기 전원을 켭니다.

주 화면이 표시되면 전화기가 시작됩니다.

사용자의 전화기 모델 변경

고객님 또는 고객님의 사용자가 사용자의 전화 모델을 변경할 수 있습니다. 예를 들어 다음과 같은 여러 가지 이유로 변경이 필요할 수 있습니다.

- 전화기 모델을 지원하지 않는 소프트웨어 버전으로 Cisco Unified Communications Manager(Unified CM)를 업데이트했습니다.
- 사용자가 현재 모델과 다른 전화기 모델을 원합니다.
- 전화기를 수리하거나 교체해야 합니다.

Unified CM은 이전 전화기를 식별하고 이전 전화기의 MAC 주소를 사용하여 이전 전화기 구성을 식별합니다. Unified CM은 이전 전화기 구성을 새 전화기에 대한 항목에 복사합니다. 그러면 새 전화기의 구성이 이전 전화기와 동일해집니다.

제한: 기존 전화기의 회선 또는 회선 버튼이 새 전화기보다 많은 경우 새 전화기에는 추가 회선 또는 회선 버튼이 구성되어 있지 않습니다.

구성이 완료되면 전화기가 재부팅됩니다.

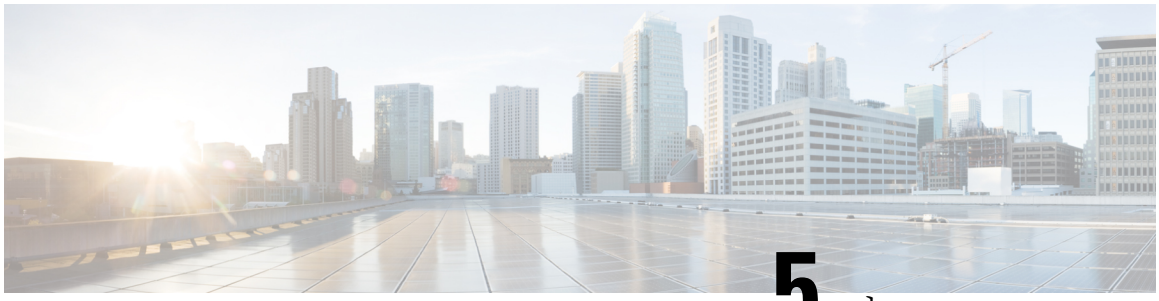
시작하기 전에

Cisco Unified Communications Manager 기능 구성 설명서의 지침에 따라 Cisco Unified Communications Manager를 설정하십시오.

펌웨어 릴리스 12.8(1) 이상이 설치된 상태로 제공되는 새로운 미사용 전화기가 필요합니다.

프로시저

단계 **1** 이전 전화기의 전원을 끕니다.
단계 **2** 새 전화기의 전원을 켭니다.
단계 **3** 새 전화기에서 기존 전화기 교체를 선택합니다.
단계 **4** 이전 전화기의 기본 내선 번호를 입력합니다.
단계 **5** 이전 전화기에 PIN이 할당된 경우 PIN을 입력합니다.
단계 **6** 제출을 누릅니다.
단계 **7** 사용자를 위한 장치가 두 개 이상인 경우 교체할 장치를 선택하고 계속을 누릅니다.



5 장

Cisco Unified Communications Manager 전화기 설치

Cisco IP 전화회의 전화기 설정

자동 등록이 비활성화되고 전화기가 Cisco Unified Communications Manager 데이터베이스에 없는 경우에는, Cisco Unified Communications Manager Administration에서 수동으로 Cisco IP 전화기를 구성해야 합니다. 시스템 및 사용자 필요에 따라 이 과정 중 일부 작업은 선택적으로 적용할 수 있습니다.

각 단계에 대한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

Cisco Unified Communications Manager Administration을 사용해 다음 과정의 각 구성 단계를 수행하십시오.

프로시저

단계 **1** 전화기에 대한 다음과 같은 정보를 수집합니다.

- 전화기 모델
- MAC 주소: 전화기 MAC 주소 결정, 62 페이지
- 전화기의 물리적 위치
- 전화기 사용자의 이름 또는 사용자 ID

- 장치 풀(pool)
- 파티션, 발신 검색 공간 및 위치 정보
- 전화기에 할당할 DN(디렉터리 번호)
- 전화기와 연결할 Cisco Unified Communications Manager 사용자
- 소프트키 템플릿, 전화 기능, IP 전화기 서비스 또는 전화기 애플리케이션에 영향을 미치는 전화기 사용 정보

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서와 관련 링크를 참조하십시오.

단계 **2** 전화기에 대한 단위 라이센스가 충분한지 확인합니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 라이센스 문서를 참조하십시오.

단계 **3** 장치 풀을 정의합니다. 시스템 > 장치 풀을 선택합니다.

장치 풀은 지역, 날짜/시간 그룹 및 소프트키 템플릿과 같은 장치에 대한 일반 특성을 정의합니다.

단계 **4** 일반 전화기 프로파일을 정의합니다. 장치 > 장치 설정 > 일반 전화기 프로파일을 선택합니다.

일반 전화기 프로파일은 방해 사절 및 기능 제어 옵션 같은 일반 전화기 설정은 물론 Cisco TFTP 서버에서 요구하는 데이터를 제공합니다.

단계 **5** 발신 검색 공간을 정의합니다. Cisco Unified Communications Manager Administration에서 통화 라우팅 > 제어 클래스 > 발신 검색 공간을 클릭합니다.

발신 검색 공간은 전화를 건 번호의 전송 방법을 결정하기 위해 검색하는 파티션 모음입니다. 디바이스에 대한 발신 검색 공간과 디렉터리 번호에 대한 발신 검색 공간은 함께 사용됩니다. 디렉터리 번호 CSS는 디바이스 CSS보다 우선합니다.

단계 **6** 장치 유형 및 프로토콜에 대한 보안 프로파일을 구성합니다. 시스템 > 보안 > 전화기 보안 프로파일을 선택합니다.

단계 **7** 전화기를 설정합니다. 장치 > 전화기를 선택합니다.

a) 수정하려는 전화기를 검색하거나 새 전화기를 추가합니다.
b) [전화기 구성] 창의 장치 정보 창에 있는 필수 항목을 입력해 전화기를 구성합니다.
   - MAC 주소(필수): 값은 12자의 16진수로 구성되어야 합니다.
   - 설명: 이 사용자에 관한 정보를 검색하려면 도움이 될 만한 유용한 설명을 입력하십시오.
   - 장치 풀(필수)
   - 일반 전화기 프로파일
   - 발신 검색 공간
   - 위치
   - 소유자(사용자 또는 익명) 및 사용자가 선택하는 경우 소유자 사용자 ID

기본 설정 상태의 장치가 Cisco Unified Communications Manager 데이터베이스에 추가됩니다.

[제품별 구성] 필드에 관한 정보는 전화기 구성 창의 "?" [전화기 구성] 창 및 관련된 링크의 단추 도움말.

참고 Cisco Unified Communications Manager 데이터베이스에 전화기와 사용자를 모두 동시에 추가하려면, 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

c) 이 창의 [프로토콜별 정보] 영역에서 [장치 보안 프로파일]을 선택하고 보안 모드를 설정합니다.

참고 회사의 전체적인 보안 전략에 맞는 보안 프로파일을 선택합니다. 전화기에서 보안 기능이 지원되지 않는 경우 비보안 프로파일을 선택합니다.

d) 이 전화기가 Cisco Extension Mobility를 지원한다면 [내선 정보] 영역에서 [내선 이동 활성화] 확인란을 선택합니다.

e) 저장을 클릭합니다.

단계 **8** 장치 > 장치 설정 > **SIP** 프로파일을 선택하여 SIP 매개변수를 설정합니다.

단계 **9** 장치 > 전화기를 선택하고, [디렉터리 번호 구성] 창의 필수 항목을 입력해 전화기의 디렉터리 번호(회선)를 구성합니다.

a) 전화기를 검색합니다.

b) [전화기 구성] 창에서 창의 왼쪽에 있는 [회선 1]을 클릭합니다.

전화회의 전화기의 회선이 하나 뿐입니다.

c) [디렉터리 번호] 필드에 전화를 걸 수 있는 유효한 번호를 입력합니다.

참고 이 필드에는 [최종 사용자 구성] 창의 [전화 번호] 필드에 있는 것과 같은 번호가 포함되어 있어야 합니다.

d) 경로 파티션 드롭다운 목록에서 디렉터리 번호가 속한 파티션을 선택합니다. 디렉터리 번호에 대한 액세스를 제한하지 않으려면 파티션에 대해 <None>을 선택합니다.

e) 발신 검색 공간 드롭다운 목록에서 해당 발신 검색 공간을 선택합니다. 선택한 값은 이 디렉터리 번호를 사용하고 있는 모든 장치에 적용됩니다.

f) [통화 착신 전환] 및 [통화 당겨받기 설정] 영역에서 항목(예: 착신 전환, 내부 착신 전환 중)과 통화를 전송할 해당 대상을 선택합니다.

예제**:**

통화 중 신호를 받는 내부 및 외부 착신 통화를 이 회선의 음성 메일로 착신 전환하고 싶다면, [통화 당겨받기] 및 [통화 착신 전환 설정] 영역의 왼쪽 열에 있는 [통화 중 착신 전환 내부] 및 [통화 중 착신 전환 외부] 항목 옆의 [음성메일] 확인란을 선택합니다.

g) 장치의 회선 1 창에서 다음 필드를 입력합니다.

- 표시(내부 발신자 ID 필드): 모든 내부 통화에 이름이 표시되도록 이 장치 사용자의 성명을 입력할 수 있습니다. 시스템에 내선 번호를 표시하려면 이 필드를 비워 둡니다.

- 외부 전화 번호 마스크: 이 회선에서 전화를 걸 때 발신자 ID 정보를 보내는 데 사용되는 전화 번호(또는 마스크)를 나타냅니다. 최대 24자의 숫자 및 "X" 문자를 입력할 수 있습니다. X는 디렉터리 번호를 나타내며, 패턴 끝 부분에 있어야 합니다.

예제:

마스크를 408902XXXX로 지정하면, 내선 번호 6640에서 발신하는 외부 통화에 발신자 ID 번호가 4089026640로 표시됩니다.

오른쪽의 확인란(공유 장치 설정 업데이트)을 선택하고 선택 항목 전파를 클릭한 경우가 아니라면 이 설정은 현재 장치에만 적용됩니다. 오른쪽의 확인란은 다른 장치가 이 디렉터리 번호를 공유하는 경우에만 표시됩니다.

h) 저장을 선택합니다.

디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서와 관련 링크를 참조하십시오.

단계 **10** (선택 사항) 전화기에 사용자를 연결합니다. [전화기 구성] 창 하단에 있는 최종 사용자 연결을 클릭하여, 구성 중인 회선에 사용자를 연결합니다.

a) [검색] 필드와 함께 검색을 사용하여 사용자를 찾습니다.
b) 사용자 이름 옆의 확인란을 선택하고, 선택 항목 추가를 클릭합니다.

[디렉터리 번호 구성] 창의 [회선에 연결된 사용자] 부분에 사용자 이름과 사용자 ID가 표시됩니다.

c) 저장을 선택합니다.

이제 사용자가 전화기의 회선 1에 연결되었습니다.

단계 **11** (선택 사항) 사용자와 장치 연결:

a) 사용자 관리 > 최종 사용자를 선택합니다.
b) 검색란과 검색을 사용해 추가한 사용자를 찾습니다.
c) 사용자 ID를 클릭합니다.
d) 화면의 [디렉터리 번호 연결] 영역에 있는 드롭다운 목록에서 [기본 내선 번호]를 설정합니다.
e) (선택 사항) [이동 정보] 영역에서 [이동 활성화] 확인란을 선택합니다.
f) [권한 정보] 영역에서 액세스 제어 그룹에 추가 단추를 사용해 원하는 사용자 그룹에 이 사용자를 추가합니다.

예를 들어, 사용자를 표준 CCM 최종 사용자 그룹이라고 정의된 그룹에 추가할 수 있습니다.

g) 그룹에 관한 세부 정보를 확인하려면 그룹을 선택한 다음 세부 정보 보기를 클릭합니다.
h) 사용자가 EMCC(Extension Mobility Cross Cluster) 서비스에 사용할 수 있다면 [내선 이동] 영역에서 [클러스터 간 내선 이동 활성화] 확인란을 선택합니다.
i) [장치 정보] 영역에서 장치 연결을 클릭합니다.
j) [검색] 필드와 검색을 사용해 사용자와 연결하고 싶은 장치를 찾습니다.
k) 장치를 선택하고 선택 항목/변경 사항 저장을 클릭합니다.
l) 화면의 오른쪽 상단에서 사용자에게 돌아가기 관련 링크 옆에 있는 "이동"을 클릭합니다.
m) 저장을 선택합니다.

단계 **12** 소프트키 템플릿을 사용자 정의합니다. 장치 > 장치 설정 > 소프트키 템플릿을 선택합니다.

기능 사용 요구 사항에 맞게 사용자 전화기에 표시되는 소프트키 기능의 순서를 추가, 삭제 또는 변경하려면 페이지를 사용하십시오.

전화회의 전화기에 특수 소프트키 요구 사항이 있습니다. 자세한 내용은 관련 링크를 참조하십시오.

단계 **13** Cisco IP 전화기 서비스를 구성하고 서비스를 할당합니다. 장치 > 장치 설정 > 전화 서비스를 선택합니다.

전화기에 IP 전화기 서비스를 제공합니다.

참고 Cisco Unified Communications 셀프 케어 포털을 사용해 전화기의 서비스를 추가 또는 변경할 수 있습니다.

단계 **14** (선택 사항) Cisco Unified Communications Manager용 글로벌 디렉터리에 사용자 정보를 추가합니다. 사용자 관리 > 최종 사용자를 선택하고 새로 추가를 클릭한 다음, 필수 항목을 입력합니다. 필수 항목은 별표(*)로 표시되어 있습니다.

참고 회사에서 사용자에 관한 정보를 저장하는 데 LDAP(Lightweight Directory Access Protocol) 디렉터리를 사용한다면, 기존 LDAP 디렉터리를 사용하도록 Cisco Unified Communications를 설치하고 구성할 수 있습니다. 회사 디렉터리 설정, 131 페이지를 참조하십시오. [LDAP 서버] 필드의 [동기화 활성화]가 활성화되면, Cisco Unified Communications Manager Administration에서 사용자를 추가할 수 없습니다.

a) 사용자 ID와 성 필드에 해당 내용을 입력합니다.
b) 암호를 지정합니다(셀프 케어 포털용).
c) PIN을 지정합니다(Cisco Extension Mobility 및 개인 디렉터리용).
d) 전화기에 사용자를 연결합니다.

전화기에 통화를 착신 전환하거나 단축 다이얼 번호나 서비스를 추가하는 것 같은 제어 기능을 제공합니다.

참고 회의실에 있는 것과 같은 일부 전화에는 연결된 사용자가 없습니다.

단계 **15** (선택 사항) 사용자와 사용자 그룹을 연결합니다. 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

사용자에게 사용자 그룹의 모든 사용자에게 적용되는 공통된 역할 및 권한 목록을 배포합니다. 관리자는 사용자 그룹, 역할 및 권한을 관리하여 시스템 사용자의 액세스 수준(과 보안 수준)을 제어할 수 있습니다.

최종 사용자가 Cisco Unified Communications 셀프 케어 포털에 액세스하려면, 표준 Cisco Communications Manager 최종 사용자 그룹에 사용자를 추가해야 합니다.

관련 항목

제품별 구성, 102 페이지
Cisco IP 전화회의 전화기 기능 및 설정, 97 페이지
Cisco Unified Communications Manager 설명서, 14 페이지

새 소프트키 템플릿 설정, 98 페이지

전화기 MAC 주소 결정

Cisco Unified Communications Manager에 전화기를 추가하려면, 전화기의 MAC 주소를 정해야 합니다.

프로시저

다음 작업 중 하나를 수행합니다.

- 전화기에서 설정 > 전화 정보를 선택하고 [MAC 주소] 필드를 확인합니다.
- 전화기 뒷면의 MAC 레이블을 확인합니다.
- 전화기의 웹 페이지를 표시하고, 장치 정보를 클릭합니다.

전화기 추가 방식

Cisco IP 전화기를 설치한 후에는 Cisco Unified Communications Manager 데이터베이스에 전화기를 추가하는 다음 옵션들 중 하나를 선택할 수 있습니다.

- Cisco Unified Communications Manager Administration을 사용해 전화기를 개별적으로 추가
- BAT(Bulk Administration Tool)를 사용해 여러 개의 전화기를 추가
- 자동 등록
- BAT 및 자동 등록된 전화기 지원을 위한 도구(TAPS)

개별적으로 또는 BAT를 사용하여 전화기를 추가하기 전에 전화기의 MAC 주소가 필요합니다. 자세한 내용은 전화기 MAC 주소 결정, 62 페이지의 내용을 참조하십시오.

BAT(Bulk Administration Tool)에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

전화기를 개별적으로 추가

Cisco Unified Communications Manager에 추가할 전화기의 MAC 주소 및 전화기 정보를 수집합니다.

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 전화기 유형을 선택합니다.

단계 4 다음을 선택합니다.

단계 5 MAC 주소를 비롯한 전화기 정보 수집을 완료합니다.

Cisco Unified Communications Manager에 관한 완벽한 지침과 개념 정보에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

단계 6 저장을 선택합니다.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

BAT 전화기 템플릿을 사용해 전화기 추가

Cisco Unified Communications BAT(Bulk Administration Tool)를 사용하면, 복수 전화기 등록을 포함한 배치 작업을 수행할 수 있습니다.

(TAPS와 함께 사용하지 않고) BAT만을 사용해 전화기를 추가하려면, 각 전화기에 대한 MAC 주소를 확보해야 합니다.

BAT에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 벌크 관리 > 전화기 > 전화기 템플릿을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 전화기 유형을 선택하고 다음을 클릭합니다.

단계 4 장치 풀, 전화기 버튼 템플릿, 장치 보안 프로파일 같은 전화기 관련 매개변수의 세부 정보를 입력합니다.

단계 5 저장을 클릭합니다.

단계 6 장치 > 전화기 > 새로 추가를 선택하고, BAT 전화기 템플릿을 사용해 전화기를 추가합니다.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

Cisco Unified Communications Manager에 사용자 추가

관리자는 Cisco Unified Communications Manager에 등록된 사용자에 관한 정보를 표시하고 유지할 수 있습니다. Cisco Unified Communications Manager를 사용하면 각 사용자가 다음과 같은 작업을 수행할 수 있습니다.

- Cisco IP 전화기에서 회사 디렉터리 및 기타 사용자 정의된 디렉터리에 액세스할 수 있습니다.
- 개인 디렉터리를 생성할 수 있습니다.
- 단축 다이얼과 통화 착신 전환 번호를 설정할 수 있습니다.
- Cisco IP 전화기에서 액세스할 수 있는 서비스에 등록할 수 있습니다.

프로시저

단계 **1** 사용자를 개별적으로 추가하려면 Cisco Unified Communications Manager에 직접 사용자 추가, 65 페이지를 참조하십시오.

단계 **2** 배치 방식으로 사용자를 추가하려면 BAT(Bulk Administration Tool)를 사용하십시오. 이 방식을 선택하면 모든 사용자에게 동일한 기본 암호를 설정할 수 있습니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

외부 LDAP 디렉터리에서 사용자 추가

LDAP 디렉터리(Cisco 제품이 아닌 Unified Communications Server 디렉터리)에 사용자를 추가했다면, 해당 LDAP 디렉터리를 사용자와 사용자 전화기를 추가할 Cisco Unified Communications Manager에 즉각 동기화해야 합니다.

참고 LDAP 디렉터리를 Cisco Unified Communications Manager에 즉각 동기화하지 않으면, [LDAP 디렉터리] 창의 [LDAP 디렉터리 동기화 일정]에서 다음 자동 동기화 일정을 결정합니다. 동기화는 장치에 새 사용자를 연결하기 전에 일어나야 합니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에 로그인합니다.

단계 **2** 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 3 찾기를 사용해 LDAP 디렉터리를 찾습니다.

단계 4 LDAP 디렉터리 이름을 클릭합니다.

단계 5 지금 전체 동기화 수행을 클릭합니다.

Cisco Unified Communications Manager에 직접 사용자 추가

LDAP(Lightweight Directory Access Protocol) 디렉터리를 사용하지 않는다면, 다음 단계를 수행하여 Cisco Unified Communications Manager Administration으로 직접 사용자를 추가할 수 있습니다.

참고 그러나 LDAP이 동기화되면 Cisco Unified Communications Manager Administration으로 사용자를 추가할 수 없습니다.

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 사용자 관리 > 최종 사용자를 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 [사용자 정보] 창에 다음 정보를 입력합니다.

- 사용자 ID: 최종 사용자의 ID 이름을 입력합니다. Cisco Unified Communications Manager를 만든 후에는 사용자 ID를 수정할 수 없습니다. 특수 문자 =, +, <, >, #,;, \,, “” 및 공백을 사용할 수 있습니다. 예: johndoe
- 암호 및 암호 확인: 최종 사용자 암호로 5자 이상의 영숫자 또는 특수 문자를 입력합니다. 특수 문자 =, +, <, >, #,;, \,, “” 및 공백을 사용할 수 있습니다.
- 성: 최종 사용자의 성을 입력합니다. =, +, <, >, #,;, \,, “” 및 공백 문자를 사용할 수 있습니다. 예: doe
- 전화 번호: 최종 사용자의 기본 디렉터리 번호를 입력합니다. 최종 사용자의 전화기에는 여러 회선이 있을 수 있습니다. 예: 26640(John Doe의 내부 회사 전화 번호)

단계 4 저장을 클릭합니다.

최종 사용자 그룹에 사용자 추가

Cisco Unified Communications Manager 표준 최종 사용자 그룹에 사용자를 추가하려면 다음 단계를 따르십시오.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

[사용자 찾기 및 나열] 창이 표시됩니다.

단계 **2** 적절한 검색 조건을 입력하고 찾기를 클릭합니다.

단계 **3** 표준 **CCM** 최종 사용자 링크를 선택합니다. 표준 CCM 최종 사용자를 위한 [사용자 그룹 구성] 창이 나타납니다.

단계 **4** 그룹에 최종 사용자 추가를 선택합니다. [사용자 찾기 및 나열] 창이 표시됩니다.

단계 **5** [사용자 찾기] 드롭다운 목록 상자를 사용하여 추가할 최종 사용자를 찾고, 찾기를 클릭합니다.

검색 조건과 일치하는 사용자 목록이 나타납니다.

단계 **6** 표시된 목록에서 이 사용자 그룹에 추가할 사용자 옆에 있는 확인란을 선택합니다. 목록이 긴 경우, 아래쪽의 링크를 사용하여 더 많은 결과를 볼 수 있습니다.

참고 검색 결과 목록에서 사용자 그룹에 이미 속해 있는 사용자는 표시되지 않습니다.

단계 **7** 선택한 항목 추가를 선택합니다.

전화기와 사용자 연결

[Cisco Unified Communications Manager 최종 사용자] 창에서 전화기와 사용자를 연결합니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 사용자 관리 > 최종 사용자를 선택합니다.

[사용자 찾기 및 나열] 창이 표시됩니다.

단계 **2** 적절한 검색 조건을 입력하고 찾기를 클릭합니다.

단계 **3** 표시되는 레코드 목록에서 사용자 링크를 선택합니다.

단계 **4** 장치 연결을 선택합니다.

[사용자 디바이스 연결] 창이 나타납니다.

단계 **5** 적절한 검색 조건을 입력하고 찾기를 클릭합니다.

단계 **6** 장치 왼쪽의 확인란을 선택하여 사용자와 연결할 장치를 선택합니다.

단계 **7** 선택 항목/변경 사항 저장을 선택하여 장치와 사용자를 연결합니다.

단계 **8** 창의 오른쪽 상단에 있는 [관련 링크] 드롭다운 목록에서 사용자에게 돌아가기를 선택하고 이동을 클릭합니다.

[최종 사용자 구성] 창이 나타나고 [제어된 장치] 창에 선택한 연결 장치가 표시됩니다.

단계 **9** 선택 항목/변경 사항 저장을 선택합니다.

SRST(Survivable Remote Site Telephony)

SRST(Survivable Remote Site Telephony)는 Cisco Unified Communications Manager를 통한 통신에 문제가 생겼을 때 기본 전화기 기능에 액세스할 수 있게 해줍니다. 이런 시나리오에서 전화기는 진행 중인 통화의 활성 상태를 유지하고, 사용자도 기능 하위 집합에 액세스할 수 있습니다. 페일오버가 발생하면 사용자는 전화기를 통해 경고 메시지를 수신합니다.

SRST에 대한 자세한 내용은 다음을 참조하십시오. https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html

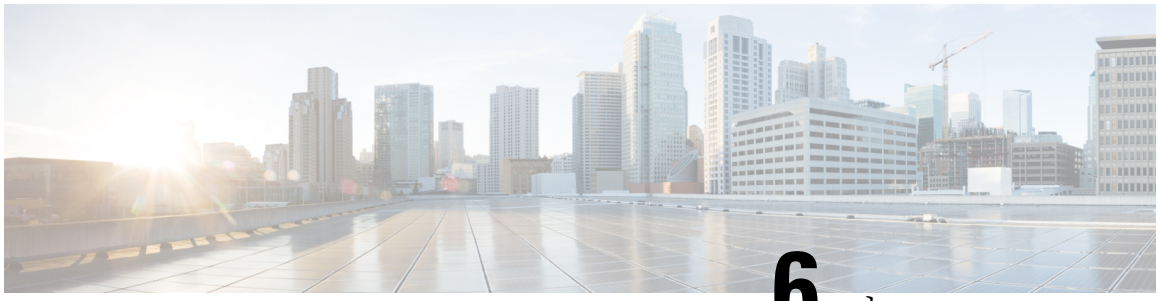
다음 표에서는 페일오버 상태에서도 사용 가능한 기능에 관해 설명합니다.

표 ***14: SRST*** 기능 지원

기능	지원됨	참고
전화걸기	예	
통화종료	예	
재다이얼	예	
전화받기	예	
보류	예	
보류해제	예	
전화회의	예	3방향 전용 및 로컬 혼합 전용
전화회의 목록	아니요	
호전환	예	상담만 가능
활성 통화로 호전환(호연결)	아니요	
자동 응답	예	
통화 대기 중	예	
발신자 ID	예	
통합 세션 프레젠테이션	예	전화회의는 다른 기능 제한으로 인해 지원되는 유일한 기능입니다.

기능	지원됨	참고
음성메일	예	음성 메일이 Cisco Unified Communications Manager 클러스터의 다른 사용자와 동기화되지 않습니다.
모든 통화 착신 전환	예	착신 전환 상태는 SRST 모드로 공유되는 회선 표시가 없기 때문에 착신 전환을 설정한 전화기에서만 제공됩니다. 모든 통화 착신 전환 설정은 페일오버 시 SRST에서 Cisco Unified Communications Manager로 또는 SRST 페일백에서 Communications Manager로 보존되지 않습니다. 그러나 Communications Manager에서 여전히 활성 상태를 유지하는 원래의 모든 통화 착신 전환은 페일오버 후에 장치가 Communications Manager에 다시 연결되면 표시되어야 합니다.
바로 호출	예	
음성메일로 전환(전환)	아니요	[전환] 소프트키가 표시되지 않습니다.
회선 필터	일부 지원	회선이 지원되지만 공유할 수 없습니다.
지정보류 모니터링	아니요	[지정보류] 소프트키가 표시되지 않습니다.
향상된 메시지 대기 중 표시	예	메시지 수 배지가 전화기 화면에 나타납니다.
직접 통화 지정보류	아니요	소프트키가 표시되지 않습니다.
보류 복귀	예	
원격 보류	아니요	통화가 로컬 보류 통화로 나타납니다.
회의개설	아니요	[회의개설] 소프트키가 표시되지 않습니다.
당겨받기	예	
그룹 당겨받기	아니요	소프트키가 표시되지 않습니다.
기타 당겨받기	아니요	소프트키가 표시되지 않습니다.
장난 전화 ID	예	
QRT	예	

기능	지원됨	참고
헌트 그룹	아니요	소프트키가 표시되지 않습니다.
이동성	아니요	소프트키가 표시되지 않습니다.
프라이버시	아니요	소프트키가 표시되지 않습니다.
콜백	아니요	[콜백] 소프트키가 표시되지 않습니다.
서비스 URL	예	서비스 URL이 할당된 프로그램 가능 회선 키가 표시되지 않습니다.



6 장

셀프 케어 포털 관리

셀프 서비스 포털 개요

Cisco Unified Communications 셀프 서비스 포털에서 사용자는 전화기 기능 및 설정을 사용자 정의하고 제어할 수 있습니다.

관리자는 셀프 서비스 포털에 대한 액세스를 제어할 수 있습니다. 또한 사용자가 셀프 서비스 포털에 액세스할 수 있도록 사용자에게 정보를 제공해야 합니다.

