



## Cisco Unified Communications Manager용 Cisco IP 전화기 8800 시리즈 관리 설명서

초판: 2015년 7월 13일

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 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패키지의 내용을 따르며 여기에 인용된 내용은 참조입니다. 소프트웨어 라이선스 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 적절한 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 적절한 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 발생하는 모든 명시적이거나 묵시적인 보증을 부인합니다.

CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없으므로 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](http://www.cisco.com/go/office))에서 확인하십시오.

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

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

© 2015–2023 Cisco Systems, Inc. 모든 권리 보유.



## 목 차

서문:

서론	xv
개요	xv
대상	xv
설명서 규칙	xv
관련 설명서	xvii
Cisco IP 전화기 8800 시리즈 설명서	xvii
Cisco Unified Communications Manager 설명서	xvii
Cisco Business Edition 6000 설명서	xvii
설명서, 지원 및 보안 지침	xvii
Cisco 제품 보안 개요	xviii

장 1

신규 및 변경된 정보	1
펌웨어 릴리스 14.2(1)에 대한 새 정보 및 변경된 정보	1
펌웨어 릴리스 14.1(1)에 대한 새 정보 및 변경된 정보	2
펌웨어 릴리스 14.0(1)에 대한 새 정보 및 변경된 정보	2
펌웨어 릴리스 12.8(1)에 대한 새 정보 및 변경된 정보	3
펌웨어 릴리스 12.7(1)에 관한 새 정보 및 변경된 정보	3
펌웨어 릴리스 12.6(1)에 대한 새 정보 및 변경된 정보	4
펌웨어 릴리스 12.5(1)SR3에 대한 새 정보	4
펌웨어 릴리스 12.1(1)SR1에 대한 새 정보	4
펌웨어 릴리스 12.1(1)SR1에 대한 새 정보	5
펌웨어 릴리스 12.1(1)에 대한 새 정보	5
펌웨어 릴리스 12.0(1)에 대한 새 정보	6
펌웨어 릴리스 11.7(1)에 대한 새 정보	6

펌웨어 릴리스 11.5(1)SR1에 대한 새 정보 6  
 펌웨어 릴리스 11.5(1)에 대한 새 정보 7  
 펌웨어 릴리스 11.0에 대한 새 정보 8

---

부 1: **Cisco IP** 전화기 정보 11

---

장 2 기술 세부사항 13

- 물리적 및 운영 환경 사양 13
- 케이블 사양 14
  - 네트워크 및 컴퓨터 포트 핀 배치도 14
  - 네트워크 포트 커넥터 15
  - 컴퓨터 포트 커넥터 15
- 전화기 전원 요구 사항 16
  - 정전 17
  - 전력 소비 감소 17
  - LLDP에 대한 전원공급 협상 17
- 네트워크 프로토콜 18
- VLAN 상호 작용 22
- Cisco Unified Communications Manager 상호 작용 22
- Cisco Unified Communications Manager Express 상호 작용 23
- 음성 메시징 시스템 상호 작용 24
- 전화기 시작 개요 24
- 외부 장치 26
- USB 포트 정보 26
- 전화기 구성 파일 27
- 네트워크 혼잡 시 전화기 동작 27
- 두 개의 네트워크 라우터가 있는 네트워크에서 네트워크 동작 28
- 애플리케이션 프로그래밍 인터페이스 28

---

장 3 **Cisco IP** 전화기 하드웨어 29

전화기 개요 29

Cisco IP Phone 8811 31  
     전화기 연결 31  
 Cisco IP 전화기 8841 및 8845 32  
     전화기 연결부 32  
 Cisco IP 전화기 8851 및 8851NR 33  
     전화기 연결 34  
 Cisco IP 전화기 8861, 8865 및 8865NR 35  
     전화기 연결부 35  
 버튼 및 하드웨어 36  
     소프트키, 회선 및 기능 버튼 38  
 비디오폰 카메라 보호 39

---

부 11:

**Cisco IP 전화기 설치 41**

---

장 4

**Cisco IP 전화기 설치 43**  
     네트워크 설정 확인 43  
     온-프레미스 전화기에 대한 활성화 코드 온보딩 44  
     활성화 코드 온보딩 및 모바일 및 Remote Access 45  
     전화기 자동 등록 활성화 45  
     Cisco IP 전화기 설치 47  
         전화기 및 컴퓨터와 네트워크 연결 공유 49  
         설정 메뉴에서 전화기 설정 49  
         전화기 암호 적용 50  
         전화기의 텍스트 및 메뉴 항목 51  
     전화기에서 무선 LAN 활성화 51  
         Cisco Unified Communications Manager에서 무선 LAN 설정 52  
         전화기에 무선 LAN 설정 53  
         WLAN 인증 시도 수 설정 55  
         WLAN 프롬프트 모드 활성화 55  
         Cisco Unified Communications Manager를 사용하여 Wi-Fi 프로파일 설정 56  
         Cisco Unified Communications Manager를 사용하여 Wi-Fi 그룹 설정 58

네트워크 설정 구성 58

이더넷 설정 필드 59

IPv4 필드 61

IPv6 필드 63

전화기가 DHCP를 사용하도록 설정 65

전화기가 DHCP를 사용하지 않도록 설정 65

로드 서버 66

전화기 시작 확인 66

사용자를 위한 전화기 서비스 구성 66

사용자의 전화기 모델 변경 67

장 5

**Cisco Unified Communications Manager 전화기 설정 69**

Cisco IP 전화기 설정 69

전화기 MAC 주소 결정 72

전화기 추가 방식 73

    전화기를 개별적으로 추가 73

    BAT 전화기 템플릿을 사용해 전화기 추가 73

Cisco Unified Communications Manager에 사용자 추가 74

    외부 LDAP 디렉터리에서 사용자 추가 75

    Cisco Unified Communications Manager에 직접 사용자 추가 75

    최종 사용자 그룹에 사용자 추가 76

    전화기와 사용자 연결 77

    SRST(Survivable Remote Site Telephony) 77

    E-SRST(Enhanced Survivable Remote Site Telephony) 80

    애플리케이션 다이얼 규칙 80

        애플리케이션 다이얼 규칙 구성 81

장 6

**셀프 케어 포털 관리 83**

    셀프 서비스 포털 개요 83

    셀프 서비스 포털에 사용자 액세스 설정 84

    셀프 서비스 포털 디스플레이 사용자 정의 84

---

부 III:	<b>Cisco IP 전화기 관리 85</b>
--------	---------------------------

---

장 7	<b>Cisco IP 전화기 보안 87</b> 전화기 네트워크의 보안 강화 87 지원 보안 기능 88 LSC(Locally Significant Certificate) 설정 93 FIPS 모드 활성화 94 전화기 통화 보안 95 보안 컨퍼런스 식별 95 보안 전화기 통화 식별 96 참여를 위한 암호화 제공 97 WLAN 보안 97 인증 모드 설정 101 무선 보안 인증서 101 사용자 이름 및 암호 설정 102 사전 공유 키 설정 102 무선 암호화 103 Microsoft Certificate Services를 사용하여 ACS에서 CA 인증서 가져오기 104 PEAP 설정 108 무선 LAN 보안 109 Cisco IP 전화기 관리 페이지 109 SCEP 설정 113 802.1X 인증 113 802.1X 인증 액세스 115 장치 인증 필드 설정 115
-----	--

---

장 8	<b>Cisco IP 전화기 사용자 정의 117</b> 사용자 지정 전화기 벨소리 117 사용자 정의 배경 이미지 117 광대역 코덱 설정 119
-----	--

휴대 디스플레이 설정 120

신호음 사용자 정의 120

장 9

전화기 기능 및 설정 123

전화기 기능 및 설정 개요 123

Cisco IP 전화기 사용자 지원 124

전화기 기능 124

기능 단추 및 소프트키 142

전화기 기능 구성 144

모든 전화기에 대해 전화기 구성 설정 145

전화기 그룹에 대해 전화기 구성 설정 145

단일 전화기에 대해 전화기 구성 설정 146

제품별 구성 146

기능 구성 모범 사례 167

통화량이 높은 환경 167

복수 회선 환경 168

세션 회선 모드 환경 168

필드: 항상 기본 회선 사용 169

전송 레이어 보안 암호 비활성화 169

공유 회선을 위한 통화 기록 활성화 169

Cisco IP 전화기의 절전 일정 170

Cisco IP 전화기에서 EnergyWise 예약 172

방해사절 설정 175

상당사 인사말 활성화 176

모니터링 및 녹음 설정 177

통화 착신 전환 알림 설정 178

통화 목록에 대한 BLF 활성화 178

스위치 및 PC 포트를 위한 EEE(Energy Efficient Ethernet) 설정 179

RTP/sRTP 포트 범위 설정 180

Expressway를 통한 모바일 및 Remote Access 181

구축 시나리오 182



- 미디어 경로 및 상호 연결 설정 지원 183
- 다음에서 사용 가능한 전화기 기능: Expressway를 통한 모바일 및 Remote Access 183
- Expressway 로그인을 위해 사용자 자격 증명 영구 구성 186
- MRA 로그인용 QR 코드 생성 186
- 문제 보고서 도구 186
  - 고객 지원 업로드 URL 구성 187
- 회선에 대한 레이블 설정 188
- 듀얼 बैं크 정보 설정 188
- 지정보류 모니터링 189
  - 지정보류 모니터링 타이머 설정 189
  - 디렉터리 번호에 대한 지정보류 모니터링 매개 변수 설정 190
  - 헌트 목록에 대한 지정보류 모니터링 설정 191
- 오디오 및 비디오 포트 범위 설정 192
- Cisco IP Manager Assistant 설정 193
- Visual VoiceMail 설정 195
  - 특정 사용자용 Visual VoiceMail 설정 196
  - 사용자 그룹용 Visual Voicemail 설정 197
- 보증된 서비스 SIP 197
- 전화기를 다중 플랫폼 전화기로 직접 마이그레이션 198
- MLPP(Multilevel Precedence and Preemption) 198
- 소프트키 템플릿 설정 198
- 전화기 버튼 템플릿 201
  - 전화기 버튼 템플릿 수정 201
  - 모든 통화에 대한 전화기 버튼 템플릿 할당 201
  - IP 전화기 서비스에 PAB 또는 단축 다이얼 설정 202
  - PAB 또는 고속 다이얼에 대한 전화기 버튼 템플릿 수정 203
- VPN 구성 204
- 추가 회선 키 설정 205
  - 고급 회선 모드에서 사용할 수 있는 기능 205
- TLS 재개 타이머 설정 208
- Intelligent Proximity 활성화 209

비디오 전송 해상도 설정 209

이전 버전의 Cisco Unified Communications Manager에서 헤드셋 관리 211

    기본 헤드셋 설정 파일 다운로드 211

    기본 헤드셋 설정 파일 수정 212

    기본 구성 파일을 Cisco Unified Communications Manager에 설치 214

    Cisco TFTP 서버 다시 시작 215

---

장 10           회사 및 개인 디렉터리 217

    회사 디렉터리 설정 217

    개인 디렉터리 설정 217

    사용자 개인 디렉터리 항목 설정 218

    Cisco IP 전화기 Address Book Synchronizer 다운로드 219

    Cisco IP 전화기 주소록 동기화 도구 구축 219

        Synchronizer 설치 219

        Synchronizer 설정 220

---

부 IV:           Cisco IP 전화기 문제 해결 221

---

장 11           전화기 시스템 모니터링 223

    Cisco IP 전화기 상태 223

        [전화기 정보] 창 표시 223

        전화기 정보 필드 224

        상태 메뉴 표시 224

        상태 메시지 창 표시 225

        네트워크 통계 화면 표시 229

        네트워크 통계 화면 표시 230

        무선 통계 화면 표시 234

        통화 통계 창 표시 235

        현재 액세스 지점 창 표시 237

    Cisco IP 전화기 웹 페이지 239

        전화기 웹 페이지 액세스 240

- 장치 정보 240
- 네트워크 설정 243
- 네트워크 통계 248
- 장치 로그 251
- 스트리밍 통계 251
- 전화기의 정보를 XML로 요청 256
- 샘플 CallInfo 출력 257
- 샘플 LineInfo 출력 257
- 샘플 ModelInfo 출력 258

장 12

- 문제 해결 259
  - 일반 문제 해결 정보 259
  - 시작 문제 260
    - Cisco IP 전화기가 정상 시작 프로세스를 수행하지 않음 261
    - Cisco IP 전화기가 Cisco Unified Communications Manager에 등록되어 있지 않음 262
    - 전화기에 오류 메시지 표시 262
      - 전화기가 TFTP 서버나 Cisco Unified Communications Manager에 접속할 수 없음 262
      - 전화기가 TFTP 서버에 접속할 수 없음 262
      - 전화기가 서버에 접속할 수 없음 263
      - 전화기가 DNS를 사용해 접속할 수 없음 263
    - Cisco Unified Communications Manager 및 TFTP 서비스가 실행되지 않음 263
    - 구성 파일 변조 263
    - Cisco Unified Communications Manager 전화기 등록 264
    - Cisco IP 전화기에서 IP 주소를 확보할 수 없음 264
    - 전화가 등록되지 않음 264
  - 전화기 재설정 문제 265
    - 간헐적인 네트워크 중단으로 인한 전화기 재설정 265
    - DHCP 설정 오류로 인한 전화기 재설정 265
    - 잘못된 고정 IP 주소로 인한 전화기 재설정 265
    - 지나친 네트워크 사용으로 인한 전화기 재설정 266
    - 국제적 재설정에 따른 전화기 재설정 266

DNS 또는 기타 연결 문제로 인한 전화기 재설정	266
전화기의 전원이 켜지지 않음	266
전화기가 LAN에 접속할 수 없음	267
Cisco IP 전화기 보안 문제	267
CTL 파일 문제	267
인증 오류, 전화기가 CTL 파일을 인증하지 못함	267
전화기가 CTL 파일을 인증하지 못함	268
CTL 파일은 인증하지만 기타 구성 파일은 인증하지 않음	268
ITL 파일은 인증하지만 기타 구성 파일은 인증하지 않음	268
TFTP 인증 실패	268
전화기가 등록되지 않음	269
서명된 구성 파일을 요청하지 않음	269
영상 통화 문제	269
두 Cisco IP Video Phone 간의 영상 없음	269
비디오 화면이 끊기거나 프레임이 손실됨	270
영상 통화를 호전환할 수 없습니다	270
전화회의 동안 영상 없음	270
일반적인 전화기 통화 문제	271
전화 통화를 설정할 수 없음	271
전화기가 DTMF 숫자가 지연되는 것을 인식하지 못함	271
문제 해결 절차	272
Cisco Unified Communications Manager에서 전화 문제 보고서 만들기	272
전화기에서 콘솔 로그 만들기	272
TFTP 설정 확인	273
DNS 또는 연결 문제 파악	273
DHCP 설정 확인	274
새 전화기 구성 파일 생성	274
802.1X 인증 문제 식별	275
DNS 설정 확인	275
서비스 시작	276
Cisco Unified Communications Manager의 디버그 제어 정보	276

추가 문제 해결 정보 277

장 13

유지 보수 279

기본 재설정 279

전화기 키패드에서 초기 설정으로 전화기 재설정 279

[전화기에서 모든 설정 재설정] 메뉴 수행 280

백업 이미지에서 전화기 재부팅 280

네트워크 구성 재설정 수행 281

사용자 네트워크 구성 재설정 수행 281

CTL 파일 삭제 281

품질 보고서 도구 282

음질 모니터링 282

음질 문제 해결 팁 283

Cisco IP 전화기 청소 284

장 14

국제 사용자 지원 285

Unified Communications Manager 엔드포인트 로케일 설치 관리자 285

국제 통화 로깅 지원 285

언어 제한 사항 286





## 서론

- 개요, xv 페이지
- 대상, xv 페이지
- 설명서 규칙, xv 페이지
- 관련 설명서, xvii 페이지
- 설명서, 지원 및 보안 지침, xvii 페이지

## 개요

*Cisco Unified Communications Manager*용 *Cisco IP* 전화기 8800 시리즈 관리 설명서는 VoIP 네트워크 상의 전화기를 이해하고, 이 네트워크에 전화기를 설치하며, 구성하고, 관리하며, 문제를 해결하는 데 필요한 정보를 제공합니다.

IP 텔레포니 네트워크의 복잡성 때문에, 이 설명서는 *Cisco Unified Communications Manager*나 기타 네트워크 장치에서 수행해야 하는 절차에 관한 완벽한 세부 정보는 제공하지 않습니다.

## 대상

네트워크 엔지니어, 시스템 관리자 및 통신 엔지니어는 *Cisco IP* 전화기를 설정하는 데 필요한 단계들을 습득하기 위해 반드시 이 설명서를 살펴봐야 합니다. 이 설명서에 나온 작업에는 전화기 사용자를 대상으로 하지 않는 네트워크 설정 구성도 포함되어 있습니다. 이 수동 작업을 수행하려면 *Cisco Unified Communications Manager*에 익숙해야 합니다.

## 설명서 규칙

이 설명서는 다음과 같은 표기 규칙을 사용합니다.

규칙	설명
굵은 글꼴	명령과 키워드는 굵게 표시됩니다.

규칙	설명
기울임꼴 글꼴	값이 제공되는 인수는 기울임꼴로 표시됩니다.
[]	대괄호로 묶인 요소는 선택적 요소입니다.
{x y z}	대체 키워드는 중괄호로 묶어 세로선으로 구분합니다.
[x y z]	선택적인 대체 키워드는 대괄호로 묶어 세로선으로 구분합니다.
문자열	따옴표 없는 문자들의 집합입니다. 문자열 주변에 따옴표를 사용하지 마십시오. 그러면 따옴표도 문자열에 포함됩니다.
화면 글꼴	시스템에서 표시하는 정보 및 터미널 세션은 화면 글꼴로 표시됩니다.
입력 글꼴	사용자가 입력해야 하는 정보는 입력 글꼴로 표시됩니다.
기울임꼴 화면 글꼴	사용자가 값을 제공하는 인수는 기울임꼴 화면 글꼴로 표시됩니다.
^	^ 표시는 Control 키를 나타냅니다. 가령, 화면에서 키조합 ^D는 컨트롤 키를 누른 상태에서 D 키를 누르는 것을 의미합니다.
<>	암호와 같이 인쇄되지 않는 문자는 꺾쇠 괄호 안에 표시됩니다.



**참고** 독자가 주목해야 할 내용을 나타냅니다. 참고에는 유용한 제안이나 이 설명서에서 다루지 않는 자료에 대한 참조 정보가 포함됩니다.



**주의** 독자가 유의해야 하는 내용을 나타냅니다. 장비 손상이나 데이터 손실이 발생할 수 있으므로 주의해야 한다는 내용이 포함됩니다.

경고에서는 다음 규칙이 사용됩니다.



**주의** 중요 안전 지침

이 경고 표시는 위험을 나타냅니다. 부상이 발생할 수 있는 상황입니다. 장비를 작동하기 전에 전기 관련 재해에 유의하고 사고 예방을 위해 표준 절차를 숙지하십시오. 각 경고의 끝에는 이 디바이스와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾을 수 있도록 명령문 번호가 제공됩니다. 설명문 1071

이 지침을 반드시 숙지하십시오.



## 관련 설명서

관련 정보는 다음 섹션을 참조하십시오.

### Cisco IP 전화기 8800 시리즈 설명서

Cisco IP 전화기 8800 시리즈에 대한 [제품 지원](#) 페이지에서 해당 언어, 전화 모델 및 통화 제어 시스템 관련 문서를 찾아보십시오.

구축 설명서는 다음 URL에 있습니다.

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

### 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 Business Edition 6000 설명서

*Cisco Business Edition 6000* 설명서 및 사용 중인 Cisco Business Edition 6000 릴리스와 관련된 기타 게시물을 참조하십시오. 다음 URL에서 찾을 수 있습니다.

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



# 1 장

## 신규 및 변경된 정보

- 펌웨어 릴리스 14.2(1)에 대한 새 정보 및 변경된 정보, 1 페이지
- 펌웨어 릴리스 14.1(1)에 대한 새 정보 및 변경된 정보, 2 페이지
- 펌웨어 릴리스 14.0(1)에 대한 새 정보 및 변경된 정보, 2 페이지
- 펌웨어 릴리스 12.8(1)에 대한 새 정보 및 변경된 정보, 3 페이지
- 펌웨어 릴리스 12.7(1)에 관한 새 정보 및 변경된 정보, 3 페이지
- 펌웨어 릴리스 12.6(1)에 대한 새 정보 및 변경된 정보, 4 페이지
- 펌웨어 릴리스 12.5(1)SR3에 대한 새 정보, 4 페이지
- 펌웨어 릴리스 12.1(1)SR1에 대한 새 정보, 4 페이지
- 펌웨어 릴리스 12.1(1)SR1에 대한 새 정보, 5 페이지
- 펌웨어 릴리스 12.1(1)에 대한 새 정보, 5 페이지
- 펌웨어 릴리스 12.0(1)에 대한 새 정보, 6 페이지
- 펌웨어 릴리스 11.7(1)에 대한 새 정보, 6 페이지
- 펌웨어 릴리스 11.5(1)SR1에 대한 새 정보, 6 페이지
- 펌웨어 릴리스 11.5(1)에 대한 새 정보, 7 페이지
- 펌웨어 릴리스 11.0에 대한 새 정보, 8 페이지

## 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, 87 페이지
Cisco 헤드셋 730 USB 어댑터를 사용한 Extension Mobility 로그인 간소화	전화기 기능, 124 페이지
Cisco 헤드셋 700 시리즈에 대한 블루투스 음소거 동기화	전화기 기능, 124 페이지
Cisco 헤드셋 500 시리즈에 대한 새로운 설정: 도킹 이벤트 및 항상 켜기 모드	전화기 기능, 124 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	<a href="#">전화기 네트워크의 보안 강화, 87 페이지</a>
헌트 그룹에 대한 향상된 통화 알림	<a href="#">전화기 기능, 124 페이지</a>
고급 회선 모드에 대한 구성 가능한 발신 번호 표시	<a href="#">제품별 구성</a>
구성 가능한 지연된 PLAR	<a href="#">전화기 기능, 124 페이지</a>
Cisco 헤드셋으로 Extension Mobility 로그인에 대한 MRA 지원	<a href="#">전화기 기능, 124 페이지</a>
전환 로드 없이 전화기 마이그레이션	<a href="#">전화기를 다중 플랫폼 전화기로 직접 마이그레이션, 198 페이지</a>

## 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	<a href="#">제품별 구성, 146 페이지</a>
SIP OAuth 개선 기능	<a href="#">전화기 네트워크의 보안 강화, 87 페이지</a>
사용자 인터페이스 개선 기능	<a href="#">SRST(Survivable Remote Site Telephony), 77 페이지</a> <a href="#">전화기 기능, 124 페이지</a>
MRA에 대한 OAuth 개선 기능	<a href="#">Expressway를 통한 모바일 및 Remote Access, 181 페이지</a>

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.html>의 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	<a href="#">사용자의 전화기 모델 변경, 67 페이지</a>
헤드셋 업데이트 강화	<a href="#">장치 정보, 240 페이지</a>
Cisco 헤드셋으로 Extension Mobility 로그인 간소화	<a href="#">전화기 기능, 124 페이지</a>
기능 제어 변경 사항	<a href="#">제품별 구성, 146 페이지</a> , 새 필드는 음성 알림을 줄이고 통화를 스캠으로 표시합니다.
일반 변경 사항	Wi-Fi 및 PC 포트 명시: <ul style="list-style-type: none"> <li>• <a href="#">설정 메뉴에서 전화기 설정, 49 페이지</a></li> <li>• <a href="#">전화기에서 무선 LAN 활성화, 51 페이지</a></li> </ul>
웹 액세스 필드에 대한 정보 추가	<a href="#">제품별 구성, 146 페이지</a>
지원하지 않는 기능 제거	<a href="#">전화기 기능, 124 페이지</a>

## 펌웨어 릴리스 12.7(1)에 관한 새 정보 및 변경된 정보

표 2: 펌웨어 릴리스 12.7(1)용 Cisco IP 전화기 8800 관리 설명서 개정

개정	업데이트된 섹션
키 확장 모듈에서 배경 무늬 내용이 업데이트됨.	<a href="#">사용자 정의 배경 이미지, 117 페이지</a>
Cisco 헤드셋 730 지원 업데이트됨	<a href="#">장치 정보, 240 페이지</a>
Cisco 헤드셋 500 시리즈 펌웨어 릴리스 2.0 업데이트됨	<a href="#">장치 정보, 240 페이지</a> <a href="#">이전 버전의 Cisco Unified Communications Manager에서 헤드셋 관리, 211 페이지</a>
수신 헌트 그룹 통화 내용이 업데이트됨.	<a href="#">전화기 기능, 124 페이지</a>
전자 흑 구성 정보가 제거되었습니다.	<a href="#">제품별 구성, 146 페이지</a>

## 펌웨어 릴리스 12.6(1)에 대한 새 정보 및 변경된 정보

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

표 3: 펌웨어 릴리스 12.6(1)용 Cisco IP 전화기 8800 관리 설명서 개정

개정	업데이트된 섹션
세션 회선 모드에서 기본 회선으로 되돌리기 업데이트됨	제품별 구성, 146 페이지 세션 회선 모드 환경, 168 페이지

## 펌웨어 릴리스 12.5(1)SR3에 대한 새 정보

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

표 4: 펌웨어 릴리스 12.5(1)SR3용 Cisco IP 전화기 8800 관리 설명서 개정

개정	업데이트된 섹션
활성화 코드 온보딩 및 모바일 및 Remote Access 지원	활성화 코드 온보딩 및 모바일 및 Remote Access, 45 페이지
Cisco Unified Communications Manager에서 문제 보고 도구 사용을 지원합니다.	Cisco Unified Communications Manager에서 전화 문제 보고서 만들기, 272 페이지
새 항목	전화기 및 컴퓨터와 네트워크 연결 공유, 49 페이지
새 항목	비디오폰 카메라 보호, 39 페이지

## 펌웨어 릴리스 12.1(1)SR1에 대한 새 정보

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

표 5: 펌웨어 릴리스 12.5(1)SR1용 Cisco IP 전화기 8800 관리 설명서 개정

개정	업데이트된 섹션
Elliptic Curve 지원에 대한 지원	지원 보안 기능, 88 페이지

개정	업데이트된 섹션
롤오버 회선으로 향상된 회선 모드를 위한 통화 기록 향상 지원	<a href="#">고급 회선 모드에서 사용할 수 있는 기능</a> , 205 페이지
Cisco Unified Communications Manager Express 지원에서 꺾속말 페이지 지원	<a href="#">Cisco Unified Communications Manager Express 상호 작용</a> , 23 페이지
중국어에 대한 지원	<a href="#">언어 제한 사항</a> , 286 페이지
활성화 코드 온보딩 지원	<a href="#">온-프리미스 전화기에 대한 활성화 코드 온보딩</a> , 44 페이지
미디어 경로 및 상호 연결 설정 지원	<a href="#">미디어 경로 및 상호 연결 설정 지원</a> , 183 페이지
TLS 암호화 비활성화에 대한 지원	<a href="#">제품별 구성</a> , 146 페이지
헤드셋에 오디오 경로를 유지할 수 있도록 헤드셋 비활성화 지원	<a href="#">제품별 구성</a> , 146 페이지
헤드셋 매개 변수의 원격 구성에 대한 지원	<a href="#">이전 버전의 Cisco Unified Communications Manager에서 헤드셋 관리</a> , 211 페이지

## 펌웨어 릴리스 12.1(1)SR1에 대한 새 정보

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

표 6: 펌웨어 릴리스 12.1(1)SR1용 Cisco IP 전화기 8800 관리 설명서 개정

개정	업데이트된 섹션
Inter-Digit 타이머 T.302 향상을 위한 Enbloc 전화 걸기.	<a href="#">제품별 구성</a> , 146 페이지

## 펌웨어 릴리스 12.1(1)에 대한 새 정보

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

표 7: 펌웨어 릴리스 12.1(1)용 Cisco IP 전화기 8800 관리 설명서 개정

개정	업데이트된 섹션
모바일 및 Expressway를 통한 Remote Access가 이제 고급 회선 모드를 지원합니다.	<a href="#">다음에서 사용 가능한 전화기 기능: Expressway를 통한 모바일 및 Remote Access, 183 페이지</a>
	<a href="#">Expressway를 통한 모바일 및 Remote Access, 181 페이지</a>
	<a href="#">고급 회선 모드에서 사용할 수 있는 기능, 205 페이지</a>
웹 서버 액세스를 위한 TLS 1.2 활성화 또는 비활성화가 이제 지원됩니다.	<a href="#">제품별 구성, 146 페이지</a>
이제 G722.2 AMR-WB 오디오 코덱이 지원됩니다.	<a href="#">전화기 개요, 29 페이지</a>
	<a href="#">통화 통계 필드, 235 페이지</a>

## 펌웨어 릴리스 12.0(1)에 대한 새 정보

모든 새 기능이 [전화기 기능, 124 페이지](#)에 추가되었습니다.