사용자가 Cisco 통합 커뮤니케이션 자가 관리 포털에 액세스하려면 먼저 Cisco Unified Communications Manager 관리를 사용하여 표준 Cisco Unified Communications Manager 최종 사용자 그룹에 사용자를 추가해야 합니다.

최종 사용자에게는 셀프 서비스 포털에 대한 다음과 같은 정보를 제공해야 합니다.

- 애플리케이션에 액세스할 수 있는 URL. 이 URL은 다음과 같습니다.

  https://<server_name:portnumber>/ucmuser/. 여기서 server_name은 웹 서버가 설치된 호스트이며, portnumber는 해당 호스트상의 포트 번호입니다.

- 애플리케이션에 액세스할 수 있는 사용자 ID 및 기본 암호
- 사용자가 포털에서 수행할 수 있는 작업에 대한 개요

이러한 설정은 Cisco Unified Communications Manager에 사용자를 추가할 때 입력했던 값과 같습니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

셀프 서비스 포털에 사용자 액세스 설정

사용자가 셀프 서비스 포털에 액세스하기 전에 먼저 관리자가 해당 액세스 권한을 부여해야 합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 사용자 관리 > 최종 사용자를 선택합니다.
단계 **2** 사용자를 검색합니다.
단계 **3** 사용자 ID 링크를 클릭합니다.
단계 **4** 사용자가 암호와 PIN을 구성했는지 확인합니다.
단계 **5** 권한 정보 섹션에서 그룹 목록이 표준 **CCM** 최종 사용자가 포함되어 있는지 확인합니다.
단계 **6** 저장을 선택합니다.

셀프 서비스 포털 디스플레이 사용자 정의

대부분의 옵션은 셀프 서비스 포털에 표시됩니다. 그러나 다음 옵션은 Cisco 통합 커뮤니케이션 매니저 관리에서 [엔터프라이즈 매개변수 구성] 설정을 사용해 설정해야 합니다.

- 벨소리 표시 설정
- 회선 레이블 표시 설정

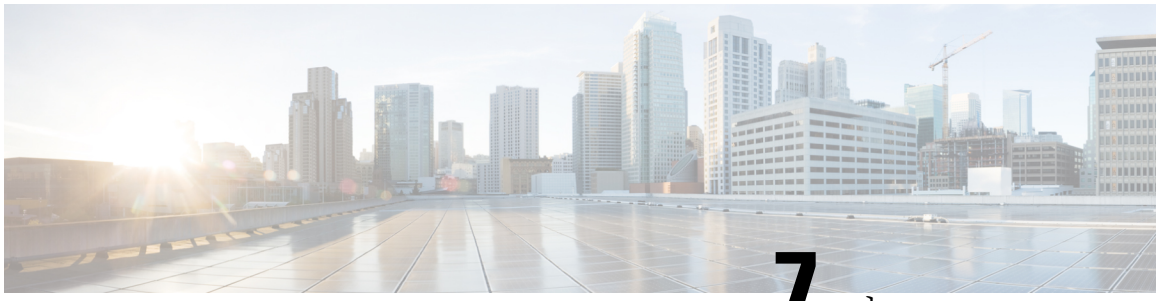
참고 설정은 사이트의 모든 셀프 서비스 포털 페이지에 적용됩니다.

프로시저

단계 **1** Cisco 통합 커뮤니케이션 매니저 관리에서 시스템 > 엔터프라이즈 매개변수를 선택합니다.
단계 **2** [셀프 서비스 포털] 영역에서 셀프 서비스 포털 기본 서버 필드를 설정합니다.
단계 **3** 사용자가 포털에서 액세스할 수 있는 매개변수를 활성화 또는 비활성화합니다.
단계 **4** 저장을 선택합니다.

III 부

Cisco IP 전화회의 전화기 관리



7 장

Cisco IP 전화회의 전화기 보안

Cisco IP 전화기 보안 개요

보안 기능은 전화기의 ID나 데이터에 대한 위협을 비롯한 몇몇 위협으로부터 전화기를 보호합니다. 이 기능은 전화기와 Cisco Unified Communications Manager 서버 사이에서 인증된 통신 스트림을 설정하고 유지하여, 전화기가 디지털 서명된 파일만 사용하게 합니다.

Cisco Unified Communications Manager 릴리스 8.5(1) 이상에는 기본값 보안이 포함되는데, 이는 CTL 클라이언트를 실행하지 않고도 Cisco IP 전화기에 다음과 같은 보안 기능을 제공합니다.

- 전화기 구성 파일 서명
- 전화기 구성 파일 암호화
- Tomcat 및 기타 웹 서비스를 사용하는 HTTPS

참고 보안 시그널링 및 미디어 기능은 여전히 CTL 클라이언트 실행 및 하드웨어 eTokens 사용을 요구합니다.

보안 기능에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

LSC(Locally Significant Certificate)는 CAPF(Certificate Authority Proxy Function)와 관련된 필수 작업을 수행한 후 전화기에 설치됩니다. LSC는 Cisco Unified Communications Manager Administration을 사용해 구성할 수 있습니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

LSC는 WLAN 인증을 사용하는 EAP-TLS의 사용자 인증서로 사용할 수 없습니다.

또는 전화기의 [보안 설정] 메뉴에서 LSC 설치를 시작할 수도 있습니다. 이 메뉴에서는 LSC를 업데이트하거나 삭제할 수도 있습니다.

Cisco IP 전화회의 전화기 8832는 FIPS(Federal Information Processing Standard)를 준수합니다. 올바르게 작동하려면 FIPS 모드는 2048비트 이상의 RSA 키 크기가 필요합니다. RSA 서버 인증서가 2048비트 이상이 아닌 경우 전화기가 Cisco Unified Communications Manager에 등록되지 않고 전화기 등록에 실패합니다. 인증서의 키 크기가 FIPS와 호환되지 않습니다. 가 전화기의 상태 메시지에 표시됩니다.

FIPS 모드에서는 개인 키(LSC 또는 MIC)를 사용할 수 없습니다.

전화기에 2048비트 보다 작은 기존 LSC가 있는 경우 FIPS를 활성화하기 전에 LSC 키 크기를 2048비트 이상으로 업데이트해야 합니다.

관련 항목

LSC(Locally Significant Certificate) 설정, 80 페이지
Cisco Unified Communications Manager 설명서, 14 페이지

전화기 네트워크의 보안 강화

Cisco Unified Communications Manager 11.5(1) 및 12.0(1)을 활성화하고 나중에 강화된 보안 환경에서 작동할 수 있습니다. 이러한 개선 기능을 이용하여 전화기 네트워크는 일련의 엄격한 보안 및 위험 관리 제어를 통해 여러분과 사용자를 보호합니다.

Cisco Unified Communications Manager 12.5(1)는 향상된 보안 환경을 지원하지 않습니다. Cisco Unified Communications Manager 12.5(1)로 업그레이드하기 전에 FIPS를 비활성화하십시오. 그렇지 않으면 TFTP 및 기타 서비스가 제대로 작동하지 않습니다.

향상된 보안 환경에는 다음과 같은 기능이 포함됩니다.

- 연락처 검색 인증.
- 원격 감사 로깅을 위한 기본 프로토콜로서의 TCP입니다.
- FIPS 모드.
- 향상된 자격 증명 정책입니다.
- 디지털 서명을 위한 해시의 SHA-2 제품군을 지원합니다.
- 512 및 4096비트의 RSA 키 크기를 지원합니다.

Cisco Unified Communications Manager 릴리스 14.0 및 Cisco IP 전화기 펌웨어 릴리스 14.0 이상에서는 전화기가 SIP OAuth 인증을 지원합니다.

OAuth는 Cisco Unified Communications Manager릴리스 14.0(1)SU 1 이상 및 Cisco IP 전화기 펌웨어 릴리스 14.1(1)이 있는 TFTP(Proxy Trivial File Transfer Protocol)에 대해 지원됩니다. MRA(Mobile Remote Access)에서는 프록시 TFTP 및 프록시 TFTP용 OAuth가 지원되지 않습니다.

보안에 대한 자세한 내용은 다음 내용을 참조하십시오.

- *Cisco Unified Communications Manager*용 시스템 구성 설명서, 릴리스 14.0(1) 이상 (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).
- *Cisco Unified Communications Manager* 보안 설명서(https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)
- SIP OAuth: *Cisco Unified Communications Manager* 기능 구성 설명서(https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)

참고 Cisco IP 전화기는 제한된 수의 신뢰 목록(ITL) 파일만 저장할 수 있습니다. ITL 파일은 전화상으로 64K 제한을 초과할 수 없으므로 Cisco Unified Communications Manager가 전화기로 전송하는 파일 수를 제한하십시오.

지원 보안 기능

보안 기능은 전화기의 ID나 데이터에 대한 위협을 비롯한 몇몇 위협으로부터 전화기를 보호합니다. 이 기능은 전화기와 Cisco Unified Communications Manager 서버 사이에서 인증된 통신 스트림을 설정하고 유지하여, 전화기가 디지털 서명된 파일만 사용하게 합니다.

Cisco Unified Communications Manager 릴리스 8.5(1) 이상에는 기본값 보안이 포함되는데, 이는 CTL 클라이언트를 실행하지 않고도 Cisco IP 전화기에 다음과 같은 보안 기능을 제공합니다.

- 전화기 구성 파일 서명
- 전화기 구성 파일 암호화
- Tomcat 및 기타 웹 서비스를 사용하는 HTTPS

참고 보안 시그널링 및 미디어 기능은 여전히 CTL 클라이언트 실행 및 하드웨어 eTokens 사용을 요구합니다.

Cisco Unified Communications Manager 시스템에 보안을 구현하면 전화기 및 Cisco Unified Communications Manager 서버의 ID 도난을 방지하고, 데이터 변조를 방지하고, 통화 시그널링 및 미디어 스트림 변조를 방지합니다.

이러한 위협을 완화하기 위해 Cisco IP 텔레포니 네트워크는 전화기와 서버 간에 보안(암호화된) 통신 스트림을 설정하고 유지 보수하고, 파일이 전화기로 전송되기 전에 파일에 디지털로 서명하고, Cisco IP 전화기 간에 미디어 스트림 및 통화 시그널링을 암호화합니다.

LSC(Locally Significant Certificate)는 CAPF(Certificate Authority Proxy Function)와 관련된 필수 작업을 수행한 후 전화기에 설치됩니다. Cisco Unified Communications Manager Administration을 사용하여

Cisco Unified Communications Manager 보안 설명서에 설명된 대로, LSC를 구성할 수 있습니다. 또는 전화기의 [보안 설정] 메뉴에서 LSC 설치를 시작할 수도 있습니다. 이 메뉴에서는 LSC를 업데이트하거나 삭제할 수도 있습니다.

LSC는 WLAN 인증을 사용하는 EAP-TLS의 사용자 인증서로 사용할 수 없습니다.

전화기는 장치가 비보안인지 보안인지를 정의하는 전화기 보안 프로파일을 사용합니다. 전화기에 보안 프로파일을 적용하는 작업에 관한 자세한 내용은 특정 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

Cisco Unified Communications Manager Administration에서 보안 관련 설정을 구성할 경우 전화기 구성 파일은 중요한 정보를 포함합니다. 구성 파일의 프라이버시를 보장하려면 암호화에 대한 설정을 구성해야 합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

Cisco Unified Communications Manager 시스템에 보안을 구현하면 전화기 및 Cisco Unified Communications Manager 서버의 ID 도난을 방지하고, 데이터 변조를 방지하고, 통화 시그널링 및 미디어 스트림 변조를 방지합니다.

다음 표에는 Cisco IP 전화회의 전화기 8832에서 지원하는 보안 기능에 대한 개요가 나와 있습니다. Cisco Unified Communications Manager 및 Cisco IP 전화기 보안에 대한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

표 ***15:*** 보안 기능 개요

기능	설명
이미지 인증	서명된 이진 파일(확장자 .sbn)이 펌웨어 이미지를 전화기에 인증 프로세스에 실패하여 새 이미지를 거부합니다.
고객측 인증서 설치	각 전화기에는 장치 인증을 위한 고유 인증서가 필요합니다(만, 추가 보안을 위해 Cisco Unified Communications Manage 증서를 설치한다고 명시할 수 있습니다. 또는 전화기의 보니다.
장치 인증	각 개체가 다른 개체의 인증서를 수락할 때는 Cisco Unified와 Cisco Unified Communications Manager 간에 보안 연결을 간에 안전한 시그널링 경로를 구축합니다. Cisco Unified C 증할 수 없는 경우만 아니라면 전화기를 등록하지 않을 것
파일 인증	전화기에서 다운로드한 디지털 서명 파일을 확인합니다. 을 확인하기 위해 서명을 확인합니다. 인증에 실패한 파일의 경우 추가 처리 없이 거부합니다.
신호 처리 인증	TLS 프로토콜을 사용해 전송되는 동안 시그널링 패킷에
MIC(Manufacturing Installed Certificate)	각 전화기에는 장치 인증에 사용할 고유한 MIC(Manufactu명하는 고유한 영구 증명서로, Cisco Unified Communicatio

기능	설명
안전한 SRST 참조	보안을 위해 SRST 참조를 구성하고 Cisco Unified Com 서버에서 전화기의 cnf.xml 파일에 SRST 인증서를 추가 SRST 활성화 라우터와 상호 작용하는 데 TLS 연결을 사
미디어 암호화	SRTP를 사용하면 지원 장치들 간의 미디어 스트림이 안 수 있습니다. 여기에는 장치를 위해 미디어 기본 키 한 안전하게 보호하는 일도 포함됩니다.
CAPF(Certificate Authority Proxy Function)	지나치게 프로세싱 집약적인 인증서 생성 절차의 일부를 는 전화기를 대신해 고객이 지정한 인증 기관에 인증서 도 있습니다.
보안 프로파일	전화기의 비보안, 인증, 암호화 여부를 정의합니다.
암호화된 구성 파일	전화기 구성 파일의 프라이버시를 보장할 수 있습니다
전화기용 웹 서버 기능의 선택적 비활성화	전화기에 관한 다양한 사용 통계를 보여주는 전화기 웹
전화기 강화	Cisco Unified Communications Manager Administration에 • 전화기 웹 페이지 액세스 비활성화 참고 전화기 구성 메뉴를 보면 GARP 활성화 및
802.1X 인증	전화기는 네트워크에 액세스 권한을 요청하고 확보하
AES 256 암호화	Cisco Unified Communications Manager 릴리스 10.5(2) 및 TLS 및 SIP를 위한 AES 256 암호화 지원을 지원합니다 FIPS(Federal Information Processing Standards)를 준수하 다. 다음은 새 암호입니다. • TLS 연결용: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH • sRTP용: • AEAD_AES_256_GCM • AEAD_AES_128_GCM 자세한 내용은 Cisco Unified Communications Manager 릴
ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서	Cisco Unified Communications Manager는 CC(공통 평가 Unified Communications Manager 11.5 이상 버전의 모든

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

LSC(Locally Significant Certificate) 설정

이 작업은 인증 문자열 방법으로 LSC를 설정하는 작업에 적용됩니다.

시작하기 전에

해당 Cisco Unified Communications Manager와 CAPF(Certificate Authority Proxy Function) 보안 구성이 완벽한지 확인합니다.

- CTL이나 ITL 파일에는 CAPF 인증서가 있습니다.
- Cisco Unified Communications 운영 체제 관리에서 CAPF 인증서 설치를 확인합니다.
- CAPF가 실행 중이며 구성되어 있습니다.

이러한 설정에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

프로시저

단계 **1** CAPF가 구성될 때 설정된 CAPF 인증 코드를 확보합니다.

단계 **2** 전화기에서 설정을 선택합니다.

단계 **3** 관리자 설정 > 보안 설정을 선택합니다.

참고 Cisco Unified Communications Manager Administration [전화기 구성] 창의 [설정 액세스] 필드를 통해 [설정] 메뉴에 대한 액세스를 제어할 수 있습니다.

단계 **4** **LSC**를 선택하고 선택 또는 업데이트를 누릅니다.

전화기에 인증 문자열이 표시됩니다.

단계 **5** 인증 코드를 입력하고 제출을 누릅니다.

CAPF 구성에 따라 전화기가 LSC를 설치, 업데이트 또는 삭제하기 시작합니다. 과정을 수행하는 동안 [보안 구성] 메뉴의 [LSC 옵션] 필드에 일련의 메시지가 표시되는데, 이를 통해 진행 상황을 모니터링할 수 있습니다. 과정이 완료되면 전화기에 [설치됨] 또는 [설치되지 않음]이 표시됩니다.

LSC 설치, 업데이트 또는 삭제 프로세스는 시간이 많이 걸릴 수 있습니다.

전화기 설치 과정이 성공적으로 완료되면 설치됨 메시지가 표시됩니다. 전화기에 설치되지 않음이라고 표시되면, 인증 문자열이 잘못되었거나 전화기를 업그레이드할 수 없는 상황일 수 있습니다. CAPF가 작동해 LSC를 삭제하면 전화기에 설치되지 않음이라고 표시되어 작업이 완료되었음을 알려줍니다. CAPF 서버는 오류 메시지를 기록합니다. 로그를 검색하고 오류 메시지의 의미를 확인하려면 CAPF 서버 문서를 참조하십시오.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

FIPS 모드 활성화

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택하고 전화기를 찾습니다.

단계 2 [제품별 구성] 영역으로 이동합니다.

단계 3 **FIPS** 모드 필드를 [활성화]로 설정합니다.

단계 4 구성 적용을 선택합니다.

단계 5 저장을 선택합니다.

단계 6 전화기를 다시 시작합니다.

전화기 통화 보안

전화기에 보안이 실행되면, 전화기 화면의 아이콘을 통해 보안 전화를 식별할 수 있습니다. 통화를 시작할 때 보안 신호음이 재생되면 연결된 전화기가 안전하고 보호되고 있는지 여부를 판단할 수 있습니다.

보안 통화에서는 모든 통화 신호 처리와 미디어 스트림이 암호화됩니다. 보안 통화는 높은 수준의 보안을 제공하여, 통화에 무결성과 프라이버시를 제공합니다. 진행 중인 통화가 암호화되면, 전화기 화면의 통화 시간 타이머 오른쪽에 있는 통화 진행 아이콘이  으로 변경됩니다.

참고 통화가 비 IP 통화 레그(예: PSTN)를 통해 라우팅되면, IP 네트워크 내에서 암호화되고 이와 연결된 잠금 아이콘이 있더라도 통화의 보안이 이루어지지 않을 수 있습니다.

보안 통화에서는 연결된 다른 전화 역시 보안된 오디오를 송수신한다는 사실을 알리기 위해 통화를 시작할 때 보안 신호음이 재생됩니다. 보안이 이루어지지 않는 전화기에 통화가 연결되면 보안 신호음이 울리지 않습니다.

참고 보안 통화는 두 전화기 사이에서 지원됩니다. 보안 전화회의, Cisco Extension Mobility 및 공유 회선은 보안 컨퍼런스 브리지를 통해 구성할 수 있습니다.

Cisco Unified Communications Manager에서 전화기를 보안(암호화되고 신뢰됨)으로 구성하면, "보호됨" 상태를 지정할 수 있습니다. 그런 다음, 원하는 경우 통화 시작 시 표시음을 재생하도록 보호된 전화기를 구성할 수 있습니다.

- 보호되는 장치: 보안 전화기의 상태를 보호됨으로 변경하려면, Cisco Unified Communications Manager Administration의 전화기 구성 창에서 보호되는 장치 확인란을 선택합니다(장치 > 전화기).
- 보안 표시음 재생: 보호되는 전화에서 보안 또는 비보안 표시음을 재생하도록 하려면, [보안 표시음 재생] 설정을 [예]로 설정합니다. 기본적으로 [보안 표시음 재생]은 [아니요]로 설정됩니다. 이 옵션은 Cisco Unified Communications Manager Administration에서 설정합니다(시스템 > 서비스 매개변수). 서버를 선택하고, Unified Communications Manager 서비스를 선택합니다. [서비스 매개변수 구성] 창에서 [기능 - 보안 신호음] 영역을 선택합니다. 기본값은 [아니요]입니다.

보안 컨퍼런스 식별

보안 전화회의를 시작하여 참가자의 보안 수준을 모니터링할 수 있습니다. 보안 전화회의는 다음과 같은 프로세스를 사용해 이루어집니다.

1. 사용자가 보안이 이루어진 전화기에서 전화회의를 시작합니다.
2. Cisco Unified Communications Manager가 통화에 보안 컨퍼런스 브리지를 할당합니다.
3. 참가자가 추가되면, Cisco Unified Communications Manager는 각 전화기의 보안 모드를 확인하고 전화회의를 위한 보안 수준을 유지합니다.
4. 전화기에 전화회의의 보안 수준이 표시됩니다. 보안 전화회의는 전화기 화면의 전화회의 오른쪽에 보안 아이콘, 을 표시합니다.

참고 보안 통화는 두 전화기 사이에서 지원됩니다. 보호되는 전화기에서는 보안 통화가 구성될 경우 전화회의 통화, 공유 회선 및 내선 이동 같은 일부 기능을 사용할 수 없습니다.

다음 표에는 개시자 전화기 보안 수준, 참가자 보안 수준, 보안 컨퍼런스 브리지 사용 가능성에 따라 바뀌는 전화회의 보안 수준에 관한 정보가 나와 있습니다.

표 ***16:*** 전화회의를 통한 보안 제한

개시자 전화기 보안 수준	사용되는 기능	참가자 보안 수준	동작 결과
비보안	전화회의	보안	비보안 컨퍼런스 브리지 비보안 전화회의
보안	전화회의	최소 1명의 구성원이 비보안 상태입니다.	보안 컨퍼런스 브리지 비보안 전화회의
보안	전화회의	보안	보안 컨퍼런스 브리지 보안 암호화 수준 전화회의

개시자 전화기 보안 수준	사용되는기능	참가자 보안 수준	동작 결과
비보안	회의개설	최소 보안 수준이 암호화되어 있습니다.	개시자는 보안 수준을 충족하지 않아 부되었습니다라는 메시지를 받습니다.
보안	회의개설	최소 보안 수준이 비보안 상태입니다.	보안 컨퍼런스 브리지 전화회의에서 모든 통화를 수용합니다.

보안 전화기 통화 식별

전화기와 상대편 전화기가 보안 통화로 구성되어 있으면 보안 통화가 이루어집니다. 상대 전화기는 같은 Cisco IP 네트워크에 속해 있을 수도 있고, IP 네트워크 밖의 네트워크에 속해 있을 수도 있습니다. 보안 통화는 두 전화기 사이에서만 이루어집니다. 보안 컨퍼런스 브리지가 설정되면 전화회의 통화는 보안 통화를 지원해야 합니다.

보안 통화는 다음과 같은 프로세스를 사용해 이루어집니다.

1. 사용자가 보안이 이루어진 전화기(보안 모드)에서 전화를 겁니다.
2. 전화기가 전화기 화면에 보안 아이콘, 을 표시합니다. 이 아이콘은 전화기가 보안 통화로 구성되어 있음을 보여줍니다. 그러나 연결된 다른 전화기도 보안된다는 뜻은 아닙니다.
3. 보안이 이루어진 다른 전화기에 통화가 연결되면 보안 신호음이 들립니다. 이는 대화의 양측이 모두 암호화되어 있고, 보안이 이루어진다는 뜻입니다. 보안이 이루어지지 않는 전화기에 통화가 연결되면, 보안 신호음이 울리지 않습니다.

참고 보안 통화는 두 전화기 사이에서 지원됩니다. 보호되는 전화기에서는 보안 통화가 구성될 경우 전화회의 통화, 공유 회선 및 내선 이동 같은 일부 기능을 사용할 수 없습니다.

오직 보호된 전화기에서만 보안 또는 비보안 표시음이 재생됩니다. 보호되지 않는 전화기에서는 신호음이 울리지 않습니다. 통화 중에 전체 통화 상태가 변경되면, 표시음이 변경되고 보호된 전화기에서 해당 표시음을 재생합니다.

보호된 전화기는 다음 상황에서 표시음을 재생하거나 재생하지 않습니다.

- [보안 표시음 재생] 옵션이 활성화된 경우:
  - 엔드 투 엔드 보안 미디어가 설정되어 있고 통화 상태가 안전하면 전화기가 보안 신호음을 재생합니다(길게 경고음 3번, 중간에 일시 중지).
  - 엔드 투 엔드 비보안 미디어가 설정되고 통화 상태가 비보안일 때 전화기는 비보안 표시음을 재생합니다(짧게 경고음 여섯 번, 중간에 짧게 일시 중지).

[보안 표시음 재생] 옵션이 비활성화되면 표시음이 재생되지 않습니다.

참여를 위한 암호화 제공

Cisco Unified Communications Manager는 전화회의가 설정되면 전화기 보안 상태를 확인하고 전화회의에 대한 보안 표시를 변경하거나 통화 완료를 차단하여 시스템의 무결성 및 보안을 유지합니다.

참여에 사용되는 전화기가 암호화에 대해 구성되지 않은 경우, 사용자는 암호화된 통화에 참여할 수 없습니다. 이 경우 참여가 실패하면 사용자가 참여를 개시한 전화기에서 다시 걸기(빠른 통화 중) 신호음이 재생됩니다.

개시자 전화기가 암호화에 대해 구성된 경우, 참여 개시자는 암호화된 전화기에서 발신된 비보안 통화에 참여할 수 있습니다. 참여가 발생하면 Cisco Unified Communications Manager는 통화를 비보안으로 분류합니다.

개시자 전화기가 암호화에 대해 구성된 경우, 참여 개시자는 암호화된 통화에 참여할 수 있으며 전화기에 통화가 암호화되었음이 표시됩니다.

WLAN 보안

범위 내에 있는 모든 WLAN 장치는 기타 모든 WLAN 트래픽을 수신할 수 있으므로, 음성 통신 보안이 WLAN에서 중요합니다. 침입자가 음성 트래픽을 조작하거나 가로채지 않도록 하기 위해 Cisco SAFE 보안 아키텍처는 Cisco IP 전화기 및 Cisco Aironet AP를 지원합니다. 네트워크의 보안에 대한 자세한 내용은 http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html을 참조하십시오.

Cisco Wireless IP 텔레포니 솔루션은 무선 Cisco IP 전화기가 지원하는 다음 인증 방법을 사용하여 인증되지 않은 로그인 및 통신 저하를 방지하는 무선 네트워크 보안을 제공합니다.

- 개방형 인증: 무선 장치가 개방형 시스템에서 인증을 요청할 수 있습니다. 요청을 수신하는 AP는 요청자에게 또는 사용자 목록에 있는 요청자에게만 인증을 허가할 수 있습니다. 무선 장치와 AP 간 통신은 암호화되지 않을 수 있거나 장치가 WEP(Wired Equivalent Privacy) 키를 사용하여 보안을 제공할 수 있습니다. WEP를 사용하는 장치만 WEP를 사용 중인 AP로 인증을 시도합니다.
- EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) 인증: 이 클라이언트 서버 보안 아키텍처는 AP와 Cisco ACS(Access Control Server)와 같은 RADIUS 서버 간 TLS(Transport Level Security) 터널 내에서 EAP 트랜잭션을 암호화합니다.

  TLS 터널은 클라이언트(전화기)와 RADIUS 서버 간 인증을 위해 PAC(Protected Access Credential)를 사용합니다. 서버가 AID(Authority ID)를 클라이언트(전화기)로 보내면, 거기서 해당 PAC를 선택합니다. 클라이언트(전화기)는 PAC-Opaque를 RADIUS 서버로 반환합니다. 서버는 기본 키로 PAC를 해독합니다. 이제 두 엔드포인트에는 PAC 키가 있고 TLS 터널이 생성됩니다. EAP-FAST는 자동 PAC 구축을 지원하지만, RADIUS 서버에서 이것을 활성화해야 합니다.

참고 Cisco ACS에서는 기본적으로 PAC가 1주일 후 만료됩니다. 전화기에 만료된 PAC가 있는 경우, 전화기가 새 PAC를 가져오는 동안 RADIUS 서버에서 인증 시간이 더 오래 걸립니다. PAC 구축 지연을 피하기 위해 PAC 만료 기간을 ACS 또는 RADIUS 서버에서 90일 이상으로 설정하십시오.

- 확장 가능 인증 프로토콜 - 전송 계층 보안 EAP-TLS) 인증: EAP-TLS에는 인증 및 네트워크 액세스를 위한 클라이언트 인증서가 필요합니다. 유선 EAP-TLS의 경우, 클라이언트 인증서는 전화기의 MIC 또는 LSC 중 하나가 될 수 있습니다. LSC는 유선 EAP-TLS에 권장되는 클라이언트 인증 인증서입니다.
- PEAP(Protected Extensible Authentication Protocol): 클라이언트(전화기)와 RADIUS 간 Cisco의 독점적 암호 기반 상호 인증 체계입니다. Cisco IP 전화기는 무선 네트워크에서 인증을 위해 PEAP를 사용할 수 있습니다. PEAP-MSCHAPV2만 지원됩니다. PEAP-GTC는 지원되지 않습니다.

다음 인증 체계는 RADIUS 서버를 사용하여 인증 키를 관리합니다.

- WPA/WPA2: RADIUS 서버 정보를 사용하여 인증을 위한 고유 키를 생성합니다. 이러한 키는 중앙 집중식 RADIUS 서버에서 생성되므로, WPA/WPA2는 AP 및 전화기에 저장된 WAP 사전 공유 키보다 더 강화된 보안을 제공합니다.
- 고속 보안 로밍: RADIUS 서버와 무선 도메인 서버(WDS) 정보를 사용하여 키를 관리하고 인증합니다. WDS는 빠르고 안전한 재인증을 위해 CCKM 사용 가능 클라이언트 장치에 대한 보안 자격 증명 캐시를 만듭니다. Cisco IP 전화기 8800 시리즈는 802.11r(FT)을 지원합니다. 11r(FT)와 CCKM 모두 고속 보안 로밍이 가능하도록 지원됩니다. 그러나 Cisco는 802.11r (FT) over air 방식을 활용할 것을 적극 권장합니다.

WPA/WPA2 및 CCKM을 사용할 때, 암호화 키는 전화기에 입력되지 않지만 AP와 전화기 간에 자동으로 파생됩니다. 그러나 인증을 위해 사용되는 EAP 사용자 이름과 암호는 각 전화기에 입력해야 합니다.

음성 트래픽이 보안되도록 하기 위해 Cisco IP 전화기는 암호화를 위해 WEP, TKIP 및 AES(Advanced Encryption Standards)를 지원합니다. 암호화를 위해 이러한 메커니즘이 사용될 때 시그널링 SIP 패킷과 음성 RTP(Real-Time Transport Protocol) 패킷은 모두 AP와 Cisco IP 전화기 사이에서 암호화됩니다.

WEP

WEP가 무선 네트워크에서 사용될 때, 인증은 개방형 또는 공유 키 인증을 사용하여 AP에서 수행됩니다. 전화기에 설정된 WEP 키는 성공적인 연결을 위해 AP에서 구성된 WEP 키와 일치해야 합니다. Cisco IP 전화기는 40비트 암호화 또는 128비트 암호화를 사용하고 전화기와 AP에서 정적 상태로 있는 WEP 키를 지원합니다.

EAP 및 CCKM 인증은 암호화를 위해 WEP 키를 사용할 수 있습니다. RADIUS 서버는 WEP 키를 관리하고 모든 음성 패킷을 암호화하기 위해 인증 후 AP로 고유 키를 전달합니다. 따라서 이러한 WEP 키는 각 인증과 함께 변경될 수 있습니다.

TKIP

WPA 및 CCKM은 WEP 상에서 여러 번 향상된 TKIP 암호화를 사용합니다. TKIP는 암호화를 강화하는 패킷당 키 암호화 또는 더 긴 초기화 벡터(IV)를 제공합니다. 뿐만 아니라, MIC(Message Integrity Check)가 암호화된 패킷을 변경하고 있지 않음을 확인합니다. TKIP는 침입자가 WEP 키를 해독하는 데 도움을 주는 WEP의 예측 가능성을 제거합니다.

AES

WPA2 인증을 위해 사용되는 암호화 방법입니다. 이 암호화 국가 표준은 암호화 및 암호 해독에 동일한 키를 가지는 대칭 알고리즘을 사용합니다. AES는 128비트 크기의 CBC(Cipher Blocking

Chain) 암호화를 최소값으로 사용하는데, CBC 암호화는 128, 192 및 256비트의 키 크기를 지원합니다. Cisco IP 전화기는 256비트의 키 크기를 지원합니다.

참고 Cisco IP 전화기는 CMIC와 함께 CKIP(Cisco Key Integrity Protocol)를 지원하지 않습니다.

인증 및 암호화 체계는 무선 LAN 내에서 설정됩니다. VLAN은 네트워크 및 AP에서 구성되고 다른 인증과 암호화의 조합을 지정합니다. SSID는 VLAN과 특정 인증 및 암호화 체계와 연결됩니다. 무선 클라이언트 장치가 성공적으로 인증하기 위해서는 AP 및 Cisco IP 전화기에 해당 인증 및 암호화 체계를 포함하는 동일한 SSID를 구성해야 합니다.

일부 인증 체계에서는 특정 유형의 암호화가 필요합니다. 개방형 인증을 사용하면 보안 강화를 위해 암호화에 대해 정적 WEP를 사용할 수 있습니다. 그러나 공유 키 인증을 사용 중이면 암호화를 위해 정적 WEP를 설정하고, 전화기에 WEP 키를 구성해야 합니다.

참고
- WPA 사전 공유 키 또는 WPA2 사전 공유 키를 사용할 때 사전 공유 키가 정적으로 전화기에 설정되어야 합니다. 이러한 키는 AP에 있는 키와 일치해야 합니다.
- Cisco IP 전화기는 자동 EAP 협상을 지원하지 않습니다. EAP-FAST 모드를 사용하려면 이 기능을 지정해야 합니다.

다음 표에서는 Cisco IP 전화기가 지원하는 Cisco Aironet AP에 구성되는 인증 및 암호화 체계의 목록을 제공합니다. 표는 AP 구성에 상응하는 전화기의 네트워크 구성 옵션을 나타냅니다.

표 ***17:*** 인증 및 암호화 체계

Cisco IP 전화기 구성	**AP** 구성			
보안 모드	보안	키 관리	암호화	고속 로밍
없음	없음	없음	없음	해당 없음
WEP	정적 WEP	정적	WEP	해당 없음
PSK	PSK	WPA	TKIP	없음
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Cisco IP 전화기 구성	AP 구성			
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

AP에서 인증 및 암호화 체계 구성에 대한 자세한 내용은 다음 URL 아래에서 해당 모델 및 릴리스에 대한 *Cisco Aironet* 구성 설명서를 참조하십시오.

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

무선 LAN 보안

Wi-Fi를 지원하는 Cisco 전화기에는 보안 요구 사항이 많으며 추가 구성이 필요합니다. 이러한 추가 단계는 전화기 및 Cisco Unified Communications Manager에서 인증서 설치 및 보안 설정을 포함합니다.

자세한 내용은 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.

Cisco IP 전화기 관리 페이지

Wi-Fi를 지원하는 Cisco 전화기에는 다른 전화기의 페이지와 다른 특수 웹 페이지가 있습니다. SCEP(Simple Certificate Enrollment Protocol)를 사용할 수 없으면 전화기 보안 구성을 위해 이러한 특수 웹 페이지를 사용합니다. 이러한 페이지를 사용하여 수동으로 전화기에 보안 인증서를 설치하거나, 보안 인증서를 다운로드하거나, 전화기 날짜 및 시간을 수동으로 구성합니다.

또한 이러한 웹 페이지는 장치 정보, 네트워크 설정, 로그 및 통계 정보를 포함하여, 다른 전화기 웹 페이지에서 보는 정보와 동일한 정보도 나타냅니다.

관리 페이지에서 전화기 구성

관리 웹 페이지는 전화기가 공장에서 배송되었고 암호가 Cisco로 설정된 경우 활성화됩니다. 그러나 전화기가 Cisco Unified Communications Manager로 등록된 경우 관리 웹 페이지를 활성화하고 새 암호를 구성해야 합니다.

이 웹 페이지를 활성화하고 로그인 자격 증명을 설정한 후에 처음으로 웹 페이지를 사용하려면 전화기를 등록해야 합니다.

활성화되면 관리 웹 페이지는 HTTPS 포트 8443(**`https://x.x.x.x:8443`**, 여기서 x.x.x.x는 전화기 IP 주소)에서 액세스할 수 있습니다.

시작하기 전에

관리 웹 페이지를 활성화하기 전에 암호를 결정합니다. 암호는 문자 또는 숫자의 조합을 사용할 수 있지만 길이는 8 ~ 127자 사이여야 합니다.

사용자 이름은 영구적으로 admin으로 설정됩니다.

프로시저

단계 **1** Cisco 통합 커뮤니케이션 매니저 관리에서 장치 > 전화기를 선택합니다.
단계 **2** 전화기를 찾습니다.
단계 **3** 제품별 구성 레이아웃 섹션에서 웹 관리를 활성화됨으로 설정합니다.
단계 **4** 관리자 암호 필드에 암호를 입력합니다.
단계 **5** 저장을 선택하고 확인을 클릭합니다.
단계 **6** 구성 적용을 선택하고 확인을 클릭합니다.
단계 **7** 전화기를 다시 시작합니다.

전화기 관리 웹 페이지 액세스

관리 웹 페이지에 액세스하려는 경우 관리 포트를 지정해야 합니다.

프로시저

단계 **1** 전화기의 IP 주소를 확보합니다.

- Cisco 통합 커뮤니케이션 매니저 관리에서 장치 > 전화기를 선택하고 전화기를 찾습니다. Cisco Unified Communications Manager에 등록한 전화기는 전화기 찾기 및 나열 창과 전화기 구성 창 상단에 IP 주소를 표시합니다.

단계 **2** 웹 브라우저를 열고, 다음 URL을 입력합니다. 여기서 *IP_address*는 Cisco IP 전화기의 IP 주소입니다.

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

단계 **3** 암호 필드에 암호를 입력합니다.
단계 **4** 제출을 클릭합니다.

전화기 관리 웹 페이지에서 사용자 인증서 설치

SCEP(Simple Certificate Enrollment Protocol)를 사용할 수 없는 경우 전화기에 수동으로 사용자 인증서를 설치할 수 있습니다.

미리 설치된 MIC(Manufacturing Installed Certificate)를 EAP-TLS에 대한 사용자 인증서로 사용할 수 있습니다.

사용자 인증서 설치 후 RADIUS 서버 신뢰 목록에 추가해야 합니다.

시작하기 전에

전화기에 대한 사용자 인증서를 설치하기 전에 다음을 확인해야 합니다.

- PC에 사용자가 인증서를 저장되어 있습니다. 인증서는 PKCS #12 형식이어야 합니다.

• 인증서의 추출 암호입니다.

프로시저

단계 **1** 전화기 관리 웹 페이지에서 인증서를 선택합니다.
단계 **2** PC에서 인증서를 찾습니다.
단계 **3** 추출 암호 필드에 인증서 추출 암호를 입력합니다.
단계 **4** 업로드를 클릭합니다.
단계 **5** 업로드가 완료된 후 전화기를 다시 시작합니다.

전화기 관리 웹 페이지에서 인증 서버 인증서를 설치

SCEP(Simple Certificate Enrollment Protocol)를 사용할 수 없는 경우 전화기에 수동으로 인증 서버 인증서를 설치할 수 있습니다.

EAP-TLS를 위해 RADIUS 서버 인증서를 발급한 루트 CA 인증서를 설치해야 합니다.

시작하기 전에

전화기에 인증서를 설치하기 전에 PC에 인증 서버 인증서를 저장해야 합니다. 인증서는 PEM (Base-64) 또는 DER로 인코딩해야 합니다.

프로시저

단계 **1** 전화기 관리 웹 페이지에서 인증서를 선택합니다.
단계 **2** 인증 서버 **CA(**관리 웹 페이지**)** 필드를 찾아 설치를 클릭합니다.
단계 **3** PC에서 인증서를 찾습니다.
단계 **4** 업로드를 클릭합니다.
단계 **5** 업로드가 완료된 후 전화기를 다시 시작합니다.

하나 이상의 인증서를 설치하는 경우 전화기를 다시 시작하기 전에 모든 인증서를 설치합니다.

전화기 관리 웹에서 보안 인증서를 수동으로 제거

Enrollment Protocol SCEP(Simple Certificate)를 사용할 수 없는 경우 전화기에서 보안 인증서를 수동으로 제거할 수 있습니다.

프로시저

단계 **1** 전화기 관리 웹 페이지에서 인증서를 선택합니다.

단계 2 인증서 페이지에서 인증서를 찾습니다.

단계 3 삭제를 클릭합니다.

단계 4 삭제 프로세스를 완료한 후 전화기를 다시 시작합니다.

전화기 날짜 및 시간 직접 설정

인증서 기반 인증을 사용하면 전화기에 정확한 날짜와 시간이 표시되어야 합니다. 인증 서버는 인증서 만료 날짜에 대해 전화기 날짜와 시간을 확인합니다. 전화기와 서버 날짜 및 시간이 일치하지 않는 경우 전화기는 작동하지 않습니다.

전화기가 네트워크로부터 올바른 정보를 수신하지 못하는 경우 이 절차를 사용하여 날짜 및 시간을 직접 설정할 수 있습니다.

프로시저

단계 1 전화기 관리 웹 페이지에서 날짜 및 시간으로 스크롤합니다.

단계 2 다음 옵션 중 하나를 수행합니다.

- 전화기를 로컬 날짜 및 시간으로 설정을 클릭하여 전화기를 로컬 서버에 동기화합니다.
- 날짜 및 시간 지정 필드에서 메뉴를 사용하여 월, 일, 년, 시간, 분 및 초를 선택하고 전화기를 특정 날짜 및 시간으로 설정을 클릭합니다.

SCEP 설정

SCEP(Simple Certificate Enrollment Protocol)는 자동으로 인증서를 제공하고 갱신하기 위한 표준입니다. 이것은 전화기에 인증서를 수동으로 설치하지 못하게 합니다.

SCEP 제품 특정 구성 매개변수 구성

전화기 웹 페이지에서 다음과 같은 SCEP 매개변수를 구성해야 합니다.

- RA IP 주소
- SCEP 서버에 대한 루트 CA 인증서의 SHA-1 또는 SHA-256 지문

Cisco IOS 등록 기관(RA)은 SCEP 서버의 프록시로 사용됩니다. 전화기의 SCEP 클라이언트는 Cisco Unified Communications Manager에서 다운로드되는 매개변수를 사용합니다. 매개변수를 구성한 후 전화기는 `SCEP getcs` 요청을 RA에 요청을 전송하고 루트 CA 인증서는 정의된 지문을 사용하여 검증됩니다.

프로시저

단계 1 Cisco 통합 커뮤니케이션 매니저 관리에서 장치 > 전화기를 선택합니다.

단계 2 전화기를 찾습니다.

단계 3 제품별 구성 레이아웃 영역으로 스크롤합니다.

단계 4 **WLAN SCEP** 서버 확인란을 선택하여 SCEP 매개변수를 활성화합니다.

단계 5 **WLAN Root CA Fingerprint (SHA256 or SHA1)** 확인란을 선택하여 SCEP QED 매개변수를 활성화합니다.

Simple Certificate Enrollment Protocol 서버 지원

SCEP(Simple Certificate Enrollment Protocol)를 사용하는 경우 서버는 사용자와 서버 인증서를 자동으로 유지할 수 있습니다. SCEP 서버에서 SCEP 등록 에이전트(RA)를 다음과 같이 구성합니다.

- PKI 신뢰 포인트로 사용
- PKI RA로 사용
- RADIUS 서버를 사용하여 장치 인증 수행

자세한 내용을 보려면 SCEP 서버 문서를 참조하십시오.

802.1x 인증

Cisco IP 전화기는 802.1X 인증을 지원합니다.

Cisco IP 전화기와 Cisco Catalyst 스위치는 일반적으로 CDP(Cisco Discovery Protocol)를 사용해 서로를 식별하고 VLAN 할당 및 인라인 전력 요구 사항 같은 매개 변수를 결정합니다.

802.1X 인증을 지원하려면 다음과 같은 몇 가지 구성 요소가 필요합니다.

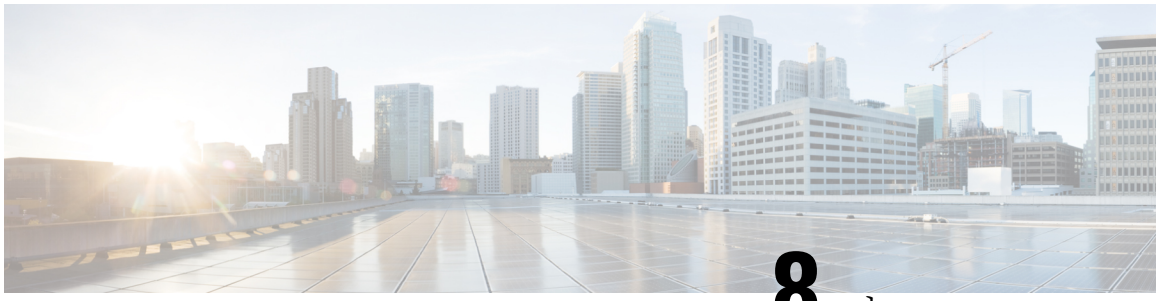
- Cisco IP 전화기: 전화기에서 네트워크 액세스 요청을 시작합니다. 전화기에는 802.1X 인증 요청자가 있습니다. 이 인증 요청자를 통해 네트워크 관리자는 IP 전화기의 LAN 스위치 포트 연결을 제어합니다. 현재 전화기 802.1X 인증 요청자 릴리스는 네트워크 인증에 EAP-FAST 및 EAP-TLS 옵션을 사용합니다.
- Cisco Catalyst 스위치(또는 기타 타사 스위치): 스위치는 반드시 802.1X를 지원해야 합니다. 그래야 인증 요청자로 작동하여 전화기와 인증 서버 사이에 메시지를 전달할 수 있습니다. 교환이 끝나면 스위치는 네트워크에 대한 전화기 액세스를 허용 또는 거부합니다.

802.1X를 구성하려면 다음과 같은 작업을 수행해야 합니다.

- 전화기에서 802.1X 인증을 활성화하기 전에, 먼저 다른 구성 요소를 구성합니다.
- 음성 VLAN 구성—802.1X 표준으로 VLAN이 설명되지 않으므로 스위치 지원을 기준으로 이 설정을 구성해야 합니다.
  - 활성화됨—멀티도메인 인증을 지원하는 스위치를 사용 중이면, 계속 음성 VLAN을 사용할 수 있습니다.
  - 비활성화됨—스위치에서 멀티도메인 인증을 지원하지 않으면, 음성 VLAN을 비활성화하고 기본 VLAN에 대한 포트 할당을 고려하십시오.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지



8 장

Cisco IP 전화회의 전화기 사용자 정의

사용자 지정 전화기 벨소리

Cisco IP 전화기에는 하드웨어에서 구현되는 두 가지 유형의 기본 벨소리인 Chirp1 및 Chirp2가 제공됩니다. 또한 Cisco Unified Communications Manager는 소프트웨어에서 PCM(Pulse Code Modulation) 파일로 구현되는 전화기 벨소리 기본 세트도 추가로 제공합니다. PCM 파일은 해당 사이트에서 사용할 수 있는 벨소리 목록 옵션을 설명하는 XML 파일과 함께 각 Cisco Unified Communications Manager 서버의 TFTP 디렉터리에 있습니다.

주의 모든 파일 이름은 대/소문자를 구분합니다. 파일 이름으로 잘못된 대/소문자를 사용하면, 전화기가 변경 사항을 적용하지 못합니다.

자세한 내용은 Cisco Unified Communications Manager 기능 구성 설명서의 "사용자 지정 전화기 벨소리 및 배경" 장을 참조하십시오.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

사용자 지정 전화기 벨소리 설정

프로시저

단계 **1** 각 사용자 지정 벨소리에 대한 PCM 파일(파일당 벨소리 하나)을 만듭니다.

PCM 파일이 [사용자 정의 벨소리 파일 형식] 섹션에 나온 형식 지침을 준수하는지 확인합니다.

단계 **2** 클러스터의 각 Cisco Unified Communications Manager를 위해 Cisco TFTP 서버에 작성한 새 PCM 파일을 업로드합니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

단계 **3** 수정 내용을 저장하고 Ringlist-wb 파일을 닫습니다.

단계 **4** Ringlist-wb 파일을 캐시하려면:

- Cisco 통합 서비스 가용성을 사용하여 TFTP 서비스를 중지했다가 시작합니다
- 고급 서비스 매개변수 영역에 있는 "시작 시 상수 및 Bin 파일에 대한 캐싱 활성화{" TFTP 서비스 매개변수를 비활성화했다가 다시 활성화합니다.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

사용자 정의 벨소리 파일 형식

Ringlist-wb.xml 파일은 전화기 벨소리 유형 목록이 포함된 XML 객체를 정의합니다. 이 파일에는 최대 50개의 벨소리 유형이 포함되어 있습니다. 각 벨소리 유형에는 해당 벨소리 유형에 사용되는 PCM 파일에 대한 포인터와 해당 벨소리에 대해 Cisco IP 전화기의 [벨소리 유형] 메뉴에 표시되는 텍스트가 포함됩니다. 각 Cisco Unified Communications Manager의 Cisco TFTP 서버에 이 파일이 포함되어 있습니다.

CiscoIPPhoneRinglist XML 객체는 다음의 간단한 태그 설정을 사용하여 정보를 기술합니다.

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

다음 특성이 정의 이름에 적용됩니다. 각 전화기 벨소리 유형별로 필요한 DisplayName과 FileName을 포함해야 합니다.

- DisplayName은 Cisco IP 전화기의 [벨소리 유형] 메뉴에 표시되는 관련된 PCM 파일의 사용자 정의 벨소리의 이름을 지정합니다.
- FileName은 사용자 정의 벨소리를 DisplayName과 연결하기 위한 PCM 파일의 이름을 지정합니다.

참고 DisplayName 및 FileName 필드는 25자를 초과해서는 안 됩니다.

다음 예는 두 개의 전화기 벨소리 유형을 정의하는 Ringlist-wb.xml 파일을 보여줍니다.

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

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

Cisco IP 전화기에서 제대로 재생되려면 벨소리용 PCM 파일이 다음 요구 사항을 충족해야 합니다.

- 원시 PCM(헤더 없음)
- 초당 8000개 샘플
- 샘플당 8비트
- Mu-law 압축
- 최대 벨소리 크기 = 16080개 샘플
- 최소 벨소리 크기 = 240개 샘플
- 벨소리 샘플 수 = 240개
- 벨소리는 부호 변화점에서 시작되고 끝납니다.

사용자 지정 전화기 벨소리용 PCM 파일을 생성하려면, 이들 파일 형식 요구 사항을 지원하는 표준 오디오 편집 패키지를 사용합니다.

신호음 사용자 정의

내부 및 외부 통화에 대해 다른 신호음이 들리도록 전화기를 설정할 수 있습니다. 사용자의 필요에 따라 세 가지 신호음 옵션 중에서 선택할 수 있습니다.

- 기본값: 내부 및 외부 통화에 다른 신호음을 사용합니다.
- 내부: 내부 신호음이 모든 통화에 사용됩니다.
- 외부: 외부 신호음이 모든 통화에 사용됩니다.

Cisco Unified Communications Manager에서는 항상 신호음 사용은 필수 필드입니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 적절한 서버를 선택합니다.

단계 **3** **Cisco CallManager**를 서비스로 선택합니다.

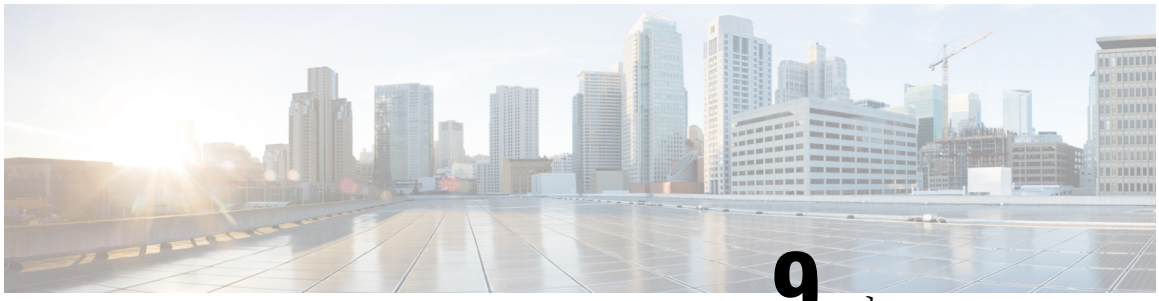
단계 **4** [클러스터 전역 매개변수] 창으로 이동합니다.

단계 **5** 항상 신호음 사용을 다음 중 하나로 설정합니다.

- 외부
- 내부
- 기본값

단계 **6** 저장을 선택합니다.

단계 **7** 전화기를 다시 시작합니다.



9 장

Cisco IP 전화회의 전화기 기능 및 설정

Cisco IP 전화기 사용자 지원

시스템 관리자는 네트워크 또는 회사에서 Cisco IP 전화기 사용자의 주요 정보 소스일 가능성이 높습니다. 최종 사용자에게 확실한 최신 정보를 제공하는 것이 중요합니다.

Cisco IP 전화기의 일부 기능(서비스 및 음성 메시지 시스템 옵션 포함)을 제대로 사용하려면, 사용자는 관리자나 관리 네트워크 팀에서 정보를 얻거나 지원을 요청할 수 있어야 합니다. 사용자에게 지원을 요청할 수 있는 사람의 이름 및 이들과 연락할 수 있는 지침을 제공해야 합니다.

Cisco는 내부 지원 사이트에 최종 사용자에게 Cisco IP 전화기에 관한 주요 정보를 제공하는 웹 페이지를 구축할 것을 권장합니다.

이 사이트에는 다음과 같은 유형을 정보를 포함시키는 것이 좋습니다.

- 지원하는 모든 Cisco IP 전화기 모델의 사용 설명서
- Cisco 통합 커뮤니케이션 자가 관리 포털 액세스 방법에 관한 정보
- 지원 기능 목록
- 음성 메일 시스템에 대한 사용자 가이드 또는 빠른 참조

전화기를 다중 플랫폼 전화기로 직접 마이그레이션

전환 펌웨어 로드를 사용하지 않고도 한 번에 회사 전화기를 다중 플랫폼 전화기로 쉽게 마이그레이션할 수 있습니다. 서버에서 마이그레이션 라이센스를 얻고 권한을 부여하는 것이 필요합니다.

자세한 내용은 https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html을 참조해 주십시오.

새 소프트키 템플릿 설정

사용자가 일부 기능에 액세스하려면 소프트키 템플릿에 소프트키를 추가해야 합니다. 예를 들어, 사용자가 방해 사절을 사용할 수 있으려면 소프트키를 활성화해야 합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

여러 템플릿을 만들 수 있습니다. 예를 들어, 회의실에 있는 전화기용 템플릿을 만들고 임원실의 전화기용 템플릿을 만들 수 있습니다.

이 절차는 새 소프트키 템플릿을 만들고 특정 전화기에 할당하는 단계를 안내합니다. 다른 전화기 기능과 마찬가지로 모든 전화 회의 전화기 또는 전화기 그룹용 템플릿을 사용할 수도 있습니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에 관리자로 로그인합니다.

단계 **2** 장치 > 장치 설정 > 소프트키 템플릿을 선택합니다.

단계 **3** 찾기를 클릭합니다.

단계 **4** 다음 옵션 중 하나를 선택합니다.

- Cisco Unified Communications Manager 11.5 이전 릴리스—표준 사용자
- Cisco Unified Communications Manager 12.0 이후 릴리스 —개인 전화회의 사용자 또는 공개 전화회의 사용자.

단계 **5** 복사를 클릭합니다.

단계 **6** 템플릿의 이름을 변경합니다.

예를 들어, 8832 회의실 템플릿으로 변경합니다.

단계 **7** 저장을 클릭합니다.

단계 **8** 오른쪽 상단 메뉴에서 소프트키 레이아웃 구성 페이지로 이동합니다.

단계 **9** 각 통화 상태에 대해 표시할 기능을 설정합니다.

단계 **10** 저장을 클릭합니다.

단계 **11** 오른쪽 상단 메뉴에서 찾기/목록 화면으로 돌아갑니다.

템플릿 목록에 새 템플릿이 표시됩니다.

단계 **12** 장치 > 전화기를 선택합니다.

단계 **13** 새 템플릿을 적용할 전화기를 찾아 선택합니다.

단계 **14** 소프트키 템플릿 필드에서 새 소프트키 템플릿을 선택합니다.

단계 **15** 저장 및 구성 적용을 클릭합니다.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

사용자를 위한 전화기 서비스 구성

사용자에게 전화기의 Cisco IP 전화기 서비스에 대한 액세스 권한을 제공할 수 있습니다. 다양한 전화기 서비스에 버튼을 지정할 수도 있습니다. IP 전화기는 각 서비스를 별개의 애플리케이션으로 관리합니다.

사용자가 서비스에 액세스하기 전 다음과 같은 작업을 수행해야 합니다.

- Cisco 통합 커뮤니케이션 매니저 관리을 사용해 기본적으로 제공되지 않는 서비스를 구성합니다.
- 사용자는 Cisco 통합 커뮤니케이션 자가 관리 포털을 사용해 서비스에 가입해야 합니다. 이 웹 기반 애플리케이션은 IP 전화기 애플리케이션의 제한된 최종 사용자 구성에 GUI(그래픽 사용자 인터페이스)를 제공합니다. 그러나 사용자는 엔터프라이즈 등록으로 구성한 서비스에는 가입할 수 없습니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

서비스를 설정하기 전에 설정하려는 사이트의 URL을 수집하여, 사용자가 회사 IP 텔레포니 네트워크에서 해당 사이트에 액세스할 수 있는지 확인합니다. 이러한 작업은 Cisco가 제공하는 기본 서비스에는 해당되지 않습니다.