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

표 8: 펌웨어 릴리스 12.0(1)용 Cisco IP 전화기 8800 관리 설명서 개정

개정	업데이트된 섹션
고급 회선 모드에서 통화 지정 보류, 통화 지정 보류 회선 상태, 그룹 당겨 받기 및 헌트 그룹이 업데이트됨	<a href="#">고급 회선 모드에서 사용할 수 있는 기능, 205 페이지</a>

## 펌웨어 릴리스 11.7(1)에 대한 새 정보

펌웨어 릴리스 11.7(1)용 사용 관리 업데이트가 필요하지 않음

## 펌웨어 릴리스 11.5(1)SR1에 대한 새 정보

모든 새 기능이 [전화기 기능, 124 페이지](#)에 추가되었습니다.

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



표 9: 펌웨어 릴리스 11.5(1)용 Cisco IP 전화기 8800 관리 설명서 개정

개정	업데이트된 섹션
Cisco IP 전화기 8865NR 지원을 위해 업데이트됨	<ul style="list-style-type: none"> <li>전화기 전원 요구 사항, 16 페이지</li> <li>네트워크 프로토콜, 18 페이지</li> <li>전화기 개요, 29 페이지</li> <li>버튼 및 하드웨어, 36 페이지</li> </ul>
고급 회선 모드에서 녹음 및 모니터링 지원을 위해 업데이트됨	고급 회선 모드에서 사용할 수 있는 기능, 205 페이지
WLAN 스캔 목록 지원을 위해 업데이트됨	전화기에서 무선 LAN 활성화, 51 페이지
	전화기에 무선 LAN 설정, 53 페이지
	네트워크 설정 구성, 58 페이지
MLPP를 지원하는 방해사절을 위해 업데이트됨	방해사절 설정, 175 페이지
구성 가능한 벨소리 지원을 위해 업데이트됨	제품별 구성, 146 페이지
강화된 보안	전화기 네트워크의 보안 강화, 87 페이지
일반 변경 사항	업데이트 대상 Cisco IP 전화기 웹 페이지, 239 페이지  Cisco Unified Communications Manager에서 전화기 기능 구성의 새 프레젠테이션 전화기 기능 구성, 144 페이지

## 펌웨어 릴리스 11.5(1)에 대한 새 정보

표 10: 펌웨어 릴리스 11.5(1)용 Cisco IP 전화기 8800 관리 설명서 개정

개정	업데이트된 섹션
고급 회선 모드는 지원됩니다.	추가 회선 키 설정, 205 페이지  고급 회선 모드에서 사용할 수 있는 기능, 205 페이지
새 표시를 위해 방해사절(DND)이 업데이트되었습니다.	방해사절 설정, 175 페이지
Opus 코덱은 지원됩니다.	전화기 개요, 29 페이지

개정	업데이트된 섹션
FIPS 모드가 추가되었습니다.	<a href="#">FIPS 모드 활성화, 94 페이지</a>
WLAN 설정이 업데이트 되었습니다.	<a href="#">전화기에 무선 LAN 설정, 53 페이지</a>
Cisco IP 전화기 8861 및 8865에 대한 WLAN 프로파일은 지원됩니다.	<a href="#">Cisco Unified Communications Manager를 사용하여 Wi-Fi 프로파일 설정, 56 페이지</a>
	<a href="#">Cisco Unified Communications Manager를 사용하여 Wi-Fi 그룹 설정, 58 페이지</a>
WLAN 인증 시도 설정은 지원됩니다.	<a href="#">WLAN 인증 시도 수 설정, 55 페이지</a>
WLAN 프롬프트 모드 활성화는 지원됩니다.	<a href="#">WLAN 프롬프트 모드 활성화, 55 페이지</a>
신호음 사용자 정의는 지원됩니다.	<a href="#">신호음 사용자 정의, 120 페이지</a>
네트워크 정보 화면 표시는 지원됩니다.	<a href="#">네트워크 통계 화면 표시, 229 페이지</a>

## 펌웨어 릴리스 11.0에 대한 새 정보

모든 새 기능이 [전화기 기능, 124 페이지](#)에 추가되었습니다.

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

표 11: 펌웨어 릴리스 11.0용 Cisco IP 전화기 8800 관리 설명서 개정

개정	업데이트된 섹션
규명과 단점을 해결하기 위해 업데이트됨	<ul style="list-style-type: none"> <li>• <a href="#">VPN 구성, 204 페이지</a></li> <li>• <a href="#">네트워크 설정 구성, 58 페이지</a></li> <li>• <a href="#">스위치 및 PC 포트를 위한 EEE(Energy Efficient Ethernet) 설정, 179 페이지</a></li> <li>• <a href="#">비디오 전송 해상도 설정, 209 페이지</a></li> <li>• <a href="#">E-SRST(Enhanced Survivable Remote Site Telephony), 80 페이지</a></li> </ul>
향상된 부분별 전화기 디버그 옵션 지원을 위해 업데이트됨	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified Communications Manager의 디버그 제어 정보, 276 페이지.</a></li> </ul>

개정	업데이트된 섹션
향상된 EAP-TLS + SCEP, PEAP-GTC 및 X.509 디지털 인증서 지원을 위해 업데이트됨	<ul style="list-style-type: none"> <li>• WLAN 보안, 97 페이지.</li> <li>• 인증 모드 설정, 101 페이지</li> <li>• 무선 보안 인증서, 101 페이지</li> </ul>
향상된 PRT(Problem Report Tool) 지원을 위해 업데이트됨	<ul style="list-style-type: none"> <li>• 문제 보고서 도구, 186 페이지.</li> <li>• 고객 지원 업로드 URL 구성, 187 페이지.</li> </ul>
애플리케이션 다이얼 규칙 지원을 위해 추가됨	<ul style="list-style-type: none"> <li>• 애플리케이션 다이얼 규칙, 80 페이지</li> </ul>
회선 텍스트 레이블을 위해 추가됨	<ul style="list-style-type: none"> <li>• 회선에 대한 레이블 설정, 188 페이지.</li> </ul>





## 부

# Cisco IP 전화기 정보

- 기술 세부사항, 13 페이지
- Cisco IP 전화기 하드웨어, 29 페이지





## 2 장

# 기술 세부사항

- 물리적 및 운영 환경 사양, 13 페이지
- 케이블 사양, 14 페이지
- 전화기 전원 요구 사항, 16 페이지
- 네트워크 프로토콜, 18 페이지
- VLAN 상호 작용, 22 페이지
- Cisco Unified Communications Manager 상호 작용, 22 페이지
- Cisco Unified Communications Manager Express 상호 작용, 23 페이지
- 음성 메시징 시스템 상호 작용, 24 페이지
- 전화기 시작 개요, 24 페이지
- 외부 장치, 26 페이지
- USB 포트 정보, 26 페이지
- 전화기 구성 파일, 27 페이지
- 네트워크 혼잡 시 전화기 동작, 27 페이지
- 두 개의 네트워크 라우터가 있는 네트워크에서 네트워크 동작, 28 페이지
- 애플리케이션 프로그래밍 인터페이스, 28 페이지

## 물리적 및 운영 환경 사양

다음 표에는 Cisco IP 전화기 8800 시리즈의 물리적 및 운영 환경 명세가 정리되어 있습니다.

표 12: 물리적 운영 사양

사양	값 또는 범위
동작 온도	0°~40°C(32°~104°F)
작동 상대 습도	작동: 10% ~ 90%(비응축) 비작동: 10% ~ 95%(비응축)
보관 온도	-10°~60°C(14°~140°F)

사양	값 또는 범위
높이	9.02in(229.1mm)
폭	10.13in(257.34mm)
깊이	1.57in(40mm)
무게	2.62lb(1.19kg)
전원	AC 어댑터 사용 시 100-240VAC, 50-60Hz, 0.5A 네트워크 케이블을 통한 인라인 전력 사용 시 48VDC, 0.2A
케이블	Category 3/5/5e/6 10Mbps 케이블, 4쌍 Category 5/5e/6 100Mbps 케이블, 4쌍 Category 5e/6 1000Mbps 케이블, 4쌍 참고 케이블에는 총 8개의 전도체를 위한 4쌍의 선이 있습니다.
거리 요구 사항	이더넷 사양에서 지원하는 대로, 각 Cisco IP 전화기와 스위치 사이의 최대 길이는 330피트(100미터)로 가정합니다.

## 케이블 사양

다음 정보는 케이블 사양을 나열합니다.

- 핸드셋 및 헤드셋 연결을 위한 RJ-9 잭(4-conductor)
- LAN 10/100/1000BaseT 연결을 위한 RJ-45 잭(전화기의 10/100/1000 네트워크 포트)
- 두 번째 10/100/1000BaseT 준수 연결을 위한 RJ-45 잭(전화기의 10/100/1000 컴퓨터 포트)
- 스피커 연결용 3.5mm 잭(Cisco IP 전화기 8861만 해당)
- 48볼트 전원 커넥터
- USB 포트/커넥터: Cisco IP 전화기 8851용 USB 포트 1개 및 Cisco IP 전화기 8861용 USB 포트 2개
- Cisco IP 전화기 8851 및 8861용 USB 커넥터로 간주되는 키 확장 모듈 커넥터 3개

## 네트워크 및 컴퓨터 포트 핀 배치도

비록 네트워크 연결에 네트워크 및 컴퓨터(액세스) 포트가 모두 사용될지라도, 이들은 각기 다른 용도를 지원하고 포트 핀 배치도가 서로 다릅니다.

- 네트워크 포트는 Cisco IP 전화기의 10/100/1000 SW 포트입니다.
- 컴퓨터(액세스) 포트는 Cisco IP 전화기의 10/100/1000 PC 포트입니다.



## 네트워크 포트 커넥터

다음 표에서는 네트워크 포트 커넥터 핀 배치도에 대해 설명합니다.

표 13: 네트워크 포트 커넥터 핀 배치도

핀 번호	기능
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
참고	BI는 양방향을 의미하고 DA, DB, DC 및 DD는 각각 데이터 A, 데이터 B, 데이터 C 및 데이터 D를 의미합니다.

## 컴퓨터 포트 커넥터

다음 표에서는 컴퓨터 포트 커넥터 핀 배치도에 대해 설명합니다.

표 14: 컴퓨터 (액세스) 포트 커넥터 핀 배치도

핀 번호	기능
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
참고	BI는 양방향을 의미하고 DA, DB, DC 및 DD는 각각 데이터 A, 데이터 B, 데이터 C 및 데이터 D를 의미합니다.

## 전화기 전원 요구 사항

Cisco IP 전화기는 외부 전원이나 PoE(Power over Ethernet)로 켤 수 없습니다. 별도의 전원 공급장치에서 외부 전원을 공급합니다. 스위치는 전화기 이더넷 케이블을 통해 PoE를 제공할 수 있습니다.

Cisco IP 전화기 8861 및 8865는 PoE 클래스 4 장치이며 추가 기능을 지원하는 클래스 4 기능이 있는 스위치 또는 회선 카드가 필요합니다.

전화기 전원 요구 사항에 대한 자세한 내용은 전화기의 데이터 시트를 참조하십시오.

외부 전원에서 전원이 공급되는 전화기를 설치할 때는 이더넷 케이블을 전화기에 연결하기 전에 전원 공급장치를 연결합니다. 외부 전원에서 전원이 공급되는 전화기를 삭제할 때는 전원 공급장치를 분리하기 전에 전화기와 이더넷 케이블의 연결을 해제합니다.

표 15: Cisco IP 전화기 전원 지침

전원 유형	지침
외부 전원: CP-PWR-CUBE-4= 외부 전원 공급장치를 통해 공급됩니다.	Cisco IP 전화기는 CP-PWR-CUBE-4 전원 공급장치를 사용합니다.
PoE 전원—전화기에 연결된 이더넷 케이블을 통해 스위치에서 공급됩니다.	Cisco IP 전화기 8851, 8851NR, 8861, 8865 및 8865NR은 액세스리용으로 802.3af을 지원합니다. 자세한 내용은 전화기의 데이터 시트를 참조하십시오. 스위치를 사용하려면 전화기의 무중단 작동을 위해 백업 전원 공급 장치가 필요합니다. 스위치에서 실행되는 CatOS 또는 IOS 버전이 원하는 전화기 배포를 지원하는지 확인합니다. 운영 체제 버전용 스위치에 관한 정보는 설명서를 참조하십시오.
UPoE(Universal Power Over Ethernet)	Cisco IP 전화기 8865 및 8865NR을 UPoE를 지원합니다.

다음 표의 문서는 다음 항목에 대한 추가 정보를 제공합니다.

- Cisco IP 전화기와 함께 작동하는 Cisco 스위치
- 양방향 전원공급 협상을 지원하는 Cisco IOS 릴리스
- 전원 요구 사항 및 제한 사항

표 16: 추가 정보

문서 항목	URL
PoE 솔루션	<a href="http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html">http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html</a>
UPoE	<a href="http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe">http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe</a>
Cisco Catalyst 스위치	<a href="http://www.cisco.com/c/en/us/products/switches/index.html">http://www.cisco.com/c/en/us/products/switches/index.html</a>

문서 항목	URL
통합 서비스 라우터	<a href="http://www.cisco.com/c/en/us/products/routers/index.html">http://www.cisco.com/c/en/us/products/routers/index.html</a>
Cisco IOS 소프트웨어	<a href="http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html">http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html</a>

## 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 송수화기를 들어올리거나 임의의 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 매개 변수를 구성합니다. 이러한 매개 변수는 전화기 구성 XML 파일 항목으로 전화기에 전송됩니다.

## LLDP에 대한 전원공급 협상

전화기와 스위치는 전화기가 소비하는 전원을 협상합니다. Cisco IP 전화기는 다중 전원 설정에서 작동하여, 사용할 수 있는 전원이 적을 때 전력 소비를 낮춥니다.

전화기가 재부팅한 후, 스위치는 전원공급 협상을 위해 한 프로토콜(CDP 또는 LLDP)에 잠깁니다. 스위치는 전화기가 전송하는 첫 번째 프로토콜(전원 TLV[Threshold Limit Value]를 포함함)에 잠깁니다. 시스템 관리자가 전화기에서 해당 프로토콜을 비활성화하면 스위치가 기타 프로토콜의 전원 요청에는 응답하지 않으므로, 전화기는 액세서리에 전원을 공급할 수 없습니다.

Cisco는 전원공급 협상을 지원하는 스위치에 연결할 때는 항상 전원공급 협상을 활성화(디폴트)할 것을 권장합니다.

전원공급 협상이 비활성화되면 스위치가 전화기의 전원을 중단할 수 있습니다. 스위치가 전원공급 협상을 지원하지 않으면 PoE를 통해 액세서리에 전원을 공급하기 전에 전원공급 협상 기능을 비활성화하십시오. 전원공급 협상 기능이 비활성화될 때 전화기는 IEEE 802.3af-2003 표준이 허용하는 최대 값까지 액세서리에 전원을 공급할 수 있습니다.



참고 • CDP 및 전원공급 협상이 비활성화될 때 전화기는 최대 15.4W까지 액세서리에 전원을 공급할 수 있습니다.

## 네트워크 프로토콜

Cisco IP 전화기 8800 시리즈는 음성 통신에 필요한 몇 개의 업계 표준과 Cisco 네트워크 프로토콜을 지원합니다. 다음 표에는 전화기에서 지원하는 네트워크 프로토콜에 대한 개요가 나와 있습니다.

표 17: Cisco IP Phone 8800 시리즈에서 지원하는 네트워크 프로토콜

네트워크 프로토콜	목적	사용 참고 사항
블루투스	블루투스는 짧은 거리에서 장치가 통신하는 방식을 지정하는 무선 개인 영역 네트워크(WPAN) 프로토콜입니다.	Cisco IP 전화기 8845, 8865 및 8851은 블루투스 4.1을 지원합니다.  Cisco IP 전화기 8861은 블루투스 4.0을 지원합니다.  Cisco IP 전화기 8811, 8841, 8851NR 및 8865NR은 블루투스를 지원하지 않습니다.
BootP(Bootstrap Protocol)	BootP는 Cisco IP 전화기와 같은 네트워크 장치를 활성화하여 IP 주소와 같은 특정 시작 정보를 확인합니다.	—
CAST(Cisco Audio Session Tunnel)	CAST 프로토콜을 통해 전화기와 관련 애플리케이션은 시그널링 구성 요소를 변경하지 않고 원격 IP 전화기와 통신할 수 있습니다.	Cisco IP 전화기는 SIP 프록시로 Cisco IP 전화기를 사용해 Cisco Unified Communications Manager와 CUVA 간의 인터페이스로 CAST를 사용합니다.
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.	Cisco IP Phone은 CDP를 사용해 Cisco Catalyst 스위치와 보조 VLAN ID, 포트별 전원 관리 세부 정보 및 QoS(Quality of Service) 구성 정보 같은 정보를 주고 받을 수 있습니다.

네트워크 프로토콜	목적	사용 참고 사항
CPPDP(Cisco Peer-to-Peer Distribution Protocol)	CPPDP는 장치의 피어 투 피어 계층 구조를 형성하는 데 사용되는 Cisco의 독점적 프로토콜입니다. 이 계층 구조는 피어 장치에서 주변 장치로 펌웨어 파일을 배포하는 데 사용됩니다.	CPPDP는 피어 펌웨어 공유 기능에 사용됩니다.
DHCP(Dynamic Host Configuration Protocol)	DHCP는 네트워크 장치에 IP 주소를 역동적으로 할당합니다.  DHCP를 사용하면 네트워크 IP 전화기를 연결하고, 수동으로 IP 주소를 할당하거나 추가 네트워크 매개 변수를 구성하지 않고도 전화기를 작동시킬 수 있습니다.	DHCP는 디폴트로 활성화됩니다. 비활성화된 경우에는 로컬에서 각 전화기에 IP 주소, 서브넷 마스크, 게이트웨이 및 TFTP 서버를 수동으로 구성해야 합니다.  DHCP 사용자 정의 옵션 150을 사용할 것을 권합니다. 이런 방식으로 TFTP 서버 IP 주소를 옵션 값으로 구성합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.  참고        옵션 150을 사용할 수 없다면, DHCP 옵션 66을 사용해 볼 수 있습니다.
HTTP(Hypertext Transfer Protocol)	HTTP는 인터넷 및 웹 상에서 정보 교환 및 문서 이동을 위해 사용하는 표준 경로입니다.	Cisco IP Phone은 XML 서비스 및 문제 해결을 위해 HTTP를 사용합니다.
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 애플리케이션에는 2개의 URL이 구성됩니다. HTTPS를 지원하는 Cisco IP 전화기는 HTTPS URL을 선택합니다.
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.	Cisco IP 전화기는 EAP-FAST 및 EAP-TLS라는 인증 방식에 대한 지원을 제공하여 IEEE 802.1X 표준을 시행합니다.  전화기에서 802.1X 인증이 활성화되면, PC 포트와 음성 VLAN을 비활성화해야 합니다.
IEEE 802.11n/802.11ac	IEEE 802.11 표준은 무선 근거리망(WLAN) 상에서 장치의 통신 방법을 지정합니다.  802.11n은 2,4 GHz 및 5GHz 대역에서 작동하고 802.11ac는 5GHz 대역에서 작동합니다.	802.11 인터페이스는 이더넷 케이블 연결을 사용할 수 없거나 원하지 않는 경우의 배포 옵션입니다.  Cisco IP 전화기 8861 및 8865만 WLAN을 지원합니다.

네트워크 프로토콜	목적	사용 참고 사항
IP(Internet Protocol)	IP는 네트워크를 통해 패킷을 처리하고 전송하는 메시징 프로토콜입니다.	<p>IP를 사용하여 통신하기 위해서는 네트워크 장치에 IP 주소, 서브넷 및 게이트웨이가 있어야 합니다.</p> <p>IP 주소, 서브넷 및 게이트웨이 ID는 Cisco IP 전화기에서 DHCP(Dynamic Host Configuration Protocol)를 사용하고 있는 경우 자동으로 할당됩니다. DHCP를 사용하지 않는다면 로컬에서 각 전화기에 수동으로 이러한 속성을 할당해야 합니다.</p> <p>Cisco IP 전화기는 IPv6 주소를 지원합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
LLDP(Link Layer Discovery Protocol)	LLDP는 일부 Cisco 및 타사 장치에서 지원되는 표준화된 네트워크 검색 프로토콜(CDP와 유사)입니다.	Cisco IP 전화기는 PC 포트에서 LLDP를 지원합니다.
LLDP-MED(Link Layer Discovery Protocol-Media Endpoint Devices)	LLDP-MED는 음성 제품을 위한 LLDP 확장 표준입니다.	<p>Cisco IP 전화기는 다음과 같은 정보를 주고받기 위해 SW 포트에서 LLDP-MED를 지원합니다.</p> <ul style="list-style-type: none"> <li>• 음성 VLAN 구성</li> <li>• 장치 검색</li> <li>• 전력 관리</li> <li>• 재고 관리</li> </ul>
RTP(Real-Time Transport Protocol)	RTP는 데이터 네트워크상에서 대화형 음성과 같은 실시간 데이터를 전송하기 위한 표준 프로토콜입니다.	Cisco IP 전화기는 RTP 프로토콜을 사용해 기타 전화기 및 게이트웨이에서 실시간 음성 트래픽을 주고받습니다.
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 SDP 기능은 일반적으로 작동 중인 Cisco Unified Communications Manager 또는 Media Gateway에 의해 전역으로 구성됩니다. 일부 SIP 엔드포인트에서는 엔드포인트 자체에 이러한 매개 변수의 구성을 허용할 수 있습니다.

네트워크 프로토콜	목적	사용 참고 사항
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 SIP는 패킷 텔레포니 네트워크 내에서 시그널링 및 세션 관리 기능을 처리합니다. 시그널링을 사용하여 네트워크 경계를 넘어서 통화 정보를 전송할 수 있습니다. 세션 관리는 엔드 투 엔드 통화 속성 제어 기능을 제공합니다.  전화기가 IPv4 전용, IPv6 전용 및 IPv4와 IPv6 둘 모두에서 작동하면 Cisco IP 전화기는 SIP 프로토콜을 지원합니다.
TCP(Transmission Control Protocol)	TCP는 연결 지향형 전송 프로토콜입니다.	Cisco IP 전화기는 TCP를 사용해 Cisco Unified Communications Manager에 연결하고, XML 서비스에 액세스합니다.
TLS(Transport Layer Security)	TLS는 통신 보안 및 인증을 위한 표준 프로토콜입니다.	보안 구현 시, Cisco IP 전화기는 Cisco Unified Communications Manager에 안전하게 등록된 경우 TLS 프로토콜을 사용합니다.
TFTP(Trivial File Transfer Protocol)	TFTP를 사용하면 네트워크상에서 파일을 전송할 수 있습니다.  Cisco IP 전화기에서 TFTP는 전화기 유형에 맞는 구성 파일을 확보할 수 있게 해줍니다.	TFTP의 경우 DHCP 서버가 자동으로 식별할 수 있는 TFTP 서버가 네트워크에 필요합니다. 전화기에서 DHCP 서버가 지정한 것이 아닌 다른 TFTP 서버를 사용하려면, 전화기의 네트워크 구성 메뉴를 사용해 해당 TFTP 서버의 IP 주소를 수동으로 할당해야 합니다.  자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
사용자 데이터그램 프로토콜	UDP는 데이터 패킷 전달을 위한 연결 메시징 프로토콜입니다.	UDP는 RTP 스트림에만 사용됩니다. 전화기에서 SIP 시그널링은 UDP를 지원하지 않습니다.

LLDP-MED 지원에 대한 자세한 내용은 LLDP-MED 및 Cisco Discovery Protocol 백서를 참조하십시오.

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

관련 항목

[802.1X 인증, 113 페이지](#)

[네트워크 설정 구성](#)

[전화기 시작 확인, 66 페이지](#)

[VLAN 상호 작용, 22 페이지](#)

[Cisco Unified Communications Manager 상호 작용, 22 페이지](#)

[Cisco Unified Communications Manager Express 상호 작용, 23 페이지](#)

[오디오 및 비디오 포트 범위 설정, 192 페이지](#)

Cisco Unified Communications Manager 설명서, xvii 페이지

## VLAN 상호 작용

Cisco IP 전화기에는 내부 이더넷 스위치가 들어 있어 전화기, 컴퓨터 (액세스) 포트, 그리고 전화기 후면의 네트워크 포트에 패킷을 착신 전환할 수 있습니다.