프로시저

단계 **1** Cisco 통합 커뮤니케이션 매니저 관리에서 장치 > 장치 설정 > 전화 서비스를 선택합니다.

단계 **2** 사용자가 구성된 서비스를 선택하고 이에 가입할 수 있는 Cisco 통합 커뮤니케이션 자가 관리 포털에 액세스할 수 있는지 확인합니다.

최종 사용자에게 반드시 제공해야 하는 정보에 관한 내용은 셀프 서비스 포털 개요, 71 페이지를 참조하십시오.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

전화기 기능 구성

사용자의 필요에 따라 다양한 기능을 가진 전화기를 설정할 수 있습니다. 모든 전화기, 전화기 그룹 또는 개별 전화기에 기능을 적용할 수 있습니다.

기능을 설정할 때 Cisco 통합 커뮤니케이션 매니저 관리 창은 모든 전화기에 적용되는 정보 및 전화기 모델에 적용되는 정보를 표시합니다. 전화기 모델에 관련된 정보는 창의 [제품별 구성 레이아웃] 영역에 있습니다.

모든 전화기 모델에 적용되는 필드에 대한 내용은 Cisco Unified Communications Manager 설명서를 참조하십시오.

필드를 설정할 때 창의 우선 순위가 있으므로 필드를 설정한 창이 중요합니다. 우선 순위는 다음과 같습니다.

1. 개별 전화기(우선 순위 최고)
2. 전화기 그룹
3. 모든 전화기(우선 순위 최저)

예를 들어, 특정 사용자는 전화기 웹 페이지에 액세스하지 못하도록 하고 나머지 사용자는 페이지에 액세스할 수 있도록 하려는 경우:

1. 모든 사용자가 전화기 웹 페이지에 액세스할 수 있게 합니다.
2. 각 개별 사용자에 대해 전화기 웹 페이지 액세스를 비활성화하거나 사용자 그룹을 설정하고 사용자 그룹에 대해 전화기 웹 페이지 액세스를 비활성화합니다.
3. 사용자 그룹의 특정 사용자가 전화기 웹 페이지에 액세스해야 하는 경우 이 특정 사용자에 대해 페이지 액세스를 활성화할 수 있습니다.

관련 항목

Expressway 로그인을 위해 사용자 자격 증명 영구 구성, 126 페이지

모든 전화기에 대해 전화기 구성 설정

프로시저

단계 **1** 관리자 권한으로 Cisco Unified Communications Manager 관리에 로그인합니다.
단계 **2** 시스템 > 엔터프라이즈 전화기 구성을 선택합니다.
단계 **3** 변경할 필드를 설정합니다.
단계 **4** 변경된 필드에 대해 엔터프라이즈 설정 무시 확인란을 선택합니다.
단계 **5** 저장을 클릭합니다.
단계 **6** 구성 적용을 클릭합니다.
단계 **7** 전화기를 다시 시작합니다.

참고 이렇게 하면 조직의 모든 전화기에 영향을 줍니다.

관련 항목

제품별 구성, 102 페이지

전화기 그룹에 대해 전화기 구성 설정

프로시저

단계 1 관리자 권한으로 Cisco Unified Communications Manager 관리에 로그인합니다.
단계 2 장치 > 장치 설정 > 일반 전화기 프로파일을 선택합니다.
단계 3 프로파일을 찾습니다.
단계 4 제품별 구성 레이아웃을 탐색하여 필드를 설정합니다.
단계 5 변경된 필드에 대해 엔터프라이즈 설정 무시 확인란을 선택합니다.
단계 6 저장을 클릭합니다.
단계 7 구성 적용을 클릭합니다.
단계 8 전화기를 다시 시작합니다.

관련 항목

제품별 구성, 102 페이지

단일 전화기에 대해 전화기 구성 설정

프로시저

단계 1 관리자 권한으로 Cisco Unified Communications Manager 관리에 로그인합니다.
단계 2 장치 > 전화기를 선택합니다.
단계 3 사용자와 연결된 전화기를 찾습니다.
단계 4 제품별 구성 레이아웃을 탐색하여 필드를 설정합니다.
단계 5 변경된 필드에 대해 일반 설정 무시 확인란을 선택합니다.
단계 6 저장을 클릭합니다.
단계 7 구성 적용을 클릭합니다.
단계 8 전화기를 다시 시작합니다.

관련 항목

제품별 구성, 102 페이지

제품별 구성

다음 표에서는 [제품별 구성 레이아웃] 창의 필드를 설명합니다. 이 표의 일부 필드는 장치 > 전화 페이지에만 표시됩니다.

표 ***18:*** 제품별 구성 필드

필드 이름	필드 유형 또는 선택 사항	기본값	설명
액세스 설정	비활성화됨 활성화됨 제한됨	활성화됨	설정 앱에서 로컬 구성 설정에 대한 액세스를 활성화, 비활성화 또는 제한합니다. 액세스가 제한된 상태에서 [환경 설정] 및 [시스템 정보] 메뉴에 액세스할 수 있습니다. Wi-Fi 메뉴의 일부 설정에도 액세스할 수 있습니다. 액세스가 비활성화된 상태에서는 [설정] 메뉴에 옵션이 표시되지 않습니다.
불필요한 ARP	비활성화됨 활성화됨	비활성화됨	Gratuitous ARP에서 MAC 주소를 학습하는 전화기 기능을 활성화 또는 비활성화합니다. 이 기능은 음성 스트림을 모니터링하거나 녹음해야 합니다.
웹 액세스	비활성화됨 활성화됨	비활성화됨	웹 브라우저를 통해 전화기 웹 페이지에 대한 액세스를 활성화 또는 비활성화합니다. 주의 이 필드를 활성화하면 전화기에 대한 중요한 정보가 노출될 수 있습니다.
웹 액세스에 대해 TLS 1.0 및 TLS 1.1 비활성화	비활성화됨 활성화됨	활성화됨	웹 서버 연결에 대해 TLS 1.2 사용을 제어합니다. • 비활성화됨—TLS1.0, TLS 1.1 또는 TLS1.2용으로 구성된 전화기는 HTTPS 서버로 작동할 수 있습니다. • 활성화됨—TLS1.2용으로 구성된 전화기만 HTTPS 서버로 작동할 수 있습니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명
Enbloc 전화 걸기	비활성화됨 활성화됨	비활성화됨	전화걸기 방법을 제어합니다. • 비활성화됨 - Cisco Unified Communications Manager는 다이얼 플랜 또는 경로 패턴이 중복될 때 interdigit 타이머가 만료될 때까지 대기합니다. • 활성화됨 - 전화걸기가 완료되면 전체 착신 문자열이 Cisco Unified Communications Manager로 전송됩니다. T.302 타이머 시간 초과를 방지하려면 다이얼 플랜 또는 라우트 패턴이 겹쳐 있을 때마다 Enbloc 다이얼링을 사용하는 것이 좋습니다. 강제 인증 코드(FAC) 또는 클라이언트 매터 코드(CMC)는 Enbloc 전화걸기를 지원하지 않습니다. FAC 또는 CMC를 사용하여 통화 액세스 및 계정을 관리하는 경우 이 기능을 사용할 수 없습니다.
백라이트 비활성화 지정일	요일		[백라이트 켜기 시간] 필드에 지정된 시간에 백라이트가 자동으로 켜지지 않는 날을 정의합니다. 드롭다운 목록 상자에서 날짜를 선택합니다. 1일 이상을 선택하려면 **Ctrl** 키를 누른 채 원하는 날짜를 클릭합니다. Cisco IP 전화기의 절전 일정, 115 페이지 참조
백라이트 켜짐 시간	hh:mm		지정한 각 날짜에 백라이트가 자동으로 켜지는 시간을 정의합니다([백라이트 디스플레이를 활성화하지 않음] 필드에 지정한 날짜는 제외). 이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 00:00은 자정입니다. 예를 들어 오전 07:00시(0700)에 자동으로 백라이트를 끄고 싶다면 07:00을 입력합니다. 오후 02:00시(1400) 에 백라이트를 켜고 싶다면 14:00을 입력합니다. 이 필드를 공백으로 두면 백라이트가 자정(0:00)에 자동으로 켜집니다. Cisco IP 전화기의 절전 일정, 115 페이지 참조

필드 이름	필드 유형 또는 선택 사항	기본값	설명
백라이트 켜짐 기간	hh:mm		[백라이트 켜기 시간] 필드에 지정된 시간에 백라이트가 켜진 뒤 유지되는 시간을 정의합니다. 예를 들어 자동으로 켜진 뒤 4시간 30분 동안 백라이트를 켠 상태로 유지하고 싶다면, 04:30을 입력합니다. 이 필드를 공백으로 두면 전화기는 자정(0:00)에 켜집니다. [백라이트 켜기 시간]이 0:00이고 [백라이트 켜기 기간]이 비어 있는 경우(또는 24:00), 백라이트가 켜지지 않습니다. Cisco IP 전화기의 절전 일정, 115 페이지 참조
백라이트 유휴 시간 초과	hh:mm		백라이트를 끄기 전까지 전화기가 유휴 상태로 유지되는 시간 길이를 정의합니다. 백라이트가 예정대로 꺼진 때와 사용자가 전화기의 버튼을 누르거나 핸드셋을 들어 올려 백라이트를 켠 경우에만 적용됩니다. 예를 들어 사용자가 백라이트를 켠 후 전화기의 유휴 상태가 1시간 30분 동안 지속되었을 때 백라이트를 끄려면 01:30을 입력합니다. Cisco IP 전화기의 절전 일정, 115 페이지 참조
전화 수신 시 백라이트 켜짐	비활성화됨 활성화됨	활성화됨	수신 통화가 있는 경우 백라이트를 켭니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명
절전 플러스 활성화	요일		전화기의 전원을 끄려는 날짜를 정의합니다. 드롭다운 목록 상자에서 날짜를 선택합니다. 1일 이상을 선택하려면 **Ctrl** 키를 누른 채 원하는 날짜를 클릭합니다. 절전 플러스 활성화를 설정하면, 긴급 상황(e911)에 대해 경고하는 메시지가 전송됩니다. 주의 절전 플러스 모드("모드")에 들어가면, 해당 모드로 구성된 엔드포인트는 긴급 전화 및 착신 전화에 대해 비활성화됩니다. 이 모드를 선택하면 다음과 같은 내용에 동의하는 것입니다. (i) 모드가 실행되는 동안 긴급 전화 및 수신 전화에 대한 대안을 제공하는 것은 전적으로 귀하의 책임이며, (ii) Cisco는 모드 선택과 관련해 어떠한 법적 책임도 없으며, 모드 활성화와 관련된 모든 책임은 귀하에게 있습니다. 그리고 (iii) 통화, 전화 걸기 및 기타 내용에 해당 모드가 미치는 영향에 대해 사용자에게 충분히 공지해야 합니다. 절전 플러스를 비활성화하려면, [EnergyWise 오버라이드 허용] 확인란을 선택 취소해야 합니다. [EnergyWise 오버라이드 허용]이 선택된 상태에서 [절전 플러스 활성화] 필드에 어떤 날짜도 선택하지 않으면, 절전 플러스는 비활성화되지 않습니다. Cisco IP 전화기에서 EnergyWise 예약, 116 페이지 참조

필드 이름	필드 유형 또는 선택 사항	기본값	설명
전화 켜기 시간	hh:mm		[절전 플러스 활성화] 필드에 지정된 일 수 동안 전화기를 자동으로 켜는 시간을 정합니다. 이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 00:00은 자정입니다. 예를 들어 오전 07:00시(0700)에 자동으로 전화기를 켜고 싶다면 07:00을 입력합니다. 오후 02:00(1400)에 에 디스플레이를 켜고 싶다면 14:00을 입력합니다. 기본값은 공란, 즉 00:00입니다. 전화 켜기 시간은 전화 끄기 시간 이후 최소 20분이 지나야 합니다. 예를 들어 전화 끄기 시간이 07:00였다면, 전화 켜기 시간은 07:20보다 빠르면 안 됩니다. Cisco IP 전화기에서 EnergyWise 예약, 116 페이지 참조
전화 끄기 시간	hh:mm		[절전 플러스 활성화] 필드에 지정된 일 수 동안 전화기의 전원을 끄는 시간을 정의합니다. [전화 켜기 시간]과 [전화 끄기 시간] 필드에 같은 값이 입력되어 있으면 전화기는 전원을 끄지 않습니다. 이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 00:00은 자정입니다. 예를 들어 오전 07:00시(0700)에 자동으로 전화기를 끄고 싶다면 7:00을 입력합니다. 오후 02:00(1400)에 에 디스플레이를 켜고 싶다면 14:00을 입력합니다. 기본값은 공란, 즉 00:00입니다. 전화 켜기 시간은 전화 끄기 시간 이후 최소 20분이 지나야 합니다. 예를 들어 전화 끄기 시간이 07:00였다면, 전화 켜기 시간은 07:20보다 빠르면 안 됩니다. Cisco IP 전화기에서 EnergyWise 예약, 116 페이지 참조

필드 이름	필드 유형 또는 선택 사항	기본값	설명
전화 끄기 유휴 시간 초과	hh:mm		전화기의 전원을 끄기 전에 전화기가 유휴 상태로 머물러야 하는 시간의 길이를 나타냅니다. 시간 초과는 다음과 같은 상황에서 발생합니다. • 예정대로 전화기가 절전 플러스 모드인 상태에서, 전화기 사용자가 선택 키를 눌러 절전 플러스 모드에서 벗어난 경우 • 연결된 스위치에서 전화기의 전원을 다시 켰을 때 • 전화 끄기 시간이 되었으나 전화기를 사용 중일 때 Cisco IP 전화기에서 EnergyWise 예약, 116 페이지 참조
알림음 사용	확인란	선택 취소됨	활성화되면 전화기에 [전화 끄기 시간] 필드에 지정한 시간보다 10분 전에 알림음을 재생하게 합니다. 이 확인란은 [절전 플러스 활성화] 목록 상자에서 1일 이상을 선택한 경우에만 적용됩니다. Cisco IP 전화기에서 EnergyWise 예약, 116 페이지 참조
EnergyWise 도메인	최대 127자		전화기가 소속된 EnergyWise 도메인을 식별합니다. Cisco IP 전화기에서 EnergyWise 예약, 116 페이지 참조
EnergyWise 비밀	최대 127자		EnergyWise 도메인에서 엔드포인트와 통신할 때 사용하는 보안 비밀 암호를 식별합니다. Cisco IP 전화기에서 EnergyWise 예약, 116 페이지 참조

필드 이름	필드 유형 또는 선택 사항	기본값	설명
EnergyWise 오버라이드 허용	확인란	선택 취소됨	EnergyWise 도메인 컨트롤러 정책에서 전화기로 전력 수준 업데이트를 전송하도록 허용할 것인지 여부를 결정합니다. 다음과 같은 조건이 적용됩니다. • [절전 플러스 활성화] 필드에서 1일 이상을 선택해야 합니다. • EnergyWise에서 오버라이드를 전송할 때에도 Cisco Unified Communications Manager Administration의 설정은 실행됩니다. 예를 들어 전화 끄기 시간이 22:00(오후 10:00)이고 전화 켜기 시간 필드의 값이 06:00(오전 6:00)라면, 절전 플러스 활성화는 1일 이상을 선택해야 합니다. • EnergyWise에서 전화기에 20:00(오후 8:00)에 전화기를 끄라고 지시하면, 이러한 지시 사항은 구성된 전화 켜기 시간인 오전 6:00까지 효력이 있습니다(전화에 사용자 개입이 전혀 없다고 가정할 경우). • 오전 6:00시가 되면 전화기가 켜지고 Cisco Unified Communications Manager Administration 설정에서 전력 수준 변경 내용을 수신하여 작동을 시작합니다. • 전화기의 전력 수준을 다시 변경하려면, EnergyWise에서 새로운 전력 수준 변경 명령을 다시 내려야 합니다. 절전 플러스를 비활성화하려면, [EnergyWise 오버라이드 허용] 확인란을 선택 취소해야 합니다. [EnergyWise 오버라이드 허용]이 선택된 상태에서 [절전 플러스 활성화] 필드에 어떤 날짜도 선택하지 않으면, 절전 플러스는 비활성화되지 않습니다. Cisco IP 전화기에서 EnergyWise 예약, 116 페이지 참조

필드 이름	필드 유형 또는 선택 사항	기본값	설명
참여 및 호연결 정책 설정	동일한 회선 활성화 동일한 회선 비활성화	동일한 회선, 회선 간 활성화	사용자의 참여 및 호전환 호출 기능을 제어합니다. • 동일한 회선 활성화 — 사용자가 직접 호전환하거나 현재 회선의 통화를 동일한 회선의 다른 통화에 참가할 수 있습니다. • 동일한 회선 비활성화 — 동일한 회선에서 사용자가 통화에 참가하거나 호전환할 수 없습니다. 참가 및 호전환 기능이 비활성화되고 사용자가 직접 호전환 또는 통화 참가 기능을 수행할 수 없습니다.
녹음 신호음	비활성화됨 활성화됨	비활성화됨	사용자가 통화를 녹음할 때 신호음 재생을 제어합니다.
녹음 신호음 로컬 볼륨	정수 0–100	100	로컬 사용자의 녹음 신호음 볼륨을 제어합니다.
녹음 신호음 원격 볼륨	정수 0–100	50	원격 사용자의 녹음 신호음 볼륨을 제어합니다.
녹음 신호음 지속 시간	정수 1 – 3000 밀리초 단위		녹음 신호음 지속 시간을 제어합니다.
로그 서버	최대 256자의 문자열		전화기 디버그 출력을 위한 IPv4 syslog 서버를 식별합니다. 주소의 형식은 **address:<port>@@base=<0-7>;pfs=<0-1>** 입니다.
원격 로그	비활성화됨 활성화됨	비활성화됨	syslog서버에 로그를 전송하는 기능을 제어합니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명
로그 프로파일	기본값 프리셋 텔레포니 SIP UI 네트워크 미디어 업그레이드 액세서리 보안 EnergyWise MobileRemoteAccess	프리셋	미리 정의된 로그 프로파일을 지정합니다. • 기본값 - 기본 디버그 로그 수준 • 프리셋 - 전화기 로컬 디버그 로깅 설정을 덮어쓰지 않음 • 텔레포니 — 텔레포니 또는 통화 기능에 대한 정보를 기록 • SIP - SIP 시그널링에 대한 정보를 기록 • UI — 전화기 사용자 인터페이스에 대한 정보를 기록 • 네트워크 — 네트워크 정보를 기록 • 미디어 — 미디어 정보를 기록 • 업그레이드 — 업그레이드 정보를 기록 • 액세서리 — 액세서리 정보를 기록 • 보안 — 보안 정보를 기록 • Energywise — 에너지 절약 정보를 기록 • MobileRemoteAccess—Expressway를 통한 모바일 및 Remote Access 정보를 기록
IPv6 로그 서버	최대 256자의 문자열		전화기 디버그 출력을 위한 IPv6 syslog 서버를 식별합니다.
Cisco Discovery Protocol(CDP): 스위치 포트	비활성화됨 활성화됨	활성화됨	전화기에서 Cisco Discovery Protocol을 제어합니다.
Link Layer Discovery Protocol - 미디어 엔드포인트 검색 (LLDP-MED): 스위치 포트	비활성화됨 활성화됨	활성화됨	SW 포트에서 LLDP-MED를 활성화합니다.
LLDP 자산 ID	최대 32자의 문자열		인벤토리 관리를 위해 전화기에 할당된 자산 ID를 식별합니다.
EEE(Energy Efficient Ethernet): 스위치 포트	비활성화됨 활성화됨	비활성화됨	스위치 포트에서 EEE를 제어합니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명
LLDP 전원 우선 순위	알 수 없음 낮음 높음 중요	알 수 없음	전화기에 전원을 공급할 수 있게 하는 스위치에 대한 전화기 전원 우선 순위를 지정합니다.
802.1x 인증	사용자 제어됨 비활성화됨 활성화됨	사용자 제어됨	802.1x 인증 기능 상태를 지정합니다. • 사용자 제어됨 - 사용자가 전화기에서 802.1 x를 구성할 수 있습니다. • 비활성화됨—802.1x 인증이 사용되지 않습니다. • 활성화됨—802.1x 인증을 사용하고 전화기에 대한 인증을 구성합니다.
스위치 포트 원격 구성	비활성화됨 자동 협상 10 반이중 10 전이중 100 반이중 100 전이중	비활성화됨	원격으로 전화기 SW 포트의 전이중/반이중 기능과 속도를 구성할 수 있습니다. 이는 구체적인 포트 설정을 사용한 대규모 구축 작업의 성과를 향상합니다. Cisco Unified Communications Manager에서 원격 포트 구성을 위해 SW 포트를 구성하면, 전화기에서 데이터를 변경할 수 없습니다.
SSH 액세스	비활성화됨 활성화됨	비활성화됨	포트 22를 통해 SSH 데몬에 대한 액세스를 제어합니다. 포트 22를 열어 두면 전화기가 DoS(Denial of Service) 공격에 취약해질 수 있습니다.
벨소리 로캘	기본값 일본	기본값	벨소리 패턴을 제어합니다.
TLS 재개 타이머	정수 0-3600초	3600	전체 TLS 인증 프로세스를 반복하지 않고 TLS 세션을 재개하는 기능을 제어합니다. 필드가 0으로 설정되면 TLS 세션 재개가 비활성화됩니다.
FIPS 모드	비활성화됨 활성화됨	비활성화됨	전화기에서 FIPS(Federal Information Processing Standards) 모드를 활성화하거나 비활성화합니다.
공유 회선의 통화 기록 기록	비활성화됨 활성화됨	비활성화됨	공유 회선의 통화 로그를 기록할지 여부를 지정합니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명
최소 벨소리 볼륨	0-무음 1–15	0-무음	전화기에 대한 최소 벨소리 볼륨을 제어합니다.
피어 펌웨어 공유	비활성화됨 활성화됨	활성화됨	전화기가 서브넷에 동일한 모델의 다른 전화기를 찾아 업데이트된 펌웨어 파일을 공유할 수 있습니다. 전화기에 새 펌웨어가 로드된 경우 다른 전화기와 해당 로드를 공유할 수 있습니다. 다른 전화기에 새 펌웨어가 로드된 경우 전화기는 TFTP 서버 대신 다른 전화기의 펌웨어를 다운로드할 수 있습니다. 피어 펌웨어 공유: • 중앙의 원격 TFTP 서버로 TFTP 호전환에 따른 혼잡을 제한합니다. • 펌웨어 업그레이드를 수동으로 관리할 필요가 없습니다. • 다수의 전화기를 동시에 재설정할 때 업그레이드를 진행하는 동안 전화기 다운타임이 줄어듦 • 대역폭이 제한된 WAN 링크를 실행하는 지점 또는 원격 사무실 구축 시나리오에서 펌웨어 업그레이드하는 데 도움이 됩니다.
로드 서버	최대 256자의 문자열		전화기가 펌웨어 로드 및 업그레이드를 사용하는 대체 IPv4 서버를 식별합니다.
IPv6 로드 서버	최대 256자의 문자열		전화기가 펌웨어 로드 및 업그레이드를 사용하는 대체 IPv6 서버를 식별합니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명
Unified CM 연결 실패 감지	정상 지연됨	정상	전화기에 백업 Unified CM/SRST에 대한 장치 페일오버가 발생하기 전의 첫 번째 단계인 Cisco Unified Communications Manager(Unified CM)에 대한 연결 실패를 감지하기 위해 설정되는 감도를 결정합니다. 유효한 값은 보통(Unified CM 연결 실패 감지가 시스템 표준 비율로 발생합니다) 또는 지연됨(Unified CM 연결 페일오버 감지가 보통보다 약 4배 느리게 발생합니다)이 있습니다. Unified CM 연결 실패를 빠르게 감지하려면 [보통]을 선택합니다. 페일오버를 약간 지연시켜 다시 연결할 기회를 제공하려는 경우 [지연됨]을 선택합니다. 보통과 지연됨 연결 오류 감지 사이의 정확한 시간 차이는 계속 변하는 여러 가지 변수에 따라 달라집니다.
특별한 요구 사항 ID	문자열		엔지니어링 전문(ES) 로드에서 사용자 정의 기능을 제어합니다.
HTTPS 서버	http 및 https 활성화됨 https만	http 및 https 활성화됨	전화기에 대한 통신 유형을 제어합니다. HTTPS만을 선택하면 전화 통신은 더 안전합니다.
Expressway 로그인을 위한 사용자 자격 증명 영구	비활성화됨 활성화됨	비활성화됨	전화기에 사용자의 사인인 인증서를 저장할지 제어합니다. 비활성화된 경우 항상 모바일 및 Remote Access(MRA)에 대한 Expressway 서버에 로그인하는 프롬프트를 표시합니다. 사용자가 로그인하기 쉽게 하려면 Expressway 로그인 자격 증명이 영구가 되도록 이 필드를 활성화합니다. 사용자는 처음에만 로그인 자격 증명을 입력합니다. 그 후에는 (전화기 전원이 오프-프레미스에서 공급될 때) 로그인 정보가 로그인 화면에 미리 입력되어 있습니다. 자세한 내용은 Expressway 로그인을 위해 사용자 자격 증명 영구 구성, 126 페이지를 참조하십시오.

필드 이름	필드 유형 또는 선택 사항	기본값	설명
고객 지원 업로드 URL	최대 256자의 문자열		문제 보고서 도구(PRT)에 대한 URL을 제공합니다. Expressway를 통해 [모바일 및 Remote Access]로 장치를 구축하는 경우, Expressway 서버의 [HTTP 서버 허용] 목록에 PRT 서버 주소도 추가해야 합니다. 자세한 내용은 Expressway 로그인을 위해 사용자 자격 증명 영구 구성, 126 페이지를 참조하십시오.
TLS 암호화 비활성화	전송 레이어 보안 암호 비활성화, 114 페이지 참조	없음	선택한 TLS 암호화를 비활성화합니다. 컴퓨터 키보드의 **Ctrl** 키를 누른 채로 둘 이상의 암호화 제품군을 비활성화합니다.
통화 대기를 위한 전용 회선	비활성화됨 활성화됨	활성화됨	통화 지정 보류된 통화가 한 회선을 차지하는지 여부를 제어합니다. 자세한 내용은 Cisco Unified Communications Manager 문서를 참조하십시오.

관련 항목

Expressway 로그인을 위해 사용자 자격 증명 영구 구성, 126 페이지

전송 레이어 보안 암호 비활성화

TLS 암호화 비활성화 매개 변수를 사용하여 TLS(Transport Layer Security) 암호를 비활성화할 수 있습니다. 이를 통해 알려진 취약점에 대한 보안을 조정하고, 암호에 대한 회사의 정책에 따라 네트워크를 조정할 수 있습니다.

없음이 기본 설정입니다.

컴퓨터 키보드의 **Ctrl** 키를 누른 채로 둘 이상의 암호화 제품군을 비활성화합니다. 전화기 암호를 모두 선택하는 경우 전화기 TLS 서비스가 영향을 받습니다. 선택 사항은 다음과 같습니다.

- 없음
- 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

전화기 보안에 대한 자세한 내용은 *Cisco IP* 전화기 *7800* 및 *8800* 시리즈 보안 개요 백서 (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html)를 참조하십시오.

Cisco IP 전화기의 절전 일정

전기를 아끼고 전화기 화면을 오래 사용할 수 있도록 필요하지 않을 때는 디스플레이가 꺼지도록 설정할 수 있습니다.

Cisco Unified Communications Manager Administration에서 특정일의 지정된 시간 및 임의의 어떤 날에 온종일 디스플레이가 꺼지도록 설정할 수 있습니다. 예를 들어 주중 근무 시간 이후 및 토요일과 일요일에 온종일 디스플레이를 끄도록 선택할 수 있습니다.

다음을 수행하면 언제든지 꺼진 디스플레이를 다시 켤 수 있습니다.

- 전화기에서 아무 버튼이나 누릅니다.

  전화기에서 디스플레이가 켜지고 해당 버튼에 지정된 작업이 수행됩니다.

- 핸드셋을 듭니다.

이렇게 켜진 디스플레이는 전화기가 지정된 시간 동안 유휴 상태를 유지하고 있을 때까지는 켜져 있다가, (해당 시간이 지나면) 자동으로 꺼집니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다.

단계 **2** 설정할 전화기를 검색합니다.

단계 **3** 제품별 구성을 탐색하여 다음 필드를 설정합니다.

- 디스플레이 비활성화 지정일
- 디스플레이 켜기 시간
- 디스플레이 켜기 지속 시간
- 디스플레이 유휴 시간 초과

표 ***19:*** 절전 구성 필드

필드	설명
디스플레이 비활성화 지정일	[디스플레이 켜기 시간] 필드에 지정된 시간에 디스플레이가 자동으로 켜지지 않는 날. 드롭다운 목록 상자에서 날짜를 선택합니다. 1일 이상을 선택하려면 Ctrl키를 누른 채 원하는 날짜를 클릭합니다.

필드	설명
디스플레이 켜기 시간	지정한 각 날짜에 디스플레이가 자동으로 켜지는 시간([디스플레이를 활성화하지 않는 날짜] 필드에 지정한 날짜는 제외). 이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 0:00은 자정입니다. 예를 들어 오전 07:00시(0700)에 자동으로 디스플레이를 *끄*고 싶다면 **07:00**을 입력합니다. 오후 02:00시(1400) 에 디스플레이를 켜고 싶다면 **14:00**을 입력합니다. 이 필드를 공백으로 두면 디스플레이가 자정(0:00)에 자동으로 켜집니다.
디스플레이 켜기 지속 시간	[디스플레이 켜기 시간] 필드에 지정된 시간에 디스플레이가 켜진 뒤 유지되는 시간. 이 필드에 시간:분 형식으로 값을 입력합니다. 예를 들어 자동으로 켜진 뒤 4시간 30분 동안 디스플레이를 켠 상태로 유지하고 싶다면, **04:30**을 입력합니다. 이 필드를 공백으로 두면 전화기는 자정(0:00)에 켜집니다. 참고 [디스플레이 켜기 시간]이 0:00이고 디스플레이 켜기 지속 시간이 공백이거나 24:00으로 되어 있으면, 디스플레이는 계속 켜진 상태로 유지됩니다.
디스플레이 유휴 시간 초과	디스플레이를 *끄*기 전까지 전화기가 유휴 상태로 유지되는 시간 길이. 디스플레이가 예정대로 꺼진 때와 사용자가 전화기의 버튼을 누르거나 핸드셋을 들어 올려 디스플레이를 켠 경우에만 적용됩니다. 이 필드에 시간:분 형식으로 값을 입력합니다. 예를 들어 사용자가 디스플레이를 켠 후 전화기의 유휴 상태가 1시간 30분 동안 지속되었을 때 디스플레이를 *끄*려면 **01:30**을 입력합니다. 기본값은 01:00입니다.

단계 **4** 저장을 선택합니다.

단계 **5** 구성 적용을 선택합니다.

단계 **6** 전화기를 다시 시작합니다.

Cisco IP 전화기에서 EnergyWise 예약

시스템에 EnergyWise 컨트롤러가 포함되어 있는 경우 전화기를 대기(절전) 및 활성화(작동)로 구성하면, 전력 소비량을 줄일 수 있습니다.

Cisco Unified Communications Manager Administration에서 EnergyWise를 활성화하도록 설정하고 대기 및 활성화 시간을 구성합니다. 이러한 매개변수는 전화기 화면 구성 매개변수와 밀접하게 연결됩니다.

EnergyWise가 활성화되고 대기 시간이 설정되면, 전화기는 스위치에 설정한 시간에 전화기를 활성화하라고 요청을 전송합니다. 스위치는 요청에 대한 수락 또는 거부 메시지를 반송합니다. 스위치가 요

청을 거부하거나 스위치에서 응답이 없는 경우, 전화기는 절전 모드로 들어가지 못합니다. 스위치에서 요청을 수락하면 유휴 상태에 있던 전화기가 대기 모드로 전환되고, 따라서 전력 소비량이 사전에 정한 수준까지 떨어집니다. 유휴 상태가 아닌 전화기는 유휴 타이머를 설정하고 유휴 타이머가 종료되면 대기 상태로 전환됩니다.

전화기를 활성화하려면 [선택]을 누릅니다. 예정된 활성화 시간이 되면 시스템은 전화기에 전원을 복구하여 전화기를 활성화합니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다.

단계 **2** 설정할 전화기를 검색합니다.

단계 **3** 제품별 구성을 탐색하여 다음 필드를 설정합니다.

- 절전 플러스 활성화
- 전화 켜기 시간
- 전화 끄기 시간
- 전화 끄기 유휴 시간 초과
- 알림음 사용
- EnergyWise 도메인
- EnergyWise 비밀
- EnergyWise 오버라이드 허용

표 *20: EnergyWise* 구성 필드

필드	설명
절전 플러스 활성화	전화기의 전원을 끄려는 날짜를 선택합니다. 일정에 포함할 날짜를 클릭하고, 컨트롤 키를 누른 채로 여러 날짜를 선택합니다. 기본적으로는 날짜가 선택되지 않습니다. 절전 플러스 활성화를 선택하면, 긴급 상황(e911)에 대해 경고하는 메시지가 전송됩니다. 주의 절전 플러스 모드("모드")에 들어가면, 해당 모드로 구성된 엔드포인트는 긴급 전화 및 착신 전화에 대해 비활성화됩니다. 이 모드를 선택하면 다음과 같은 내용에 동의하는 것입니다. (i) 모드가 실행되는 동안 긴급 전화 및 수신 전화에 대한 대안을 제공하는 것은 전적으로 귀하의 책임이며, (ii) Cisco는 모드 선택과 관련해 어떠한 법적 책임도 없으며, 모드 활성화와 관련된 모든 책임은 귀하에게 있습니다. 그리고 (iii) 통화, 전화 걸기 및 기타 내용에 해당 모드가 미치는 영향에 대해 사용자에게 충분히 공지해야 합니다. 참고 절전 플러스를 비활성화하려면, [EnergyWise 오버라이드 허용] 확인란을 선택 취소해야 합니다. [EnergyWise 오버라이드 허용]이 선택된 상태에서 [절전 플러스 활성화] 필드에 어떤 날짜도 선택하지 않으면, 절전 플러스는 비활성화되지 않습니다.
전화 켜기 시간	[절전 플러스 활성화] 필드에 지정된 일 수 동안 전화기를 자동으로 켜는 시간을 정합니다. 이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 00:00은 자정입니다. 예를 들어 오전 07:00시(0700)에 자동으로 전화기를 켜고 싶다면 07:00을 입력합니다. 오후 02:00(1400)에 에 디스플레이를 켜고 싶다면 14:00을 입력합니다. 기본값은 공란, 즉 00:00입니다. 참고 전화 켜기 시간은 전화 끄기 시간 이후 최소 20분이 지나야 합니다. 예를 들어 전화 끄기 시간이 07:00였다면, 전화 켜기 시간은 07:20보다 빠르면 안 됩니다.
전화 끄기 시간	[절전 플러스 활성화] 필드에 지정된 일 수 동안 전화기의 전원을 끄는 시간을 정합니다. [전화 켜기 시간]과 [전화 끄기 시간] 필드에 같은 값이 입력되어 있으면 전화기는 전원을 끄지 않습니다. 이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 00:00은 자정입니다. 예를 들어 오전 07:00시(0700)에 자동으로 전화기를 끄고 싶다면 7:00을 입력합니다. 오후 02:00(1400)에 에 디스플레이를 켜고 싶다면 14:00을 입력합니다. 기본값은 공란, 즉 00:00입니다. 참고 전화 켜기 시간은 전화 끄기 시간 이후 최소 20분이 지나야 합니다. 예를 들어 전화 끄기 시간이 07:00였다면, 전화 켜기 시간은 07:20보다 빠르면 안 됩니다.

필드	설명
전화 끄기 유휴 시간 초과	전화기의 전원을 끄기 전에 전화기가 유휴 상태로 머물러야 하는 시간의 길이. 시간 초과는 다음과 같은 상황에서 발생합니다. • 예정대로 전화기가 절전 플러스 모드인 상태에서, 전화기 사용자가 선택 키를 눌러 절전 플러스 모드에서 벗어난 경우 • 연결된 스위치에서 전화기의 전원을 다시 켰을 때 • 전화 끄기 시간이 되었으나 전화기를 사용 중일 때 필드의 범위는 20~1440분입니다. 기본값은 60분입니다.
알림음 사용	활성화되면 전화기에 [전화 끄기 시간] 필드에 지정한 시간보다 10분 전에 알림음을 재생하게 합니다. 알림음으로는 전화기 벨소리를 사용하며, 경고 시간 10분 동안 몇 차례 짧게 재생됩니다. 알림 벨소리는 사용자가 정한 소리 크기로 재생됩니다. 알림음은 다음과 같은 순서로 울립니다. • 전원이 꺼지기 10분 전, 벨소리가 4번 재생됩니다. • 전원이 꺼지기 7분 전, 벨소리가 4번 재생됩니다. • 전원이 꺼지기 4분 전, 벨소리가 4번 재생됩니다. • 전원이 꺼지기 30초 전에 벨소리가 15번 또는 전화기 전원이 꺼질 때까지 재생됩니다. 이 확인란은 [절전 플러스 활성화] 목록 상자에서 1일 이상을 선택한 경우에만 적용됩니다.
EnergyWise 도메인	전화기가 소속된 EnergyWise 도메인입니다. 이 필드의 최대 길이는 127자입니다.
EnergyWise 비밀	EnergyWise 도메인에서 엔드포인트와 통신할 때 사용하는 보안 비밀 암호입니다. 이 필드의 최대 길이는 127자입니다.

필드	설명
EnergyWise 오버라이드 허용	이 확인란은 EnergyWise 도메인 컨트롤러 정책에서 전화기로 전력 수준 업데이트를 전송하도록 허용할 것인지 여부를 결정합니다. 다음과 같은 조건이 적용됩니다. • [절전 플러스 활성화] 필드에서 1일 이상을 선택해야 합니다. • EnergyWise에서 오버라이드를 전송할 때에도 Cisco Unified Communications Manager Administration의 설정은 실행됩니다. 예를 들어 전화 끄기 시간이 22:00(오후 10:00)이고 전화 켜기 시간 필드의 값이 06:00(오전 6:00)라면, 절전 플러스 활성화는 1일 이상을 선택해야 합니다. • EnergyWise에서 전화기에 20:00(오후 8:00)에 전화기를 끄라고 지시하면, 이러한 지시 사항은 구성된 전화 켜기 시간인 오전 6:00까지 효력이 있습니다(전화에 사용자 개입이 전혀 없다고 가정할 경우). • 오전 6:00시가 되면 전화기가 켜지고 Unified Communications Manager Administration 설정에서 전력 수준 변경 내용을 수신하여 작동을 시작합니다. • 전화기의 전력 수준을 다시 변경하려면, EnergyWise에서 새로운 전력 수준 변경 명령을 다시 내려야 합니다. 참고 절전 플러스를 비활성화하려면, [EnergyWise 오버라이드 허용] 확인란을 선택 취소해야 합니다. [EnergyWise 오버라이드 허용]이 선택된 상태에서 [절전 플러스 활성화] 필드에 어떤 날짜도 선택하지 않으면, 절전 플러스는 비활성화되지 않습니다.

단계 **4** 저장을 선택합니다.

단계 **5** 구성 적용을 선택합니다.

단계 **6** 전화기를 다시 시작합니다.

방해사절 설정

방해 사절(DND)이 켜져 있으면 전화 회의 전화기 화면에 있는 헤더가 빨간색입니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서의 방해사절 정보를 참조하십시오.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다.

단계 **2** 구성할 전화기를 검색합니다.

단계 **3** 다음과 같은 파라미터를 설정합니다.

- 방해사절(DND): 이 확인란을 사용하면 전화기에서 방해사절을 활성화할 수 있습니다.
- 방해사절 옵션: 벨소리 꺼짐, 통화 거부 또는 일반 전화기 프로파일 설정 사용.
- 방해사절 착신 전화 알림: 이러한 유형의 알림을 선택하면, 방해사절이 활성화되었을 때 걸려오는 전화에 대해 전화기에서 알림음이 울립니다.

  참고 이 매개변수는 [일반 전화기 프로파일] 창과 [전화기 구성] 창에서 확인할 수 있습니다. 이 중 우선값은 [전화기 구성] 창의 값입니다.

단계 **4** 저장을 선택합니다.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

통화 착신 전환 알림 설정

통화 착신 전환 설정을 제어할 수 있습니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다.

단계 **2** 설정할 전화기를 검색합니다.

단계 **3** [통화 착신 전환 알림] 필드를 구성합니다.

필드	설명
발신자 이름	이 확인란을 선택하면 알림 창에 발신자 이름이 표시됩니다. 기본적으로 이 확인란은 선택이 취소되어 있습니다.
발신자 번호	이 확인란을 선택하면 알림 창에 발신자 번호가 표시됩니다. 기본적으로 이 확인란은 선택되어 있지 않습니다.
재전송된 번호	이 확인란을 선택하면 알림 창에 통화를 마지막으로 착신 전환한 발신자에 관한 정보가 표시됩니다. 예: 발신자 A가 B에게 전화를 걸었으나 B가 모든 전화를 C로 착신 전환했고 C가 모든 통화를 D로 착신 전환했다면, D가 보는 알림 창에는 발신자 C에 관한 전화기 정보가 표시됩니다. 기본적으로 이 확인란은 선택되어 있지 않습니다.

필드	설명
전화 건 번호	이 확인란을 선택하면 알림 창에 해당 통화의 원래 수신자에 관한 정보가 표시됩니다. 예: 발신자 A가 B에게 전화를 걸었으나 B가 모든 전화를 C로 착신 전환했고 C가 모든 통화를 D로 착신 전환했다면, D가 보는 알림 창에는 발신자 B에 관한 전화기 정보가 표시됩니다. 기본적으로 이 확인란은 선택이 취소되어 있습니다.

단계 **4** 저장을 선택합니다.

UCR 2008 설정

Cisco Unified Communications Manager Administration에는 UCR 2008을 지원하는 매개변수가 있습니다. 다음 표에서는 매개변수에 대해 설명하고, 설정을 변경하는 경로를 보여줍니다.

표 ***21: UCR 2008*** 매개변수 위치

매개변수	관리 경로
FIPS 모드	장치 > 장치 설정 > 일반 전화기 프로파일
	시스템 > 엔터프라이즈 전화기 구성
	장치 > 전화기
SSH 액세스	장치 > 전화기
	장치 > 장치 설정 > 일반 전화기 프로파일
웹 액세스	장치 > 전화기
	시스템 > 엔터프라이즈 전화기 구성
	장치 > 장치 설정 > 일반 전화기 프로파일
시스템 > 엔터프라이즈 전화기 구성	장치 > 장치 설정 > 일반 장치 구성
IP 주소 지정 모드	
신호 처리용 IP 주소 지정 모드 기본 설정	장치 > 장치 설정 > 일반 장치 구성

일반 장치 구성에 UCR 2008 설정

이 절차에 따라 다음 UCR 2008 매개변수를 설정합니다.

- IP 주소 지정 모드
- 신호 처리용 IP 주소 지정 모드 기본 설정

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 장치 > 장치 설정 > 일반 장치 구성을 선택합니다.
단계 2 IP 주소 지정 모드 매개변수를 설정합니다.
단계 3 시그널링을 위한 IP 주소 지정 모드 기본 설정 매개변수를 설정합니다.
단계 4 저장을 선택합니다.

일반 전화기 프로파일에 UCR 2008 설정

이 절차에 따라 다음 UCR 2008 매개변수를 설정합니다.

- FIPS 모드
- SSH 액세스
- 웹 액세스

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 장치 > 장치 설정 > 일반 전화기 프로파일을 선택합니다.
단계 2 FIPS 모드 매개변수를 활성화로 설정합니다.
단계 3 SSH 액세스 매개변수를 비활성화로 설정합니다.
단계 4 웹 액세스 매개변수를 비활성화로 설정합니다.
단계 5 80비트 SRTCP 매개변수를 활성화로 설정합니다.
단계 6 저장을 선택합니다.

엔터프라이즈 전화기 구성에 UCR 2008 설정

이 절차에 따라 다음 UCR 2008 매개변수를 설정합니다.

- FIPS 모드
- 웹 액세스

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 시스템 > 엔터프라이즈 전화기 구성을 선택합니다.

단계 2 FIPS 모드 매개변수를 활성화로 설정합니다.

단계 3 웹 액세스 매개변수를 비활성화로 설정합니다.

단계 4 저장을 선택합니다.

전화기에 UCR 2008 설정

이 절차에 따라 다음 UCR 2008 매개변수를 설정합니다.

- FIPS 모드
- SSH 액세스
- 웹 액세스

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다.

단계 2 SSH 액세스 매개변수를 비활성화로 설정합니다.

단계 3 FIPS 모드 매개변수를 활성화로 설정합니다.

단계 4 웹 액세스 매개변수를 비활성화로 설정합니다.

단계 5 저장을 선택합니다.

Expressway를 통한 모바일 및 Remote Access

Expressway를 통한 모바일 및 Remote Access(MRA)를 통해 원격 근로자는 VPN(가상 사설망) 클라이언트 터널을 사용하지 않고도 회사 네트워크에 쉽고 안전하게 연결할 수 있습니다. Expressway는 TLS(Transport Layer Security)를 사용하여 네트워크 트래픽을 보호합니다. 전화기에서 Expressway 인증서를 인증하고 TLS 세션을 구축하려면, 전화기 펌웨어가 신뢰하는 공공 인증 기관에서 Expressway 인증서를 서명해야 합니다. Expressway 인증서를 인증하기 위해 전화기에 다른 CA 인증서를 설치하거나 신뢰할 수 없습니다.

전화기 펌웨어에 추가된 CA 인증서 목록은 http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html 을 참조하십시오.

Expressway를 통한 모바일 및 Remote Access (MRA)는 Cisco Expressway에서 작동합니다. 사용자는 Cisco Expressway 문서(*Cisco Expressway* 관리자 설명서 및 *Cisco Expressway* 기본 구성 구축 설명서 포함)에 익숙해야 합니다. Cisco Expressway 문서는

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html 에서 구할 수 있습니다

Expressway를 통한 모바일 및 Remote Access 사용자에 대해서는 IPv4 프로토콜만 지원됩니다.

Expressway를 통한 모바일 및 Remote Access 작동에 관한 추가 정보는 다음을 참조하십시오.

- *Cisco Preferred Architecture for Enterprise Collaboration, Design Overview(*엔터프라이즈 협업을 위한 *Cisco* 기본 아키텍처, 설계 개요*)*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD(*엔터프라이즈 협업을 위한 *Cisco* 기본 아키텍처, *CVD)*
- *Unified Communications Mobile and Remote Access via Cisco VCS* 구축 설명서
- *Cisco TelePresence Video Communication Server(VCS),* 설정 가이드
- *Cisco Expressway*를 통한 모바일 및 *Remote Access* 구축 설명서

전화기 등록 프로세스 중에 전화기는 표시된 날짜 및 시간과 NTP(Network Time Protocol) 서버를 동기화합니다. MRA에서는 날짜 및 시간 동기화를 위해 설계된 NTP 서버의 IP 주소를 찾는 데 DHCP 옵션 42 태그를 사용합니다. 구성 정보에서 DHCP 옵션 42 태그를 찾지 못하면, 전화기는 NTP 서버 확인을 위해 0.tandberg.pool.ntp.org 태그를 검색합니다.

등록 이후 전화기는 Cisco Unified Communications Manager 전화기 구성에 NTP 서버가 구성되어 있지 않으면 SIP 메시지의 정보를 사용해 표시된 날짜 및 시간을 동기화합니다.

참고 전화기의 전화기 보안 프로파일에 [TFTP 암호화 구성]이 선택되어 있으면 모바일 및 Remote Access로 전화기를 사용할 수 없습니다. MRA 솔루션은 CAPF(Certificate Authority Proxy Function)와 상호 작용하는 장치를 지원하지 않습니다.

MRA에는 SIP OAuth 모드가 지원됩니다. 이 모드를 사용하면 보안 환경에서 인증을 위해 OAuth 액세스 토큰을 사용할 수 있습니다.

참고 MRA(모바일 및 Remote Access) 모드의 SIP OAuth의 경우 전화기를 구축할 때 모바일 및 Remote Access를 사용하여 활성화 코드 온보딩만 사용합니다. 사용자 이름 및 암호를 사용한 활성화는 지원되지 않습니다.

SIP OAuth 모드를 사용하려면 Expressway x14.0(1) 이상 또는 Cisco Unified Communications Manager 14.0(1) 이상이 필요합니다.

SIP OAuth 모드에 대한 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서 릴리스 14.0(1) 이상을 참조하십시오.

구축 시나리오

다음 표에는 Expressway를 통한 모바일 및 Remote Access에 대한 다양한 배포 시나리오가 나와 있습니다.

시나리오	작업
온프레미스 사용자는 Expressway를 통한 모바일 및 Remote Access를 구축한 후 엔터프라이즈 네트워크에 로그인합니다.	엔터프라이즈 네트워크가 감지되면, 전화기가 정상적으로 Cisco Unified Communications Manager에 등록합니다.
오프프레미스 사용자는 Expressway를 통한 모바일 및 Remote Access를 통해 엔터프라이즈 네트워크에 로그인합니다.	전화기가 오프프레미스 모드에 들어간 것을 감지하면 Expressway를 통한 모바일 및 Remote Access 로그인 창이 나타나고, 사용자가 회사 네트워크에 연결합니다. 사용자가 네트워크에 연결하려면 유효한 서비스 이름, 사용자 이름 및 암호가 필요합니다. 또한 사용자가 회사 네트워크에 액세스하려면 서비스 모드를 재설정하여 대체 TFTP 설정을 지워야 합니다. 전화기에서 오프 프레미스 네트워크를 감지하도록 대체 TFTP 서버 설정이 지워집니다. 전화기가 바로 사용할 수 있게 구현된다면, [네트워크 설정] 요구 사항을 재설정을 생략할 수도 있습니다. 사용자가 네트워크 라우터에 DHCP 옵션 150 또는 옵션 66을 활성화했다면, 회사 네트워크에 로그인하지 못할 수도 있습니다. 사용자는 이러한 DHCP 설정을 비활성화하거나 고정 IP 주소를 직접 구성해야 합니다.

Expressway 로그인을 위해 사용자 자격 증명 영구 구성

사용자가 Expressway를 통한 모바일 및 Remote Access로 네트워크에 로그인하면 서비스 도메인, 사용자 이름 및 암호를 입력하라는 메시지가 표시됩니다. Expressway 로그인을 위한 사용자 자격 증명 영구 매개변수를 활성화하면, 이 정보를 다시 입력할 필요가 없도록 사용자 로그인 자격 증명이 저장됩니다. 이 매개변수는 기본적으로 비활성화되어 있습니다.

단일 전화기, 전화기 그룹 또는 모든 전화기에 대해 사용할 인증서를 설정할 수 있습니다.

관련 항목

전화기 기능 구성, 99 페이지
제품별 구성, 102 페이지

문제 보고서 도구

사용자는 문제 보고서 도구를 사용해 관리자에게 문제 보고서를 제출합니다.

참고 문제를 해결할 때 Cisco TAC에서는 문제 보고서 도구 로그를 요구합니다. 전화기를 다시 시작하면 로그가 지워집니다. 전화기를 다시 시작하기 전에 로그를 수집합니다.

문제 보고서를 작성하려면, 사용자는 문제 보고서 도구에 액세스하여 문제가 발생한 날짜 및 시간과 문제에 대한 설명을 입력해야 합니다.

PRT 업로드에 실패하는 경우, 다음 URL(**http://<phone-ip-address>/FS/<prt-file-name>**)에서 전화기용 PRT 파일에 액세스할 수 있습니다. 다음과 같은 경우 이 URL이 전화기에 표시됩니다.

- 전화기가 공장 기본 설정 상태에 있는 경우. URL은 1시간 동안 활성화 상태입니다. 1시간이 경과하면 사용자는 전화기 로그 제출을 다시 시도해야 합니다.
- 전화기가 구성 파일을 다운로드했다면, 통화 제어 시스템에서 전화기에 대한 웹 액세스를 허용합니다.

Cisco Unified Communications Manager의 고객 지원 업로드 **URL** 필드에 서버 주소를 추가해야 합니다.

Expressway를 통해 [모바일 및 Remote Access]로 장치를 구축하고 있다면, Expressway 서버의 [HTTP 서버 허용] 목록에 PRT 서버 주소도 추가해야 합니다.

고객 지원 업로드 **URL** 구성

PRT 파일을 수신하려면 업로드 스크립트가 있는 서버를 사용해야 합니다. PRT는 업로드에 포함된 다음과 같은 매개변수와 함께 HTTP POST 메커니즘을 사용합니다(다중 MIME 인코딩 활용).

- devicename(예: "SEP001122334455")
- serialno(예: "FCH12345ABC")
- 사용자 이름(Cisco Unified Communications Manager에 구성되어 있는 사용자 이름, 장치 소유자)
- prt_file(예: "probrep-20141021-162840.tar.gz")

샘플 스크립트는 아래와 같습니다. 이 스크립트는 참조용으로만 제공됩니다. Cisco는 고객 서버에 설치된 업로드 스크립트에 대한 지원은 제공하지 않습니다.

```
<?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.");
}

?>
```

참고 전화기는 HTTP URL만 지원합니다.

프로시저

단계 **1** PRT 업로드 스크립트를 실행할 수 있는 서버를 설정합니다.

단계 **2** 위에 나온 매개변수를 처리할 수 있는 스크립트를 작성하거나, 요구 사항에 맞는 제공된 샘플 스크립트를 편집합니다.

단계 **3** 서버에 스크립트를 업로드합니다.

단계 **4** Cisco Unified Communications Manager에서 [개별 장치 구성] 창, [일반 전화 프로파일] 창 또는 [엔터프라이즈 전화기 구성] 창의 [제품별 구성 레이아웃] 영역으로 이동합니다.

단계 **5** 고객 지원 업로드 **URL**을 선택하고 업로드 서버 URL을 입력합니다.

예제**:**

http://example.com/prtscript.php

단계 **6** 변경 내용을 저장합니다.

회선에 대한 레이블 설정

전화기에 디렉터리 번호 대신 텍스트 레이블을 표시하도록 설정할 수 있습니다. 이 레이블을 사용하면 이름이나 기능별로 회선을 확인할 수 있습니다. 예를 들어 사용자가 전화기에서 회선을 공유한다면, 회선을 공유하는 사람의 이름으로 회선을 식별할 수 있습니다.

레이블을 키 확장 모듈에 추가할 때 회선에 처음 25자만 표시됩니다.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다.

단계 **2** 구성할 전화기를 검색합니다.

단계 **3** 회선 인스턴스를 찾아 [회선 텍스트 레이블] 필드를 설정합니다.

단계 **4** (선택 사항) 다른 장치 공유 회선에 레이블을 적용해야 한다면, [공유 장치 설정 업데이트] 확인란을 선택하고 선택 항목 전파를 클릭합니다.

단계 **5** 저장을 선택합니다.

10 장

회사 및 개인 디렉터리

회사 디렉터리 설정

회사 디렉터리를 통해 사용자는 동료의 전화 번호를 검색할 수 있습니다. 이 기능을 지원하려면 회사 디렉터리를 구성해야 합니다.

Cisco Unified Communications Manager에서는 LDAP(Lightweight Directory Access Protocol) 디렉터리를 사용해 Cisco Unified Communications Manager과 상호 작용하는 Cisco Unified Communications Manager 애플리케이션 사용자에 관한 인증 정보를 저장합니다. 인증은 시스템에 액세스할 수 있는 사용자 권한을 제공합니다. 인증은 특정 전화 내선 번호와 같이 사용자에게 사용이 허용된 텔레포니 리소스를 확인합니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

LDAP 디렉터리 구성이 끝나면, 사용자는 자신의 전화기에서 회사 디렉터리 서비스를 사용해 회사 디렉터리에서 사용자를 검색할 수 있습니다.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

개인 디렉터리 설정

개인 디렉터리를 사용하면 사용자가 개인 번호를 저장할 수 있습니다.

개인 디렉터리는 다음과 같은 기능으로 구성됩니다.

- PAB(개인 주소록)
- 바로 호출

사용자는 다음과 같은 방법을 사용해 개인 디렉터리 기능에 액세스할 수 있습니다.

- 웹 브라우저에서 - 사용자는 Cisco Unified Communications 셀프 서비스 포털에서 PAB 및 단축 다이얼 기능에 액세스할 수 있습니다.
- Cisco IP 전화기에서 - 회사 디렉터리 또는 사용자 개인 디렉터리를 검색할 연락처를 선택합니다.

웹 브라우저에서 개인 디렉터리를 구성하려는 사용자는 셀프 서비스 포털에 액세스해야 합니다. 관리자는 사용자에게 URL과 로그인 정보를 제공해야 합니다.

IV 부

Cisco IP 전화회의 전화기 문제 해결

11 장

전화기 시스템 모니터링

전화기 시스템 모니터링 개요

전화기 웹 페이지와 전화기의 [전화기 상태] 메뉴를 사용하면 전화기에 관한 다양한 정보를 확인할 수 있습니다. 다음과 같은 정보를 확인할 수 있습니다.

- 장치 정보
- 네트워크 설정 정보
- 네트워크 통계
- 장치 로그
- 스트리밍 통계

이 장에서는 전화기 웹 페이지에서 확보할 수 있는 정보에 관해 설명합니다. 이 정보를 사용하면 원격으로 전화기 작동을 모니터링하고 문제 해결을 지원할 수 있습니다.

관련 항목

전화기 문제 해결, 163 페이지

Cisco IP 전화기 상태

다음 장에서는 Cisco IP 전화기에서 모델 정보, 상태 메시지 및 네트워크 통계를 확인하는 방법을 설명합니다.

- 모델 정보: 전화기에 대한 하드웨어 및 소프트웨어 정보를 표시합니다.

- 상태 메뉴: 현재 통화의 상태 메시지, 네트워크 통계 및 통계를 표시하는 화면에 액세스할 수 있습니다.