컴퓨터가 컴퓨터 (액세스) 포트에 연결되면, 컴퓨터와 전화기는 스위치에 대해 같은 물리적 링크를 공유하고 스위치에서 같은 포트를 공유합니다. 이렇게 공유된 링크는 네트워크상의 VLAN 구성에 다음과 같은 영향을 미칩니다.

- 현재 VLAN은 IP 서브넷 기반으로 구성되어 있을 수 있습니다. 그러나 동일한 포트에 연결된 다른 장치로 동일한 서브넷에 전화기를 할당하기 위해 추가 IP 주소가 제공되지 않을 수 있습니다.
- VLAN 지원 전화기의 데이터 트래픽으로 인해 VoIP 트래픽 품질이 떨어질 수 있습니다.
- 네트워크 보안상 VLAN 데이터 트래픽에서 VLAN 음성 트래픽을 격리해야 할 필요가 생길 수도 있습니다.

음성 트래픽을 별도의 VLAN으로 격리시키면 이러한 문제를 해결할 수 있습니다. 전화기가 연결된 스위치 포트는 다음을 처리하도록 별도의 VLAN에 구성됩니다.

- IP 전화기와 주고받는 음성 트래픽(예: Cisco Catalyst 6000 시리즈의 보조 VLAN)
- IP 전화기의 컴퓨터 (액세스) 포트를 통해 스위치와 연결된 PC와 주고받는 데이터 트래픽(기본 VLAN)

별도의 보조 VLAN에 전화기를 격리하면 음성 트래픽의 품질이 향상되고, 각 전화기를 위한 IP 주소가 충분하지 않은 기존 네트워크에 다수의 전화기를 추가할 수 있습니다.

자세한 내용은 Cisco 스위치에 포함된 문서를 참조하십시오. 스위치 정보는 다음 URL에서도 확인할 수 있습니다.

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

## 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](#), xvii 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 후플래시 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 페이지링이라고도 하는 인터콤 전화를 지원합니다. 하지만 통화 중 전화기에 의해 페이지가 거부됩니다.

CME 모드에서는 세션 라인 모드와 고급 라인 모드가 모두 지원됩니다.

## 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 사용자에게 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 시작 개요

VoIP 네트워크에 연결할 때 Cisco IP 전화기는 표준 시작 프로세스를 통과합니다. 특정 네트워크 구성에 따라, 이러한 단계 중 일부만 Cisco IP 전화기에서 발생할 수 있습니다.

1. 스위치에서 전원을 연습니다. 전화기가 외부 전원을 사용하고 있지 않으면 스위치는 전화기에 연결된 이더넷 케이블을 통해 인라인 전원을 제공합니다.
2. (무선 LAN의 Cisco IP 전화기 8861 및 8865 전용) 액세스 지점을 검색합니다. Cisco IP 전화기 8861 및 8865의 경우 무선 통신으로 RF 적용 범위를 검색합니다. 전화기는 네트워크 프로파일을 검색하고 일치하는 SSID 및 인증 유형을 포함하는 액세스 지점을 검색합니다. 전화기는 네트워크 프로파일과 일치하는 최고 RSSI를 사용하여 액세스 지점과 연결됩니다.
3. (무선 LAN의 Cisco IP 전화기 8861 및 8865 전용) 액세스 지점에서 인증합니다. Cisco IP 전화기가 인증 프로세스를 시작합니다. 다음 표에서는 인증 프로세스에 대해 설명합니다.

인증 유형	키 관리 옵션	설명
열기	없음	아무 장치나 액세스 지점에 인증할 수 있습니다. 보안 강화를 위해 정적 WEP 암호화가 선택적으로 사용될 수 있습니다.

인증 유형	키 관리 옵션	설명
공유 키	없음	전화기는 WEP 키를 사용하여 도전 텍스트를 암호화하고 액세스 지점은 네트워크 액세스를 사용하려면 도전 텍스트를 암호화하는 데 사용된 WEP 키를 확인해야 합니다.
PEAP 또는 EAP-FAST	없음	네트워크 액세스를 사용할 수 있으려면 RADIUS 서버가 사용자 이름 및 암호를 인증해야 합니다.

4. 저장된 전화기 이미지를 로드합니다. 시작 시, 전화기는 플래시 메모리에 저장되는 전화기 펌웨어 이미지를 로드하는 부트스트랩 로더를 실행합니다. 이 이미지를 사용하는 경우 전화기는 소프트웨어와 하드웨어를 초기화합니다.
5. VLAN을 구성합니다. Cisco IP 전화기가 Cisco Catalyst 스위치에 연결된 경우 스위치는 스위치에 정의된 음성 VLAN에 대해 전화기에 알립니다. IP 주소에 대한 DHCP(Dynamic Host Configuration Protocol) 요청으로 진행하려면 전화기에서 VLAN 구성원 자격을 알고 있어야 합니다.
6. IP 주소를 얻습니다. Cisco IP 전화기가 DHCP를 사용하여 IP 주소를 얻으려면 전화기에서 DHCP 서버를 조회하여 IP 주소를 얻습니다. 네트워크에서 DHCP를 사용하지 않는다면 로컬에서 각 전화기에 로컬로 정적 IP 주소를 할당해야 합니다.
7. CTL 파일을 요청합니다. TFTP 서버는 CTL 파일을 저장합니다. 이 파일은 전화기와 Cisco Unified Communications Manager 간에 보안 연결을 설정하는 데 필요한 인증서를 포함합니다.  
자세한 내용은 특정 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
8. ITL 파일을 요청합니다. 전화기는 CTL 파일을 요청한 후 ITL 파일을 요청합니다. ITL 파일은 전화기가 신뢰할 수 있는 엔티티의 인증서를 포함합니다. 인증서는 서버와 보안 연결을 인증하거나 서버에서 서명한 디지털 서명을 인증하는 데 사용됩니다. Cisco Unified Communications Manager 8.5 이상은 ITL 파일을 지원합니다.
9. TFTP 서버에 액세스합니다. IP 주소를 할당할 뿐만 아니라, DHCP 서버는 Cisco IP 전화기를 TFTP 서버에 연결합니다. 전화기가 통계적으로 정의된 IP 주소를 가질 경우, 전화기에 로컬로 TFTP 서버를 구성해야 합니다. 그런 다음 전화기는 TFTP 서버에 직접 연결합니다.



참고 또한 DHCP가 할당하는 서버 대신 사용할 대체 TFTP 서버를 할당할 수 있습니다.

10. 구성 파일을 요청합니다. TFTP 서버에는 Cisco Unified Communications Manager에 연결하기 위한 매개 변수와 전화기용 기타 정보를 정의하는 구성 파일이 있습니다.
11. Cisco Unified Communications Manager에 연결합니다. 구성 파일은 Cisco IP 전화기가 Cisco Unified Communications Manager와 통신하고 전화기에 로드 ID를 제공하는 방법을 정의합니다. 전화기는 TFTP 서버에서 파일을 얻은 후, 목록에서 가장 우선 순위가 높은 Cisco Unified Communications Manager에 연결을 시도합니다.

보안 시그널링(암호화되거나 인증됨)을 위해 전화기의 보안 프로파일이 구성되고 Cisco Unified Communications Manager가 보안 모드로 설정된 경우 전화기는 TLS 연결을 설정합니다. 그렇지 않으면, 전화기는 비보안 TCP 연결을 설정합니다.

전화기가 수동으로 데이터베이스에 추가되었으면 Cisco Unified Communications Manager가 전화를 식별합니다. 전화기가 수동으로 데이터베이스에 추가되지 않았고 자동 등록이 Cisco Unified Communications Manager에서 활성화된 경우 전화기가 Cisco Unified Communications Manager 데이터베이스에서 자동 등록을 시도합니다.



참고 CTL 클라이언트를 구성할 때 자동 등록은 비활성화됩니다. 이 경우, 전화를 수동으로 Cisco Unified Communications Manager 데이터베이스에 추가해야 합니다.

관련 항목

[Cisco Unified Communications Manager 설명서, xvii 페이지](#)

## 외부 장치

잘못된 RF(무선 주파수) 및 AF(오디오 주파수) 신호를 차단하는 우수한 품질의 외부 장치를 사용하는 것이 좋습니다. 외부 장치로는 헤드셋, 케이블 및 커넥터가 있습니다.

이러한 장치의 품질과 휴대 전화 또는 양방향 무선 장치 등과 같은 기타 장치와의 근접 정도에 따라 약간의 오디오 잡음이 계속 발생할 수도 있습니다. 이러한 경우 다음 중 한 가지 이상의 작업을 수행하는 것이 좋습니다.

- 외부 장치를 RF 또는 AF 신호 발생지로부터 멀리 옮기십시오.
- 외부 장치 케이블의 경로를 RF 또는 AF 신호 발생지로부터 멀리 지정하십시오.
- 외부 장치에 차폐된 케이블을 사용하거나 보호성이 좋은 케이블과 커넥터를 사용하십시오.
- 외부 장치 케이블의 길이를 줄이십시오.
- 외부 장치용 케이블에 페라이트 또는 이와 유사한 기타 물질을 바르십시오.

Cisco에서는 기존 장치, 케이블 및 커넥터의 성능을 보장할 수 없습니다.



주의 EU(유럽 연합) 국가에서는 EMC 규정 [89/336/EC]를 엄격히 준수하는 외부 스피커, 마이크 및 헤드셋만 사용하십시오.

## USB 포트 정보

Cisco IP 전화기 8851, 8851NR, 8861, 8865 및 8865NR은 각 USB 포트에 연결하는 장치를 최대 5개까지 지원합니다. 전화기에 연결하는 각 장치는 최대 장치 수에 포함됩니다. 예를 들어 전화기에서 측

면 포트에 있는 5개 USB 장치를 지원하고 후면 포트에서 5개 이상의 표준 USB 장치를 지원할 수 있습니다. 다양한 타사 USB 제품은 다수의 USB 장치로 간주합니다. 예를 들면 USB 허브 및 헤드셋을 포함하는 장치는 두 개의 USB 장치로 계산될 수 있습니다. 자세한 내용은 USB 장치 설명서를 참조하십시오.



- 참고
- 전원이 공급되지 않은 허브는 지원되지 않고, 전원이 공급되지만 5개 이상의 포트가 있는 허브는 지원되지 않습니다.
  - USB 허브를 통해 전화기에 연결하는 USB 헤드셋은 지원되지 않습니다.

전화기에 연결된 각 키 확장 모듈은 USB 장치로 계산됩니다. 3개의 키 확장 모듈이 전화기에 연결된 경우 이들은 3개의 USB 장치로 계산됩니다.

## 전화기 구성 파일

전화기에 대한 구성 파일은 TFTP 서버에 저장되고 Cisco Unified Communications Manager에 연결하기 위한 매개 변수를 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 이미지가 로드된 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.

관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## 네트워크 혼잡 시 전화기 동작

네트워크 성능을 저하시키는 것이라면 무엇이든 전화기 오디오 및 비디오 품질에 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)

## 두 개의 네트워크 라우터가 있는 네트워크에서 네트워크 동작

Cisco IP 전화기 8800 시리즈는 방화벽을 사용하여 중간자 공격과 같은 사이버 침투에 대한 보호를 제공합니다. 이 방화벽은 비활성화할 수 없습니다. 그러나 동일한 서브넷의 두 네트워크 라우터 2개 및 IP 재전송으로 네트워크를 구성하는 경우에는 전화기의 트래픽을 중지할 수 있습니다.

이 네트워크 설정은 중간자 공격과 유사하므로 전화기 방화벽이 트래픽을 중지합니다. 전화기는 전화기의 다른 서브넷에서 다른 대상 IP에 대한 재전송 패킷을 수신합니다. 전화기는 두 개 이상의 라우터가 있는 네트워크에 있고 기본 라우터는 트래픽을 두 번째 라우터로 보냅니다.

방화벽이 트래픽을 중지하는 것으로 의심되는 경우 전화기 로그를 살펴보세요. 연결 설정을 시도할 때 운영 체제에서 오류 코드 1 알람을 살펴봅니다. 서명 중 하나는 다음과 같습니다.

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

동일한 서브넷에 두 개의 네트워크 라우터가 있고 IP 재전송 기능이 있는 네트워크는 일반 구성이 아닙니다. 이 네트워크 설정을 사용하는 경우 서브넷의 한 라우터만 사용할 것을 고려하십시오. 그러나 동일한 서브넷에 두 개의 네트워크 라우터가 필요한 경우 라우터의 IP 재전송을 비활성화하고 전화기를 재부팅하십시오.

## 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.



# 3 장

## Cisco IP 전화기 하드웨어

- 전화기 개요, 29 페이지
- Cisco IP Phone 8811, 31 페이지
- Cisco IP 전화기 8841 및 8845, 32 페이지
- Cisco IP 전화기 8851 및 8851NR, 33 페이지
- Cisco IP 전화기 8861, 8865 및 8865NR, 35 페이지
- 버튼 및 하드웨어, 36 페이지
- 비디오폰 카메라 보호, 39 페이지

### 전화기 개요

Cisco IP 전화기 8800 시리즈는 IP(Internet Protocol) 네트워크를 통해 음성 통신을 제공합니다. Cisco IP Phone은 디지털 비즈니스 전화와 유사한 기능을 수행하며, 전화를 걸고, 음소거, 보류, 호전환 등의 기능에 액세스할 수 있습니다. 뿐만 아니라 전화기가 데이터 네트워크에 연결되므로 네트워크 정보 및 서비스와 사용자 정의 가능한 기능과 서비스에 대한 액세스를 포함한 향상된 IP 텔레포니 기능을 제공합니다.

Cisco IP 전화기 8811은 그레이스케일 LCD 화면을 가집니다. Cisco IP 전화기 8841, 8845, 8851, 8851NR, 8861 및 8865는 24비트 컬러 LCD 화면을 가집니다.

기능을 전화 회선 키에 추가할 때 사용 가능한 회선 키의 수에 따라 제한이 있습니다. 전화기에는 회선 키 수보다 많은 기능을 추가할 수 없습니다.

Cisco IP 전화기에는 다음과 같은 기능이 있습니다.

- 세션 회선 모드에서 최대 5개 회선 또는 고급 회선 모드에서 최대 10개의 회선을 지원하는 프로그램 가능 기능 버튼
- 전체 비디오 기능(Cisco IP 전화기 8845, 8865 및 8865NR만)
- 기가비트 이더넷 연결
- 무선 헤드셋에 블루투스 지원(Cisco IP 전화기 8845, 8851, 8861 및 8865만 해당. 이 기능은 Cisco IP 전화기 8811, 8841, 8851NR 및 8865NR에서는 지원되지 않습니다.)
- 외부 마이크 및 스피커에 대한 지원(Cisco IP 전화기 8861, 8865 및 8865NR만)

- Wi-Fi에 의한 네트워크 연결(Cisco IP 전화기 8861 및 8865만. Wi-Fi는 Cisco IP 전화기 8865NR에서 지원되지 않습니다.)
- USB 포트:
  - Cisco IP 전화기 8851 및 8851NR용 USB 포트 1개
  - Cisco IP 전화기 8861, 8865 및 8865NR용 USB 포트 2개

Cisco IP 전화기 8845, 8865 및 8865NR은 내장된 비디오 카메라로 영상 통화를 지원합니다. 이 기능을 사용하면 친구나 동료들과 협업을 할 수도 있고 해당 전화기로 직접 얼굴을 보며 회의를 열 수도 있습니다.



**참고** Cisco IP 전화기 8845, 8865 및 8865NR용 상자와 포장용 보관해야 합니다. 이러한 전화기의 카메라는 파손되기 쉽습니다. 전화기를 이동하는 경우 카메라를 보호하기 위해 전화기를 원래 상자에 포장하는 것이 좋습니다. 자세한 내용은 [비디오폰 카메라 보호, 39 페이지](#)의 내용을 참조하십시오.

영상 통화는 다음 기능을 포함합니다.

- PIP - 오른쪽 아래, 오른쪽 위, 왼쪽 위, 왼쪽 아래의 4개 위치 중에 선택합니다. PIP를 끌 수도 있습니다.
- 통화 변경 - PIP 보기의 화면을 전환합니다. 통화 변경 소프트웨어는 PIP가 꺼진 경우 비활성화됩니다.
- 셀프 뷰 비디오 - 내 모습을 비디오에 표시되는 대로 보려면 셀프 뷰 비디오를 선택합니다.
- 비디오 UI 및 전화회의/호전환 초기화 - 전화회의를 시작하려면 선택합니다.

영상 통화에 대한 추가 정보는 *Cisco Unified Communications Manager*용 *Cisco IP* 전화기 8800 시리즈 사용 설명서 및 해당 특정 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

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
- iSAC





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 있는 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.

관련 항목

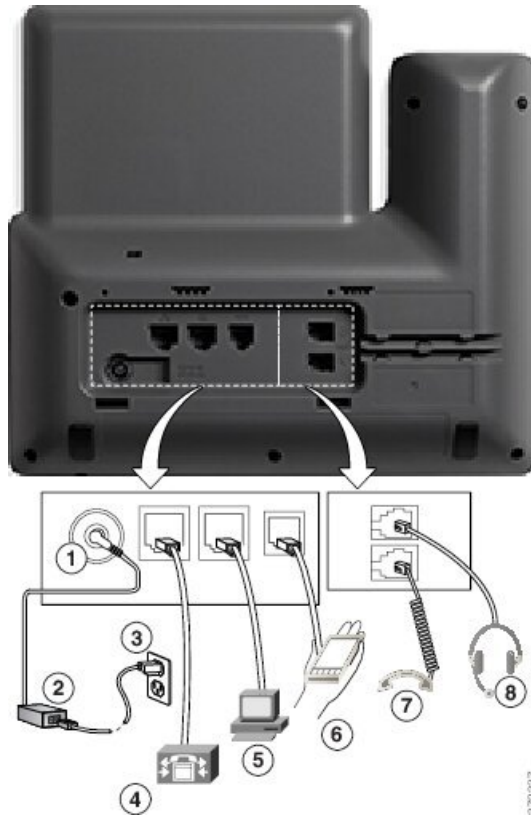
[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## Cisco IP Phone 8811

다음 섹션에서는 Cisco IP Phone 8811 특성에 대해 설명합니다.

### 전화기 연결

다음 다이어그램에 나타난 대로, 전화기를 조직의 IP 텔레포니 네트워크에 연결합니다.



1	DC 어댑터 포트(DC48V)	5	액세스 포트(10/100/1000 PC) 연결
2	AC-DC 간 전원 공급 장치(선택 사항)	6	보조 포트
3	AC 전원 콘센트(선택 사항)	7	핸드셋 연결
4	네트워크 포트(10/100/1000 SW) 연결. IEEE 802.3at 전원 사용됨	8	아날로그 헤드셋 연결(선택 사항)



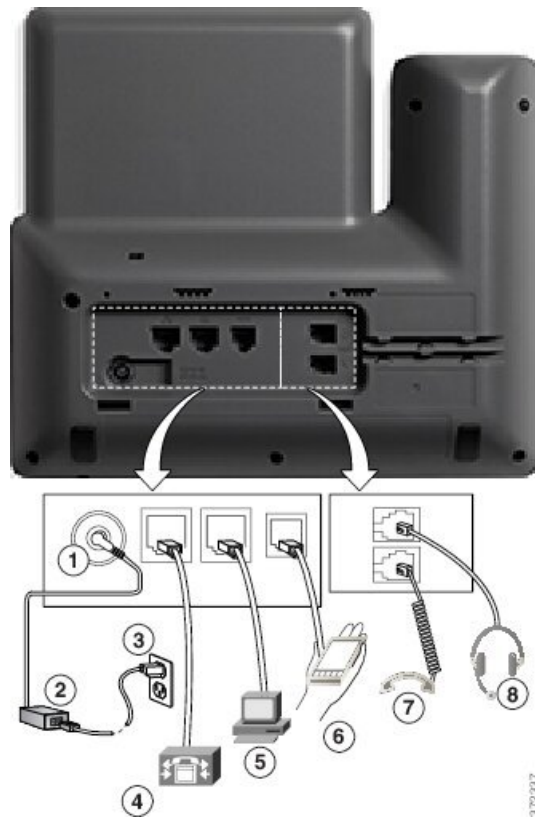
참고 Cisco IP Phone 8811은 키 확장 모듈을 지원하지 않습니다.

## Cisco IP 전화기 8841 및 8845

다음 섹션에서는 Cisco IP 전화기 8841 및 8845의 특성을 설명합니다.

### 전화기 연결부

다음 다이어그램을 사용하여 전화기를 회사 IP 전화 통신 네트워크에 연결합니다.



1	DC 어댑터 포트(DC48V)	5	액세스 포트(10/100/1000 PC) 연결
2	AC-DC 간 전원 공급 장치(선택 사항)	6	보조 포트
3	AC 전원 콘센트(선택 사항)	7	핸드셋 연결
4	네트워크 포트(10/100/1000 SW) 연결. IEEE 802.3at 전원 사용됨	8	아날로그 헤드셋 연결(선택 사항)



참고 Cisco IP 전화기 8841 및 8845는 키 확장 모듈을 지원하지 않습니다.

## Cisco IP 전화기 8851 및 8851NR

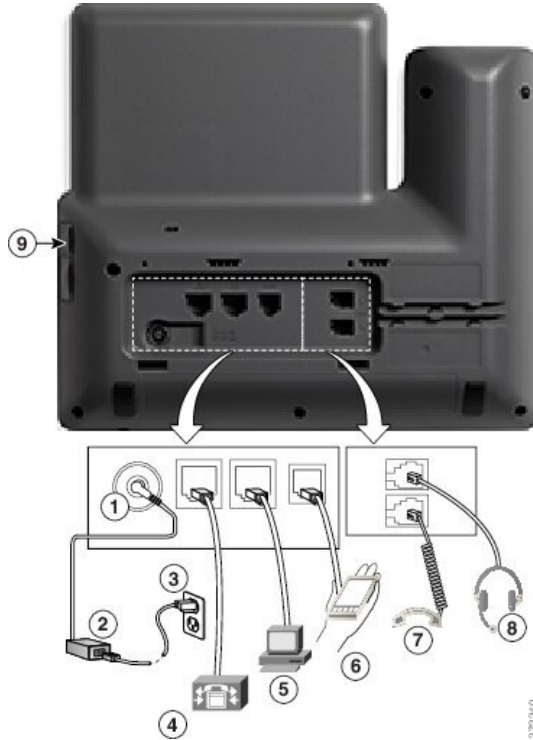
다음 섹션에서는 Cisco IP 전화기 8851 및 8851NR의 특성을 설명합니다.



참고 Cisco IP 전화기 8851NR은 블루투스를 지원하지 않습니다. 그렇지 않으면, Cisco IP 전화기 8851과 Cisco IP 전화기 8851NR은 같은 기능을 지원합니다.

## 전화기 연결

다음 다이어그램에 나타난 대로, 전화기를 회사 IP 텔레포니 네트워크에 연결합니다.



1	DC 어댑터 포트(DC48V)	6	보조 포트
2	AC-DC 간 전원 공급 장치(선택 사항)	7	핸드셋 연결
3	AC 전원 콘센트(선택 사항)	8	아날로그 헤드셋 연결(선택 사항)
4	네트워크 포트(10/100/1000 SW) 연결. IEEE 802.3at 전원 사용됨	9	USB 포트
5	액세스 포트(10/100/1000 PC) 연결		



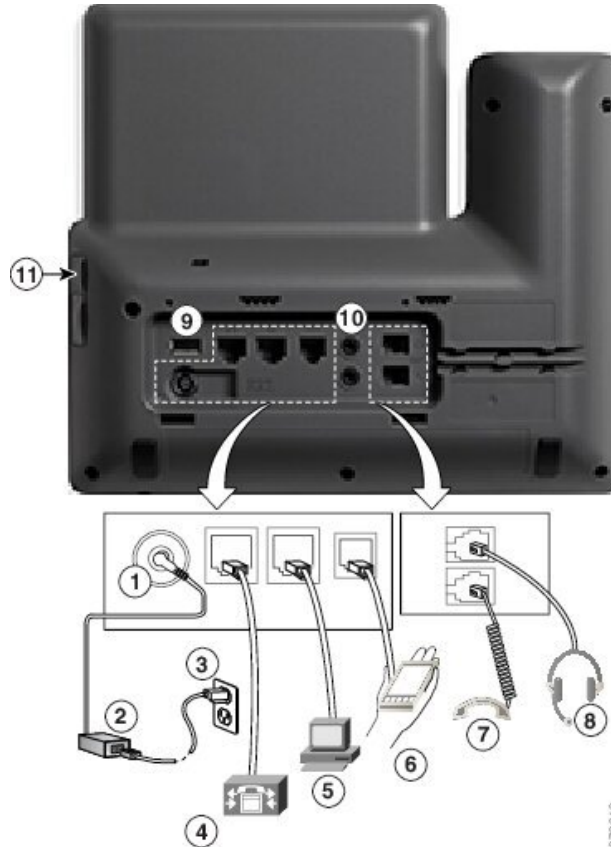
**참고** 각 USB 포트는 최대 5개 지원 및 비 지원 장치와의 연결을 지원합니다. 전화기에 연결된 각 장치는 최대 장치 수에 포함됩니다. 예를 들어 전화기의 측면 포트에서 5개 USB 장치를 지원할 수 있습니다(예: 키 확장 모듈 2개, 헤드셋 1개, 허브 1개 및 다른 표준 USB 장치 1개). 다양한 타사 USB 제품은 다수의 USB 장치로 간주합니다. 예를 들면 USB 허브 및 헤드셋을 포함하는 장치는 두 개의 USB 장치로 계산될 수 있습니다. 자세한 내용은 USB 장치 설명서를 참조하십시오.

# Cisco IP 전화기 8861, 8865 및 8865NR

다음 섹션에서는 Cisco IP 전화기 8861, 8865 및 8865NR의 특성을 설명합니다.

## 전화기 연결부

다음 다이어그램에 나타난 대로, 전화기를 회사 IP 텔레포니 네트워크에 연결합니다.



1	DC 어댑터 포트(DC48V)	7	핸드셋 연결
2	AC-DC 간 전원 공급 장치(선택 사항)	8	아날로그 헤드셋 연결(선택 사항)
3	AC 전원 콘센트(선택 사항)	9	USB 포트
4	네트워크 포트(10/100/1000 SW) 연결. IEEE 802.3at 전원 사용됨	10	오디오 입력/출력 포트
5	액세스 포트(10/100/1000 PC) 연결	11	USB 포트
6	보조 포트		



참고 각 USB 포트는 최대 5개 지원 및 비 지원 장치와의 연결을 지원합니다. 전화기에 연결된 각 장치는 최대 장치 수에 포함됩니다. 예를 들어 전화기의 측면 포트에서 5개의 USB 장치(예: 키 확장 모듈 3개, 허브 1개, 기타 표준 USB 장치 1개)를 지원하고 후면 포트에서 5개의 표준 USB 장치를 추가 지원할 수 있습니다. 다양한 타사 USB 제품은 다수의 USB 장치로 간주합니다. 예를 들면 USB 허브 및 헤드셋을 포함하는 장치는 두 개의 USB 장치로 계산될 수 있습니다. 자세한 내용은 USB 장치 설명서를 참조하십시오.