이 화면에 표시되는 정보를 사용하면 전화기 작동을 모니터링하고 문제 해결을 지원할 수 있습니다.

전화기 웹 페이지에서도 원격으로 이러한 많은 정보와 기타 관련 정보를 확보할 수 있습니다.

[전화기 정보] 창 표시

프로시저

단계 **1** 설정 > 시스템 정보를 누릅니다.
단계 **2** 메뉴를 종료하려면 종료를 누릅니다.

상태 메뉴 표시

프로시저

단계 **1** 설정 > 상태를 누릅니다.
단계 **2** 메뉴를 종료하려면 종료를 누릅니다.

[상태 메시지] 창 표시

프로시저

단계 **1** 설정 > 상태 > 상태 메시지를 누릅니다.
단계 **2** 메뉴를 종료하려면 종료를 누릅니다.

상태 메시지 필드

다음 표에서는 전화기의 상태 메시지 화면에 나타난 상태 메시지에 관해 설명합니다.

표 *22: Cisco IP* 전화기의 상태 메시지

메시지	설명	이유 설명 및 조치
DHCP에서 IP 주소를 획득할 수 없습니다.	전화기가 DHCP 서버에서 이전에 IP 주소를 받지 않았습니다. 이는 독립적으로 또는 초기 재설정을 수행할 때 발생할 수 있습니다.	DHCP 서버를 사용할 수 있고 IP 수 있는지 확인합니다.
TFTP 크기 오류	전화기의 파일 시스템에 비해 구성 파일이 너무 큽니다.	전화기 전원을 껐다가 다시 켭니
ROM 체크섬 오류	다운로드한 소프트웨어 파일이 손상되었습니다.	전화기 펌웨어에서 새 사본을 확 에 저장합니다. TFTP 서버 소프트 디렉터리에 파일을 복사만 해야 일이 손상될 수 있습니다.
중복 IP	또 다른 장치에서 해당 전화기에 할당된 IP 주소를 사용하고 있습니다.	전화기에 고정 IP 주소가 있다면, 지 않았는지 확인합니다. DHCP를 사용 중이라면 DHCP 서
CTL 및 ITL 파일 지우기	CTL이나 ITL 파일이 지워집니다.	없음 이 메시지는 정보 제공용일

로케일 업데이트 오류	TFTP 경로 디렉터리에서 1개 이상의 현지화 파일을 찾을 수 없거나 파일이 유효하지 않습니다. 로케일이 변경되지 않았습니다.	Cisco Unified Operating System Ad 일 관리의 하위 디렉터리에 다음 지 확인합니다.
		• 네트워크 로케일과 동일한 이 장된 파일:
		  • tones.xml
		• 사용자 로케일과 동일한 이름 된 파일:
		  • glyphs.xml
		  • dictionary.xml
		  • kate.xml

메시지	설명	이유 설명 및 조치
파일을 찾을 수 없음 <Cfg File>	TFTP 서버에 이름 기반의 기본 구성 파일이 없습니다.	Cisco Unified Communications Manag 화기가 추가되면 전화기에 대한 구성 그런데 Cisco Unified Communication 스에 전화기가 존재하지 않으면, TF 을 찾을 수 없음이라는 응답을 생 • 전화기가 Cisco Unified Commun 록되어 있지 않습니다. 전화기의 자동 등록을 허용하지 Communications Manager에 수동 야 합니다. • DHCP를 사용하고 있다면, DHC 버를 지정하고 있는지 확인합니 • 고정 IP 주소를 사용하고 있다면 인합니다.
파일을 찾을 수 없습니다. <CTLFile.tlv>	이 메시지는 Cisco Unified Communications Manager 클러스터가 보안 모드가 아닐 때 전화기에 표시됩니다.	별 다른 영향은 없습니다. 문제 없이 Communications Manager에 전화기를
IP 주소 해제됨	전화기가 IP 주소를 해제하도록 구성되어 있습니다.	전원을 껐다 켜거나 DHCP 주소를 재 상태로 남아 있습니다.
IPv4 DHCP 시간 초과	IPv4 DHCP 서버가 응답하지 않았습니다.	네트워크 사용 중: 네트워크 로드가 체적으로 해결됩니다. IPv4 DHCP 서버와 전화기 사이의 네 지 않음: 네트워크 연결을 확인합니 IPv4 DHCP 서버 중단: IPv4 DHCP 서 오류 지속: 고정 IPv4 주소 할당을 고
IPv6 DHCP 시간 초과	IPv6 DHCP 서버가 응답하지 않았습니다.	네트워크 사용 중 - 네트워크 로드가 체적으로 해결됩니다. IPv6 DHCP 서버와 전화기 사이의 네 지 않음: 네트워크 연결을 확인합니 IPv6 DHCP 서버 중단: IPv6 DHCP 서 오류 지속: 고정 IPv6 주소 할당을 고

메시지	설명	이유 설명 및 조치
IPv4 DNS 시간 초과	IPv4 DNS 서버가 응답하지 않았습니다.	네트워크 사용 중: 네트워크 로드 체적으로 해결됩니다. IPv4 DNS 서버와 전화기 사이의 않음: 네트워크 연결을 확인합니 IPv4 DNS 서버 중단: IPv4 DNS
IPv6 DNS 시간 초과	IPv6 DNS 서버가 응답하지 않았습니다.	네트워크 사용 중: 네트워크 로드 체적으로 해결됩니다. IPv6 DNS 서버와 전화기 사이의 않음: 네트워크 연결을 확인합니 IPv6 DNS 서버 중단: IPv6 DNS
DNS에서 확인할 수 없는 IPv4 호스트	IPv4 DNS에서 TFTP 서버나 Cisco Unified Communications Manager의 이름을 확인할 수 없습니다.	IPv4 DNS에 TFTP 서버나 Cisco U Manager의 호스트 이름이 적절히 합니다. 호스트 이름이 아닌 IPv4 주소 사
DNS에서 확인할 수 없는 IPv6 호스트	IPv6 DNS에서 TFTP 서버나 Cisco Unified Communications Manager의 이름을 확인할 수 없습니다.	IPv6 DNS에 TFTP 서버나 Cisco U Manager의 호스트 이름이 적절히 합니다. 호스트 이름이 아닌 IPv6 주소 사
거부된 HC 로드	다운로드된 애플리케이션이 전화기 하드웨어와 호환되지 않습니다.	전화기의 하드웨어 변경 사항을 버전을 전화기에 설치하려고 할 전화기에 할당된 로드 ID를 확인 Communications Manager에서 장 에 표시되는 로드를 다시 입력합
기본 라우터 없음	DHCP 또는 고정 구성에서 기본 라우터를 지정하지 않았습니다.	전화기에 고정 IP 주소가 있다면, 있는지 확인합니다. DHCP를 사용하고 있다면, DHCP 제공하지 않은 것입니다. DHCP
IPv4 DNS 서버가 없음	이름이 지정되었으나, DHCP 또는 고정 IP 구성에서 IPv4 DNS 서버 주소를 지정하지 않은 경우입니다.	전화기에 고정 IP 주소가 있다면, 어 있는지 확인합니다. DHCP를 사용하고 있다면, DHCP 를 제공하지 않은 것입니다. DHC 다.

메시지	설명	이유 설명 및 조치
IPv6 DNS 서버가 없음	이름이 지정되었으나, DHCP 또는 고정 IP 구성에서 IPv6 DNS 서버 주소를 지정하지 않은 경우입니다.	전화기에 고정 IP 주소가 있다면, IPv 어 있는지 확인합니다. DHCP를 사용하고 있다면, DHCP 서 를 제공하지 않은 것입니다. DHCP 서 다.
설치된 신뢰 목록이 없음	전화기에 CTL 파일이나 ITL 파일이 설치되어 있지 않습니다.	Cisco Unified Communications Manag 되어 있지 않아서, 디폴트로 보안을 신뢰 목록이 구성되어 있지 않습니다 신뢰 목록에 관한 자세한 내용은 해 Communications Manager 릴리스용 문
전화기를 등록하지 못했습니다. 인증서의 키 크기가 FIPS와 호환되지 않습니다.	FIPS는 RSA 서버 인증서가 2048비트 이상일 것을 요구합니다.	인증서를 업데이트합니다.
Cisco Unified Communications Manager에서 재시작 요청	Cisco Unified Communications Manager의 요청에 따라 전화기를 재시작합니다.	Cisco Unified Communications Manag 변경을 했을 가능성이 높습니다. 그 하기 위해 구성 적용이 눌러졌을 것
TFTP 액세스 오류	TFTP 서버에서 존재하지 않는 디렉터리를 지정하고 있습니다.	DHCP를 사용하고 있다면, DHCP에서 지정하고 있는지 확인합니다. 고정 IP 주소를 사용하고 있다면, TF 니다.
TFTP 오류	전화기에서 TFTP 서버가 제공한 오류 코드를 인식하지 못합니다.	Cisco TAC에 문의하십시오.
TFTP 시간 초과	TFTP 서버가 응답하지 않았습니다.	네트워크 사용 중: 네트워크 로드가 체적으로 해결됩니다. TFTP 서버와 전화기 사이의 네트워크 음: 네트워크 연결을 확인합니다. TFTP 서버 중단: TFTP 서버 구성을
시간 초과	802.1X 트랜잭션을 시도했으나 인증자의 부재로 시간이 초과되었습니다.	스위치에 802.1X가 구성되어 있지 않 이 초과됩니다.

메시지	설명	이유 설명 및 조치
신뢰 목록 업데이트 실패	CTL 및 ITL 파일 업데이트에 실패했습니다.	전화기에 CTL 및 ITL 파일이 설치 파일을 업데이트하는 데 실패했습 가능한 실패 이유: • 네트워크 문제가 발생했습니 • TFTP 서버가 중단되었습니다 • CTL 파일을 서명하는 데 사용 일을 서명하는 데 사용된 TF 만, 현재 전화기의 CTL 및 IT 니다. • 내부 전화기 문제가 발생했습 가능한 해결 방법: • 네트워크 연결을 확인합니다 • TFTP 서버가 활성화되었고 작 지 확인합니다. • Cisco Unified Communication TVS(Transactional Vsam Serv TVS 서버가 활성화되어 정상 합니다. • 보안 토큰과 TFTP 서버가 유 앞의 모든 해결 방법이 실패했다면 으로 삭제한 다음 전화기를 재설 신뢰 목록에 관한 자세한 내용은 Communications Manager 릴리스
신뢰 목록 업데이트	CTL 파일이나 ITL 파일 또는 두 파일 모두 업데이트되었습니다.	없음 이 메시지는 정보 제공용일 신뢰 목록에 관한 자세한 내용은 Communications Manager 릴리스
버전 오류	전화기 로드 파일의 이름이 잘못되었습니다.	전화기 로드 파일의 이름이 정확
XmlDefault.cnf.xml 또는 전화기 장치 이름에 해당하는 .cnf.xml	구성 파일의 이름입니다.	없음 이 메시지에는 전화기를 위 시됩니다.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

[네트워크 통계] 창 표시

프로시저

단계 **1** 설정 > 상태 > 네트워크 통계를 누릅니다.
단계 **2** 메뉴를 종료하려면 종료를 누릅니다.

네트워크 통계 필드

다음 표에서는 네트워크 통계 화면에 포함되어 있는 정보에 관해 설명합니다.

표 ***23:*** 네트워크 통계 필드

항목	설명
Tx Frames	전화기에서 전송한 패킷 수
Tx broadcast	전화기에서 전송한 브로드캐스트 패킷 수
Tx unicast	전화기에서 전송한 총 유니캐스트 패킷 수
Rx Frames	전화기에서 수신한 패킷 수
Rx broadcast	전화기에서 수신한 브로드캐스트 패킷 수
Rx unicast	전화기에서 수신한 총 유니캐스트 패킷 수
CDP 인접 장치 ID	CDP 프로토콜이 발견한 이 포트에 연결된 장치 식별자
CDP 인접 IP 주소	CDP 프로토콜이 IP를 사용하여 발견한 이 포트에 연결된 장치 식별자
CDP 인접 포트	CDP 프로토콜이 발견한 이 포트에 연결된 장치 식별자

항목	설명
재시작 이유: 다음 중 하나입니다. • 하드웨어 재설정 (전원 켜기 재설정) • 소프트웨어 재설정(메모리 컨트롤러도 재설정) • 소프트웨어 재설정(메모리 컨트롤러는 재설정 안 함) • Watchdog 재설정 • 초기화됨 • 알 수 없음	전화기를 가장 최근에 재설정한 이유
포트 1	네트워크 포트 연결 및 링크 상태(예: **100 Full**은 PC 포트가 연결 상태고, 자동 설정된 전이중, 100-Mbps 연결 상태라는 뜻입니다.)
IPv4	DHCP 상태에 관한 정보입니다. 여기에는 다음과 같은 상태가 포함됩니다. • 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

항목	설명
IPv6	

항목	설명
	DHCP 상태에 관한 정보입니다. 여기에는 다음과 같은 상태가 포함됩니다. • 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

항목	설명

[통화 통계] 창 표시

프로시저

단계 **1** 설정 > 상태 > 통화 통계를 누릅니다.
단계 **2** 메뉴를 종료하려면 종료를 누릅니다.

통화 통계 필드

다음 표에서는 통화 통계 화면에 포함되어 있는 항목에 관해 설명합니다.

표 ***24:*** 통화 통계 항목

항목	설명
수신자 코덱	수신된 음성 스트림의 유형(코덱으로부터의 RTP 스트리밍 오디오): • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
송신자 코덱	전송한 음성 스트림의 유형(코덱으로부터의 RTP 스트리밍 오디오): • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS

항목	설명
수신자 크기	수신 음성 스트림(RTP 스트리밍 오디오)의 음성 패킷 크기, 밀리초 단위
송신자 크기	송신 음성 스트림의 음성 패킷 크기, 밀리초 단위
수신자 패킷	음성 스트림이 개방된 이후 수신한 RTP 음성 패킷 수 참고 이 수는 통화가 대기 중 상태였을 수도 있기 때문에 통화가 시작되고 수신한 RTP 음성 패킷의 수와 일치할 필요는 없습니다.
송신자 패킷	음성 스트림이 개방된 이후 전송한 RTP 음성 패킷 수 참고 이 수는 통화가 대기 중 상태였을 수도 있기 때문에 통화가 시작되고 전송한 RTP 음성 패킷의 수와 일치할 필요는 없습니다.
평균 지터	수신 음성 스트림이 개방된 이후 관찰된 RTP 패킷 지터 예상 평균, 밀리초 단위(네트워크를 통해 이동할 때 패킷이 겪는 동적 지연 현상).
최대 지터	수신 음성 스트림이 개방된 이후 관찰된 최대 지터, 밀리초 단위
수신자 폐기됨	수신 음성 스트림에서 폐기된 RTP 패킷 수(잘못된 패킷이나 너무 늦은 패킷 등) 참고 전화기는 Cisco Gateways에서 생성한 페이로드 유형 19 통신 소음(comfort noise) 패킷을 폐기합니다. 해당 패킷이 이 수치를 높이기 때문입니다.
수신자 손실 패킷	누락된 RTP 패킷(전송 중 상실)
음질 메트릭	
누적 숨김률	음성 스트림을 시작하고 수신한 총 스피치 프레임(speech frame) 수로 숨긴 전체 프레임의 수를 나눈 값
간격 숨김률	활성 스피치 앞의 3초 간격 동안 스피치 프레임에 포함된 숨김 프레임 비율. VAD(voice activity detection)를 사용하면, 3초의 활성 스피치를 모으는 데 더 긴 시간이 필요할 수도 있습니다.
최대 숨김률	음성 스트림을 시작한 이후 가장 높은 간격 숨김률
숨김(초)	음성 스트림을 시작한 이후 숨김 이벤트가 발생한 시간(초 단위, 엄격하게 숨겨진 시간이 포함됨)
엄격한 숨김(초)	음성 스트림을 시작한 이후 5%가 넘는 숨김 이벤트(손실 프레임)가 발생한 시간(초 단위)

항목	설명
대기 시간	밀리초 단위로 표시되는 네트워크 대기 시간 추정치. RTCP 수신자 보고서 차단이 수신되었을 때 측정된 왕복 지연 실행 평균을 나타냅니다.

Cisco IP 전화기 웹 페이지

각 Cisco IP 전화기에는 다음을 비롯해 전화기에 관한 다양한 정보를 확인할 수 있는 웹 페이지가 있습니다.

- 장치 정보: 장치 설정과 전화기 관련 정보가 표시됩니다.
- 네트워크 설정: 네트워크 설정 정보 및 기타 전화기 설정에 관한 정보가 나와 있습니다.
- 네트워크 통계: 네트워크 트래픽에 관한 정보를 제공하는 하이퍼링크를 표시합니다.
- 장치 로그: 문제 해결에 사용할 수 있는 정보를 제공하는 하이퍼링크를 표시합니다.
- 스트리밍 통계: 다양한 스트리밍 통계에 대한 하이퍼링크를 표시합니다.

이 장에서는 전화기 웹 페이지에서 확보할 수 있는 정보에 관해 설명합니다. 이 정보를 사용하면 원격으로 전화기 작동을 모니터링하고 문제 해결을 지원할 수 있습니다.

이러한 정보 중 다수는 전화기에서 직접 수집할 수도 있습니다.

전화기 웹페이지 액세스

참고 웹 페이지에 액세스할 수 없다면, 기본적으로 비활성화되어 있을 수 있습니다.

프로시저

단계 **1** 다음 중 한 가지 방법을 사용해 Cisco IP 전화기의 IP 주소를 확보합니다.

a) 장치 > 전화기를 선택하여 Cisco 통합 커뮤니케이션 매니저 관리에서 전화기를 검색합니다. Cisco Unified Communications Manager에 등록한 전화기는 [전화기 찾기 및 나열] 창과 [전화기 구성] 창 상단에 IP 주소를 표시합니다.

b) 전화기에서 설정 > 시스템 정보를 선택하고 IPv4 주소 필드로 스크롤합니다.

단계 **2** 웹 브라우저를 열고, 다음 URL을 입력합니다. 여기서 *IP_address*는 Cisco IP 전화기의 IP 주소입니다.

http://<IP_address>

장치 정보 웹 페이지

전화기 웹 페이지의 [장치 정보] 영역에는 장치 설정과 전화기 관련 정보가 표시됩니다. 해당 항목이 아래 표에 정리되어 있습니다.

[장치 정보] 영역을 표시하려면 전화기의 웹 페이지에 액세스한 다음, 장치 정보 하이퍼링크를 클릭합니다.

표 ***25:*** 장치 정보 웹 페이지 필드

필드	설명
서비스 모드	전화기에 대한 서비스 모드입니다.
서비스 도메인	서비스에 대한 도메인입니다.
서비스 상태	서비스의 현재 상태입니다.
MAC 주소	전화기의 MAC(Media Access Control) 주소입니다.
호스트 이름	MAC 주소를 기반으로 전화기에 자동 할당된 고정된 고유한 이름
전화 번호	전화기에 할당된 디렉터리 번호
애플리케이션 로드 ID	애플리케이션 로드 버전을 식별합니다.
부트 로드 ID	부트 로드 버전을 표시합니다.
버전	전화기에서 실행되는 펌웨어 식별자
하드웨어 개정	전화기 하드웨어 마이너 개정 값
일련 번호	전화기의 고유 일련 번호
모델 번호	전화기의 모델 번호
메시지 대기 중	이 전화기의 기본 회선에 음성 메시지가 대기 중인지 알려줍니다.
UDI	다음과 같은 전화기의 Cisco UDI(Unique Device Identifier) 정보를 표시합니다. • 하드웨어 유형 • 전화기 모델 이름 • 제품 ID • 버전 ID(VID) - 주요 하드웨어 버전 번호를 지정합니다. • 일련 번호

필드	설명
시간	전화기가 속한 날짜/시간 그룹의 시간. 이 정보는 Cisco Unified Communications Manager에서 제공합니다.
표준 시간대	전화기가 속한 날짜/시간 그룹의 시간대. 이 정보는 Cisco Unified Communications Manager에서 제공합니다.
날짜	전화기가 속한 날짜/시간 그룹의 날짜. 이 정보는 Cisco Unified Communications Manager에서 제공합니다.
시스템 사용 가능 메모리	사용 가능한 시스템 메모리 용량
Java Heap 사용 가능 메모리	Java Heap의 사용 가능한 메모리 용량
Java Pool 사용 가능 메모리	Java Pool의 사용 가능한 메모리 용량
FIPS 모드 활성화	FIPS(Federal Information Processing Standard) 모드의 활성화 여부를 표시합니다.

네트워크 설정 웹 페이지

전화기 웹 페이지의 [네트워크 설정] 영역에는 네트워크 설정 정보 및 기타 전화기 설정에 관한 정보가 나와 있습니다. 해당 항목이 아래 표에 정리되어 있습니다.

Cisco IP 전화기의 네트워크 설정 메뉴에서도 이와 같은 많은 항목을 확인 및 설정할 수 있습니다.

[네트워크 설정] 영역을 표시하려면 전화기의 웹 페이지에 액세스한 다음, 네트워크 설정 하이퍼링크를 클릭하십시오.

표 ***26:*** 네트워크 설정 항목

항목	설명
MAC 주소	전화기의 MAC(Media Access Control) 주소입니다.
호스트 이름	DHCP 서버가 전화기에 할당한 호스트 이름입니다.
도메인 이름	전화기가 위치한 DNS(Domain Name System) 도메인의 이름입니다.
DHCP 서버	전화기가 IP 주소를 받는 DHCP(Dynamic Host Configuration Protocol) 서버의 IP 주소입
BOOTP 서버	전화기가 BootP(Bootstrap Protocol) 서버에서 구성을 받는지 알려줍니다.
DHCP	전화기에서 DHCP를 사용하는지를 알려줍니다.
IP 주소	전화기의 IP(인터넷 프로토콜) 주소입니다.

항목	설명
서브넷 마스크	전화기가 사용하는 서브넷 마스크입니다.
기본 라우터 1	전화기가 사용하는 기본 라우터입니다.
DNS 서버 1–3	전화기가 사용하는 기본 DNS 서버 (DNS Server 1)와 옵션 항목인 백업 DNS 서버(D 및 3)입니다.
대체 TFTP	전화기에서 대체 TFTP 서버를 사용하는지 알려줍니다.
TFTP 서버 1	전화기에서 사용하는 기본 TFTP(Trivial File Transfer Protocol) 서버입니다.
TFTP 서버 2	전화기에서 사용하는 백업 TFTP(Trivial File Transfer Protocol) 서버입니다.
DHCP 주소 해제됨	[DHCP 주소 해제됨] 옵션 설정을 보여줍니다.
사용 가능한 VLAN ID	전화기가 속해 있는 Cisco Catalyst 스위치에 구성된 사용 가능한 VLAN(Virtual Loca Network)입니다.
관리자 VLAN ID	전화기가 속해 있는 보조 LAN입니다.
Unified CM 1-5	전화기가 등록할 수 있는 Cisco Unified Communications Manager 서버의 호스트 이름 소(우선 순위 순서)입니다. 또한 제한된 Cisco Unified Communications Manager 기능 수 있는 SRST 라우터의 IP 주소가 항목에 표시될 수도 있습니다(해당 라우터가 제공 사용 가능한 서버의 경우 Cisco Unified Communications Manager 서버 IP 주소와 다 하나가 항목에 표시됩니다. • 활성: 전화기가 현재 통화 처리 서비스를 받고 있는 Cisco Unified Communicatio 서버 • 대기: 현재 서버가 서비스를 제공하지 못하는 경우 전화기가 대신 연결하는 Ci Communications Manager 서버 • 공란: Cisco Unified Communications Manager 서버에 현재 연결되어 있지 않음 또한 SRST(Survivable Remote Site Telephony) 지정 사항이 항목에 포함될 수 있습니 사항을 통해 제한된 기능 집합으로 Cisco Unified Communications Manager 기능을 제 는 SRST 라우터를 파악할 수 있습니다. 모든 기타 Cisco Unified Communications Ma 에 연결할 수 없게 되면 이 라우터가 통화 처리를 제어합니다. SRST Cisco Unified Com Manager는 항상 서버 목록의 마지막에 표시됩니다(활성 상태인 경우도 마찬가지입 우터 주소는 [Cisco Unified Communications Manager Configuration] 창의 [장치 풀] 섹 성할 수 있습니다.
정보 URL	전화기에 표시되는 도움말 텍스트의 URL입니다.
디렉터리 URL	전화기에서 디렉터리 정보를 가져오는 서버의 URL입니다.
메시지 URL	전화기에서 메시지 서비스를 가져오는 서버의 URL입니다.
서비스 URL	전화기에서 Cisco IP 전화기 서비스를 가져오는 서버의 URL입니다.

항목	설명
유휴 URL	[유휴 URL 시간] 필드에 지정한 시간 동안 전화기가 유휴 상태일 때 전화기에서 표시하 입니다. 그리고 이 시간 동안 열리는 메뉴는 없습니다.
유휴 URL 시간	URL에서 지정한 XML 서비스가 활성화되기 전에 전화기가 유휴 상태로 메뉴가 열리지 시간(초 단위)입니다.
프록시 서버 URL	전화기의 HTTP 클라이언트를 대신해 비로컬 호스트 주소에 HTTP 요청을 하고, 비로컬 에서 전화기의 HTTP 클라이언트로 응답을 전송하는 프록시 서버의 URL입니다.
인증 URL	전화기에서 전화기 웹 서버에 생성되는 요청을 확인하는 데 사용하는 URL입니다.
SW 포트 설정	스위치 포트의 속도 및 전이중/반이중: • A = 자동 설정 • 10H = 10-BaseT/반이중 • 10F = 10-BaseT/전이중 • 100H = 100-BaseT/반이중 • 100F = 100-BaseT/전이중 • 1000F = 1000-BaseT/전이중 • 링크 없음= 스위치 포트에 대한 연결 없음
사용자 로케일	전화기 사용자와 관련된 사용자 로케일입니다. 언어, 글꼴, 날짜 및 시간 서식, 영숫자 텍스트 정보 등 자세한 사용자 지원 정보를 식별합니다.
네트워크 로캘	전화기 사용자와 관련된 네트워크 로케일입니다. 전화기에서 사용하는 신호음 및 신호 에 대한 정의를 비롯해, 특정 지역의 자세한 전화기 지원 정보를 식별합니다.
사용자 로케일 버전	전화기에 로드된 사용자 로케일 버전입니다.
네트워크 로케일 버전	전화기에 로드된 네트워크 로케일 버전입니다.
스피커 사용	전화기의 스피커폰 활성화 여부를 알려줍니다.
그룹 수신	전화기에서 그룹 수신 기능이 활성화되어 있는지 여부를 나타냅니다. 그룹 수신을 사용 드셋을 사용하여 말하고 동시에 스피커를 통해 들을 수 있습니다.
GARP 사용	전화기가 Gratuitous ARP 응답에서 MAC 주소를 확보하는지를 보여줍니다.
자동 회선 선택	전화기가 모든 회선에서 수신 전화로 통화 포커스를 전환하는지 여부를 보여줍니다.
통화 제어를 위한 DSCP	통화 제어 신호 처리를 위한 DSCP IP 분류입니다.
구성을 위한 DSCP	전화 구성 호전환을 위한 DSCP IP 분류입니다.
서비스를 위한 DSCP	전화 기반 서비스를 위한 DSCP IP 분류입니다.
보안 모드	전화기에 설정된 보안 모드입니다.

항목	설명
웹 액세스 사용	웹 액세스가 활성(예) 상태인지 비활성(아니요) 상태인지를 알려줍니다.
SSH 액세스 활성화	전화기에서 SSH 연결을 수락하는지 차단하는지를 알려줍니다.
CDP: SW 포트	스위치 포트에 CDP 지원(기본값은 활성화)이 존재하는지를 알려줍니다. 전화기, 전원공급 협상, QoS 관리 및 802.1x 보안용 VLAN 할당에 대해 스위치 포트 활성화합니다. 전화기가 Cisco 스위치에 연결했을 때 스위치 포트의 CDP를 활성화합니다. Cisco Unified Communications Manager에서 CDP가 비활성화되면, 전화기가 Cisco 스위치에 연결된 경우에만 스위치 포트의 CDP를 비활성화해야 한다는 내용의 경 니다. 설정 메뉴에 현재 PC와 스위치 포트 CDP 값이 표시됩니다.
LLDP-MED: SW 포트	스위치 포트에 LLDP-MED(Link Layer Discovery Protocol Media Endpoint Discovery) 어 있는지를 알려줍니다.
LLDP 전원 우선 순위	스위치에 전화기 전원 우선 순위를 알려서 전화기에 전원을 공급할 수 있게 합니다 음과 같습니다. • 알 수 없음: 기본값입니다. • 낮음 • 높음 • 중요
LLDP 자산 ID	인벤토리 관리를 위해 전화기에 할당된 자산 ID를 식별합니다.
CTL 파일	CTL 파일을 식별합니다.
ITL 파일	초기 신뢰 목록이 포함된 ITL 파일입니다.
ITL 서명	CTL과 ITL 파일의 보안 해시 알고리즘(SHA-1)을 사용해 보안을 향상합니다.
CAPF 서버	전화기에서 사용하는 CAPF 서버의 이름입니다.
TVS	기본적인 주요 보안 구성 요소입니다. TVS(Trust Verification Services)는 HTTPS가 는 동안 Cisco 유니파이드 IP 전화기에서 EM 서비스, 디렉터리 및 MIDlet 같은 애플 서버를 인증하게 합니다.
TFTP 서버	전화기에서 사용하는 TFTP 서버의 이름입니다.
자동 포트 동기화	포트를 패킷 손실을 없애는 낮은 속도로 동기화합니다.
스위치 포트 원격 구성	관리자가 Cisco Unified Communications Manager Administration을 사용해 Cisco Des Collaboration Experience 테이블 포트의 속도와 기능을 원격에서 구성할 수 있습니다

항목	설명
PC 포트 원격 구성	PC 포트에 대한 속도 및 반이중/전이중 모드의 원격 포트 구성이 활성화되어 있는지 또 성화되어 있는지를 알려줍니다.
IP 주소 지정 모드	전화기에 제공되는 IP 주소 지정 모드를 표시합니다.
IP 기본 설정 모드 제어	전화기에 IPv4 및 IPv6가 모두 제공될 때, Cisco Unified Communications Manager로 시그 는 동안 전화기가 사용하는 IP 주소 버전을 보여줍니다.
미디어용 IP 기본 설정 모드	미디어를 위해 장치에서 IPv4 주소를 사용해 Cisco Unified Communications Manager에 고 있음을 보여줍니다.
IPv6 자동 구성	전화기의 자동 구성 활성화/비활성화 여부를 표시합니다.
IPv6 DAD	인터페이스에 주소가 할당되기 전, 새 유니캐스트 IPv6 주소의 고유성을 식별합니다.
IPv6의 재전송 메시지 수락	전화기에서 대상 번호에 사용되는 것과 동일한 라우터의 재전송 메시지를 수락하는지 줍니다.
IPv6 멀티캐스트 에코 요청 회신	IPv6 주소로 전송된 에코 요청 메시지에 응답하여 전화기에서 에코 회신 메시지를 전송 를 알려줍니다.
IPv6 로드 서버	전화기 펌웨어 업그레이드를 위한 설치 시간을 최적화하고 이미지를 로컬로 저장해 각 업그레이드를 위해 WAN 링크를 이동할 필요가 없도록 하여 WAN을 오프로드하는 데 니다.
IPv6 로그 서버	전화기가 로그 메시지를 보내는 원격 로깅 시스템의 IP 주소 및 포트를 보여줍니다.
IPv6 CAPF 서버	전화기에서 사용하는 CAPF의 공통 이름(Cisco Unified Communications Manager 인증서 입니다.
DHCPv6	DHCP(Dynamic Host Configuration Protocol)는 네트워크에 장치를 연결할 때 자동으로 IPv6 주소를 할당합니다. Cisco 유니파이드 IP 전화기는 기본적으로 DHCP를 활성화합
IPv6 주소	전화기의 현재 IPv6 주소를 표시하거나 사용자가 새 IPv6 주소를 입력할 수 있게 합니다
IPv6 접두사 길이	서브넷에 대한 현재 접두사 길이를 표시하거나 사용자가 새 접두사 길이를 입력할 수 니다.
IPv6 기본 라우터 1	전화기에서 사용하는 기본 라우터를 표시하거나 사용자가 새 IPv6 기본 라우터를 입력 게 합니다.
IPv6 DNS 서버 1	전화기에서 사용하는 기본 DNSv6 서버를 표시하거나 사용자가 새 서버를 입력할 수 있 다.
IPv6 DNS 서버 2	전화기에서 사용하는 보조 DNSv6 서버를 표시하거나 사용자가 새 보조 DNSv6 서버를 수 있게 합니다.
IPv6 대체 TFTP	사용자가 대체(보조) IPv6 TFTP 서버의 사용을 활성화할 수 있습니다.

항목	설명
IPv6 TFTP 서버 1	전화기에서 사용하는 기본 IPv6 TFTP 서버를 표시하거나 사용자가 새 기본 TFTP 서 할 수 있게 합니다.
IPv6 TFTP 서버 2	기본 IPv6 TFTP 서버를 사용할 수 없게 되었을 때 사용되는 보조 IPv6 TFTP 서버를 사용자가 새 보조 TFTP 서버를 설정할 수 있게 합니다.
IPv6 주소 해제됨	사용자가 IPv6 관련 정보를 해제할 수 있습니다.
Energywise 전력 레벨	EnergyWise 네트워크에서 장치가 사용하는 에너지의 측정값입니다.
Energywise 도메인	전원 모니터링 및 제어를 위한 장치 관리 그룹입니다.

이더넷 정보 웹 페이지

다음 표에서는 이더넷 정보 웹 페이지의 콘텐츠에 관해 설명합니다.

표 ***27:*** 이더넷 정보 항목

항목	설명
Tx Frames	전화기에서 전송하는 총 패킷 수
Tx broadcast	전화기에서 전송하는 총 브로드캐스트 패킷 수
Tx multicast	전화기에서 전송하는 총 멀티캐스트 패킷 수
Tx unicast	전화기에서 전송하는 총 유니캐스트 패킷 수
Rx Frames	전화기에서 수신한 총 패킷 수
Rx broadcast	전화기에서 수신하는 총 브로드캐스트 패킷 수
Rx multicast	전화기에서 수신하는 총 멀티캐스트 패킷 수
Rx unicast	전화기에서 수신하는 총 유니캐스트 패킷 수
Rx PacketNoDes	DMA(Direct Memory Access) 설명자가 유발하지 않은 총 보관 패킷 수

네트워크 웹 페이지

다음 표에서는 네트워크 액세스 웹 페이지에 포함되어 있는 정보에 관해 설명합니다.

참고 네트워크 통계 아래의 네트워크 링크를 클릭하면 페이지 제목이 “포트 정보”로 표시됩니다.

표 *28:* 네트워크 영역 항목

항목	설명
Rx totalPkt	전화기에서 수신한 총 패킷 수
Rx multicast	전화기에서 수신한 총 멀티캐스트 패킷 수
Rx broadcast	전화기에서 수신한 총 브로드캐스트 패킷 수
Rx unicast	전화기에서 수신한 총 유니캐스트 패킷 수
Rx tokenDrop	리소스 부족(예: FIFO 오버플로)으로 인해 중단된 총 패킷 수
Tx totalGoodPkt	전화기에서 수신한 올바른 패킷(멀티캐스트, 브로드캐스트 및 유니캐스트)의 총 수
Tx broadcast	전화기에서 전송한 총 브로드캐스트 패킷 수
Tx multicast	전화기에서 전송한 총 멀티캐스트 패킷 수
LLDP FramesOutTotal	전화기에서 전송한 총 LLDP 프레임 수
LLDP AgeoutsTotal	캐시에서 시간이 초과한 총 LLDP 프레임 수
LLDP FramesDiscardedTotal	필수 TLV가 누락되었거나 문제가 발생한 경우 또는 스트링 길이가 범위를 벗어나 폐기된 총 LLDP 프레임 수
LLDP FramesInErrorsTotal	1개 이상의 발견 가능한 오류와 함께 수신된 총 LLDP 프레임 수
LLDP FramesInTotal	전화기에서 수신한 총 LLDP 프레임 수
LLDP TLVDiscardedTotal	폐기된 총 LLDP TLV 수
LLDP TLVUnrecognizedTotal	전화기에서 인식하지 못한 총 LLDP TLV 수
CDP 인접 장치 ID	CDP가 발견한 이 포트에 연결된 장치 식별자
CDP 인접 IP 주소	CDP가 발견한 인접 장치의 IP 주소
CDP 인접 IPv6 주소	CDP가 발견한 인접 장치의 IPv6 주소
CDP 인접 포트	CDP가 발견한 전화기에 연결된 인접 장치 포트
LLDP 인접 장치 ID	LLDP가 발견한 이 포트에 연결된 장치 식별자
LLDP 인접 IP 주소	LLDP가 발견한 인접 장치의 IP 주소
LLDP 인접 IPv6 주소	CDP가 발견한 인접 장치의 IPv6 주소
LLDP 인접 포트	LLDP가 발견한 전화기에 연결된 인접 장치 포트
포트 정보	속도 및 전이중/반이중 정보

콘솔 로그, 코어 덤프, 상태 메시지 및 디버그 표시 웹 페이지

장치 로그 제목 아래의 콘솔 로그, 코어 덤프, 상태 메시지 및 디버그 표시 하이퍼링크는 전화기를 모니터링하고 문제를 해결하는 데 도움이 되는 정보를 제공합니다.

- 콘솔 로그—개별 로그 파일에 하이퍼링크를 포함합니다. 콘솔 로그 파일에는 전화기가 수신한 디버그 및 오류 메시지가 포함됩니다.
- 코어 덤프—개별 덤프 파일에 하이퍼링크를 포함합니다. 코어 덤프 파일에는 전화기 충돌 데이터가 포함됩니다.
- 상태 메시지—가장 최근에 전화기 전원을 켠 후 현재까지 전화기가 생성한 10개의 가장 최신 상태 메시지가 표시됩니다. 또한 전화기의 [상태 메시지] 화면에서도 이 정보를 가져올 수 있습니다.
- 디버그 표시—문제 해결에 도움이 필요할 경우, Cisco TAC에게 유용할 수도 있는 디버그 메시지를 표시합니다.

스트리밍 통계 웹 페이지

Cisco IP 전화기는 최대 5개의 장치를 대상으로 동시에 정보를 스트리밍할 수 있습니다. 전화기는 통화 중이거나 오디오 또는 데이터를 송수신하는 서비스를 실행 중일 때 정보를 스트리밍합니다.

전화기 웹 페이지의 스트리밍 통계는 스트림에 관한 정보를 제공합니다.

스트리밍 통계를 살펴보려면, 전화기 웹 페이지에 액세스하여 스트림 하이퍼링크를 클릭합니다.

다음 표에서는 스트리밍 통계에 포함되어 있는 항목에 관해 설명합니다.

표 ***29:*** 스트리밍 통계 필드

항목	설명
원격 주소	스트림 대상의 IP 주소 및 UDP 포트
로컬 주소	전화기의 IP 주소 및 UDP 포트
시작 시간	내부 타임 스탬프는 Cisco Unified Communications Manager에서 전화기에 패킷 시작하라고 요청하는 때를 보여줍니다.
스트림 상태	스트리밍이 활성화 상태인지를 표시합니다.
호스트 이름	MAC 주소를 기반으로 전화기에 자동 할당된 고정된 고유한 이름
송신자 패킷	연결을 시작한 이후 전화기에서 전송한 총 RTP 데이터 패킷의 수. 연결이 수신 드로 설정되면 값은 0입니다.
송신자 옥텟	연결을 시작한 이후 전화기가 RTP 데이터 패킷으로 전송한 총 페이로드 옥텟 이 수신 전용 모드로 설정되면 값은 0입니다.
송신자 코덱	전송된 스트림을 위한 오디오 인코딩 유형

항목	설명
전송된 송신자 보고서 (설명 참조)	RTCP 송신자 보고서가 전송된 횟수
송신자 보고서 전송 시간 (설명 참조)	최종 RTCP 송신자 보고서가 전송된 시간에 관한 내부 타임 스탬프 표시
수신자 손실 패킷	이 연결에서 데이터 수신이 시작된 이후 손실된 총 RTP 데이터 패킷의 수. 실제로 한 패킷 수보다 적은 예상 패킷 수로 정의하고, 여기서 수신한 패킷 수에는 지연되 나 중복된 모든 패킷이 포함됩니다. 연결이 송신 전용 모드로 설정되면 값은 0으로 됩니다.
평균 지터	밀리초 단위로 측정되는 RTP 데이터 패킷 도착 간격 시간의 표준 편차 추정치. 연 송신 전용 모드로 설정되면 값은 0으로 표시됩니다.
수신자 코덱	수신된 스트림에 사용된 오디오 인코딩 유형
전송된 수신자 보고서 (설명 참조)	RTCP 수신자 보고서가 전송된 횟수
수신자 보고서 전송 시간 (설명 참조)	RTCP 수신자 보고서가 전송된 시간에 관한 내부 타임 스탬프 표시
수신자 패킷	이 연결에서 데이터 수신이 시작된 이후 수신된 총 RTP 데이터 패킷의 수. 통화가 캐스트 통화인 경우 다양한 소스에서 수신한 패킷이 포함됩니다. 연결이 송신 전 드로 설정되면 값은 0으로 표시됩니다.
수신자 옥텟	연결을 시작한 이후 장치가 RTP 데이터 패킷으로 수신한 총 페이로드 옥텟 수. 통 멀티캐스트 통화인 경우 다양한 소스에서 수신한 패킷이 포함됩니다. 연결이 송신 모드로 설정되면 값은 0으로 표시됩니다.
누적 숨김률	음성 스트림을 시작하고 수신한 총 스피치 프레임(speech frame) 수로 숨긴 전체 프 의 수를 나눈 값
간격 숨김률	활성 스피치 앞의 3초 간격 동안 스피치 프레임에 포함된 숨김 프레임 비율. VAD(activity detection)가 사용되면, 3초의 활성 스피치를 모으는 데 더 긴 시간이 필요할 있습니다.
최대 숨김률	음성 스트림을 시작한 이후 가장 높은 간격 숨김률
숨김(초)	음성 스트림을 시작한 이후 숨김 이벤트가 발생한 시간(초 단위, 엄격하게 숨겨진 이 포함됨)
엄격한 숨김(초)	음성 스트림을 시작한 이후 5%가 넘는 숨김 이벤트(손실 프레임)가 발생한 시간(위)

항목	설명
대기 시간 (설명 참조)	밀리초 단위로 표시되는 네트워크 대기 시간 추정치. RTCP 수신자 보고서 차 되었을 때 측정된 왕복 지연 실행 평균을 나타냅니다.
최대 지터	즉각적 지터의 최대 값(밀리초)
송신자 크기	전송된 스트림을 위한 RTP 패킷 크기(밀리초)
수신된 송신자 보고서 (설명 참조)	RTCP 송신자 보고서가 수신된 횟수
송신자 보고서 수신 시간 (설명 참조)	RTCP 송신자 보고서가 수신된 가장 최근 시간
수신자 크기	수신된 스트림을 위한 RTP 패킷 크기(밀리초).
수신자 폐기됨	네트워크에서 수신되었으나 지터 버퍼에서 폐기된 RTP 패킷
수신된 수신자 보고서 (설명 참조)	RTCP 수신자 보고서가 수신된 횟수
수신자 보고서 수신 시간 (설명 참조)	RTCP 수신자 보고서가 수신된 가장 최근 시간

참고 RTP 제어 프로토콜이 비활성화되면, 이 필드에 어떤 데이터도 생성되지 않기 때문에 이 값은 0으로 표시됩니다.

전화기의 정보를 XML로 요청

문제 해결 목적을 위해 전화기에서 정보를 요청할 수 있습니다. 결과 정보는 XML 형식입니다. 다음 정보를 사용할 수 있습니다.

- CallInfo는 특정 회선에 대한 통화 세션 정보입니다.
- LineInfo는 전화기에 대한 회선 구성 정보입니다.
- ModeInfo는 전화기 모드 정보입니다.

시작하기 전에

정보를 얻으려면 웹 액세스를 활성화해야 합니다.

전화기가 사용자와 연결되어야 합니다.

프로시저

단계 1 통화 정보의 경우 브라우저에 URL: **http://<phone ip address>/CGI/Java/CallInfo<x>**를 입력합니다.

여기서

- <*phone ip address*>는 전화기의 IP 주소입니다.
- <*x*>는 정보를 얻기 위한 회선 번호입니다.

명령은 XML 문서를 반환합니다.

단계 2 회선 정보의 경우 브라우저에 URL: **http://<phone ip address>/CGI/Java/LineInfo**를 입력합니다.

여기서

- <*phone ip address*>는 전화기의 IP 주소입니다.

명령은 XML 문서를 반환합니다.

단계 3 모델 정보의 경우 브라우저에 URL: **http://<phone ip address>/CGI/Java/ModeInfo**를 입력합니다.

여기서

- <*phone ip address*>는 전화기의 IP 주소입니다.

명령은 XML 문서를 반환합니다.

샘플 CallInfo 출력

다음 XML 코드는 CallInfo 명령의 출력 예입니다.

```
<?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>
```

샘플 LineInfo 출력

다음 XML 코드는 LineInfo 명령의 출력 예입니다.

```
<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>
```

샘플 ModeInfo 출력

다음 XML 코드는 ModeInfo 명령의 출력 예입니다.

```
<?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>
```

12 장

전화기 문제 해결

일반 문제 해결 정보

다음 표에서는 Cisco IP 전화기의 일반적인 문제 해결 정보를 제공합니다.

표 ***30: Cisco IP*** 전화기 문제 해결

요약	설명
장기적인 브로드캐스트 스톰으로 인해 IP 전화기가 재설정되거나 전화를 걸거나 받을 수 없게 됨	음성 VLAN상에서 장기적인 레이어 2 브로드캐스트 스톰(몇 분간 생하여 IP 전화기가 재설정되거나, 진행 중인 통화가 중단되거나, 하거나 전화를 받을 수 없게 될 수 있습니다. 전화기는 브로드캐스 끝날 때까지 작동하지 않을 수도 있습니다.

요약	설명
전화기에서 워크스테이션으로 네트워크 연결 이동	네트워크 연결을 통해 전화기에 전원을 공급한다면, 전화기의 네트워 케이블을 뽑아 데스크톱 컴퓨터에 꽂을 때 주의해야 합니다. 주의 컴퓨터의 네트워크 카드는 네트워크 연결을 통해 전원을 을 수 없습니다. 따라서 전원이 이 연결을 통해 공급된다면 워크 카드가 손상될 수 있습니다. 네트워크 카드를 보호하 서는 전화기에서 케이블을 뽑아 컴퓨터에 꽂을 때까지 10 기다리십시오. 이렇게 하면 스위치에서 해당 회선에 전화 이상 존재하지 않음이 인식되고 케이블에 대한 전원 공급 할 충분한 시간을 줄 수 있습니다.
전화기 구성 변경	기본적으로 관리자 암호 설정은 사용자가 네트워크 연결에 영향을 미 는 변경 작업을 수행하지 못하도록 잠겨 있습니다. 따라서 관리자 암호 구성하려면 설정 잠금을 해제해야 합니다. 자세한 내용은 전화기 암호 적용, 41 페이지을 참조하십시오. 참고 일반 전화기 프로파일에 관리자 암호가 설정되어 있지 않 용자가 네트워크 설정을 수정할 수 있습니다.
전화기와 기타 장치 간의 코덱 불일치	RxType 및 TxType 통계는 이 Cisco IP 전화기와 기타 장치 간의 대화에 코덱을 보여줍니다. 이 통계값은 일치해야 합니다. 만약 이 값이 일치 으면, 기타 장치에서 코덱 대화를 처리할 수 있는지 또는 트랜스코더가 를 처리할 준비가 되어 있는지 확인합니다. 자세한 내용은 [통화 통계] 146 페이지를 참조하십시오.
전화기와 기타 장치 간의 사운드 샘플 불일치	RxSize 및 TxSize 통계는 이 Cisco IP 전화기와 기타 장치 간의 대화에 음성 패킷의 크기를 보여줍니다. 이 통계값은 일치해야 합니다. 자세한 [통화 통계] 창 표시, 146 페이지를 참조하십시오.
루프백 조건	루프백 조건은 다음 조건이 만족하면 발생합니다. • 전화기의 SW 포트 구성 옵션이 10 반이중(10-BaseT/반이중)으로 어 있을 때 • 전화기가 외부 부전원 공급 장치에서 전원을 공급받을 때 • 전화기의 전원을 끈 상태일 때(전원 공급 장치 연결이 끊어짐) 이 경우 전화기의 스위치 포트는 비활성화될 수 있고, 스위치 콘솔 로 음과 같은 메시지가 표시됩니다. HALF_DUX_COLLISION_EXCEED_THRESHOLD 이 문제를 해결하려면 스위치에서 포트를 다시 활성화합니다.

시작 문제

네트워크에 전화기를 설치하고 이를 Cisco Unified Communications Manager에 추가한 후에는 아래의 관련 주제에 설명된 대로 전화기가 시작되어야 합니다.

전화기가 제대로 시작되지 않으면, 문제 해결 정보를 위해 다음 장을 참조하십시오.

관련 항목

전화기 시작 확인, 54 페이지

Cisco IP 전화기가 정상 시작 프로세스를 수행하지 않음

문제

Cisco IP 전화기를 네트워크 포트에 연결하면, 전화기가 관련 주제에서 언급한 대로 정상 시작 프로세스를 수행하지 않고 전화기 화면에 정보가 표시되지 않습니다.

원인

전화기가 시작 프로세스를 실행하지 않는 경우, 그 이유는 케이블 문제, 양호하지 못한 연결 상태, 네트워크 중단, 전력 부족 또는 전화기가 작동하지 않기 때문일 수 있습니다.

해결 방법

전화기가 작동하는지 확인하려면 다음을 사용하여 기타 잠재적 문제를 해결하십시오.

- 네트워크 포트 작동 확인:
  - 이더넷 케이블을 제대로 작동 중인 다른 케이블로 교환합니다.
  - 다른 포트에서 작동 중인 Cisco IP 전화기의 연결을 해제한 후, 이를 이 네트워크 포트에 연결하여 포트가 활성 상태인지 확인합니다.
  - 시작되지 않는 Cisco IP 전화기를 정상 상태가 확인된 다른 네트워크 포트에 연결합니다.
  - 시작되지 않는 Cisco IP 전화기를 스위치 포트에 직접 연결하여, 사무실에서 패치 패널 연결을 없앱니다.
- 전화기의 전원 공급 상태 확인:
  - 외부 전원을 사용하는 경우, 전기 콘센트가 잘 작동하는지 확인합니다.
  - 인라인 전원을 사용하는 경우, 대신 외부 전원 공급장치를 사용합니다.
  - 외부 전원 공급장치를 사용하는 경우, 제대로 작동하는 장치로 바꿉니다.
- 전화기가 여전히 제대로 시작되지 않으면, 백업 소프트웨어 이미지를 사용하여 전화기를 켭니다.
- 전화기가 여전히 제대로 시작되지 않으면, 전화기의 초기 재설정을 수행합니다.

- 이러한 해결책을 시도했는데도 Cisco IP 전화기 전화기 화면에 최소 5분이 지난 다음에도 글자가 표시되지 않으면, Cisco 기술 지원 담당자에게 추가 지원을 문의하십시오.

관련 항목

전화기 시작 확인, 54 페이지

Cisco IP 전화기가 Cisco Unified Communications Manager에 등록되어 있지 않음

전화기가 시작 프로세스의 첫 번째 단계(LED 버튼 깜박임 켜기 및 끄기)를 마쳐도 전화기 화면에 표시되는 메시지를 계속 오가면, 전화기가 제대로 시작되지 않습니다. 전화기가 이더넷 네트워크에 연결되어 있지 않고 Cisco Unified Communications Manager 서버에 등록하지 않으면 전화기는 성공적으로 시작할 수 없습니다.

또한 보안 문제 때문에 전화기가 제대로 시작되지 않을 수도 있습니다. 자세한 내용은 문제 해결 절차, 176 페이지를 참조하십시오.

전화기에 오류 메시지 표시

문제

시작하는 동안 상태 메시지에서 오류를 표시합니다.

해결 방법

시작 프로세스를 통해 전화기가 전원을 껐다 켜기 때문에, 문제의 원인에 관한 정보를 제공할 수도 있는 상태 메시지에 액세스할 수 있습니다. 상태 메시지 액세스 지침과 잠재적 오류, 설명 및 해결책에 관한 목록은 “상태 메시지 표시 창” 섹션을 참조하십시오.

관련 항목

[상태 메시지] 창 표시, 136 페이지

전화기가 TFTP 서버나 Cisco Unified Communications Manager에 접속할 수 없음

문제

전화기와 TFTP 서버나 Cisco Unified Communications Manager 사이의 네트워크가 중단되면, 전화기가 제대로 시작되지 못합니다.

해결 방법

현재 네트워크가 실행 중인지 확인합니다.

전화기가 TFTP 서버에 접속할 수 없음

문제

TFTP 서버 설정이 정확하지 않을 수 있습니다.

해결 방법

TFTP 설정을 확인합니다.

관련 항목

TFTP 설정 확인, 176 페이지

전화기가 서버에 접속할 수 없음

문제

IP 주소 지정 및 라우팅 필드가 제대로 구성되어 있지 않을 수 있습니다.

해결 방법

전화기의 IP 주소 지정 및 라우팅 설정을 확인해야 합니다. DHCP를 사용하고 있다면, DHCP 서버에서 이 값을 제공해야 합니다. 전화기에 고정 IP 주소를 지정했다면, 이 값을 수동으로 입력해야 합니다.

관련 항목

DHCP 설정 확인, 177 페이지

전화기가 DNS를 사용해 접속할 수 없음

문제

DNS 설정이 잘못되었을 수 있습니다.

해결 방법

DNS를 사용해 TFTP 서버 또는 Cisco Unified Communications Manager에 액세스한다면, DNS 서버를 지정해야 합니다.

관련 항목

DNS 설정 확인, 179 페이지

Cisco Unified Communications Manager 및 TFTP 서비스가 실행되지 않음

문제

Cisco Unified Communications Manager 또는 TFTP 서비스가 실행되지 않으면, 전화기가 제대로 시작되지 않을 수도 있습니다. 이런 경우에는 시스템 차원에 문제가 발생했을 가능성이 높고, 따라서 기타 전화기 및 장치가 제대로 시작되지 않을 수 있습니다.

해결 방법

Cisco Unified Communications Manager 서비스가 실행되지 않으면, 전화를 걸 때 해당 서비스에 의존하는 네트워크상의 모든 장치가 영향을 받습니다. TFTP 서비스가 실행되지 않으면, 많은 장치를 성공적으로 시작할 수 없습니다. 자세한 내용은 서비스 시작, 179 페이지의 내용을 참조하십시오.

구성 파일 변조

문제

특정 전화기의 문제가 이 장의 기타 제안 사항으로 해결되지 않고 지속된다면, 구성 파일이 손상되었을 수 있습니다.

해결 방법

새 전화기 구성 파일을 작성합니다.

관련 항목

새 전화기 구성 파일 생성, 178 페이지

Cisco Unified Communications Manager 전화기 등록

문제

전화기가 Cisco Unified Communications Manager에 등록되어 있지 않습니다.

해결 방법

Cisco IP 전화기는 전화기가 서버에 추가되어 있거나 자동 등록이 활성화되어 있는 경우에만 Cisco Unified Communications Manager 서버에 등록할 수 있습니다. 전화기가 Cisco Unified Communications Manager 데이터베이스에 추가되어 있는지 확인하려면 전화기 추가 방식, 62 페이지에서 정보 및 절차를 검토하십시오.

Cisco Unified Communications Manager 데이터베이스에 전화기가 존재하는지 확인하려면 Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다. 찾기를 클릭하여 MAC 주소를 기반으로 전화기를 검색합니다. MAC 주소 결정에 관한 자세한 내용은 전화기 MAC 주소 결정, 62 페이지를 참조하십시오.

이미 Cisco Unified Communications Manager 데이터베이스에 전화기가 존재한다면 구성 파일이 손상되었을 수도 있습니다. 자세한 내용은 구성 파일 변조, 168 페이지를 참조하십시오.

Cisco IP 전화기에서 IP 주소를 확보할 수 없음

문제

전화기가 시작될 때 IP 주소를 확보할 수 없으면, 전화기가 DHCP 서버와 동일한 네트워크 또는 VLAN 상에 있지 않거나 전화기가 연결된 스위치 포트가 비활성화되어 있을 수 있습니다.

해결 방법

전화기가 연결된 네트워크나 VLAN이 DHCP 서버에 액세스할 수 있는지 확인하고, 스위치 포트가 활성화되어 있는지 확인합니다.

전화기 재설정 문제

사용자가 통화 중에 또는 전화기가 유휴 상태인 동안 전화기가 재설정 작업을 수행한다고 보고하면, 관리자는 그 원인을 조사해야 합니다. 네트워크 연결과 Cisco Unified Communications Manager 연결이 안정적이면, 전화기는 재설정 작업을 수행하지 않습니다.

보통 전화기는 네트워크나 Cisco Unified Communications Manager와의 연결에 문제가 있는 경우 재설정 작업을 수행합니다.

간헐적인 네트워크 중단으로 인한 전화기 재설정

문제

네트워크에 간헐적인 중단 현상이 발생한 것일 수 있습니다.

해결 방법

간헐적인 네트워크 중단은 데이터와 음성 트래픽에 다른 영향을 미칩니다. 네트워크에서는 간헐적인 중단 현상이 일어나도 감지하지 못할 수 있습니다. 따라서 데이터 트래픽이 손실 패킷을 다시 전송하고, 패킷이 잘 수신되고 전송되었는지 확인할 수 있습니다. 그러나 음성 트래픽은 손실 패킷을 다시 캡처할 수 없습니다. 따라서 전화기는 손상된 네트워크 연결을 재전송하는 것이 아니라, 재설정을 수행하고 네트워크에 재연결을 시도합니다. 음성 네트워크의 알려진 문제에 관한 자세한 내용은 시스템 관리자에게 문의하십시오.