## 버튼 및 하드웨어

Cisco IP 전화기 8800 시리즈에는 두 가지 하드웨어 유형이 있습니다.

- Cisco IP 전화기 8811, 8841, 8851, 8851NR 및 8861 - 카메라 없음
- Cisco IP 전화기 8845, 8865 및 8865NR - 내장된 카메라가 있음

다음 그림은 Cisco IP 전화기 8845를 나타냅니다.
















그림 1: Cisco IP 전화기 8845 버튼 및 하드웨어




다음 표에서는 Cisco IP 전화기 8800 시리즈 버튼에 대해 설명합니다.

표 18: Cisco IP 전화기 8800 시리즈 버튼

1	핸드셋과 핸드셋 표시등	착신 통화(빨간색 깜박임)인지 새 음성 메시지(빨간색 지속)인지 나타냅니다.
---	--------------	--

2	카메라 Cisco IP 전화기 8845, 8865 및 8865NR 전용	영상 통화를 위해 카메라를 사용합니다.
3	프로그램 가능한 기능 버튼 및 회선 버튼	 전화기 회선, 기능 및 통화 세션에 액세스합니다. 기능을 전화 회선 키에 추가할 때 사용 가능한 회선 키의 수에 따라 제한이 있습니다. 전화기에는 회선 키 수보다 많은 기능을 추가할 수 없습니다. 자세한 내용은 "Cisco IP 전화기 하드웨어" 창의 소프트키, 회선 및 기능 버튼 섹션을 참조하십시오.
4	소프트키 버튼	 기능 및 서비스에 액세스합니다. 자세한 내용은 "Cisco IP 전화기 하드웨어" 창의 소프트키, 회선 및 기능 버튼 섹션을 참조하십시오.
5	뒤로, 탐색 클러스터 및 릴리스	뒤로  이전 화면 또는 메뉴로 돌아갑니다. 탐색 클러스터  탐색 벨소리 및 선택 버튼 - 메뉴를 스크롤하고 항목을 강조 표시하며 강조 표시된 항목을 선택합니다. 릴리스  연결된 통화 또는 세션을 종료합니다.
6	보류/보류해제, 전화회의 및 호전환	보류/보류해제  활성 통화를 보류하고 보류 통화를 해제합니다. 전화회의  전화회의를 작성합니다. 호전환  통화를 호전환합니다.
7	스피커폰, 음소거 및 헤드셋	스피커폰  스피커폰을 켜거나 끕니다. 스피커폰을 켜면 버튼에 불이 들어옵니다. 음소거  마이크를 켜거나 끕니다. 마이크를 음소거하면 버튼에 불이 들어옵니다. 헤드셋  헤드셋을 켭니다. 헤드셋을 설정하면 버튼이 켜집니다. 헤드셋 모드를 종료하려면 헤드셋을 들거나 스피커폰  을 선택합니다.
8	연락처, 애플리케이션 및 메시지	연락처  개인 또는 회사 디렉터리에 액세스합니다. 애플리케이션  최근 통화 기록, 사용자 환경 설정, 전화기 설정 및 전화기 모델 정보에 액세스합니다. 메시지  음성 메시징 시스템에 자동 다이얼합니다.







9	볼륨 버튼	 핸드셋, 헤드셋 및 스피커폰 볼륨(오프 훅)과 벨소리 장치 볼륨(온 훅)을 조절합니다.
---	-------	--

## 소프트키, 회선 및 기능 버튼

여러 가지 방법으로 전화기의 기능과 상호 작용할 수 있습니다.

- 화면 아래에 있는 소프트키를 통해 소프트키 위 화면에 표시된 기능에 액세스할 수 있습니다. 소프트키는 당시 수행 중인 작업에 따라 달라집니다. 추가... 소프트키는 추가 기능을 사용할 수 있음을 나타냅니다.
- 화면의 측면에 있는 기능 및 회선 버튼을 사용하여 전화기 기능 및 전화 회선에 액세스할 수 있습니다.
  - 기능 버튼—단축 다이얼 또는 당겨받기, 같은 기능 및 다른 회선에서 사용자 상태를 보는 데 사용됩니다.
  - 회선 버튼—전화를 받거나 보류된 통화를 보류 해제하는 데 사용됩니다. 활성 통화에 사용되지 않을 경우 부재 중 통화 표시와 같은 전화기 기능을 시작하는 데 사용됩니다.

기능 및 회선 버튼이 켜져서 다음 상태를 나타냅니다.

LED 색상 및 상태	일반 회선 모드: 회선 버튼	일반 회선 모드: 기능 버튼 고급 회선 모드
 녹색, 지속 LED	활성 통화 또는 양방향 인터콤 통화, 보류된 통화, 사용 중 프라이버시	활성 통화 또는 양방향 인터콤 통화, 사용 중 프라이버시
 녹색, 깜박이는 LED	해당 없음	보류 중인 통화
 황색, 지속 LED	걸려오는 전화, 되돌리기 통화, 단방향 인터콤 통화, 힌트 그룹에 로그인됨	단방향 인터콤 통화, 힌트 그룹에 로그인됨
 황색, 깜박이는 LED	해당 없음	걸려오는 통화, 되돌리기 통화
 빨간색, 지속 LED	원격 회선 사용 중, 원격 회선 보류 중, 방해 금지 활성화	원격 회선 사용 중, 방해 금지 활성화
 빨간색, 깜박이는 LED	해당 없음	원격 회선 대기 중

관리자는 일부 기능을 소프트키 또는 기능 버튼으로 설정할 수 있습니다. 또한 소프트키 또는 연결된 하드 버튼으로 일부 기능에 액세스할 수 있습니다.



## 비디오폰 카메라 보호

비디오폰의 카메라는 파손되기 쉬우며 전화기를 운송하는 동안 파손될 수 있습니다.

시작하기 전에

다음 중 하나가 필요합니다.

- 원래 전화기 상자 및 포장 재료
- 폼 또는 버블랩과 같은 포장 재료

프로시저

---

**단계 1** 원래 상자가 있는 경우:

- a) 렌즈가 잘 보호되도록 카메라에 폼을 넣습니다.
- b) 전화기를 원래 상자에 넣습니다.

**단계 2** 상자가 없는 경우 카메라를 보호하기 위해 조심스럽게 전화기를 폼이나 버블랩으로 감싸줍니다. 폼으로 카메라를 보호하고 둘러싸 어떤 방향으로도 카메라가 눌리지 않도록 하십시오. 그렇지 않으면 운반 중에 카메라가 손상될 수 있습니다.

---





## II 부

# Cisco IP 전화기 설치

- [Cisco IP 전화기 설치, 43 페이지](#)
- [Cisco Unified Communications Manager 전화기 설정, 69 페이지](#)
- [셀프 케어 포털 관리, 83 페이지](#)





## 4 장

# Cisco IP 전화기 설치

- 네트워크 설정 확인, 43 페이지
- 온-프레미스 전화기에 대한 활성화 코드 온보딩, 44 페이지
- 활성화 코드 온보딩 및 모바일 및 Remote Access, 45 페이지
- 전화기 자동 등록 활성화, 45 페이지
- Cisco IP 전화기 설치, 47 페이지
- 설정 메뉴에서 전화기 설정, 49 페이지
- 전화기에서 무선 LAN 활성화, 51 페이지
- 네트워크 설정 구성, 58 페이지
- 전화기 시작 확인, 66 페이지
- 사용자를 위한 전화기 서비스 구성, 66 페이지
- 사용자의 전화기 모델 변경, 67 페이지

## 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](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](#), xvii 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 알려주세요.

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 라이선스도 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.

## Cisco IP 전화기 설치

전화기를 네트워크에 연결한 후, 전화기 시작 프로세스가 시작되고 전화기가 Cisco Unified Communications Manager에 등록합니다. DHCP 서비스 활성화 또는 비활성화 여부에 따라 전화기에 네트워크 설정을 구성하면 전화기 설치가 끝납니다.

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



참고 외부 장치 사용 전에 [외부 장치, 26 페이지](#)를 읽어보십시오.

설치 액세스서에 대한 자세한 내용은 *Cisco IP* 전화기 7800 및 8800 시리즈의 *Cisco Unified Communications Manager*용 액세스서 설명서를 참조하십시오.

사무실에 LAN 케이블이 1개만 있는 경우 전화기를 SW 포트가 있는 LAN에 연결한 다음 컴퓨터를 PC 포트에 연결할 수 있습니다. 자세한 내용은 [전화기 및 컴퓨터와 네트워크 연결 공유, 49 페이지](#)의 내용을 참조하십시오.

두 전화기도 데이지 체인으로 함께 연결할 수 있습니다. 첫 번째 전화기의 PC 포트를 두 번째 전화기의 SW 포트에 연결합니다.



주의 PC와 SW 포트는 LAN에 연결하지 마십시오.

프로시저

단계 1 전화기의 전원 공급지를 선택합니다.

- PoE(Power over Ethernet)
- 외부 전원 공급 장치

자세한 내용은 [전화기 전원 요구 사항, 16 페이지](#)의 내용을 참조하십시오.

**단계 2** 핸드셋을 핸드셋 포트에 연결하고 케이블을 전화기의 케이블 채널 안으로 누릅니다.

광대역이 가능한 핸드셋은 Cisco IP 전화기에서 사용하도록 특별히 설계된 제품입니다. 핸드셋에는 수신 통화와 대기 음성 메시지를 표시하는 조명 스트립이 포함되어 있습니다.

**주의** 케이블을 전화기의 채널 안으로 밀어 넣지 않으면 전화기 내부의 인쇄 회로 기판이 손상될 수 있습니다. 케이블 채널은 커넥터 및 인쇄 회로 기판의 변형을 줄여줍니다.

**단계 3** 헤드셋 또는 무선 헤드셋을 연결합니다. 지금 연결하지 않고 나중에 추가할 수도 있습니다.

케이블을 케이블 채널 안으로 눌러 넣습니다.

**주의** 케이블을 전화기의 채널 안으로 밀어 넣지 않으면 전화기 내부의 인쇄 회로 기판이 손상될 수 있습니다. 케이블 채널은 커넥터 및 인쇄 회로 기판의 변형을 줄여줍니다.

**단계 4** 스위치의 바로 연결 이더넷 케이블을 Cisco IP 전화기의 10/100/1000 SW라는 네트워크 포트에 연결합니다. 각 Cisco IP 전화기에는 이더넷 케이블이 1개씩 들어 있습니다.

10Mbps 연결을 위해서는 3, 5, 5e 또는 6 케이블링을, 100Mbps 연결을 위해서는 5, 5e 또는 6 케이블링을, 그리고 1000Mbps 연결을 위해서는 5e 또는 6 케이블링을 사용합니다. 지침에 대한 자세한 내용은 [네트워크 및 컴퓨터 포트 핀 배치도, 14 페이지](#)를 참조하십시오.

**단계 5** 데스크톱 컴퓨터 같은 다른 네트워크 장치의 바로 연결 이더넷 케이블을 Cisco IP 전화기의 컴퓨터 포트에 연결합니다. 다른 네트워크 장치는 지금 연결하지 않고 나중에 연결할 수도 있습니다.

10Mbps 연결을 위해서는 3, 5, 5e 또는 6 케이블링을, 100Mbps 연결을 위해서는 5, 5e 또는 6 케이블링을, 그리고 1000Mbps 연결을 위해서는 5e 또는 6 케이블링을 사용합니다. 지침에 대한 자세한 내용은 [네트워크 및 컴퓨터 포트 핀 배치도, 14 페이지](#)를 참조하십시오.

**단계 6** 전화기를 책상 위에 둔 경우에는 받침대를 조정합니다. 벽에 장착된 전화기의 경우 수신기가 받침대에서 미끄러지지 않도록 핸드셋 거치대를 조정해야 할 수 있습니다.

**단계 7** 전화기 시작 프로세스를 모니터링합니다. 이 단계는 기본 및 보조 디렉터리 번호와 디렉터리 번호와 연결되는 기능을 전화기에 추가하고 전화기가 적절하게 구성되었음을 확인합니다.

**단계 8** 전화기에 네트워크 설정을 구성할 때는 DHCP 서버를 사용하거나 수동으로 IP 주소를 입력하여 전화기에 IP 주소를 설정할 수 있습니다.

[네트워크 설정 구성, 58 페이지](#) 및 [네트워크 설정, 243 페이지](#)를 참조하십시오.

**단계 9** 전화기에 현재 펌웨어 이미지를 업그레이드합니다.

WLAN 인터페이스를 통한 펌웨어 업그레이드는 무선 연결의 품질 및 대역폭에 따라 유선 인터페이스를 통한 업그레이드보다 시간이 더 걸릴 수도 있습니다. 일부 업그레이드는 1시간 이상이 걸릴 수도 있습니다.

**단계 10** Cisco IP 전화기으로 전화를 걸어 전화기와 기능이 정확하게 작동하는지 확인합니다.

Cisco IP 전화기 8800 시리즈 사용 설명서를 참조하십시오.

**단계 11** 최종 사용자에게 전화기 사용법과 전화기 옵션 구성 방법에 관한 정보를 제공합니다. 이 단계에서는 사용자에게 Cisco IP Phone을 잘 사용하기 위한 적절한 정보가 있는지 확인합니다.

## 전화기 및 컴퓨터와 네트워크 연결 공유

전화기와 컴퓨터가 모두 작동하려면 네트워크에 연결해야 합니다. 이더넷 포트가 하나만 있는 경우 장치에서 네트워크 연결을 공유할 수 있습니다.

시작하기 전에

관리자가 Cisco Unified Communications Manager에서 PC 포트를 활성화해야 이 포트를 사용할 수 있습니다.

프로시저

**단계 1** 이더넷 케이블을 사용하여 전화기 SW 포트를 LAN에 연결합니다.

**단계 2** 이더넷 케이블을 사용하여 컴퓨터를 전화기 PC 포트에 연결합니다.

## 설정 메뉴에서 전화기 설정

Cisco IP 전화기는 다음 구성 메뉴를 포함합니다.

- 네트워크 설정: IPv4 전용, IPv6 전용, WLAN 및 이더넷과 같은 네트워크 설정을 보고 구성하기 위한 옵션을 제공합니다.
- 이더넷 설정: 이 하위 메뉴의 메뉴 항목은 이더넷 네트워크 상에서 Cisco IP 전화기를 구성하는 구성 옵션을 제공합니다.
- WiFi 클라이언트 설정: 이 하위 메뉴의 메뉴 항목은 무선 근거리망(WLAN)으로 Cisco IP 전화기를 구성하는 구성 옵션을 제공합니다. Wi-Fi는 Cisco IP 전화기 8861 및 8861에서만 지원됩니다.



**참고** 전화기에서 Wi-Fi를 활성화하면 전화기 PC 포트가 비활성화됩니다.

- IPv4 설정 및 IPv6 설정: 이더넷 설정 메뉴 및 WiFi 클라이언트 설정 메뉴의 이러한 하위 메뉴는 추가 네트워크 옵션을 제공합니다.
- 보안 설정: 보안 모드, 신뢰 목록 및 802.1X 인증과 같은 보안 설정을 보고 구성하기 위한 옵션을 제공합니다.

네트워크 설정 메뉴의 옵션 설정을 변경하려면 편집을 위해 옵션을 잠금 해제해야 합니다.




**참고** 전화기가 이 메뉴의 옵션이나 [설정] 메뉴에 액세스할 수 있는지 여부는 Cisco 통합 커뮤니케이션 매니저 관리 전화기 구성 창의 [설정 액세스] 필드를 사용해 제어할 수 있습니다. [설정 액세스] 필드는 다음과 같은 값을 허용합니다.

- 활성화됨: [설정] 메뉴에 대한 액세스를 허용합니다.
- 비활성화됨: [설정] 메뉴에 대한 액세스를 차단합니다.
- 제한: [사용자 기본 설정] 메뉴에 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.

#### 프로시저

단계 1 애플리케이션  을 누릅니다.

단계 2 관리 설정을 선택합니다.


단계 3 네트워크 설정 또는 보안 설정을 선택합니다.

단계 4 필요한 경우, 사용자 ID 및 암호를 입력하고 로그인을 클릭합니다.

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 종료 또는 뒤로 화살표  를 누릅니다.

## 전화기 암호 적용

전화기에 암호를 적용할 수 있습니다. 이렇게 하면 [관리자 설정] 전화기 화면에 암호를 입력하지 않으면 전화기에서 관리 옵션을 변경할 수 없습니다.

#### 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 사용해 편집하려는 필드를 강조 표시한 다음, 탐색 패드에서 선택을 눌러 해당 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.
- 실수한 경우 화살표 소프트키 를 누릅니다. 그럼 소프트키가 커서 왼쪽의 문자를 삭제합니다.
- 저장을 누르기 전에 취소를 누르면 변경한 내용이 모두 지워집니다.
- IP 주소를 입력하려면 이미 분할된 네 세그먼트에 값을 입력합니다. 첫 번째 점 앞에 맨 왼쪽 숫자 입력을 마치면 오른쪽 화살표 키를 사용하여 다음 세그먼트로 이동합니다. 맨 왼쪽 숫자 다음에 오는 점은 자동으로 삽입됩니다.
- IPv6 주소를 위해 콜론을 입력하려면 키패드의 \*를 누릅니다.



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

관련 항목

[기본 재설정](#), 279 페이지

[전화기 암호 적용](#), 50 페이지

## 전화기에서 무선 LAN 활성화

무선 LAN을 설정하기 전에 전화기에서 무선 사용을 지원하는지 확인합니다. Cisco IP 전화기 8861 및 8865는 무선 LAN 구축을 지원합니다. Cisco IP 전화기 8865NR은 무선 LAN을 지원하지 않습니다.

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

음성을 위해 Wi-Fi 연결을 활성화하고 EAP-FAST 또는 PEAP 보안 모드를 사용하는 경우 WLAN 로그인 애플리케이션을 사용하여 Wi-Fi 네트워크를 인증합니다. WEP, PSK 및 개방형 보안 모드가 Wi-Fi 네트워크에서 인증합니다.

빠른 보안 로밍 방법은 Wi-Fi 사용자에게 권장합니다.



참고 전화기에서 Wi-Fi를 활성화하면 전화기 PC 포트가 비활성화됩니다.

전체 구성 정보는 다음 위치에 있는 *Cisco IP* 전화기 8800 *Wireless LAN* 배포 안내서를 참조하십시오.

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

*Cisco IP* 전화기 8800 *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 애플리케이션  을 누릅니다.

단계 2 관리 설정 > 네트워크 설정 > **Wi-Fi** 클라이언트 설정 > 네트워크 이름으로 이동합니다.  
연결할 수 있는 사용 가능한 무선 액세스 지점 목록이 나타납니다.

단계 3 무선 네트워크를 활성화합니다.

---

## Cisco Unified Communications Manager에서 무선 LAN 설정

Cisco Unified Communications Manager Administration에서 무선 Cisco IP 전화기에 대해 “Wi-Fi”라는 매개 변수를 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 매개 변수에 대한 활성화된 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 매개 변수에 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 매개 변수에 대한 활성화됨 설정을 선택합니다.

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

- c) 일반 설정 무시 확인란을 선택합니다.

## 전화기에 무선 LAN 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 전화기에서 Wi-Fi를 활성화하면 전화기 PC 포트가 비활성화됩니다.



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


자세한 내용은 <http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>에서 Cisco IP 전화기 8800 Series WLAN 구축 설명서를 참조하십시오.

무선 LAN 프로파일의 사용자 수정 가능 필드는 전화기에서 보안 모드를 구성하는 사용자의 기능을 제어합니다. 사용자가 필드 중 일부를 변경할 수 없는 경우 필드는 회색으로 표시됩니다.

시작하기 전에

Cisco Unified Communications Manager에서 무선 LAN을 구성합니다.

## 프로시저

단계 1 애플리케이션  을 누릅니다.

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

단계 3 다음 표에 설명된 대로 무선 구성을 설정합니다.

표 19: WiFi 클라이언트 설정 메뉴 옵션

옵션	설명	변경
네트워크 이름	무선 액세스 지점에 액세스하기 위한 고유 식별자, SSID(Service Set Identifier)를 지정합니다. 사용 가능한 무선 액세스 지점 목록을 표시합니다.	<a href="#">네트워크 설정 구성, 58 페이지</a> 참조
IPv4 전용 설정	IPv4 설정 구성 하위 메뉴에서 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> <li>전화기에서 DHCP 서버가 할당하는 IP 주소를 사용할 수 있도록 설정하거나 설정을 해제합니다.</li> <li>수동으로 IP 주소, 서브넷 마스크, 기본 라우터, DNS 서버 및 대체 TFTP 서버를 설정합니다.</li> </ul> IPv4 주소 필드에 대한 자세한 내용은 <a href="#">IPv4 필드, 61 페이지</a> 를 참조하십시오.	IPv4 설정으로 스크롤하고 선택을
IPv6 전용 설정	IPv6 설정 구성 하위 메뉴에서 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> <li>사용자가 DHCPv6 서버에서 할당하거나 SLAAC에서 IPv6 사용 가능 라우터를 통해 획득하는 IPv6 주소를 사용할 수 있도록 설정하거나 설정을 해제합니다.</li> <li>수동으로 IPv6 주소, 접두사 길이, 기본 라우터, DNS 서버 및 대체 TFTP 서버를 설정합니다.</li> </ul> IPv6 주소 필드에 대한 자세한 내용은 <a href="#">IPv6 필드, 63 페이지</a> 를 참조하십시오.	IPv6 설정으로 스크롤하고 선택을
MAC 주소	전화기의 고유한 MAC(Media Access Control) 주소입니다.	표시 전용입니다. 구성할 수 없습니다.
도메인 이름	전화기가 위치한 DNS(Domain Name System) 도메인의 이름입니다.	<a href="#">네트워크 설정 구성, 58 페이지</a> 참조

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 매개 변수를 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 프로파일 모드 활성화

사용자가 전화기의 전원이 켜질 때 또는 재설정할 때 Wi-Fi 네트워크에 로그인하도록 하려면 WLAN 프로파일 1 프로파일 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 프로파일 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 매개 변수가 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.



**참고** Expressway를 통해 모바일 및 Remote Access를 사용하여 Cisco Unified Communications Manager에 연결하는 전화기는 Wi-Fi 프로파일을 사용할 수 없습니다. 사용자의 전화기의 SSID, 인증 모드 및 로그인 자격 증명이 없으므로 해당 전화기에 대해 무선 LAN 프로파일을 구성할 수 없습니다.

### 프로시저

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

**단계 2** 새로 추가를 클릭합니다.

**단계 3** 무선 LAN 프로파일 정보 섹션에서 매개 변수를 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 매개 변수를 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 사용자에게 대한 프로파일을 생성해야 합니다.

참고 네트워크 액세스 프로파일 필드는 Cisco IP 전화기 8861 및 8865에서 지원되지 않습니다.

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 프로파일 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.

## 네트워크 설정 구성

프로시저

**단계 1** 애플리케이션  을 누릅니다.

**단계 2** 네트워크 설정 메뉴에 액세스하려면 관리 설정 > 이더넷 설정을 선택합니다.

**단계 3** 이더넷 설정 필드, 59 페이지에 설명된 대로 필드를 설정합니다.

**단계 4** 필드를 설정한 후에 적용 및 저장을 선택합니다.

**단계 5** 전화기를 재부팅합니다.

## 이더넷 설정 필드

[네트워크 설정] 메뉴는 IPv4 및 IPv6에 대한 필드 및 하위 메뉴를 포함합니다. 일부 필드를 변경하려면 먼저 DHCP를 비활성화합니다.

VPN 연결을 설정하면 이더넷 데이터 필드를 덮어씁니다.

표 20: 이더넷 설정 메뉴 옵션

항목	유형	설명
IPv4 설정	메뉴	IPv4 필드 섹션을 참조하십시오. 이 옵션은 전화기가 IPv4 전용 모드 또는 IPv4 및 IPv6 모드에서 작동하는 경우에만 유효합니다.
IPv6 설정	메뉴	"IPv6 필드" 섹션을 참조하십시오.
MAC 주소	문자열	전화기의 고유한 MAC(Media Access Control) 주소입니다. 표시 전용입니다. 구성할 수 없습니다.
도메인 이름	문자열	전화기가 위치한 DNS(Domain Name System) 도메인의 이름입니다. 이 필드를 변경하려면 DHCP를 해제합니다.
사용 가능한 VLAN ID		전화기가 속해 있는 Cisco Catalyst 스위치에 구성된 보조 VLAN(VLAN) ID 목록입니다. 보조 VLAN 또는 관리 VLAN이 구성된 경우 이 설정은 공백입니다. 전화기가 보조 VLAN을 수신하지 않으면 이 옵션은 관리 VLAN ID를 표시합니다. 전화기는 Cisco Discovery Protocol 또는 Link Level Discovery Protocol을 사용하여 관리자 VLAN에서 사용 가능한 VLAN을 상수적으로 식별합니다. 관리자 VLAN ID를 수동으로 할당하려면 관리자 VLAN ID 옵션을 사용하십시오.
관리자 VLAN ID		전화기가 속해 있는 보조 VLAN입니다. 전화기가 스위치에서 보조 VLAN을 수신하지 않는 경우에만 사용 가능합니다. 이 옵션은 무시됩니다.
PC VLAN		전화기가 음성 VLAN을 지원하지 않는 타사 스위치와 상호 작용하는 경우에만 유효합니다. 이 옵션을 설정하려면 관리자 VLAN ID 옵션을 설정해야 합니다.

항목	유형	설명
SW 포트 설정	자동 협상 1000 전이중 100 반이중 10 반이중 10 전이중	<p>네트워크 포트의 속도 및 전이중/반이중 유효한 값은 다음 사항을 지</p> <ul style="list-style-type: none"> <li>• 자동 협상(기본값)</li> <li>• 1000 Full:1000-BaseT/전이중</li> <li>• 100 Half:100-BaseT/반이중</li> <li>• 100 Full:100-BaseT/전이중</li> <li>• 10 Half:10-BaseT/반이중</li> <li>• 10 Full:10-BaseT/전이중</li> </ul> <p>전화기가 스위치에 연결된 경우 스위치 포트를 전화기와 동일한 속</p> <p>동 협상되도록 구성합니다.</p> <p>이 설정을 편집하려면 네트워크 구성 옵션을 잠금 해제합니다. 이 옵션</p> <p>PC 포트 구성 옵션을 동일한 설정으로 변경해야 합니다.</p>
PC 포트 설정	자동 협상 1000 전이중 100 반이중 10 반이중 10 전이중	<p>컴퓨터(액세스) 포트의 속도 및 전이중/반이중 유효한 값:</p> <ul style="list-style-type: none"> <li>• 자동 협상(기본값)</li> <li>• 1000 Full:1000-BaseT/전이중</li> <li>• 100 Half:100-BaseT/반이중</li> <li>• 100 Full:100-BaseT/전이중</li> <li>• 10 Half:10-BaseT/반이중</li> <li>• 10 Full:10-BaseT/전이중</li> </ul> <p>전화기가 스위치에 연결된 경우 스위치의 포트를 전화기와 동일한</p> <p>자동 협상되도록 구성합니다.</p> <p>이 필드를 변경하려면 네트워크 구성 옵션을 잠금 해제합니다. 설정</p> <p>구성 옵션을 동일한 설정으로 변경해야 합니다.</p> <p>다중 전화기의 설정을 동시에 구성하려면 엔터프라이즈 전화기 구성</p> <p>을 활성화합니다(시스템 &gt; 엔터프라이즈 전화기 구성).</p> <p>Cisco Unified Communications Manager Administration에서 원격 포트</p> <p>하면, 전화기에서 데이터를 변경할 수 없습니다.</p>

## IPv4 필드

표 21: IPv4 설정 메뉴 옵션

항목	설명
DHCP 사용	<p>전화기에 DHCP가 활성화 또는 비활성화되었는지를 나타냅니다.</p> <p>DHCP가 활성화되었을 때 DHCP 서버는 전화기에 IP 주소를 할당합니다. DHCP가 비활성화되었을 때 관리자는 수동으로 IP 주소를 전화기에 할당해야 합니다.</p> <p>자세한 내용은 <a href="#">전화기가 DHCP를 사용하도록 설정, 65 페이지</a> 및 <a href="#">전화기가 DHCP를 사용하지 않도록 설정, 65 페이지</a>를 참조하십시오.</p>
IP 주소	<p>전화기의 IP(인터넷 프로토콜) 주소입니다.</p> <p>이 옵션으로 IP 주소를 할당하면 서브넷 마스크와 기본 라우터도 할당해야 합니다. 이 표의 서브넷 마스크 및 기본 라우터 옵션을 참조하십시오.</p>
서브넷 마스크	전화기가 사용하는 서브넷 마스크입니다.
기본 라우터	전화기가 사용하는 기본 라우터입니다.
DNS 서버 1 DNS 서버 2 DNS 서버 3	전화기가 사용하는 기본 DNS 서버 (DNS Server 1)와 옵션 항목인 백업 DNS 서버(DNS Server 2 및 3)입니다.
대체 TFTP	전화기에서 대체 TFTP 서버를 사용하는지 알려줍니다.

항목	설명
TFTP 서버 1	<p>전화기에서 사용하는 기본 TFTP(Trivial File Transfer Protocol) 서버입니다. 네트워크에서 DHCP를 사용하지 않는 경우 이 서버를 변경하려면 TFTP 서버 1 옵션을 사용해야 합니다. 대체 TFTP 옵션을 켜기로 설정하면 TFTP 서버 1 옵션에 대해 0이 아닌 값을 입력해야 합니다.</p> <p>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.</p> <p>전화기가 TFTP 서버를 찾을 때 전화기는 프로토콜과 관계없이, 수동으로 할당된 TFTP 서버에 우선 순위를 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 우선 순위를 지정합니다. 전화기는 다음 순서로 TFTP 서버를 찾습니다.</p> <ol style="list-style-type: none"> <li>1. 수동으로 할당된 IPv4 TFTP 서버</li> <li>2. 수동으로 할당된 IPv6 서버</li> <li>3. DHCP 할당 TFTP 서버</li> <li>4. DHCPv6 할당 TFTP 서버</li> </ol> <p>참고 CTL 및 ITL 파일에 대한 자세한 내용은 <i>Cisco Unified Communications Manager</i> 보안 설명서를 참조하십시오.</p>



항목	설명
TFTP 서버 2	<p>기본 TFTP 서버를 사용할 수 없는 경우 전화기가 사용하는 선택적 백업 TFTP 서버.</p> <p>기본 TFTP 서버 또는 백업 TFTP 서버가 전화기의 CTL 또는 ITL 파일에 나열되어 있지 않은 경우 TFTP 서버 2 옵션에 변경 사항을 저장하려면 두 파일 중 하나를 잠금 해제해야 합니다. 이 경우, TFTP 서버 2 옵션에 변경 사항을 저장할 때 전화기는 두 파일 중 하나를 삭제합니다. 새 CTL 또는 ITL 파일이 새 TFTP 서버 2 주소에서 다운로드됩니다.</p> <p>CTL 또는 ITL 파일의 잠금 해제를 잊은 경우 두 파일 중 하나에서 TFTP 서버 2 주소를 변경한 다음, [보안 구성] 메뉴에서 [지우기]를 눌러 잠금을 지울 수 있습니다. 새 CTL 또는 ITL 파일이 새 TFTP 서버 2 주소에서 다운로드됩니다.</p> <p>전화기가 TFTP 서버를 찾을 때 전화기는 프로토콜과 관계없이, 수동으로 할당된 TFTP 서버에 우선 순위를 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 우선 순위를 지정합니다. 전화기는 다음 순서로 TFTP 서버를 찾습니다.</p> <ol style="list-style-type: none"> <li>1. 수동으로 할당된 IPv4 TFTP 서버</li> <li>2. 수동으로 할당된 IPv6 서버</li> <li>3. DHCP 할당 TFTP 서버</li> <li>4. DHCPv6 할당 TFTP 서버</li> </ol> <p>참고 CTL 또는 ITL 파일에 대한 자세한 내용은 Cisco Unified Communications Manager 보안 설명서를 참조하십시오.</p>
BOOTP 서버	전화기가 DHCP 서버가 아닌 BOOTP 서버에서 IP 주소를 수신했는지 여부를 나타냅니다.
DHCP 주소 해제됨	<p>DHCP가 할당한 IP 주소를 해제합니다.</p> <p>DHCP가 활성화된 경우 이 필드를 편집할 수 있습니다. VLAN에서 전화기를 제거하고 재할당하기 위해 IP 주소를 해제하려면 이 옵션을 [예]로 설정하고 [적용]을 누르십시오.</p>

## IPv6 필드

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.

IPv6 구축에 대한 자세한 내용은 [IPv6 Deployment Guide for Cisco Collaboration Systems 릴리스 12.0](#)을 참조하십시오.

다음 메뉴 중 하나에서 IPv6를 설정합니다.

- Wi-Fi가 비활성화되었을 때: 이더넷 설정 > **IPv6** 설정
- Wi-Fi가 활성화되었을 때: **Wi-Fi** 클라이언트 설정 > **IPv6** 설정

전화기 키패드를 사용하여 IPv6 주소를 를 입력하거나 편집합니다. 콜론(:)을 입력하려면 키패드의 별표(\*)를 누릅니다. 16진수 숫자 a, b, c를 입력하려면 키패드의 2를 누르고 스크롤하여 필수 숫자를 선택하고 **Enter**를 누릅니다. 16진수 숫자 d, e, f를 입력하려면 키패드의 3을 누르고 스크롤하여 필수 숫자를 선택하고 **Enter**를 누릅니다.

다음 표는 IPv6 메뉴에서 검색된 IPv6 관련 정보에 대해 설명합니다.

표 22: IPv6 설정 메뉴 옵션


항목	기본값	설명
DHCPv6 활성화됨	예	전화기가 IPv6-전용 주소를 가져오기 위해 DHCPv6를 사용하는지 여부를 나타냅니다. DHCPv6가 활성화되었을 때 전화기는 DHCPv6 주소를 가져옵니다. 그리고 DHCPv6 서버(SLAAC에서) IPv6 주소를 가지지 않습니다.
IPv6 주소	::	전화기의 현재 IPv6-전용 주소를 표시합니다. 유효한 IPv6 주소의 길이는 서브넷 마스크와 일치합니다. <ul style="list-style-type: none"> <li>• 콜론으로 구분된 16진수 숫자의 그룹</li> <li>• 연속 0 그룹의 1회 연속을 허용합니다.</li> </ul> 이 옵션으로 IP 주소가 할당된 경우 16진수 주소가 표시됩니다.
IPv6 접두사 길이	0	서브넷에 대한 현재 접두사 길이를 표시합니다. 서브넷 접두사 길이는 1-128의 십진수 값입니다.
IPv6 기본 라우터	::	전화기에서 사용하는 기본 라우터를 표시합니다.
IPv6 DNS 서버 1	::	전화기에서 사용하는 기본 DNSv6 서버를 표시합니다.
IPv6 DNS 서버 2	::	전화기에서 사용하는 보조 DNSv6 서버를 표시합니다.
IPv6 대체 TFTP	아니요	사용자가 대체(보조) IPv6 TFTP 서버를 설정했는지 여부를 나타냅니다.
IPv6 TFTP 서버 1	::	전화기에서 사용하는 기본 IPv6 TFTP 서버를 표시합니다.

항목	기본값	설명
IPv6 TFTP 서버 2	::	(선택사항) 기본 IPv6 TFTP 서버가 새 보조 TFTP 서버를 설정할
IPv6 주소 해제됨	아니요	사용자가 IPv6 관련 정보를 해제

## 전화기가 DHCP를 사용하도록 설정

DHCP를 활성화하고 DHCP 서버가 Cisco IP 전화기에 자동으로 IP 주소를 할당하고 전화기를 TFTP 서버에 연결할 수 있게 하려면 다음 단계를 수행합니다.

프로시저

단계 1 애플리케이션  을 누릅니다.

단계 2 관리 설정 > 네트워크 설정 > 이더넷 설정 > IPv4 설정을 선택합니다.

단계 3 DHCP를 활성화하려면 [DHCP 활성화됨]을 예로 설정합니다. DHCP는 기본값으로 활성화됩니다.

단계 4 대체 TFTP 서버를 사용하려면 [대체 TFTP 서버]를 예로 설정하고, TFTP 서버에 대한 IP 주소를 입력합니다.


참고 네트워크 관리자와 논의하여 DHCP가 할당하는 TFTP 서버를 사용하는 대신, 대체 TFTP 서버를 할당해야 하는지 여부를 판별하십시오.

단계 5 적용을 누릅니다.

## 전화기가 DHCP를 사용하지 않도록 설정

DHCP를 사용하지 않을 때 전화기에 로컬로 IP 주소, 서브넷 마스크, TFTP 서버 및 기본 라우터를 구성해야 합니다.

프로시저

단계 1 애플리케이션  을 누릅니다.

단계 2 관리 설정 > 네트워크 설정 > 이더넷 설정 > IPv4 설정을 선택합니다.

단계 3 DHCP를 비활성화하고 수동으로 IP 주소를 설정하려면:

- [DHCP 활성화]를 아니요로 설정합니다.
- 전화기의 정적 IP 주소를 입력합니다.
- 서브넷 마스크를 입력합니다.
- 기본 라우터 IP 주소를 입력합니다.

e) 대체 TFTP 서버를 예로 설정하고, TFTP 서버 1에 대한 IP 주소를 입력합니다.

단계 4 적용을 누릅니다.

## 로드 서버

로드 서버는 전화기 펌웨어 업그레이드를 위한 설치 시간을 최적화하고 이미지를 로컬로 저장해 각 전화기 업그레이드를 위해 WAN 링크를 이동할 필요가 없도록 하여 WAN을 오프로드하는 데 사용됩니다.

로드 서버를 전화기 업그레이드를 위해 전화기 펌웨어를 검색할 수 있는 (TFTP 서버 1 또는 TFTP 서버 2가 아닌) 다른 TFTP 서버 IP 주소 또는 이름으로 설정할 수 있습니다. 로드 서버 옵션이 설정될 때 전화기는 펌웨어 업그레이드용으로 지정된 서버에 연결합니다.



**참고** 로드 서버 옵션을 사용하여 전화기 업그레이드만을 위한 대체 TFTP 서버를 지정할 수 있습니다. 전화기는 계속해서 TFTP 서버 1 또는 TFTP 서버 2를 사용하여 구성 파일을 얻습니다. 로드 서버 옵션은 파일 전송, 압축 또는 삭제와 프로세스 및 파일 관리를 제공하지 않습니다.

로드 서버는 [엔터프라이즈 전화기 구성] 창에서 구성됩니다. Cisco Unified Communications Manager Administration에서 장치 > 전화기 > 엔터프라이즈 전화기 구성을 선택합니다.

## 전화기 시작 확인

Cisco IP 전화기가 전원에 연결된 후, 전화기는 다음 단계를 순환하여 시작 진단 프로세스를 시작합니다.

1. 전화기에서 하드웨어를 확인함에 따라 여러 부팅 단계를 거치면서 기능 및 세션 버튼이 호박색으로 번쩍이다가 녹색으로 차례로 바뀝니다.
2. 기본 화면이 Cisco Unified Communications Manager에 등록 중을 표시합니다.

전화기가 이러한 단계를 성공적으로 완료하면 전화기가 적절하게 시작했으며 선택 버튼이 선택될 때까지 점등됩니다.

## 사용자를 위한 전화기 서비스 구성

사용자에게 전화기의 Cisco IP 전화기 서비스에 대한 액세스 권한을 제공할 수 있습니다. 다양한 전화기 서비스에 버튼을 지정할 수도 있습니다. 이러한 서비스는 전화기에서 텍스트와 그래픽을 사용하여 대화형 콘텐츠를 표시할 수 있는 XML 애플리케이션 및 Cisco 서명 Java MIDlet로 구성됩니다. IP 전화기는 각 서비스를 별개의 애플리케이션으로 관리합니다. 서비스 예는 로컬 동영상 시간, 주식 정보 및 날씨 보고서를 포함합니다.

사용자가 서비스에 액세스하기 전 다음과 같은 작업을 수행해야 합니다.

- Cisco 통합 커뮤니케이션 매니저 관리를 사용해 기본적으로 제공되지 않는 서비스를 구성해야 합니다.
- 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 구성된 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 케어 포털 관리, 83 페이지](#)를 참조하십시오.

관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## 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.
- 전화를 수리하거나 교체해야 합니다.

Unified CM은 이전 전화를 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.

SCCP 펌웨어를 사용하여 이전 전화를 Cisco IP 전화기 8800 시리즈에 있는 모델로 변경하면 새 전화기가 세션 회선 모드에 맞게 구성됩니다.

이전 전화기에 키 확장 모델이 구성되어 있는 경우 Unified CM은 확장 모듈 정보를 새 전화기로 동시에 복사합니다. 사용자가 호환되는 키 확장 모듈을 새 전화기에 연결하면 새 확장 모듈은 마이그레이션한 확장 모듈 정보를 가져옵니다.

이전 전화기에 키 확장 모델이 구성되어 있고 새 전화기에서 확장 모듈을 지원하지 않는 경우 Unified CM은 확장 모듈 정보를 복사하지 않습니다.

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 설정

- Cisco IP 전화기 설정, 69 페이지
- 전화기 MAC 주소 결정, 72 페이지
- 전화기 추가 방식, 73 페이지
- Cisco Unified Communications Manager에 사용자 추가, 74 페이지
- 최종 사용자 그룹에 사용자 추가, 76 페이지
- 전화기와 사용자 연결, 77 페이지
- SRST(Survivable Remote Site Telephony), 77 페이지
- E-SRST(Enhanced Survivable Remote Site Telephony), 80 페이지
- 애플리케이션 다이얼 규칙, 80 페이지

### Cisco IP 전화기 설정

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

Cisco Unified Communications Manager Administration에 관한 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

- 전화기의 물리적 위치
- 전화기 사용자의 이름 또는 사용자 ID
- 장치 풀(pool)
- 파티션, 발신 검색 공간 및 위치 정보
- 전화기에 할당할 회선 및 연결된 DN(디렉터리 번호) 수
- 전화기와 연결할 Cisco Unified Communications Manager 사용자
- 전화기 버튼 템플릿, 전화 기능, IP 전화기 서비스 또는 전화기 애플리케이션에 영향을 미치는 전화기 사용 정보

정보는 전화기를 설정하기 위한 구성 요구 사항 목록을 제공하고 전화기 버튼 템플릿과 같은 개별 전화기를 구성하기 전에 수행해야 하는 사전 구성을 식별합니다.

**단계 2** 전화기에 대한 단위 라이선스가 충분한지 확인합니다.

**단계 3** 회선 버튼 수, 단축 다이얼 버튼 또는 서비스 URL 버튼을 변경하여 (필요한 경우) 전화기 버튼 템플릿을 사용자 정의합니다. 장치 > 장치 설정 > 전화기 버튼 템플릿을 선택하여 템플릿을 작성하고 업데이트합니다.

프라이버시, 모든 통화 또는 이동성 버튼을 추가하여 사용자의 필요성을 충족시킬 수 있습니다.

자세한 내용은 [전화기 버튼 템플릿, 201 페이지](#)의 내용을 참조하십시오.

**단계 4** 장치 풀을 정의합니다. 시스템 > 장치 풀을 선택합니다.

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

**단계 5** 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 6** 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 7** 장치 유형 및 프로토콜에 대한 보안 프로파일을 구성합니다. 시스템 > 보안 > 전화기 보안 프로파일을 선택합니다.

**단계 8** [전화기 구성] 창의 필수 필드를 완료하여 전화기를 추가하고 구성합니다. 필드 이름 옆에 있는 별표 (\*)는 필수 필드를 나타냅니다(예: MAC 주소 및 장치 풀).

이 단계는 기본 설정을 가지는 장치를 Cisco Unified Communications Manager 데이터베이스에 추가합니다.

[제품별 구성] 필드에 관한 정보는 [전화기 구성] 창의 “?” 버튼 도움말을 참조하십시오.



- 참고 Cisco Unified Communications Manager 데이터베이스에 전화기와 사용자를 모두 동시에 추가하려면, 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
- 단계 9** [디렉터리 번호 구성] 창의 필수 항목을 입력해 전화기를 추가하고 전화기에 디렉터리 번호(회선)를 구성합니다. 필드 이름 옆에 있는 별표(\*)는 필수 필드를 나타냅니다.(예: 디렉터리 번호 및 존재 그룹). 이 단계는 기본 및 보조 디렉터리 번호와 디렉터리 번호와 연결된 기능을 전화기에 추가합니다.
- 참고 기본 디렉터리 번호를 구성하지 않으면 전화기에 제공 취소됨 메시지가 나타납니다.
- 단계 10** 단축 다이얼 단추를 구성하고 단축 다이얼 번호를 지정합니다.
- 사용자는 Cisco 유니파이드 Communications 셀프 케어 포털을 사용해 전화기의 단축 다이얼 설정을 변경할 수 있습니다.
- 단계 11** Cisco 유니파이드 IP 전화기 서비스를 구성하고 IP Phone 서비스를 제공하는 서비스(선택 사항)를 할당합니다.
- Cisco 유니파이드 Communications 셀프 케어 포털을 사용하여 전화기의 서비스를 추가 또는 변경할 수 있습니다.
- 참고 사용자는 Cisco Unified Communications Manager Administration에서 IP 전화기 서비스를 처음 구성할 때 [엔터프라이즈 가입] 확인란을 선택 취소한 경우에만 IP 전화기 서비스에 가입할 수 있습니다.
- 참고 일부 Cisco에서 제공한 기본 서비스는 엔터프라이즈 가입으로 분류되므로, 사용자가 셀프 케어 포털을 통해 이러한 서비스를 추가할 수 없습니다. 이러한 서비스는 기본적으로 전화기에 있고, Cisco Unified Communications Manager Administration에서 해당 서비스를 비활성화한 경우에만 전화기에서 제거할 수 있습니다.
- 단계 12** 서비스를 프로그램 가능 버튼(선택 사항)에 할당하여 IP 전화기 서비스 또는 URL에 대한 액세스를 제공합니다.
- 단계 13** 필수 필드를 구성하여 사용자 정보를 추가합니다. 필드 이름 옆에 있는 별표(\*)는 필수 필드를 나타냅니다.(예: 사용자 ID 및 성). 이 단계는 Cisco Unified Communications Manager용 글로벌 디렉터리에 사용자 정보를 추가합니다.
- 참고 암호(셀프 케어 포털용) 및 PIN(Cisco Extension Mobility 및 개인 디렉터리용)을 할당합니다.
- 참고 회사에서 사용자에게 관한 정보를 저장하는 데 LDAP(Lightweight Directory Access Protocol) 디렉터리를 사용한다면, 기존 LDAP 디렉터리를 사용하도록 Cisco Unified Communications를 설치하고 구성할 수 있습니다.
- 참고 Cisco Unified Communications Manager 데이터베이스에 전화기와 사용자를 모두 동시에 추가하려면, 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
- 단계 14** 사용자를 사용자 그룹에 연결합니다. 이 단계는 사용자에게 사용자 그룹의 모든 사용자에게 적용되는 공통된 역할 및 권한 목록을 구축합니다. 관리자는 사용자 그룹, 역할 및 권한을 관리하여 시스템

사용자의 액세스 수준(과 보안 수준)을 제어할 수 있습니다. 예를 들어 사용자가 Cisco Unified Communications Manager 셀프 케어 포털에 액세스할 수 있도록 사용자를 표준 Cisco CCM 최종 사용자 그룹에 추가해야 합니다.

**단계 15** 사용자를 전화기와 연결합니다(선택 사항). 이 단계는 전화기에 통화를 착신 전환하거나 단축 다이얼 번호나 서비스를 추가하는 것 같은 제어 기능을 제공합니다.

회의실에 있는 것과 같은 일부 전화에는 연결된 사용자가 없습니다.

**단계 16** 아직 [최종 사용자 구성] 창에 있지 않으면 사용자 관리 > 최종 사용자를 선택하여 몇 가지 최종 구성 작업을 수행합니다. [검색] 필드와 찾기를 사용하여 사용자(예: John Doe)를 찾은 다음, 사용자 ID를 클릭하여 사용자에 대한 [최종 사용자 구성] 창을 가져옵니다.

**단계 17** 화면의 [디렉터리 번호 연결] 영역에 있는 드롭다운 목록에서 [기본 내선 번호]를 설정합니다.

**단계 18** [이동 정보] 영역에서 [이동 활성화] 확인란을 선택합니다.

**단계 19** [권한 정보] 영역에서 사용자 그룹 버튼을 사용하여 이 사용자를 사용자 그룹에 추가합니다.

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

**단계 20** 구성된 모든 사용자 그룹을 보려면 사용자 관리 > 사용자 그룹을 선택합니다.

**단계 21** 사용자가 EMCC(Extension Mobility Cross Cluster) 서비스에 사용할 수 있다면 [내선 이동] 영역에서 [클러스터 간 내선 이동 활성화] 확인란을 선택합니다.

**단계 22** 저장을 선택합니다.

---

관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 페이지


## 전화기 MAC 주소 결정

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

프로시저

---

다음 작업 중 하나를 수행합니다.

- 전화기에서 애플리케이션  을 누르고 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, 72 페이지](#)의 내용을 참조하십시오.

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

## 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, xvii 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, xvii 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, 75 페이지](#)를 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](#), xvii 페이지

## 외부 LDAP 디렉터리에서 사용자 추가

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



**참고** LDAP 디렉터를 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 디렉터를 선택합니다.
- 단계 3 찾기를 사용해 LDAP 디렉터를 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) 디렉터를 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 호선이 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 WAN 연결이 끊길 때도 기본 전화 기능에 여전히 액세스할 수 있도록 합니다. 이런 시나리오에서 전화기는 진행 중인 통화의 활성 상태를 유지하고, 사용자도 기능 하위 집합에 액세스할 수 있습니다. 페일오버가 발생하면 사용자는 전화기를 통해 경고 메시지를 수신합니다.

지원되는 펌웨어 및 SRST(Survivable Remote Site Telephony)에 대한 자세한 내용은 Cisco.com의 Cisco 유니파이드 *Survivable Remote Site Telephony* 호환성 정보 페이지

(<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html>)를 참조하십시오.

다음 표에서는 페일오버 상태에서도 사용 가능한 기능에 관해 설명합니다.

표 23: SRST 기능 지원

기능	지원됨	참고
전화걸기	예	
통화종료	예	
재다이얼	예	
전화받기	예	
보류	예	
보류해제	예	
전화회의	예	
활성 통화로 전화회의(통화참가)	아니요	활성 통화 소프트키가 표시되지 않습니다.
전화회의 목록	아니요	
호전환	예	
활성 통화로 호전환(호연결)	아니요	
자동 응답	예	
통화 대기 중	예	
발신자 ID	예	
음성 메시지 대기 중 표시기	예	
모든 통화 프로그래밍 가능 회선 키	예	
전화받기 프로그래밍 가능 회선 키	예	
통합 세션 프레젠테이션	예	전화회의는 다른 기능 제한으로 인해 지원되는 유일한 기능입니다.
음성메일	예	음성 메일이 Cisco Unified Communications Manager 클러스터의 다른 사용자와 동기화되지 않습니다.



기능	지원됨	참고
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	
서비스 IRL 프로그래밍 가능 회선 키	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.
참여	아니요	참여 소프트키가 표시되지 않습니다.
향상된 메시지 대기 중 표시	아니요	메시지 수 배지가 전화기 화면에 나타나지 않습니다. 메시지 대기 중 아이콘만 표시됩니다.
직접 통화 지정보류	아니요	소프트키가 표시되지 않습니다.
BLF	일부 지원	BLF 기능 키가 단축 다이얼 키처럼 작동합니다.
보류 복귀	아니요	통화가 계속 보류 상태로 유지됩니다.
원격 보류	아니요	통화가 로컬 보류 통화로 나타납니다.
회의개설	아니요	[회의개설] 소프트키가 표시되지 않습니다.
당겨받기	아니요	소프트키로 인한 동작이 없습니다.
그룹 당겨받기	아니요	소프트키로 인한 동작이 없습니다.

기능	지원됨	참고
기타 당겨받기	아니요	소프트키로 인한 동작이 없습니다.
장난 전화 ID	아니요	소프트키로 인한 동작이 없습니다.
QRT	아니요	소프트키로 인한 동작이 없습니다.
헌트 그룹	아니요	소프트키로 인한 동작이 없습니다.
인터콤	아니요	소프트키로 인한 동작이 없습니다.
이동성	아니요	소프트키로 인한 동작이 없습니다.
프라이버시	아니요	소프트키로 인한 동작이 없습니다.
콜백	아니요	[콜백] 소프트키가 표시되지 않습니다.
비디오	예	화상 회의는 지원되지 않습니다.
비디오	예	화상 회의는 지원되지 않습니다.
공유 회선	아니요	
BLF 단축 다이얼	예	

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

E-SRST(Enhanced Survivable Remote Site Telephony)는 WAN 연결이 끊길 때도 추가 전화 기능에 여전히 액세스할 수 있도록 합니다. SRST(Survivable Remote Site Telephony)가 지원하는 기능 외에도 E-SRST는 다음 기능을 지원합니다.