DHCP 설정 오류로 인한 전화기 재설정

문제

DHCP 설정이 잘못되었을 수 있습니다.

해결 방법

DHCP를 사용하도록 전화기가 제대로 구성되어 있는지 확인합니다. DHCP 서버가 제대로 설정되어 있는지 확인합니다. DHCP 임대 기간을 확인합니다. 임대 기간은 8일로 설정하는 것이 좋습니다.

관련 항목

DHCP 설정 확인, 177 페이지

잘못된 고정 IP 주소로 인한 전화기 재설정

문제

전화기에 할당된 고정 IP 주소가 잘못되었을 수 있습니다.

해결 방법

전화기에 고정 IP 주소가 할당되면, 정확한 설정을 입력했는지 확인합니다.

지나친 네트워크 사용으로 인한 전화기 재설정

문제

네트워크 사용량이 많을 때 전화기가 재설정을 수행하는 것 같다면, 음성 VLAN 구성되어 있지 않을 가능성이 높습니다.

해결 방법

별도의 보조 VLAN에서 전화기를 격리하면 음성 트래픽의 품질이 향상됩니다.

국제적 재설정에 따른 전화기 재설정

문제

Cisco Unified Communications Manager에 액세스할 수 있는 관리자가 1명이 아니라면, 누군가 고의로 전화기를 재설정하지 않았는지 확인해야 합니다.

해결 방법

전화기에서 설정을 누르고 관리자 설정 > 상태 > 네트워크 통계를 선택하면 Cisco IP 전화기가 Cisco Unified Communications Manager로부터 재설정 명령을 받았는지 여부를 확인할 수 있습니다.

- [재시작 원인] 필드에 재설정-재설정이라고 표시되면, 전화기는 Cisco Unified Communications Manager Administration에서 재설정/재설정 명령을 수신합니다.
- [재시작 원인] 필드에 재설정-재시작이라고 표시되면, 전화기는 Cisco Unified Communications Manager Administration에서 재설정/재시작 명령을 수신하기 때문에 종료됩니다.

DNS 또는 기타 연결 문제로 인한 전화기 재설정

문제

전화기 재설정이 계속되므로 DNS 또는 기타 연결 문제가 의심됩니다.

해결 방법

전화기가 계속 재설정을 하는 경우, DNS 또는 연결 문제 파악, 177 페이지에 나온 절차를 수행하여 DNS나 기타 연결 오류를 제거합니다.

전화기의 전원이 켜지지 않음

문제

전화기의 전원이 켜지지 않은 것처럼 보입니다.

해결 방법

대부분의 경우, 외부 전원을 사용해 전원을 공급하는 상황에서 해당 연결이 끊겨 PoE로 전환되면 전화기가 재시작됩니다. 마찬가지로 PoE를 사용해 전원을 공급하면 전화기가 재시작될 수 있고, 그런 다음 외부 전원 공급장치에 연결됩니다.

전화기가 LAN에 접속할 수 없음

문제

LAN에 대한 물리적 연결이 손상되었습니다.

해결 방법

Cisco IP 전화기가 접속하는 이더넷 연결이 제대로 작동하는지 확인합니다. 예를 들어 전화기가 연결된 특정 포트나 스위치가 꺼져 있지 않은지, 그리고 스위치가 재부팅하지 않는지 확인합니다. 케이블이 손상되지 않았는지도 확인합니다.

Cisco IP 전화기 보안 문제

다음 장에는 Cisco IP 전화기의 보안 기능에 관한 문제 해결 정보가 나와 있습니다. 이러한 문제에 관한 해결책과 보안 관련 추가 문제 해결 정보에 관한 자세한 내용은 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.

CTL 파일 문제

다음 섹션에서는 CTL 파일로 문제를 해결하는 방법에 대해 설명합니다.

인증 오류, 전화기가 CTL 파일을 인증하지 못함

문제

장치 인증 오류가 발생합니다.

원인

CTL 파일에 Cisco Unified Communications Manager 인증서가 없거나 잘못된 인증서입니다.

해결 방법

정확한 인증서를 설치합니다.

전화기가 CTL 파일을 인증하지 못함

문제

전화기가 CTL 파일을 인증하지 못합니다.

원인

업데이트된 CTL 파일에 서명한 보안 토큰이 전화기의 CTL 파일 내에 존재하지 않습니다.

해결 방법

CTL 파일의 보안 토큰을 변경하고 전화기에 새 파일을 설치합니다.

CTL 파일은 인증하지만 기타 구성 파일은 인증하지 않음

문제

전화가 CTL 파일 외의 다른 구성 파일을 인증하지 못합니다.

원인

잘못된 TFTP 레코드가 존재하거나 전화기 신뢰 목록에 있는 해당 인증서에서 구성 파일에 서명하지 않았을 수 있습니다.

해결 방법

TFTP 레코드와 신뢰 목록의 인증서를 확인합니다.

ITL 파일은 인증하지만 기타 구성 파일은 인증하지 않음

문제

전화가 ITL 파일 외의 다른 구성 파일을 인증하지 못합니다.

원인

전화기 신뢰 목록에 있는 해당 인증서에서 구성 파일에 서명하지 않았을 수도 있습니다.

해결 방법

정확한 인증서를 사용하여 구성 파일을 다시 서명합니다.

TFTP 인증 실패

문제

전화기에서 TFTP 인증 실패를 보고합니다.

원인

CTL 파일에 전화기에 대한 TFTP 주소가 존재하지 않습니다.

새 TFTP 레코드로 새 CTL 파일을 작성하면, 전화기의 기존 CTL 파일에 새 TFTP 서버에 대한 레코드가 포함되지 않을 수도 있습니다.

해결 방법

[전화기 CTL 파일에 TFTP 주소 구성]을 선택합니다.

전화기가 등록되지 않음

문제

전화기가 Cisco Unified Communications Manager에 등록되지 않습니다.

원인

CTL 파일에 Cisco Unified Communications Manager 서버에 대한 정확한 정보가 포함되어 있지 않습니다.

해결 방법

CTL 파일의 Cisco Unified Communications Manager 서버 정보를 변경합니다.

서명된 구성 파일을 요청하지 않음

문제

전화기에서 서명된 구성 파일을 요청하지 않습니다.

원인

CTL 파일에 인증서가 있는 TFTP 항목이 포함되어 있지 않습니다.

해결 방법

CTL 파일의 인증서로 TFTP 항목을 구성합니다.

오디오 문제

다음 섹션에서는 오디오 문제를 해결하는 방법에 대해 설명합니다.

통화 경로 없음

문제

통화 시 1명 이상의 통화자가 오디오를 전혀 들을 수 없습니다.

해결 방법

통화 당사자 중 최소 1명이 오디오를 수신하지 못한다면, 전화기 사이의 IP 연결이 성립되어 있지 않은 것입니다. IP 연결이 적절하게 구성되어 있는지 라우터 및 스위치의 구성을 확인합니다.

통화가 끊김

문제

사용자가 통화가 끊긴다고 불평합니다.

원인

지터 구성에 문제가 있을 수 있습니다.

해결 방법

AvgJtr 및 MaxJtr 통계를 확인합니다. 이 통계치에 큰 차이가 있다는 것은 네트워크의 지터에 문제가 있거나 네트워크 사용률이 주기적으로 높다는 뜻일 수 있습니다.

데이지 체인 모드에서 하나의 전화기가 작동하지 않음

문제

데이지 체인 모드에서 회의전화 전화기 중 하나가 작동하지 않습니다.

해결 방법

스마트 어댑터에 연결된 케이블이 올바른 케이블인지 점검하십시오. 2개의 두꺼운 케이블은 전화기를 스마트 어댑터에 연결합니다. 얇은 케이블은 스마트 어댑터를 전원 어댑터에 연결합니다.

관련 항목

데이지 체인 모드, 31 페이지
데이지 체인 모드로 전화회의 전화기 설치, 38 페이지

일반적인 전화기 통화 문제

다음 섹션은 일반적인 전화기 통화 문제를 해결하는 데 도움이 됩니다.

전화 통화를 설정할 수 없음

문제

사용자가 전화를 걸 수 없다고 불평합니다.

원인

전화기에 DHCP IP 주소가 없으면 Cisco Unified Communications Manager에 등록할 수 없습니다. LCD 화면이 있는 전화기에는 `IP 구성` 또는 등록이라는 메시지가 표시됩니다. LCD 화면이 없는 전화기에서는 사용자가 전화를 걸려고 할 때 핸드셋에서 (다이얼 소리가 아닌) 다시걸기 신호음이 재생됩니다.

해결 방법

1. 다음을 확인하십시오.
    1. 이더넷 케이블이 연결되어 있습니다.
    2. Cisco CallManager 서비스는 Cisco Unified Communications Manager 서버에서 실행됩니다.
    3. 두 전화기 모두 같은 Cisco Unified Communications Manager에 등록됩니다.
2. 두 전화기 모두 오디오 서버 디버그와 캡처 로그가 활성화됩니다. 필요할 경우 Java 디버그를 활성화합니다.

전화기가 DTMF 숫자가 지연되는 것을 인식하지 못함

문제

사용자가 키패드를 사용할 때 숫자가 누락되거나 지연된다고 불평합니다.

원인

키를 너무 빨리 누르면 숫자가 누락되거나 지연될 수 있습니다.

해결 방법

키를 너무 빠르게 누르지 마십시오.

문제 해결 절차

이 절차를 사용해 문제를 확인하고 수정할 수 있습니다.

Cisco Unified Communications Manager에서 전화 문제 보고서 만들기

Cisco Unified Communications Manager에서 전화기에 대한 문제 보고서를 생성할 수 있습니다. 이 작업을 수행하면 PRT(문제 보고서 도구) 소프트 키가 전화기에서 생성하는 것과 동일한 정보가 생성됩니다.

문제 보고서에는 전화기와 헤드셋에 대한 정보가 포함되어 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 장치 > 전화기를 선택합니다.

단계 **2** 찾기를 클릭하고 하나 이상의 Cisco IP 전화기를 선택합니다.

단계 **3** 선택한 Cisco IP 전화기에 사용된 헤드셋에 대한 PRT 로그를 수집하려면 선택 항목에 대한 **PRT** 생성을 클릭합니다.

TFTP 설정 확인

프로시저

단계 **1** TFTP 서버 1 필드를 확인합니다.

전화기에 고정 IP 주소를 지정했다면, TFTP Server 1 옵션에 대한 설정을 수동으로 입력해야 합니다.

DHCP를 사용하고 있다면, 전화기는 DHCP 서버에서 TFTP 서버에 대한 주소를 확보합니다. 옵션 150에 IP 주소가 구성되어 있는지 확인합니다.

단계 **2** 전화기에서 대체 TFTP 서버를 사용하도록 할 수도 있습니다. 그러한 설정은 최근 전화기가 원래 위치에서 다른 곳으로 이동한 경우 특히 유용합니다.

단계 **3** 로컬 DHCP가 정확한 TFTP 주소를 제공하지 않으면, 전화기에서 대체 TFTP 서버를 사용하도록 합니다.

이는 보통 VPN 시나리오에서 필요합니다.

DNS 또는 연결 문제 파악

프로시저

단계 **1** [설정 재설정] 메뉴를 사용하여 전화기 설정을 디폴트로 재설정합니다.

단계 **2** DHCP 및 IP 설정을 수정합니다.

a) DHCP를 비활성화합니다.

b) 전화기에 고정 IP 값을 할당합니다. 다른 기능 전화기가 사용하는 것과 같은 기본 라우터 설정을 사용합니다.

c) TFTP 서버를 지정합니다. 다른 기능 전화기가 사용하는 것과 같은 TFTP 서버를 사용합니다.

단계 **3** Cisco Unified Communications Manager 서버에서, 로컬 호스트 파일에 정확한 Cisco Unified Communications Manager 서버 이름이 정확한 IP 주소에 매핑되어 있는지 확인합니다.

단계 **4** Cisco Unified Communications Manager에서 시스템 > 서버를 선택하고, 서버에 대한 참조가 DNS 이름이 아닌 IP 주소를 통해 이루어지는지 확인합니다.

단계 **5** Cisco Unified Communications Manager에서 장치 > 전화기를 선택합니다. 찾기를 클릭하여 전화기를 검색합니다. Cisco IP 전화기에 정확한 MAC 주소가 할당되었는지 확인합니다.

단계 **6** 전화기 전원을 껐다가 다시 켭니다.

관련 항목

전화기 MAC 주소 결정, 62 페이지
전화회의 전화기를 다시 시작 또는 재설정, 183 페이지

DHCP 설정 확인

프로시저

단계 **1** 전화기에서 설정을 누릅니다.

단계 **2** 관리자 설정 > 이더넷 설정 > **IPv4** 설정을 선택합니다.

단계 **3** DHCP 서버 필드를 확인합니다.

전화기에 고정 IP 주소를 지정했다면, DHCP 서버 옵션에 대한 값을 입력할 필요가 없습니다. 그러나 DHCP 서버를 사용하고 있다면, 이 옵션에 대한 값이 있어야 합니다. 값이 없다면, IP 라우팅과 VLAN 구성을 확인합니다. 다음 URL에서 스위치 포트 및 인터페이스 문제 해결 문서를 참조하십시오.

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

단계 **4** IP 주소, 서브넷 마스크 및 기본 라우터 필드를 확인합니다.

전화기에 고정 IP 주소를 지정했다면, 이러한 옵션의 설정을 수동으로 입력해야 합니다.

단계 **5** DHCP를 사용 중이라면, DHCP 서버에서 배포한 IP 주소를 확인합니다.

다음 URL에서 *Catalyst* 스위치나 엔터프라이즈 네트워크에서의 *DHCP* 문제 해결 문서를 참조하십시오.

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

새 전화기 구성 파일 생성

Cisco Unified Communications Manager 데이터베이스에서 전화기를 제거하면 Cisco Unified Communications Manager TFTP 서버에서 구성 파일이 삭제됩니다. 그러나 전화기 디렉터리 번호는 Cisco Unified Communications Manager 데이터베이스에 남습니다. 이는 할당되지 않은 DN이라 불리며, 다른 장치에 사용할 수 있습니다. 만약 할당되지 않은 DN을 다른 장치에서 사용하지 못한다면, 이러한 DN은 Cisco Unified Communications Manager 데이터베이스에서 삭제하십시오. 할당되지 않은 참조 번호를 확인하고 삭제하기 위해 경로 플랜 보고서를 사용할 수 있습니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

전화기 버튼 템플릿에서 버튼을 변경하거나 전화기에 다른 전화기 버튼 템플릿을 할당하면 전화기에서 디렉터리 번호에 더 이상 액세스하지 못할 수도 있습니다. Cisco Unified Communications Manager 데이터베이스에서 전화기에 여전히 디렉터리 번호가 할당되지만, 전화기에 전화를 받을 수 있는 버튼이 없습니다. 따라서 필요할 경우 이러한 디렉터리 번호는 전화기에서 제거하고 삭제해야 합니다.

프로시저

단계 **1** Cisco Unified Communications Manager에서 장치 > 전화기를 선택하고, 검색을 클릭하여 문제가 발생한 전화기를 찾습니다.

단계 **2** 삭제를 선택하여 Cisco Unified Communications Manager 데이터베이스에서 전화기를 삭제합니다.

참고 Cisco Unified Communications Manager 데이터베이스에서 전화기를 제거하면 Cisco Unified Communications Manager TFTP 서버에서 구성 파일이 삭제됩니다. 그러나 전화기 디렉터리 번호는 Cisco Unified Communications Manager 데이터베이스에 남습니다. 이는 할당되지 않은 DN이라 불리며, 다른 장치에 사용할 수 있습니다. 만약 할당되지 않은 DN을 다른 장치에서 사용하지 못한다면, 이러한 DN은 Cisco Unified Communications Manager 데이터베이스에서 삭제하십시오. 할당되지 않은 참조 번호를 확인하고 삭제하기 위해 경로 플랜 보고서를 사용할 수 있습니다.

단계 3 Cisco Unified Communications Manager 데이터베이스에 다시 전화기를 추가합니다.

단계 4 전화기 전원을 껐다가 다시 켭니다.

관련 항목

전화기 추가 방식, 62 페이지
Cisco Unified Communications Manager 설명서, 14 페이지

DNS 설정 확인

프로시저

단계 1 전화기에서 설정을 누릅니다.

단계 2 관리자 설정 > 이더넷 설정 > **IPv4** 설정을 선택합니다.

단계 3 DNS 서버 1 필드가 올바르게 설정되었는지 확인합니다.

단계 4 또한 Cisco Unified Communications Manager 시스템과 TFTP 서버에 대한 DNS 서버에 CNAME 항목을 구성했는지도 확인해야 합니다.

더불어 DNS가 역방향 조회를 수행하도록 구성되어 있어야 합니다.

서비스 시작

서비스는 시작하거나 중단하기 전에 활성화해야 합니다.

프로시저

단계 1 Cisco 통합 커뮤니케이션 매니저 관리의 탐색 드롭다운 목록에서 **Cisco Unified Serviceability**를 선택하고 이동을 클릭합니다.

단계 2 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 3 서버 드롭다운 목록에서 기본 Cisco Unified Communications Manager 서버를 선택합니다.

창에 선택했던 서버에 대한 서비스 이름, 서비스 상태 및 서비스를 시작하거나 중단하는 서비스 제어 판이 표시됩니다.

단계 4 서비스가 중단되면, 해당 라디오 버튼을 클릭한 다음 시작을 클릭합니다.

서비스 상태 기호가 사각형에서 화살표 모양으로 변경됩니다.

Cisco Unified Communications Manager의 디버그 제어 정보

해결할 수 없는 전화기 문제를 겪고 있다면, Cisco TAC이 도와드리겠습니다. 전화기에서 디버깅 기능을 켜고, 문제를 다시 발생시킨 다음, 디버깅 기능을 끄고, 해당 로그를 분석을 위해 TAC에 보내십시오.

디버깅이 상세한 정보를 캡처하기 때문에 통신 트래픽으로 인해 전화기 작동이 느려져 응답 속도가 떨어질 수 있습니다. 로그를 캡처한 후에는 전화기 작동이 원활해지도록 디버깅을 꺼야 합니다.

디버그 정보에는 상황의 심각성을 반영하기 위해 한 자릿수의 숫자 코드가 포함될 수도 있습니다. 각 상황은 다음과 같은 등급으로 나눌 수 있습니다.

- 0 - 긴급
- 1 - 경보
- 2 - 중요
- 3 - 오류
- 4 - 경고
- 5 - 알림
- 6 - 정보
- 7 - 디버깅

자세한 정보 및 지원은 Cisco TAC에 문의하십시오.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 다음 창 중 하나를 선택합니다.

- 장치 > 장치 설정 > 일반 전화기 프로파일
- 시스템 > 엔터프라이즈 전화기 구성
- 장치 > 전화기

단계 **2** 다음과 같은 파라미터를 설정합니다.

- 로그 프로파일 - 값: 프리셋(기본), 기본, 전화 통신, SIP, UI, 네트워크, 미디어, 업그레이드, 액세서리, 보안, Energywise, MobileRemoteAccess
- 원격 로그 - 값: 비활성화(기본), 활성화
- IPv6 로그 서버 또는 로그 서버 - IP 주소(IPv4 또는 IPv6 주소)

참고 로그 서버에 도달하지 못하면 전화기는 디버그 메시지 전송을 중단합니다.

- IPv4 로그 서버 주소의 형식은 **address:<port>@@base=<0-7>;pfs=<0-1>**입니다.

- IPv6 로그 서버 주소의 형식은 **[address]:<port>@@base=<0-7>;pfs=<0-1>**입니다.
- 여기서:
  - IPv4 주소는 마침표(.)로 구분합니다.
  - IPv6 주소는 콜론(:)으로 구분합니다.

추가 문제 해결 정보

전화기 문제 해결에 관한 추가 질문이 있는 경우 다음 Cisco 웹 사이트로 이동해 원하는 전화기 모델을 탐색합니다.

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

13 장

유지 보수

전화회의 전화기를 다시 시작 또는 재설정

전화기에 오류가 발생하는 경우 복구하려면 전화기의 기본 재설정을 수행합니다. 또한 구성 및 보안 설정을 초기 기본 설정으로 복원할 수 있습니다.

전화회의 전화기 다시 시작

전화기를 다시 시작하면 전화기의 플래시 메모리에 적용하지 않은 모든 사용자 및 네트워크 설정 변경이 손실됩니다.

프로시저

설정 > 관리자 설정 > 설정 재설정 > 장치 재설정을 누릅니다.

관련 항목

전화기의 텍스트 및 메뉴 항목, 41 페이지

전화기 메뉴에서 전화회의 전화기 설정 재설정

프로시저

단계 **1** 설정을 누릅니다.

단계 **2** 관리자 설정 > 설정 재설정을 선택합니다.

단계 **3** 재설정 유형을 선택합니다.

- 모두—초기 설정을 복원합니다.
- 장치 재설정—장치를 재설정합니다. 기존 설정은 변경하지 마십시오.
- 네트워크—기본 설정으로 네트워크 구성을 재설정합니다.
- 서비스 모드—현재 서비스 모드를 지우고 VPN을 비활성화한 후 전화기를 다시 시작합니다.
- 네트워크—기본 설정으로 보안 구성을 재설정합니다. 이 옵션은 CTL 파일을 삭제합니다.

단계 **4** 재설정 또는 취소를 누릅니다.

관련 항목

전화기의 텍스트 및 메뉴 항목, 41 페이지

키패드에서 초기 기본값으로 전화회의 전화기 재설정

키패드에서 전화기를 재설정하면 전화기가 초기 설정으로 돌아갑니다.

프로시저

단계 **1** 전화기의 플러그를 뺍니다.

- PoE를 사용한다면, LAN 케이블을 분리합니다.
- 전원 어댑터를 사용한다면, 어댑터를 분리합니다.

단계 **2** 5초 동안 기다립니다.

단계 **3** **#**를 길게 누르고, 전화기의 플러그를 다시 연결합니다.

단계 **4** 전화기가 부팅되면 LED 표시등이 켜집니다. LED 표시등이 꺼지면 **123456789*0#** 순서대로 누릅니다.

이 버튼을 다 누르고 나면, 전화기가 초기 재설정 프로세스를 시작합니다.

이 버튼을 순서대로 누르지 않으면, 그냥 보통 때처럼 전화기의 전원이 켜집니다.

주의 초기 재설정 프로세스가 완료될 때까지 전화기의 전원을 끄지 마십시오. 프로세스가 완료되면 기본 화면이 나타납니다.

관련 항목

전화기의 텍스트 및 메뉴 항목, 41 페이지

음질 모니터링

네트워크에서 주고받는 통화의 음질을 측정하기 위해, Cisco IP 전화기는 숨김 이벤트를 기반으로 한 다음과 같은 통계 메트릭을 사용합니다. DSP는 음성 패킷 스트림에서의 프레임 손실을 감추기 위해 숨김 프레임을 실행합니다.

- 숨김률 메트릭 - 총 대화 프레임에 대한 숨김 프레임의 비율을 표시합니다. 간격 숨김률은 3초 단위로 계산됩니다.
- 숨김 초 메트릭 - 손실 프레임으로 인해 DSP가 숨김 프레임을 재생하는 시간(초)을 보여줍니다. "숨김 초"는 정확하게 DSP가 5%가 넘는 숨김 프레임을 재생하는 시간(초)입니다.

참고 숨김률과 숨김 초는 프레임 손실을 기반으로 한 기본 측정값입니다. 숨김률이 0이라는 것은 IP 네트워크가 손실 없이 제시간에 프레임과 패킷을 제공하고 있다는 뜻입니다.

음질 메트릭은 [통화 통계] 화면을 사용해 Cisco IP 전화기에서 또는 [스트리밍 통계]를 사용해 원격에서 액세스할 수 있습니다.

음질 문제 해결 팁

메트릭에 중요하고 지속적인 변화가 관찰되면, 다음 표에서 일반적인 문제 해결 정보를 확인하십시오.

표 ***31:*** 음질 메트릭의 변화

메트릭 변화	조건
숨김률 및 숨김(초)이 크게 증가합니다.	패킷 손실이나 높은 지터로 인한 네트워크 손상
숨김률이 0이거나 0에 가깝지만 음질이 좋지 않습니다.	• 에코 또는 오디오 수준 같은 오디오 채널의 잡음 또는 왜곡 • 셀룰러 네트워크나 전화 카드 네트워크에 대한 통화처럼 여러 개의 인코딩/디코딩을 거치는 탠덤 통화 • 스피커폰, 핸즈프리 휴대폰 또는 무선 헤드셋으로 인해 발생하는 음향 문제 패킷 전송(TxCnt)과 패킷 수신(RxCnt) 카운터를 확인하여 음성 패킷이 잘 전달되는지 확인합니다.
MOS LQK 지수가 크게 감소합니다.	패킷 손실이나 높은 지터 수준으로 인한 네트워크 손상 • 평균 MOS LQK 감소는 광범위하면서 획일적인 손상을 의미할 수 있습니다. • 개별 MOS LQK 감소는 버스티 손상을 의미할 수 있습니다. 숨김률과 숨김(초)을 대조 검토하여 패킷 손실 및 지터의 증거를 찾습니다.

메트릭 변화	조건
MOS LQK 지수가 크게 증가합니다.	• 전화기가 예상했던 것과는 다른 코덱을 사용하고 있지 않은지 확인합니다(RxType 및 TxType). • 펌웨어 업그레이드 후에 MOS LQK 버전이 변경되었는지 확인합니다.

참고 음질 메트릭은 잡음이나 왜곡의 이유는 되지 않으며, 오직 프레임 손실에만 영향을 미칩니다.

Cisco IP 전화기 청소

Cisco IP 전화기를 청소하려면 부드러운 마른 천만을 사용하여 전화기와 전화기 화면을 가볍게 닦습니다. 전화기에 물이나 가루가 직접적으로 묻지 않도록 하십시오. 모든 비내후성 전자기기가 그렇듯이, 액체와 가루는 구성 요소를 손상시키고 장애를 일으킬 수 있습니다.

전화기가 대기 모드인 경우, 화면이 빈 상태로 나타나며 선택 버튼이 켜져 있지 않습니다. 전화기가 이러한 조건에 있으면, 청소를 마친 후까지 전화기가 대기 상태로 유지되는 경우 화면을 청소할 수 있습니다.

14 장

국제 사용자 지원

Unified Communications Manager 엔드포인트 로케일 설치 관리자

기본적으로, Cisco IP 전화기는 영어(미국) 로케일로 설정됩니다. 다른 로케일에서 Cisco IP 전화기를 사용하려면, 클러스터의 모든 Cisco Unified Communications Manager 서버에 해당 로케일 버전의 Unified Communications Manager 엔드포인트 로케일 설치 관리자를 설치해야 합니다. 로케일 설치 관리자는 Cisco IP 전화기에 전화기 사용자 인터페이스 및 국가별 전화기 소리가 제공되도록 시스템에 해당하는 최신 번역 텍스트를 설치합니다.

릴리스에 필요한 로케일 설치 관리자에 액세스하려면 소프트웨어 다운로드 페이지에 액세스하여 사용 중인 전화기 모델을 찾아 Unified Communications Manager 엔드포인트 로케일 설치 관리자 링크를 선택합니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

참고 최신 로케일 설치 관리자가 곧바로 제공되지 않을 수도 있으므로 웹 사이트에서 수시로 업데이트를 확인하십시오.

관련 항목

Cisco Unified Communications Manager 설명서, 14 페이지

국제 통화 로깅 지원

전화기 시스템이 국제 통화 로깅(발신자 정규화)에 맞게 구성되어 있는 경우 통화 로그, 재다이얼 또는 통화 디렉터리 항목이 현재 위치의 국제 이스케이프 코드를 표시하기 위해 플러스(+) 기호를 표시

할 수도 있습니다. 전화기 시스템에 대한 구성에 따라 +가 정확한 국제 지역 번호를 대체할 수도 있고, 전화를 걸기 전에 + 기호를 현재 위치에 대한 국제 이스케이프 코드로 직접 교체해 번호를 편집해야 할 수도 있습니다. 또한 통화 로그 또는 디렉터리 항목은 수신된 전화의 국제 번호 전체를 표시할 수 있지만, 전화기 디스플레이는 국제 또는 국가 코드가 생략된 축약 버전의 지역 번호를 표시할 수도 있습니다.

언어 제한 사항

다음 아시아 로캘의 경우 지역화된 KATE(Keyboard Alphanumeric Text Entry)를 지원하지 않습니다.

- 중국어(중국)
- 중국어(홍콩)
- 중국어(대만)
- 일본어(일본)
- 한국어(대한민국)

기본 영어(미국) KATE가 대신 사용자에게 표시됩니다.

예를 들어, 전화기 화면에 한국어 텍스트가 표시되지만 키패드의 **2** 키는 **a b c 2 A B C**를 표시합니다.