- 공유 회선
- 통화 중 램프(BLF)
- 영상 통화

지원되는 펌웨어 및 SRST(Survivable Remote Site Telephony)에 대한 자세한 내용은 Cisco.com의 Cisco 유니파이드 *Survivable Remote Site Telephony* 호환성 정보 페이지 (<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html>)를 참조하십시오.

## 애플리케이션 다이얼 규칙

공유 모바일 연락처를 위한 번호를 네트워크에서 전화를 걸 수 있는 번호로 변경하려면 애플리케이션 다이얼 규칙을 사용합니다. 애플리케이션 다이얼 규칙은 사용자가 직접 전화 번호를 누를 때나 사용자가 전화를 걸기 전에 번호를 편집한 경우에는 적용되지 않습니다.

애플리케이션 다이얼 규칙은 Cisco Unified Communications Manager에서 설정합니다.

다이얼 규칙에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서, “다이얼 규칙 구성” 장을 참조하십시오.

## 애플리케이션 다이얼 규칙 구성

### 프로시저

- 
- 단계 1** Cisco Unified Communications Manager 관리에서 통화 라우팅 > 다이얼 규칙 > 애플리케이션 다이얼 규칙으로 이동합니다.
- 단계 2** 새로 추가를 선택하여 새로운 애플리케이션 다이얼 규칙을 작성하거나 기존 애플리케이션 다이얼 규칙을 선택해 편집합니다.
- 단계 3** 다음 필드를 입력합니다.
- 이름 이 필드는 다이얼 규칙의 고유한 이름으로 구성됩니다. 여기에는 최대 20자의 영숫자와 공백, 마침표(.), 하이픈(-) 및 밑줄(\_) 조합이 포함될 수 있습니다.
  - 설명 이 필드에는 다이얼 규칙을 위해 입력한 간략한 설명이 표시됩니다.
  - 시작 숫자 이 필드는 이 애플리케이션 다이얼 규칙을 적용할 디렉터리 번호의 첫 번째 숫자로 구성됩니다.
  - 숫자의 수 이 필드는 이 애플리케이션 다이얼 규칙을 적용할 디렉터리 번호의 첫 번째 숫자로 구성됩니다.
  - 삭제할 총 숫자 이 필드는 이 다이얼 규칙에 적용되는 디렉터리 번호에서 Cisco Unified Communications Manager가 제거하려고 하는 숫자의 개수로 구성됩니다.
  - 패턴이 있는 접두사 이 필드에는 이 애플리케이션 다이얼 규칙에 적용되는 디렉터리 번호 앞에 추가할 패턴이 입력됩니다.
  - 애플리케이션 다이얼 규칙 우선 순위 이 필드는 [패턴이 있는 접두사] 정보를 입력할 때 나타납니다. 이 필드에서는 애플리케이션 다이얼 규칙의 우선 순위 순서를 설정할 수 있습니다.
- 단계 4** Cisco Unified Communications Manager을 재시작합니다.
-





## 6 장

# 셀프 케어 포털 관리

- [셀프 서비스 포털 개요, 83 페이지](#)
- [셀프 서비스 포털에 사용자 액세스 설정, 84 페이지](#)
- [셀프 서비스 포털 디스플레이 사용자 정의, 84 페이지](#)

## 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_name`은 웹 서버가 설치된 호스트이며, `portnumber`는 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](#), xvii 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 매개 변수 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 매개 변수를 선택합니다.

단계 2 [셀프 서비스 포털] 영역에서 셀프 서비스 포털 기본 서버 필드를 설정합니다.

단계 3 사용자가 포털에서 액세스할 수 있는 매개 변수를 활성화 또는 비활성화합니다.

단계 4 저장을 선택합니다.



## III 부

# Cisco IP 전화기 관리

- Cisco IP 전화기 보안, 87 페이지
- Cisco IP 전화기 사용자 정의, 117 페이지
- 전화기 기능 및 설정, 123 페이지
- 회사 및 개인 디렉터리, 217 페이지







# 7 장

## Cisco IP 전화기 보안

- 전화기 네트워크의 보안 강화, 87 페이지
- 지원 보안 기능, 88 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 Manager 릴리스 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 Manager용 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 IP 전화기 7800 및 8800 시리즈 보안 개요(<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.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>)



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 IP 전화기 8800 시리즈는 FIPS(Federal Information Processing Standard)를 준수합니다. 올바르게 작동하려면 FIPS 모드는 2048비트 이상의 키 크기가 필요합니다. 인증서가 2048비트 이상이 아닌 경우 전화기가 Cisco Unified Communications Manager에 등록되지 않고 전화기 등록에 실패합니다. 인증서의 키 크기가 FIPS와 호환되지 않습니다. 가 전화기에 표시됩니다.

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

다음 표에는 전화기에서 지원하는 보안 기능에 대한 개요가 나와 있습니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.


보안 모드, 신뢰 목록 및 802.1 X 인증을 포함하여 전화기에서 현재 보안 설정을 보려면 애플리케이션  을 누르고 관리자 설정 > 보안 설정을 선택합니다.

표 24: 보안 기능 개요

기능	설명
이미지 인증	서명된 이진 파일(확장자 .sbn)이 이미지를 전화기에 로드하기 전에 펌웨어 이미지를 변경할 수 없게 합니다. 이미지를 함부로 변경하면 인증 프로세스에 실패하여 새 이미지를 거부합니다.
이미지 암호화	암호화된 이진 파일(확장자 .sebn)이 이미지를 전화기에 로드하기 전에 펌웨어 이미지를 변경할 수 없게 합니다. 이미지를 함부로 변경하면 인증 프로세스에 실패하여 새 이미지를 거부합니다.
고객 사이트 인증서 설치	각 Cisco IP 전화기에는 장치 인증을 위한 고유 인증서가 필요합니다. 전화기에는 MIC(Manufacturing Installed Certificate)가 포함되어 있지만, 추가 보안을 위해 CAPF(Certificate Authority Proxy Function)를 사용하여 Cisco Unified Communications Manager Administration에 인증서 설치를 지정할 수 있습니다. 또는 전화기의 보안 구성 메뉴에서 LSC(Locally Significant Certificate)를 설치할 수도 있습니다.

기능	설명
장치 인증	각 개체가 다른 개체의 인증서를 수락할 때는 Cisco Unified Communications Manager 서버와 전화기 사이에서 이루어집니다. 전화기와 Cisco Unified Communications Manager 간에 보안 연결을 시행할 것인지를 결정하고 필요할 경우, TLS 프로토콜을 사용해 개체 간에 안전한 시그널링 경로를 구축합니다. Cisco Unified Communications Manager는 전화기를 인증할 수 없으면 전화기를 등록하지 않습니다.
파일 인증	전화기에서 다운로드한 디지털 서명 파일을 확인합니다. 전화기는 파일이 작성된 후에 부당한 파일 변경이 일어나지 않았다는 것을 확인하기 위해 서명을 확인합니다. 인증에 실패한 파일은 전화기의 플래시 메모리에 기록되지 않습니다. 전화기는 그러한 파일의 경우 추가 처리 없이 거부합니다.
파일 암호화	암호화는 파일이 전화기로 전송되는 과정에서 중요 정보가 노출되지 않게 합니다. 뿐만 아니라, 전화기는 파일이 작성된 후에 부당한 파일 변경이 일어나지 않았다는 것을 확인하기 위해 서명을 확인합니다. 인증에 실패한 파일은 전화기의 플래시 메모리에 기록되지 않습니다. 전화기는 그러한 파일의 경우 추가 처리 없이 거부합니다.
시그널링 인증	TLS 프로토콜을 사용해 전송되는 동안 시그널링 패킷에 변조되지 않았는지를 확인합니다.
MIC(Manufacturing Installed Certificate)	각 Cisco IP 전화기에는 장치 인증에 사용할 고유한 MIC(Manufacturing Installed Certificate)가 포함되어 있습니다. MIC는 전화기의 ID를 증명하는 고유한 영구 증명서를 제공하고, Cisco Unified Communications Manager는 이를 사용해 전화기를 인증합니다.
미디어 암호화	SRTP를 사용하면 지원 장치들 간의 미디어 스트림이 안전하다는 것을 증명하고, 의도한 장치에서만 데이터를 주고 받도록 할 수 있습니다. 여기에는 장치를 위해 미디어 기본 키 한 쌍을 생성하고, 장치에 이 키를 전달하며, 키가 전송되는 동안 키의 전달을 안전하게 보호하는 일도 포함됩니다.
CAPF(Certificate Authority Proxy Function)	지나치게 프로세싱 집약적인 인증서 생성 절차의 일부를 수행하고, 키 생성 및 인증서 설치를 위해 전화기와 상호 작용합니다. CAPF는 전화기를 대신해 고객이 지정한 인증 기관에 인증서를 요청하도록 구성할 수도 있고, 로컬에서 인증서를 생성하도록 구성할 수도 있습니다.
보안 프로파일	전화기의 비보안, 인증, 암호화 또는 보호 여부를 정의합니다. 이 표의 기타 항목에서 보안 기능을 설명합니다.
암호화된 구성 파일	전화기 구성 파일의 프라이버시를 보장할 수 있습니다.
전화기에 대한 선택적 웹 서버 비활성화	보안 목적을 위해 전화기에 대한 웹 페이지(전화기에 대한 다양한 작업 통계를 표시함) 및 셀프 케어 포털에 대한 액세스를 방지할 수 있습니다.

기능	설명
전화기 강화	<p>Cisco Unified Communications Manager Administration에서 제어하는 추가 보안 옵션:</p> <ul style="list-style-type: none"> <li>• PC 포트 비활성화</li> <li>• GARP(Gratuitous ARP) 비활성화</li> <li>• PC 음성 VLAN 액세스 비활성화</li> <li>• 설정 메뉴 액세스 비활성화 또는 기본 설정 메뉴 액세스를 허용하는 제한된 액세스 제공 또는 볼륨 변경 사항만 저장</li> <li>• 전화기 웹 페이지 액세스 비활성화</li> <li>• 블루투스 액세스서리 포트 비활성화</li> <li>• TLS 암호화 제한</li> </ul>
802.1X 인증	<p>Cisco IP 전화기는 네트워크에 액세스 권한을 요청하고 확보하는 데 802.1X 인증을 사용할 수 있습니다. 자세한 내용은 <a href="#">802.1X 인증</a>, <a href="#">113 페이지</a>를 참조하십시오.</p>
SRST용 보안 SIP 페일오버	<p>보안을 위해 SRST(Survivable Remote Site Telephony) 참조를 구성하고 Cisco Unified Communications Manager Administration에서 종속 장치를 재설정하고 나면, TFTP 서버에서 전화기의 cnf.xml 파일에 SRST 인증서를 추가하고 전화기에 해당 파일을 전송합니다. 그럼 보안이 이루어진 전화기는 SRST 활성화 라우터와 상호 작용하는 데 TLS 연결을 사용합니다.</p>
시그널링 암호화	<p>장치와 Cisco Unified Communications Manager 서버 간에 전송된 모든 SIP 시그널링 메시지가 암호화되도록 합니다.</p>
신뢰 목록 업데이트 알람	<p>전화기에 신뢰 목록 업데이트가 있으면 Cisco Unified Communications Manager는 업데이트의 성공 또는 실패를 나타내는 알람을 수신합니다. 자세한 내용은 다음 표를 참조하십시오.</p>
AES 256 암호화	<p>Cisco Unified Communications Manager 릴리스 10.5(2) 또는 그 이후 버전에 연결하면, 전화기는 시그널링 및 미디어 암호화를 위해 TLS 및 SIP를 위한 AES 256 암호화 지원을 지원합니다. 이렇게 하면 전화기에서 SHA-2(Secure Hash Algorithm) 표준을 따르고 FIPS(Federal Information Processing Standards)를 준수하는 AES-256 기반 암호를 사용해 TLS 1.2 연결을 시작하고 지원할 수 있습니다. 암호에는 다음이 포함됩니다.</p> <ul style="list-style-type: none"> <li>• TLS 연결용: <ul style="list-style-type: none"> <li>• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</li> <li>• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</li> </ul> </li> <li>• sRTP용: <ul style="list-style-type: none"> <li>• AEAD_AES_256_GCM</li> <li>• AEAD_AES_128_GCM</li> </ul> </li> </ul> <p>자세한 내용은 Cisco Unified Communications Manager 문서를 참조하십시오.</p>

기능	설명
ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서	Cisco Unified Communications Manager는 CC(공통 평가 기준) 인증의 일부로 버전 11.0에 ECDSA 인증서를 추가했습니다. 이는 CUCM 11.5 이상 버전의 모든 VOS(Voice Operating System) 제품에 영향을 줍니다.

다음 표는 신뢰 목록 업데이트 알람 메시지와 의미를 포함합니다. 자세한 내용은 Cisco Unified Communications Manager 문서를 참조하십시오.

표 25: 신뢰 목록 업데이트 알람 메시지

코드와 메시지	설명
1 - TL_SUCCESS	새 CTL 및/또는 ITL을 수신했음
2 - CTL_INITIAL_SUCCESS	새 CTL을 수신했음, 기존 TL 없음
3 - ITL_INITIAL_SUCCESS	새 ITL을 수신했음, 기존 TL 없음
4 - TL_INITIAL_SUCCESS	새 CTL 및 ITL을 수신했음, 기존 TL 없음
5 - TL_FAILED_OLD_CTL	새 CTL 업데이트 실패, 이전 TL이 있음
6 - TL_FAILED_NO_TL	새 TL 업데이트 실패, 이전 TL 없음
7 - TL_FAILED	일반 실패
8 - TL_FAILED_OLD_ITL	새 ITL 업데이트 실패, 이전 TL이 있음
9 - TL_FAILED_OLD_TL	새 TL 업데이트 실패, 이전 TL이 있음

보안 설정 메뉴는 다양한 보안 설정에 대한 정보를 제공합니다. 또한 메뉴는 신뢰 목록 메뉴에 대한 액세스를 제공하고 CTL 또는 ITL 파일이 전화기에 설치되었는지 여부를 나타냅니다.

다음 표는 [보안 설정] 메뉴의 옵션에 대해 설명합니다.

표 26: 보안 설정 메뉴

옵션	설명	옵션을 변경하려면
보안 모드	전화기에 설정된 보안 모드가 표시됩니다.	Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다. 설정은 [전화기 구성] 창의 프로토콜별 정보 부분에 나타납니다.
LSC	전화기에 보안 기능을 위해 사용되는 LSC(Locally Significant Certificate)가 설치되어 있는지(예) 또는 설치되어 있지 않은지(아니요)를 표시합니다.	전화기에 대한 LSC를 관리하는 작업에 관한 자세한 내용은 특정 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

옵션	설명	옵션을 변경하려면
신뢰 목록	<p>신뢰 목록은 CTL, ITL 및 서명된 구성 파일에 대한 하위 메뉴를 제공합니다.</p> <p>CTL 파일 하위 메뉴는 CTL 파일의 내용을 표시합니다. ITL 파일 하위 메뉴는 ITL 파일의 내용을 표시합니다.</p> <p>또한 신뢰 목록 메뉴는 다음 정보를 표시합니다.</p> <ul style="list-style-type: none"> <li>• CTL 서명: CTL 파일의 SHA1 해시</li> <li>• 통합 CM/TFTP 서버: 전화기가 사용하는 Cisco Unified Communications Manager 및 TFTP 서버의 이름입니다. 이 서버에 대한 인증서가 설치된 경우 인증서 아이콘을 표시합니다.</li> <li>• CAPF 서버: 전화기가 사용하는 CAPF 서버의 이름입니다. 이 서버에 대한 인증서가 설치된 경우 인증서 아이콘을 표시합니다.</li> <li>• SRST 라우터: 전화기가 사용할 수 있는 신뢰된 SRST 라우터의 IP 주소입니다. 이 서버에 대한 인증서가 설치된 경우 인증서 아이콘을 표시합니다.</li> </ul>	<p>자세한 내용은 <a href="#">LSC(Locally Significant Certificate) 설정, 93 페이지</a>의 내용을 참조하십시오.</p>
802.1X 인증	이 전화기에 802.1X 인증을 활성화할 수 있습니다.	<a href="#">802.1X 인증, 113 페이지</a> 참조

관련 항목

[Cisco Unified Communications Manager 설명서, xvii 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 애플리케이션  을 누릅니다.

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 LSC를 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.

## 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 사이의 연결에만 지원됩니다. 보안 통화가 구성되면 전화회의 통화, 공유 회선 등의 일부 기능이 제공되지 않습니다.


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 매개 변수). 서버를 선택하고, Unified Communications Manager 서비스를 선택합니다. [서비스 매개 변수 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 27: 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
비보안	회의개설	최소 보안 수준이 암호화되어 있습니다.	개시자는 보안 수준을 충족하지 않아 통부되었습니다라는 메시지를 받습니다.
보안	회의개설	최소 보안 수준이 비보안 상태입니다.	보안 컨퍼런스 브리지 전화회의에서 모든 통화를 수용합니다.

## 보안 전화기 통화 식별

전화기와 상대방 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.html](http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html)을 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 인증서입니다.
- PEAP(Protected Extensible Authentication Protocol): 클라이언트(전화기)와 RADIUS 간 Cisco의 독점 암호 기반 상호 인증 체계입니다. Cisco IP 전화기는 무선 네트워크에서 인증을 위해 PEAP를 사용할 수 있습니다. PEAP-MSCHAPV2 및 PEAP-GTC 인증 방법이 모두 지원됩니다.

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 28: 인증 및 암호화 체계

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

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>

## 인증 모드 설정

이 프로파일에 대한 인증 모드를 선택하려면 다음 단계를 수행합니다.

프로시저

**단계 1** 구성할 네트워크 프로파일을 선택합니다.

**단계 2** 인증 모드를 선택합니다.

**참고** 선택한 항목에 따라, 무선 보안 또는 무선 암호화에 추가 옵션을 구성해야 합니다. 자세한 내용은 [WLAN 보안, 97 페이지](#)를 참조하십시오.

**단계 3** 저장을 클릭하여 변경 사항을 작성합니다.

## 무선 보안 인증서

네트워크가 사용자 인증을 위해 EAP-FAST 및 PEAP를 사용할 때 원격 인증 전화 접속 사용자 서비스 (RADIUS)와 전화기에 필요한 경우 사용자 이름과 암호를 모두 구성해야 합니다.



**참고** 네트워크 내에서 도메인을 사용하는 경우 도메인 이름\사용자 이름 형식으로 도메인 이름과 함께 사용자 이름을 입력해야 합니다.

다음 작업을 수행하면 기존 Wi-Fi 암호가 지워질 수 있습니다.

- 잘못된 사용자 ID 또는 암호 입력
- EAP 유형이 PEAP-MSCHAPV2 또는 PEAP-GTC로 설정되었을 때 잘못되었거나 만료된 루트 CA 설치
- 전화기를 새 EAP 유형으로 변경하기 전에 전화기에서 사용되는 RADIUS 서버에서 EAP 유형을 비활성화

EAP 유형을 변경하려면 명시된 순서대로 다음을 수행합니다.

- RADIUS에서 새 EAP 유형을 활성화합니다.
- 전화기의 EAP 유형을 새 EAP 유형으로 변경합니다.

새 EAP 유형이 RADIUS 서버에서 활성화될 때까지 전화기에 구성된 현재 EAP 유형을 유지합니다. 새 EAP 유형이 RADIUS 서버에서 활성화되면 전화기의 EAP 유형을 변경할 수 있습니다. 모든 전화기에서 새로운 EAP 유형으로 변경된 후 원할 경우 이전 EAP 유형을 비활성화할 수 있습니다.

## 사용자 이름 및 암호 설정

네트워크 프로파일에 대한 사용자 이름 또는 암호를 입력하거나 변경하려면 RADIUS 서버에 구성된 것과 동일한 사용자 이름 및 암호 문자열을 사용해야 합니다. 사용자 이름 또는 암호의 최대 길이는 64자입니다.

무선 보안 인증서에 사용자 이름 및 암호를 설정하려면 다음 단계를 수행합니다.

프로시저

---

단계 1 네트워크 프로파일을 선택합니다.

단계 2 [사용자 이름] 필드에 이 프로파일에 대한 네트워크 사용자 이름을 입력합니다.

단계 3 [암호] 필드에 이 프로파일에 대한 네트워크 암호 문자열을 입력합니다.

단계 4 저장을 클릭하여 변경 사항을 작성합니다.

---

## 사전 공유 키 설정

사전 공유 키를 설정할 때 다음 섹션을 참조하십시오.

### 사전 공유 키 형식

Cisco IP 전화기는 ASCII 및 16진수 형식을 지원합니다. WEP 사전 공유 키를 설정할 때 다음 형식 중 하나를 사용해야 합니다.

#### 16진수

16진수 키의 경우 64개의 16진수(0-9 및 A-F)를 입력합니다(예:  
AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C).

#### ASCII

ASCII 키의 경우 기호를 포함하여 0-9, A-Z(대문자 및 소문자)를 사용하고 8~63자 길이인 문자를 입력합니다(예: GREG12356789ZXYW).

### PSK 설정

무선 인증서 영역에서 PSK를 설정하려면 다음 단계를 수행하십시오.

프로시저

---

단계 1 WPA 사전 공유 키 또는 WPA2 사전 공유 키를 활성화하는 네트워크 프로파일을 선택합니다.

단계 2 키 유형 영역에서 해당 키를 입력합니다.

단계 3 암호/사전 공유 키 필드에 ASCII 문자열 또는 16진수를 입력합니다.

단계 4 저장을 클릭하여 변경 사항을 작성합니다.

---



## 무선 암호화

무선 네트워크가 WEP 암호화를 사용하고 인증 모드를 개방형 + WEP로 설정하면 ASCII 또는 16진수 WEP 키를 입력해야 합니다.

전화기용 WEP 키가 액세스 지점에 할당된 WEP 키와 일치해야 합니다. Cisco IP 전화기 및 Cisco Aironet 액세스 지점은 40비트 및 128비트 암호화 키를 모두 지원합니다.

### WEP 키 형식

WEP 키를 설정할 때 다음 형식 중 하나를 사용해야 합니다.

#### 16진수

16진수 키의 경우 다음 키 크기 중 하나를 사용합니다.

##### 40비트

16진수 숫자(0-9 및 A-F)를 사용하는 10자릿수 암호화 키 문자열을 입력합니다(예: ABCD123456).

##### 128비트

16진수 숫자(0-9 및 A-F)를 사용하는 26자릿수 암호화 키 문자열을 입력합니다(예: AB123456789CD01234567890EF).

#### ASCII

ASCII 키의 경우 0-9, A-Z(대문자 및 소문자) 및 모든 기호를 사용하는 문자열을 다음 키 크기 중 하나로 입력합니다.

##### 40비트

5자 문자열을 입력합니다(예: GREG5).

##### 128비트

13자 문자열을 입력합니다(예: GREGSSECRET13).

### WEP 키 설정

WEP 키를 설정하려면 다음 단계를 따르십시오.

#### 프로시저

**단계 1** 개방형+WEP 또는 공유+WEP를 사용하는 네트워크 프로파일을 선택합니다.

**단계 2** 키 유형 영역에서 해당 키를 입력합니다.

**단계 3** 키 크기 영역에서 다음 문자열 길이 중 하나를 선택합니다.

- 40
- 128

단계 4 [암호화 키] 필드에서 선택한 키 유형과 키 크기에 기반한 적절한 키 문자열을 입력합니다. [WEP 키 형식, 103 페이지](#) 참조

단계 5 저장을 클릭하여 변경 사항을 작성합니다.

## Microsoft Certificate Services를 사용하여 ACS에서 CA 인증서 가져오기

ACS에서 루트 CA 인증서를 내보냅니다. 자세한 내용은 다음의 CA 또는 RADIUS 문서를 참조하십시오.

### MIC(Manufacturing Installed Certificate)

Cisco는 출하 시 전화기에 MIC(Manufacturing Installed Certificate)를 포함시켰습니다.

EAP-TLS 인증 도중 ACS 서버는 전화기의 신뢰를 확인해야 하고 전화기는 ACS 서버의 신뢰를 확인해야 합니다.

MIC를 확인하려면 제조 루트 인증서 및 제조 인증 기관(CA) 인증서를 Cisco IP 전화기에서 내보내고 Cisco ACS 서버에 설치해야 합니다. 이러한 두 가지 인증서는 Cisco ACS 서버가 MIC를 확인하는 데 사용되는 신뢰된 인증서 고리의 부분입니다.

Cisco ACS 인증서를 확인하려면 신뢰된 하위 인증서(있는 경우)와 Cisco ACS 서버의 (CA에서 작성된) 루트 인증서를 내보내고 전화기에 설치해야 합니다. 이러한 인증서는 ACS 서버에서 인증서 신뢰를 확인하는 데 사용되는 신뢰된 인증서 고리의 부분입니다.

### 사용자 설치 인증서

사용자 설치 인증서를 사용하려면 CSR(Certificate Signing Request)이 생성되고 CA로 승인을 위해 전송됩니다. CSR 없이 CA에서 사용자 인증서를 생성할 수도 있습니다.

EAP-TLS 인증 도중 ACS 서버는 전화기의 신뢰를 확인하고 전화기는 ACS 서버의 신뢰를 확인합니다.

사용자 설치 인증서의 인증을 확인하려면 Cisco ACS 서버에서 사용자 인증서를 승인한 CA에서 신뢰된 하위 인증서(있는 경우) 및 루트 인증서를 설치해야 합니다. 이러한 인증서는 사용자 설치 인증서의 신뢰를 확인하는 데 사용되는 신뢰된 인증서 고리의 부분입니다.

Cisco ACS 인증서를 확인하려면 신뢰된 하위 인증서(있는 경우)와 Cisco ACS 서버의 (CA에서 작성된) 루트 인증서를 내보내고 내보낸 인증서는 전화기에 설치됩니다. 이러한 인증서는 ACS 서버에서 인증서 신뢰를 확인하는 데 사용되는 신뢰된 인증서 고리의 부분입니다.

### EAP-TLS 인증서 설치

EAP-TLS에 대한 인증서를 설치하려면 다음 단계를 수행합니다.

#### 프로시저

단계 1 전화기 웹 페이지에서 전화기에 Cisco Unified Communications Manager 날짜와 시간을 설정합니다.

단계 2 제조 설치 인증서(MIC)를 사용하는 경우:

- a) 전화기 웹 페이지에서 CA 루트 인증서 및 제조 CA 인증서를 내보냅니다.
- b) Internet Explorer에서 Cisco ACS 서버에 인증서를 설치하고 신뢰 목록을 편집합니다.
- c) 루트 CA를 전화기로 가져옵니다.

자세한 내용은 다음 링크를 참조하십시오.

- [ACS에서 인증서 내보내기 및 설치, 105 페이지](#)
- [Microsoft Certificate Services를 사용하여 ISE에서 CA 인증서 가져오기, 106 페이지](#)

**단계 3** ACS 구성 도구를 사용하여 사용자 계정을 설정합니다.

자세한 내용은 다음 링크를 참조하십시오.

- [ACS 사용자 계정 설정 및 인증서 설치, 108 페이지](#)
- [Windows용 Cisco Secure ACS 사용 설명서](http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html)(<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>)

## 날짜 및 시간 설정

EAP-TLS는 Cisco IP 전화기의 내부 시계가 올바르게 설정되어야 하는 인증서 기반 인증을 사용합니다. 전화기가 Cisco Unified Communications Manager에 등록될 때 전화기의 날짜와 시간을 변경할 수 있습니다.



**참고** 새 서버 인증서가 요청되고 있고 로컬 시간이 GMT(Greenwich Mean Time)보다 늦으면 인증서 검증이 실패할 수 있습니다. GMT보다 빠른 로컬 날짜 및 시간을 설정하는 것이 좋습니다.

전화기를 올바른 로컬 날짜 및 시간으로 설정하려면 다음 단계를 수행합니다.

### 프로시저

**단계 1** 왼쪽 탐색 창에서 날짜 및 시간을 선택합니다.

**단계 2** [현재 전화기 날짜 및 시간] 필드의 설정이 [로컬 날짜 및 시간] 필드와 다른 경우 전화기를 로컬 날짜 및 시간으로 설정을 클릭합니다.

**단계 3** 전화기 재시작을 클릭한 다음 확인을 클릭합니다.

## ACS에서 인증서 내보내기 및 설치

MIC를 사용하려면 제조 루트 인증서 및 제조 CA 인증서를 내보내고 Cisco ACS 서버에서 인증서를 설치하십시오.

제조 루트 인증서 및 제조 CA 인증서를 ACS 서버로 내보내려면 다음 단계를 따르십시오.

### 프로시저

- 
- 단계 1 전화기 웹 페이지에서 인증서를 선택합니다.
  - 단계 2 제조 루트 인증서 옆에 있는 내보내기를 클릭합니다.
  - 단계 3 인증서를 저장하고 ACS 서버에 복사합니다.
  - 단계 4 제조 CA 인증서에 대해 1-2단계를 반복합니다.
  - 단계 5 ACS 서버 시스템 구성 페이지에서 각 인증서에 대한 파일 경로를 입력하고 인증서를 설치합니다.

참고 ACS 구성 도구 사용에 대한 자세한 내용은 ACS 온라인 도움말 또는 Windows용 Cisco Secure ACS 사용 설명서(<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>)를 참조하십시오.

- 단계 6 인증서 신뢰 목록(CTL) 페이지를 사용하여 ACS에서 신뢰하는 인증서를 추가합니다.
- 

### ACS 인증서 내보내기 방법

ACS에서 내보내는 인증서 유형에 따라 다음 방법 중 하나를 사용합니다.

- 사용자가 설치한 인증서 또는 ACS 인증서에 서명한 ACS 서버에서 CA 인증서를 내보내려면 [Microsoft Certificate Services](#)를 사용하여 ISE에서 CA 인증서 가져오기, 106 페이지를 참조하십시오.
- 자체 서명 인증서를 사용하는 ACS 서버에서 CA 인증서를 내보내려면 [Internet Explorer](#)를 사용하여 ACS에서 CA 인증서 내보내기, 107 페이지를 참조하십시오.

### Microsoft Certificate Services를 사용하여 ISE에서 CA 인증서 가져오기

이 방법을 사용하여 사용자가 설치한 인증서 또는 ISE 인증서에 서명한 ISE 서버에서 CA 인증서를 내보낼 수 있습니다.

Microsoft Certificate Services 웹 페이지를 사용하여 CA 인증서를 내보내려면 다음 단계를 따르십시오.

### 프로시저

- 
- 단계 1 Microsoft Certificate Services 웹 페이지에서 CA 인증서, 인증서 고리 또는 CRL 다운로드를 선택합니다.
  - 단계 2 다음 페이지의 텍스트 상자에서 현재 CA 인증서를 강조 표시하고 인코딩 방법 아래에서 DER을 선택하고 CA 인증서 다운로드를 클릭합니다.
  - 단계 3 CA 인증서를 저장합니다.
-

## Internet Explorer를 사용하여 ACS에서 CA 인증서 내보내기

이 방법을 사용하여 자체 서명 인증서를 사용하는 ACS 서버에서 CA 인증서를 내보낼 수 있습니다. Internet Explorer를 사용하여 ACS 서버에서 인증서를 내보내려면 다음 단계를 따르십시오.

### 프로시저

- 
- 단계 1 Internet Explorer에서 도구 > 인터넷 옵션을 선택한 다음 [내용] 탭을 클릭합니다.
  - 단계 2 [인증서] 아래에서 인증서를 클릭한 다음 [신뢰할 수 있는 루트 인증 기관] 탭을 클릭합니다.
  - 단계 3 루트 인증서를 강조 표시하고 내보내기를 클릭합니다. 인증서 내보내기 마법사가 표시됩니다.
  - 단계 4 다음을 클릭합니다.
  - 단계 5 다음 창에서 **DER** 인코딩된 바이너리 **X.509(.CER)**을 선택하고 다음을 클릭합니다.
  - 단계 6 인증서의 이름을 지정하고 다음을 클릭합니다.
  - 단계 7 전화기에 설치할 CA 인증서를 저장합니다.
- 

## 사용자가 설치한 인증서 요청 및 가져오기

전화기에서 인증서를 요청하고 설치하려면 다음 단계를 수행합니다.

### 프로시저

- 
- 단계 1 전화기 웹 페이지에서 EAP-TLS를 사용하는 네트워크 프로파일을 선택하고 EAP-TLS 인증서 필드에서 사용자 설치됨을 선택합니다.
  - 단계 2 인증서를 클릭합니다.  
사용자 인증서 설치 페이지에서 일반 이름 필드가 ACS 서버의 사용자 이름과 일치해야 합니다.  
참고 원하는 경우 일반 이름 필드를 편집할 수 있습니다. 이 이름이 ACS 서버에서의 사용자 이름과 일치하는지 확인하십시오. [ACS 사용자 계정 설정 및 인증서 설치, 108 페이지](#) 참조
  - 단계 3 인증서에 표시될 정보를 입력하고 제출을 클릭하여 CSR(Certificate Signing Request)을 생성합니다.
- 

## 인증 서버 루트 인증서 설치

전화기에 인증 서버 루트 인증서를 설치하려면 다음 단계를 수행합니다.

### 프로시저

- 
- 단계 1 ACS에서 인증 서버 루트 인증서를 내보냅니다. [ACS 인증서 내보내기 방법, 106 페이지](#) 참조
  - 단계 2 전화기 웹 페이지로 이동하고 인증서를 선택합니다.
  - 단계 3 인증 서버 루트 인증서 옆에 있는 가져오기를 클릭합니다.

단계 4 전화기를 다시 시작합니다.

## ACS 사용자 계정 설정 및 인증서 설치

사용자 계정 이름을 설정하고 ACS에 전화기에 대한 MIC 루트 인증서를 설치하려면 다음 단계를 수행합니다.



참고 ACS 구성 도구 사용에 대한 자세한 내용은 ACS 온라인 도움말 또는 Windows용 Cisco Secure ACS 사용 설명서를 참조하십시오.

### 프로시저

단계 1 ACS 구성 도구 사용자 설정 페이지에서 전화기 사용자 계정 이름이 아직 설정되어 있지 않으면 새로 만듭니다.

일반적으로 사용자 이름은 끝에 전화기 MAC 주소를 포함합니다. EAP-TLS에 필요한 암호가 없습니다.

참고 사용자 이름이 사용자 인증서 설치 페이지의 일반 이름 필드와 일치하는지 확인하십시오. [사용자가 설치한 인증서 요청 및 가져오기, 107 페이지](#) 참조

단계 2 시스템 구성 페이지의 EAP-TLS 섹션에서 다음 필드를 활성화합니다.

- EAP-TLS 허용
- CN 비교 인증서

단계 3 ACS 인증서 설정 페이지에서 제조 루트 인증서 및 제조 CA 인증서를 ACS 서버에 추가합니다.

단계 4 ACS 인증서 신뢰 목록에서 제조 루트 인증서와 제조 CA 인증서를 모두 활성화합니다.

## PEAP 설정

PEAP(Protected Extensible Authentication Protocol)는 서버측 공개 키 인증서를 사용하여 클라이언트와 인증 서버 간에 암호화된 SSL/TLS 터널을 만들어 클라이언트를 인증합니다.

Cisco IP 전화기 8865는 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.



참고 인증 서버 검증은 인증 서버 인증서를 가져와서 활성화할 수 있습니다.

## 시작하기 전에

전화기에 대한 PEAP 인증을 구성하려면 다음 Cisco Secure ACS 요구 사항을 충족하는지 확인하십시오.

- ACS 루트 인증서를 설치해야 합니다.
- PEAP에 대한 서버 검증을 활성화하기 위해 인증서를 설치할 수도 있습니다. 하지만 서버 인증서가 설치된 경우 서버 검증이 활성화됩니다.
- [EAP-MSCHAPv2 허용] 설정이 활성화되어 있어야 합니다.
- 사용자 계정 및 암호를 구성해야 합니다.
- 암호 인증을 위해 로컬 ACS 데이터베이스 또는 외부 데이터베이스(예: Windows 또는 LDAP)를 사용할 수 있습니다.

## PEAP 인증 활성화

### 프로시저

단계 1 전화기 구성 웹 페이지에서 PEAP를 인증 모드로 선택합니다.

단계 2 사용자 이름과 암호를 입력합니다.

## 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.

### 관련 항목

[Cisco IP 전화기 웹 페이지](#), 239 페이지

## 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 등록된 전화기는 전화기 찾기 및 나열 창과 전화기 구성 창 상단에 IP 주소를 표시합니다.
- 전화기에서 애플리케이션  을 누르고 전화기 정보를 선택하고 IPv4 주소 필드로 스크롤합니다.

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 사용자 설치 필드를 찾아 설치를 클릭합니다.

단계 3 PC에서 인증서를 찾습니다.

단계 4 추출 암호 필드에 인증서 추출 암호를 입력합니다.

단계 5 업로드를 클릭합니다.

단계 6 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 매개 변수 구성

전화기 웹 페이지에서 다음과 같은 SCEP 매개 변수를 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 매개 변수를 사용합니다. 매개 변수를 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 매개 변수를 활성화합니다.

단계 5 **WLAN Root CA Fingerprint (SHA256 or SHA1)** 확인란을 선택하여 SCEP QED 매개 변수를 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. CDP는 로컬로 연결된 워크스테이션은 식별하지 않습니다. Cisco IP 전화기는 EAPOL 패스스루 메커니즘을 제공합니다.

다. 이 메커니즘을 통해 Cisco IP 전화기에 연결된 워크스테이션은 LAN 스위치의 802.1X 인증자에게 EAPOL 메시지를 전달합니다. 패스스루 메커니즘은 네트워크에 접속하기 전 데이터 엔드포인트를 인증하기 위해 IP 전화기가 LAN 스위치로 작동하지 않도록 합니다.

Cisco IP 전화기는 프록시 EAPOL 로그오프 메커니즘도 제공합니다. 로컬로 연결된 PC에서 IP 전화기와의 연결을 끊어도, LAN 스위치와 IP 전화기 사이의 링크는 유지되기 때문에 LAN 스위치는 물리적인 링크 문제를 발견하지 못합니다. 네트워크 무결성이 손상되지 않도록 IP 전화기는 다운스트림 PC를 대신해 스위치에 EAPOL 로그오프 메시지를 전송합니다. 그러면 LAN 스위치에서 다운스트림 PC에 대한 인증 항목을 지웁니다.

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

- Cisco IP 전화기: 전화기에서 네트워크 액세스 요청을 시작합니다. Cisco IP 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 Secure Access Control Server(ACS)(또는 기타 타사 인증 서버): 인증 서버와 전화기가 모두 전화기를 인증하는 공유 비밀로 구성되어야 합니다.
- 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.
- PC 포트 구성: 802.1X 표준은 VLAN을 고려하지 않기 때문에 특정 스위치 포트에서 단일 장치만 인증하도록 권장합니다. 그러나 일부 스위치(Cisco Catalyst 스위치 포함)는 멀티도메인 인증을 지원합니다. PC를 전화기의 PC 포트에 연결할 수 있는지 여부는 스위치 구성에서 결정합니다.
  - 활성화됨: 멀티도메인 인증을 지원하는 스위치를 사용 중이면, PC 포트를 활성화하고 여기에 PC를 연결할 수 있습니다. 이 경우 Cisco IP 전화기는 스위치와 연결된 PC 간의 인증 교환을 모니터링하기 위해 프록시 EAPOL 로그오프를 지원합니다. Cisco Catalyst 스위치의 IEEE 802.1X 지원에 관한 자세한 내용은 Cisco Catalyst 스위치 구성 설명서를 참조하십시오.  
[http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)
  - 비활성화됨: 스위치가 같은 포트에서 여러 개의 802.1X 준수 장치를 지원하지 않는다면, 802.1X 인증이 활성화될 때 PC 포트를 비활성화해야 합니다. 이 포트를 비활성화하지 않은 상태에서 나중에 PC와 연결하려고 하면, 스위치에서 전화기와 PC 모두에 대한 네트워크 액세스를 거부합니다.
- 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.

## 802.1X 인증 액세스

다음 단계를 수행하여 802.1X 인증 설정에 액세스할 수 있습니다.

프로시저

단계 1 애플리케이션  을 누릅니다.

단계 2 관리 설정 > 보안 설정 > **802.1X** 인증을 선택합니다.

단계 3 [802.1X 인증 옵션](#), 115 페이지에 설명된 것처럼 옵션을 구성합니다.

단계 4 이 메뉴를 종료하려면 종료를 누릅니다.

### 802.1X 인증 옵션


다음 표에서는 802.1X 인증 옵션에 대해 설명합니다.

표 29: 802.1X 인증 설정

옵션	설명	변경
장치 인증	802.1X 인증의 활성화 여부를 판별합니다. <ul style="list-style-type: none"> <li>활성화: 전화기는 802.1X 인증을 사용하여 네트워크 액세스를 요청합니다.</li> <li>비활성화: 기본 설정입니다. 전화기는 CDP를 사용하여 VLAN 및 네트워크 액세스를 획득합니다.</li> </ul>	<a href="#">장치 인증 필드 설정</a> , 115 페이지
트랜잭션 상태	상태: 802.1x 인증의 상태를 표시합니다. <ul style="list-style-type: none"> <li>연결 끊김: 802.1x 인증이 전화기에 구성되지 않았음을 나타냅니다.</li> <li>인증됨: 전화기가 인증되었음을 나타냅니다.</li> <li>보류됨: 인증 프로세스가 진행 중임을 나타냅니다.</li> </ul> 프로토콜: 802.1x 인증에 사용되는 EAP 메서드를 표시합니다(EAP-FAST 또는 EAP-TLS일 수 있음).	표시 전용입니다. 구성할 수 없음

### 장치 인증 필드 설정

프로시저

단계 1 애플리케이션  을 누릅니다.

단계 2 관리 설정 > 보안 설정 > **802.1X** 인증을 선택합니다.

단계 3 장치 인증 옵션을 설정합니다.

- 예
- 아니요

단계 4 적용을 누릅니다.

---



## 8 장

# Cisco IP 전화기 사용자 정의

- 사용자 지정 전화기 벨소리, 117 페이지
- 사용자 정의 배경 이미지, 117 페이지
- 광대역 코덱 설정, 119 페이지
- 유휴 디스플레이 설정, 120 페이지
- 신호음 사용자 정의, 120 페이지

## 사용자 지정 전화기 벨소리

전화기는 하드웨어에 세 가지 벨소리(Sunshine, Chirp, Chirp1)가 구현되어 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 파일(Ringlist-wb.xml)과 함께 각 Cisco Unified Communications Manager 서버의 TFTP 디렉터리에 있습니다.



주의 모든 파일 이름은 대/소문자를 구분합니다. 파일 이름으로 Ringlist-wb.xml을 사용하면, 전화기가 변경 사항을 적용하지 못합니다.

자세한 내용은 Cisco Unified Communications Manager 릴리스 12.0(1) 이상의 경우 [Cisco Unified Communications Manager 기능 구성 설명서](#)의 "사용자 지정 전화기 벨소리 및 배경" 장을 참조하십시오.

## 사용자 정의 배경 이미지

배경 이미지 또는 배경 무늬로 Cisco IP 전화기를 사용자 지정할 수 있습니다. 사용자 지정된 배경 무늬는 회사 로고나 이미지를 표시하는 일반적인 방법이며 많은 조직에서 이 기능을 사용하여 전화기를 돋보이게 합니다.

펌웨어 릴리스 12.7(1)부터는 전화기와 키 확장 모듈 모두에서 배경화면을 사용자 정의할 수 있습니다. 그러나 전화기용 이미지, 확장 모듈용 이미지 하나씩이 필요합니다.

전화기는 배경화면의 색을 분석하고 글꼴의 색상과 아이콘을 사용자가 읽을 수 있도록 바꿉니다. 배경 무늬가 어두운 경우에는 전화기에서 글꼴과 아이콘을 흰색으로 변경합니다. 배경 무늬가 밝은 경우에는 전화기에서 글꼴과 아이콘이 검정색으로 표시됩니다.

배경에는 단색 또는 패턴과 같은 간단한 이미지를 선택하는 것이 좋습니다. 고대비 이미지는 피하십시오.

다음 두 가지 방법 중 하나로 사용자 지정된 배경 무늬를 추가할 수 있습니다.

- 목록 파일 사용
- 일반 전화기 프로파일 사용

전화기에서 사용할 수 있는 다양한 배경 화면에서 이미지를 선택할 수 있게 하려면 목록 파일을 수정하십시오. 그러나 이미지를 전화기로 푸시하려면 일반 전화 프로파일을 작성하거나 수정합니다.

접근 방식에 관계없이 다음 사항에 유의하십시오.

- 이미지는 PNG 형식이어야 하며 전체 이미지의 크기는 다음 치수 이내여야 합니다.
  - 썸네일 이미지 - 139픽셀(폭) X 109픽셀(높이)
  - Cisco IP 전화기 8800 시리즈 - 800픽셀 x 480픽셀
  - 듀얼 LCD 화면을 사용하는 Cisco IP 전화기 8851 및 8861 키 확장 모듈 - 320 x 480픽셀
  - 듀얼 LCD 화면을 사용하는 Cisco IP 전화기 8865 키 확장 모듈 - 320 x 480픽셀
  - Cisco IP 전화기 8800 키 확장 모듈 (단일 LCD 화면) - 272 x 480픽셀
- 이미지, 썸네일 및 목록 파일을 TFTP 서버에 업로드합니다. 디렉터리는 다음과 같습니다.
  - Cisco IP 전화기 8800 시리즈—Desktops/800x480x24
  - Cisco IP 전화기 8851 및 8861 키 확장 모듈(듀얼 LCD 화면—데스크톱/320x480x24)
  - Cisco IP 전화기 8865 키 확장 모듈(듀얼 LCD 화면)—Desktops/320x480x24
  - Cisco IP 전화기 8800 키 확장 모듈(단일 LCD 화면)—Desktops/272x480x24

업로드가 완료된 후 TFTP 서버를 다시 시작합니다.

- 사용자가 자신의 배경 화면을 선택하지 않게 하려면 전화 배경 이미지 설정에 최종 사용자 액세스 스활성화를 비활성화합니다. 전화기 프로파일을 저장하고 적용합니다. 변경 사항이 적용되도록 전화기를 다시 시작합니다.



**참고** 일반 전화기 프로파일을 사용하여 전화기 배경 이미지를 대량으로 적용할 수 있습니다. 그러나 대량 구성을 사용하려면 전화기 배경 이미지 설정에 대해 최종 사용자 액세스 사용을 비활성화해야 합니다. 배경 이미지의 대량 구성에 대한 자세한 내용은 [사용자 지정 배경 화면 Cisco IP 전화기 8800 시리즈](#)의 “공통 전화기 프로파일 구성” 장을 참조하십시오.



배경 무늬 사용자 지정에 대한 자세한 내용은 다음 설명서를 참조하십시오.

- 사용자 지정 배경 무늬 모범 사례 Cisco IP 전화기 8800 시리즈).
- Cisco Unified Communications Manager 릴리스 12.0(1) 이상의 경우 Cisco Unified Communications Manager 기능 구성 설명서의 "사용자 지정 전화기 벨소리 및 배경" 장.
- Cisco IP 전화기 8800 시리즈 사용 설명서의 “설정” 장.

## 광대역 코덱 설정

Cisco IP 전화기에 대해서는 기본적으로 G.722 코덱이 활성화됩니다. Cisco Unified Communications Manager가 G.722를 사용하도록 구성되었거나 엔드포인트에서 G.722를 지원한다면, 통화는 G.711 대신 G.722 코덱을 사용해 연결됩니다.

이러한 상황은 사용자가 광대역 헤드셋이나 광대역 핸드셋을 활성화했는지에 상관없이 발생하지만, 헤드셋이나 핸드셋이 활성화되어 있다면, 사용자는 통화 중에 오디오 감도가 더욱 향상되었음을 감지할 수도 있습니다. 감도가 향상되었다는 것은 오디오의 선명도가 향상되었다는 뜻이며, 더불어 엔드포인트에서 종이 스치는 소리나 가까운 곳의 대화 내용 같은 배경 소음을 들을 수 있다는 뜻이기도 합니다. 심지어 광대역 헤드셋이나 핸드셋이 없어도, 일부 사용자는 집중을 방해하는 G.722의 향상된 감도를 선호할 수도 있습니다. 그 밖의 사용자들은 G.722의 향상된 감도를 선호할 수도 있습니다.

Advertise G.722 및 iSAC 코덱 서비스 매개 수는 매개 수가 구성되어 있는 Cisco Unified Communications Manager Administration 창에 따라 광대역 지원을 이 Cisco Unified Communications Manager 서버에 등록된 모든 장치를 대상으로 할 것인지, 아니면 특정 전화기를 대상으로 할 것인지를 결정합니다.

### 프로시저

**단계 1** 모든 장치에 대한 광대역 지원을 구성하려면:

- Cisco Unified Communications Manager Administration에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.
- [Advertise G.722 및 iSAC 코덱] 필드를 설정합니다.

이 엔터프라이즈 매개 변수의 기본값이 참인 것은 이 Cisco Unified Communications Manager에 등록된 모든 Cisco IP 전화기 모델이 Cisco Unified Communications Manager에 G.722를 광고한다는 뜻입니다. 시도된 통화의 각 엔드포인트가 기능 집합에서 G.722를 지원하면, Cisco Unified Communications Manager는 가능하면 언제나 통화에 해당 코덱을 선택합니다.

**단계 2** 특정 장치에 대한 광대역 지원을 구성하려면:

- Cisco Unified Communications Manager Administration에서 장치 > 전화기를 선택합니다.
- 제품별 구성 영역에서 [Advertise G.722 및 iSAC 코덱] 매개 변수를 설정합니다.

이 제품별 매개 변수의 기본값은 엔터프라이즈 매개 변수가 지정하는 값을 사용하는 것입니다. 전화별 단위로 이 설정을 재지정하려면 활성화됨 또는 비활성화됨을 선택하십시오.

## 유휴 디스플레이 설정

전화기 화면에 표시되는 유휴 디스플레이(텍스트만, 텍스트 파일은 1M 바이트를 초과하면 안 됨)를 지정할 수 있습니다. 유휴 디스플레이는 전화기가 지정된 시간 동안 유휴 상태(사용하지 않는 상태)이고 어떤 기능 메뉴도 열리지 않았을 때 전화기에서 실행하는 XML 서비스입니다.

유휴 디스플레이 작성 및 표시에 관한 자세한 지시 사항은 다음 URL에서 *Cisco IP* 전화기에 유휴 URL 그래픽 작성을 참조하십시오.

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

그리고 해당 Cisco Unified Communications Manager 릴리스용 문서에서는 다음과 같은 정보를 확인할 수 있습니다.

- 유휴 디스플레이 XML 서비스의 URL 지정:
  - 단일 전화기용: Cisco Unified Communications Manager Administration의 [전화기 구성] 창의 유휴 필드
  - 여러 대의 전화를 동시에: [엔터프라이즈 매개 변수 구성] 창의 URL 유휴 필드 또는 BAT(Bulk Administration Tool)의 유휴 필드
- 유휴 디스플레이 XML 서비스가 시작되기 전에 전화기를 사용하지 않은 시간 길이 지정:
  - 단일 전화기용: Cisco Unified Communications Manager Administration의 [전화기 구성] 창의 유휴 타이머 필드
  - 여러 대의 전화를 동시에: [엔터프라이즈 매개 변수 구성] 창의 URL 유휴 시간 필드 또는 BAT(Bulk Administration Tool)의 유휴 타이머 필드

프로시저

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

단계 2 [유휴] 필드에서 유휴 디스플레이 XML 서비스에 URL을 입력합니다.

단계 3 [유휴 타이머] 필드에 유휴 디스플레이 XML 서비스를 표시하기 전에 유휴 전화기가 대기하는 시간을 입력합니다.

단계 4 저장을 선택합니다.

## 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 매개 변수를 선택합니다.
  - 단계 2 적절한 서버를 선택합니다.
  - 단계 3 **Cisco CallManager**를 서비스로 선택합니다.
  - 단계 4 [클러스터 전역 매개 변수] 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

## 전화기 기능 및 설정

- 전화기 기능 및 설정 개요, 123 페이지
- Cisco IP 전화기 사용자 지원, 124 페이지
- 전화기 기능, 124 페이지
- 기능 단추 및 소프트키, 142 페이지
- 전화기 기능 구성, 144 페이지
- 소프트키 템플릿 설정, 198 페이지
- 전화기 버튼 템플릿, 201 페이지
- VPN 구성, 204 페이지
- 추가 회선 키 설정, 205 페이지
- TLS 재개 타이머 설정, 208 페이지
- Intelligent Proximity 활성화, 209 페이지
- 비디오 전송 해상도 설정, 209 페이지
- 이전 버전의 Cisco Unified Communications Manager에서 헤드셋 관리, 211 페이지

## 전화기 기능 및 설정 개요

네트워크에 Cisco IP 전화기를 설치하고, 네트워크 설정을 구성하고, 이러한 설정을 Cisco Unified Communications Manager에 추가한 후에는 Cisco Unified Communications Manager Administration 애플리케이션을 사용하여 텔레포니 기능을 구성하고, 선택적으로 전화기 템플릿을 수정하고, 서비스를 설정하고, 사용자를 할당해야 합니다.

Cisco Unified Communications Manager Administration에서 Cisco IP 전화기에 대한 추가 설정을 수정할 수 있습니다. 이 웹 기반 애플리케이션을 사용하여 전화기 등록 기준 및 발신 검색 공간을 설정하고 전화기 단추 템플릿을 수정하십시오.

기능을 전화 회선 키에 추가할 때 사용 가능한 회선 키의 수에 따라 제한이 있습니다. 전화기에는 회선 키 수보다 많은 기능을 추가할 수 없습니다.

## 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

## 전화기 기능

Cisco Unified Communications Manager에 Cisco IP 전화기를 추가해야, 전화기에 기능을 추가할 수 있습니다. 다음 표에는 지원되는 텔레포니 기능이 정리되어 있는데, 이중 다수는 Cisco Unified Communications Manager Administration을 사용해 구성할 수 있습니다.

전화기에서 이런 대부분의 기능을 사용하는 방법에 관한 자세한 내용은 *Cisco IP* 전화기 8800 시리즈 사용자 설명서를 참조하십시오. 프로그램 가능 버튼과 전용 소프트키 및 기능 버튼으로 구성할 수 있는 기능 목록은 [기능 단추 및 소프트키, 142 페이지](#)를 참조하십시오.



**참고** Cisco Unified Communications Manager Administration은 다양한 텔레포니 기능을 구성할 때 사용할 수 있는 몇 가지 서비스 매개 변수도 제공합니다. 서비스 매개변수 액세스 및 구성에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

서비스 기능에 대한 자세한 내용은 [제품별 구성](#) 창에서 매개 변수 이름이나 물음표(?) 도움말 버튼을 선택하십시오.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

기능	설명 및 세부 정보
단축 다이얼	<p>전화기 keypad에 할당된 인덱스 코드(1-199)를 입력하면 단축 다이얼로 빠르게 전화를 걸 수 있습니다.</p> <p>참고 온 훅 및 오프 훅 상태에서 단축 다이얼을 사용할 수 있습니다.</p> <p>사용자는 셀프 케어 포털에서 인덱스 코드를 할당합니다.</p>
대응 선택 착신 통화 알림	<p>착신 통화 알림 관리를 위한 다양한 옵션을 제공합니다. 통화 알림을 사용 또는 사용하지 않을 수 있습니다. 발신자 ID 표시도 활성화 또는 비활성화할 수 있습니다.</p> <p>대응 선택 착신 통화 알림 제품별 구성, 146 페이지.</p>
AES 256 암호화 지원	<p>TLS 1.2와 새 암호를 지원해 보안을 강화합니다. 자세한 내용은 지원 보안 기능, 88 페이지를 참조하십시오.</p>
상당사 인사말	<p>상당사는 발신자와 대화를 시작하기 전에 고객 통화 시작 시 재생되는 사전 녹음된 인사말을 만들고 업데이트할 수 있습니다. 상당사는 필요에 따라 하나 또는 여러 개의 인사말을 사전 녹음할 수 있습니다.</p> <p>상당사 인사말 활성화, 176 페이지를 참조하십시오.</p>
모든 통화 당겨받기	<p>사용자는 통화의 라우팅 방식에 상관없이 통화 당겨받기 그룹의 모든 회선 통화를 당겨받을 수 있습니다.</p> <p>해당 Cisco Unified Communications Manager 릴리스용 문서에서 통화 당겨받기를 참조하십시오.</p>
애플리케이션 다이얼 규칙	<p>공유 모바일 연락처의 번호를 네트워크의 전화를 걸 수 있는 번호로 변환합니다.</p> <p>애플리케이션 다이얼 규칙, 80 페이지를 참조하십시오.</p>
지원된 직접 통화 지정정보류	<p>직접 지정정보류 기능을 사용해 버튼 누르기 한 번으로 통화를 지정정보류할 수 있습니다. 관리자는 [BLF(통화 중 램프 필드) 지원된 직접 통화 지정정보류] 버튼을 구성해야 합니다. 사용자가 활성 통화에 대해 유휴 상태의 [BLF 지원된 직접 통화 지정정보류] 버튼을 누르면, 활성 통화는 [지원된 직접 통화 지정정보류] 버튼과 연결된 직접 지정정보류 슬롯에 지정정보류됩니다.</p> <p>해당 Cisco Unified Communications Manager 릴리스용 문서에서 지원된 직접 통화 지정정보류를 참조하십시오.</p>
AMWI(음성 메시지 대기 중 표시기)	<p>전화를 걸 때 핸드셋, 헤드셋 또는 스피커폰에서 나는 셔터음은 회선에 1개 이상의 새 음성 메시지가 있다는 뜻입니다.</p> <p>참고 셔터음은 회선에 좌우됩니다. 이 셔터음은 대기 중인 메시지가 있는 회선을 사용하는 경우에만 들립니다.</p>

기능	설명 및 세부 정보
자동 응답	벨이 1회 또는 2회 울린 후 자동으로 착신 통화에 연결합니다. 자동 응답 기능은 스피커폰 또는 헤드셋 중 하나를 사용합니다. 디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
자동 포트 동기화	포트를 전화의 포트 간 최저 속도로 동기화하여 패킷 유실을 제거합니다. 자동 포트 동기화를 참조하십시오 <a href="#">제품별 구성, 146 페이지</a> .
자동 당겨받기	사용자가 통화 당겨받기 기능을 위해 원터치 당겨받기 기능을 사용할 수 있습니다. 해당 Cisco Unified Communications Manager 릴리스용 문서에서 통화 당겨받기를 참조하십시오.
참여	사용자가 대상 전화기의 내장 컨퍼런스 브리지를 사용해 3방향 전화회의를 설정하면 통화에 참여할 수 있습니다. 이 표의 “회의끼기”를 참조하십시오.
외부 호전환 차단	사용자가 다른 외부 번호로 외부 통화를 호전환하는 것을 막습니다. 외부 통화 호전환 정보에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
블루투스 다중 연결	사용자는 다중 장치를 전화기에 페어링할 수 있습니다. 그런 다음 사용자는 블루투스와 블루투스 헤드셋을 동시에 사용하여 모바일 장치를 연결할 수 있습니다. Cisco IP 전화기 8851NR은 블루투스를 지원하지 않습니다.
BLF(통화 중 램프 필드)	전화기의 단축 다이얼 버튼과 연결된 디렉터리 번호의 통화 상태를 모니터링할 수 있습니다. Presence에 대한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
BLF(통화 중 램프 필드) 당겨받기	BLF 단축 다이얼에 대한 개선 기능을 제공합니다. 걸려오는 전화를 모니터링할 수 있는 DN(디렉터리 번호)을 구성할 수 있습니다. DN에서 걸려오는 전화를 받는 경우 모니터링 사용자에게 이를 알리면 모니터링 사용자가 통화를 당겨받을 수 있습니다. 통화 당겨받기에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
콜백	통화 중이거나 전화를 받을 수 없는 상대방이 전화를 받을 수 있게 되면 전화기에 음성 및 시각적 알림 메시지를 제공합니다. 콜백에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.



기능	설명 및 세부 정보
통화 표시 제한	<p>통화에 관련된 상대방에 따라 발신 또는 연결된 회선에 대해 표시할 정보를 결정합니다.</p> <p>라우팅 계획 및 통화 표시 제한에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
통화 착신 전환	<p>착신 통화를 다른 번호로 재전송할 수 있습니다. [통화 착신 전환] 옵션에는 [모든 통화 착신 전환], [통화 중 착신 전환], [응답 없음 착신 전환] 및 [통화권 아님 착신 전환]이 포함됩니다.</p> <p>디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서와 <a href="#">셀프 서비스 포털 디스플레이 사용자 정의, 84 페이지</a>를 참조하십시오.</p>
모든 통화 착신 전환 루프 차단	모든 통화 착신 전환 루프를 찾아 차단합니다. 모든 통화 착신 전환 루프가 발견되면, 모든 통화 착신 전환 구성이 무시되고 전화가 울립니다.
모든 통화 착신 전환 루프 방지	모든 통화 착신 전환 루프를 찾아 차단합니다. 모든 통화 착신 전환 루프가 발견되면, 모든 통화 착신 전환 구성이 무시되고 전화가 울립니다.
착신 전환 구성 가능 표시	<p>기존 착신 전환 최대 홉 수 서비스 매개 변수의 허용치보다 홉 수가 더 많은 모든 통화 착신 전환을 생성하거나 모든 통화 착신 전환 루프를 생성하는 모든 통화 착신 전환 대상을 전화기에서 직접 구성하지 못하게 합니다.</p> <p>디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
착신 전환 대상 오버라이드	<p>CFA(모든 통화 착신 전환) 대상이 CFA 개시자에게 전화를 거는 경우 CFA를 오버라이드할 수 있습니다. 이 기능을 사용하면 CFA 대상이 중요한 통화에 대해 CFA 개시자에게 연락할 수 있습니다. 오버라이드는 내부 또는 외부 CFA 대상 전화번호에 상관없이 작동합니다.</p> <p>디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
통화 착신 전환 알림	<p>착신 전환된 전화를 받을 때 사용자가 볼 수 있는 정보를 구성할 수 있습니다.</p> <p><a href="#">통화 착신 전환 알림 설정, 178 페이지</a>를 참조하십시오.</p>
공유 회선에 대한 통화 기록	<p>전화기 통화 기록에서 공유 회선 활동을 확인할 수 있습니다. 이 기능의 이점은 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>• 공유 회선의 부재 중 전화 기록</li> <li>• 공유 회선의 모든 받은 전화 및 걸려온 전화 기록</li> </ul>

기능	설명 및 세부 정보
통화 지정보류	<p>Cisco Unified Communications Manager 시스템에서 또 다른 전화를 사용하여 통화를 지정보류(임시 저장)한 다음 검색할 수 있습니다.</p> <p>제품별 구성 레이아웃 창에서 필드 통화 지정 보류에 대한 전용 회선을 구성하여 통화를 원래 회선이나 다른 회선으로 지정 보류시킬 수 있습니다.</p> <p>이 필드를 활성화하면 지정 보류된 통화는 사용자의 회선에 남아 있고 다시 시작 소프트웨어를 사용하여 통화를 당겨 받을 수 있습니다. 사용자는 전화기 디스플레이에서 지정 보류된 통화의 내선 번호를 볼 수 있습니다.</p> <p>이 필드를 비활성화하면 지정 보류된 통화가 통화 지정 보류 회선으로 전송됩니다. 사용자의 회선이 유휴 상태로 반환되고 통화 지정 보류 내선 번호가 팝업 창에 표시됩니다. 사용자가 내선 번호로 전화를 걸어 통화를 당겨 받습니다.</p> <p>통화 지정보류에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
통화 당겨받기	<p>통화 당겨받기 그룹에 있는 다른 전화기에서 올리는 전화를 자신의 전화기로 재전송할 수 있습니다.</p> <p>전화기의 주 회선에 대한 음성 및 시각적 알림 메시지를 구성할 수 있습니다. 그러면 당겨받기 그룹의 전화가 울릴 때 이를 사용자에게 알려줍니다.</p> <p>통화 당겨받기에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
통화 녹음	<p>감독자가 활성 통화를 녹음할 수 있습니다. 사용자는 통화가 녹음되는 경우 통화 중에 녹음 알림음을 들을 수도 있습니다.</p> <p>통화에 대한 보안이 이루어지는 경우 통화의 보안 상태가 Cisco IP 전화기에 잠금 아이콘 형태로 표시됩니다. 통화가 연결된 당사자는 통화에 대한 보안이 이루어지고 통화 내용이 녹음되고 있음을 알리는 알림음을 듣게 될 수도 있습니다.</p> <p><b>참고</b>      활성 통화를 모니터링하거나 녹음할 때, 사용자가 인터콤 전화를 받거나 걸 수 있습니다. 그런데 이처럼 사용자가 인터콤 전화를 걸면, 활성 통화가 보류 상태가 되어 녹음 세션이 종료되거나 모니터링 세션이 중단됩니다. 모니터링 세션을 다시 시작하려면 모니터링되던 전화를 건 사람이 통화를 재시작해야 합니다.</p> <p>모니터링 및 녹음에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
통화 대기 중	<p>다른 통화를 하는 동안 올린 착신 통화를 표시하여 사용자가 받을 수 있게 합니다. 전화기 화면에 착신 통화 정보가 표시됩니다.</p> <p>디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>

기능	설명 및 세부 정보
통화 대기 벨	통화 대기 사용자에게 표준 신호음이 아닌 다른 벨소리 옵션을 제공합니다. 옵션은 벨소리와 한 번 울림입니다. 디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
발신자 ID	전화 번호, 이름 또는 기타 설명과 같은 발신자 ID가 전화기 화면에 표시됩니다. 라우팅 계획, 통화 표시 제한 및 디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
발신자 ID 차단	발신자 ID가 활성화되어 있는 전화기의 전자 메일 주소나 전화 번호를 차단할 수 있습니다. 라우팅 계획 및 디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
발신자 정규화	발신자 정규화는 사용자에게 전화를 걸 수 있는 전화 번호가 있는 전화 통화를 알려줍니다. 번호에 이스케이프 코드가 추가되어 사용자가 쉽게 발신자에게 다시 연락할 수 있습니다. 전화를 걸 수 있는 번호는 통화 기록에 저장되며, 개인 주소록에도 저장할 수 있습니다.
SIP용 캐스트	CUVA(Cisco 유니파이드 Video Advantage)와 Cisco IP 전화기 간의 통신을 수립하여 IP 전화기에 비디오 기능이 없는 경우에도 PC를 통해 비디오를 지원할 수 있습니다.
회의끼기	공유 전화 회선에서 개인 통화가 아닌 통화에 참여할 수 있습니다. 회의끼기 기능을 사용하면 사용자를 통화에 추가하고 이를 전화회의로 전환하여, 사용자와 다른 통화자가 전화회의 기능에 액세스할 수 있게 합니다. 전화회의는 Cisco Unified Communications Manager 전화회의 브리지 기능을 사용하여 생성됩니다. 회의끼기가 올바르게 작동하려면 소프트키와 컨퍼런스 브리지 기능을 모두 활성화해야 합니다. 펌웨어 릴리스 10.2(2) 이후에서는 참여 소프트키를 사용하여 회의끼기 기능에 액세스합니다. 자세한 내용은 <a href="#">Cisco Unified Communications Manager 기능 구성 설명서</a> 의 "참여" 장을 참조하십시오.
모바일 장치 충전	사용자는 모바일 장치를 Cisco IP 전화기의 USB 포트에 연결하여 장치를 충전할 수 있습니다. <i>Cisco IP</i> 전화기 8800 시리즈 사용 설명서를 참조하십시오.

기능	설명 및 세부 정보
Cisco Extension Mobility	공유 Cisco IP 전화기에서 사용자가 회선 모양, 서비스 및 단축 다이얼 같은 Cisco IP 전화기 구성에 액세스할 수 있습니다.  Cisco Extension Mobility는 사용자가 사내 여러 장소에서 근무하거나 동료와 작업 공간을 공유할 때 유용합니다.
Cisco 확장 모빌리티 크로스 클러스터 (EMCC)	한 클러스터에 구성된 사용자가 다른 클러스터의 Cisco IP 전화기에 로그인할 수 있습니다. 홈 클러스터의 사용자가 방문 중인 클러스터의 Cisco IP 전화기에 로그인할 수 있습니다.  참고 EMCC를 구성하기 전에 먼저 Cisco IP 전화기에 Cisco Extension Mobility를 구성하십시오.
Cisco IP Manager Assistant(IPMA)	관리자와 보조자가 통화를 보다 효율적으로 처리할 수 있도록 도와주는 통화 라우팅 기능 및 기타 통화 관리 기능을 제공합니다.  <a href="#">Cisco IP Manager Assistant 설정, 193 페이지</a> 를 참조하십시오.
Cisco IP Phone 8800 Key Expansion Module Cisco IP Phone 8851/8861 Key Expansion Module Cisco IP Phone 8865 Key Expansion Module	확장 모듈을 전화기에 추가하여 추가 키를 제공합니다.  추가 정보는 <i>Cisco IP</i> 전화기 7800 및 8800 시리즈의 <i>Cisco Unified Communications Manager</i> 용 액세서리 설명서를 참조하십시오.
Cisco IP Phone 8811 지원	Cisco IP Phone 8811에 대한 지원을 제공합니다.
Cisco IP 전화기 8851NR 지원	Cisco IP 전화기 8851NR에 대한 지원을 제공합니다.
Cisco Unified Communications Manager Express(Unified CME) 버전 협상	Cisco 유니파이드 CME(Unified Communications Manager Express)는 전화기에 전송되는 정보에 특별 태그를 사용합니다. 이 태그를 사용하면 전화기에서 스위치가 지원되는 사용자에게 서비스를 제공할 수 있습니다.  참조: <ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified Communications Manager Express</a> 시스템 관리자 설명서</li> <li>• <a href="#">Cisco Unified Communications Manager Express 상호 작용, 23 페이지</a></li> </ul>
CUVA(Cisco 유니파이드 Video Advantage)	Cisco IP 전화기, 개인 컴퓨터 및 외부 비디오 카메라를 사용해 영상 통화를 할 수 있습니다.  참고 [전화기 구성]의 [제품별 구성 레이아웃] 섹션에서 비디오 기능 매개 변수를 구성합니다.  Cisco 유니파이드 Video Advantage 문서를 참조하십시오.
Cisco WebDialer	사용자가 웹 및 데스크톱 애플리케이션에서 전화를 걸 수 있습니다.

기능	설명 및 세부 정보
클래식 벨소리	<p>전화기 펌웨어에 내장되거나 Cisco Unified Communications Manager에서 다운로드된 벨소리를 지원합니다. 이 기능은 사용 가능한 벨소리를 다른 Cisco IP 전화기에서도 사용할 수 있게 합니다.</p> <p><a href="#">사용자 지정 전화기 벨소리, 117 페이지</a>를 참조하십시오.</p>
전화회의	<p>각 참가자에게 개별적으로 전화하여 여러 명과 동시에 대화할 수 있습니다. 전화회의 기능에는 전화회의 및 회의개설 기능이 있습니다.</p> <p>표준 (임시) 전화회의에서 게시자가 아닌 사람이 참가자를 추가 또는 삭제할 수 있고, 모든 전화회의 참가자가 동일 회선으로 2개의 표준 전화회의에 참여할 수 있습니다.</p> <p>이 기능은 고급 임시 전화회의 서비스 매개 변수(Cisco Unified Communications Manager Administration에서는 기본값으로 비활성화됨)를 통해 활성화할 수 있습니다.</p> <p>참고            그리고 사용자에게는 기능 활성화 여부를 알려야 합니다.</p>
PC 및 스위치 포트를 위한 구성 가능 EEE(Energy Efficient Ethernet)	<p>EEE를 활성화 또는 비활성화하여 개인 컴퓨터 포트 및 스위치 포트의 EEE 기능을 제어할 수 있는 방식을 제공합니다. 이 기능은 두 유형의 포트 모두를 개별적으로 관리합니다. 기본값은 활성화 상태입니다.</p> <p><a href="#">스위치 및 PC 포트를 위한 EEE(Energy Efficient Ethernet) 설정, 179 페이지</a>를 참조하십시오.</p>
구성 가능한 글꼴 크기	<p>사용자는 글꼴 크기를 변경하여 IP 전화기가 통화 기록 및 통화 화면에 대해 표시하는 최대 문자 수를 늘이거나 줄일 수 있습니다.</p> <p>글꼴을 줄이면 표시되는 최대 문자 수가 늘어나고, 글꼴을 크게 하면 표시되는 최대 문자 수가 줄어듭니다.</p>
CTI 애플리케이션	<p>CTI(Computer Telephony Integration) 경로 포인트는 애플리케이션에 의해 제어되는 재전송을 위해 여러 동시 통화를 받을 수 있는 가상 장치를 지정할 수 있습니다.</p>
모두 거부	<p>사용자가 벨소리가 울리고 있는 전화, 연결된 전화 또는 보류 중인 전화를 직접 음성 메시징 시스템으로 호전환할 수 있습니다. 통화가 거부되면 해당 회선에서 새 통화를 걸거나 받을 수 있습니다.</p> <p>지정전환에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>

기능	설명 및 세부 정보
장치 호출 녹음	<p>최종 사용자에게 소프트키를 통해 전화 통화를 녹음할 수 있는 기능을 제공합니다.</p> <p>그리고 관리자는 CTI 사용자 인터페이스를 통해 전화 통화를 계속 녹음할 수도 있습니다.</p> <p>모니터링 및 녹음에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
직접 통화 지정보류	<p>전화를 걸거나 단축 다이얼을 통해 직접 통화 지정보류 번호로 활성 통화를 호전환할 수 있습니다. [통화 지정보류 BLF] 버튼은 직접 통화 지정보류 번호가 사용 중인지, 그리고 직접 통화 지정보류 번호에 단축 다이얼 액세스를 제공하고 있는지를 표시합니다.</p> <p>참고        직접 통화 지정보류를 실행하는 경우 [지정보류] 소프트키를 구성하지 마십시오. 이렇게 하면 사용자들이 2개의 통화 지정보류 기능을 혼동하지 않게 됩니다.</p> <p>통화 지정보류에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
배터리 세기 및 신호 세기 아이콘 표시	<p>모바일 전화기가 블루투스를 사용하여 IP 전화기에 연결될 때 IP 전화기에 모바일 전화기의 배터리 및 신호 세기를 표시합니다.</p> <p>Cisco IP 전화기 8851NR은 블루투스를 지원하지 않습니다.</p>
벨소리 구분	<p>사용자는 전화기에서 착신 통화 및 새 음성 메일 메시지를 표시하는 방법을 사용자 정의할 수 있습니다.</p> <p>통화 당겨받기에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
방해사절(DND)	<p>방해사절을 설정하면, 전화벨이 울리는 동안 벨소리가 나지 않거나 어떤 종류의 시각적 또는 청각적 알람도 일어나지 않습니다.</p> <p>활성화되면 전화기 헤더가 빨간색으로 변하고 전화기에 방해 사절이 표시됩니다.</p> <p>MLPP(multilevel precedence and preemption)가 구성되고 사용자가 우선 순위 통화를 수신하는 경우 전화기에서 특수 벨소리가 울립니다.</p> <p><a href="#">방해사절 설정, 175 페이지</a>를 참조하십시오.</p>
JAL/TAL 활성화/비활성화	<p>관리자는 JAL(Join Across Lines) 및 직접 TAL(Transfer Across Lines) 기능을 제어할 수 있습니다.</p> <p><a href="#">참여 및 호연결 정책 설정을 참조하십시오</a> <a href="#">제품별 구성, 146 페이지</a>.</p>
EnergyWise	<p>IP 전화기를 미리 정한 시간 동안 대기(절전) 및 활성화(작동)로 설정하면 에너지를 절약할 수 있습니다.</p> <p><a href="#">Cisco IP 전화기에서 EnergyWise 예약, 172 페이지</a>를 참조하십시오.</p>

기능	설명 및 세부 정보
고급 회선 모드	고급 회선 모드를 활성화하여 전화기 화면의 양면에 있는 버튼을 회선 키로 사용할 수 있습니다. 를 참조하십시오. <a href="#">추가 회선 키 설정, 205 페이지</a>
보안 EMCC(Extension Mobility Cross Cluster) 개선	로그인 전화기에 네트워크 및 보안 구성을 저장하여 보안 EMCC(Extension Mobility Cross Cluster) 기능을 향상합니다. 이렇게 하면 보안 정책이 유지되고, 네트워크 대역폭이 보존되며, VC(방문 중인 클러스터)에서 네트워크 문제를 예방할 수 있습니다.
고속 다이얼 서비스	고속 다이얼 코드를 입력해 전화를 걸 수 있습니다. 고속 다이얼 코드는 전화 번호나 개인 주소록 항목에 할당할 수 있습니다. 이 표의 “서비스”를 참조하십시오. <a href="#">PAB 또는 고속 다이얼에 대한 전화기 버튼 템플릿 수정, 203 페이지</a> 를 참조하십시오.
그룹 통화 당겨받기	다른 그룹의 디렉터리 번호에서 울리는 전화를 받을 수 있습니다. 통화 당겨받기에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
헤드셋 측음 조정	관리자가 유선 헤드셋의 측음 수준을 설정할 수 있습니다.
보류 복귀	통화를 보류한 전화기로 통화를 되돌리고 사용자에게 이를 알리기 전에 통화 보류 상태를 유지할 시간을 제한합니다. 되돌리기 통화는 단일 벨소리(또는 경고음, 회선의 새 통화 표시기 설정에 따라 달라짐)로 착신 통화와 구분됩니다. 이 알림은 제시작하지 않는 한 일정 시간을 두고 반복됩니다. 보류 복귀를 설정한 통화에는 움직이는 아이콘이 표시됩니다. 착신 통화나 되돌리기 통화에 대해 통화 포커스 우선 순위를 설정할 수 있습니다.
보류 상태	공유 회선이 있는 전화기를 통화 보류 상태의 로컬 및 원격 회선과 구분할 수 있습니다.
보류/보류해제	연결된 통화를 활성 상태에서 보류 상태로 전환할 수 있습니다. <ul style="list-style-type: none"> <li>음악 대기를 사용하지 않는 한 별도의 구성이 필요하지 않습니다. 자세한 내용은 이 표의 “음악 대기”를 참조하십시오.</li> <li>이 표의 “보류 복귀”를 참조하십시오.</li> </ul>
HTTP 다운로드	전화기에 대한 파일 다운로드 프로세스를 개선하여 디폴트로 HTTP를 사용할 수 있게 합니다. HTTP 다운로드에 실패하면, 전화기는 TFTP 다운로드 사용으로 전환됩니다.

기능	설명 및 세부 정보
헌트 그룹	<p>기본 디렉터리 번호로 걸려온 통화에 로드 공유 기능을 제공합니다. 헌트 그룹에는 수신 전화를 받을 수 있는 일련의 디렉터리 번호가 포함됩니다. 헌트 그룹의 첫 번째 디렉터리 번호가 통화 중인 경우 시스템은 사전 구성된 순서대로 해당 그룹에서 사용 가능한 다음 디렉터리 번호를 찾아 통화를 해당 전화기로 전송합니다.</p> <p>헌트 그룹 호출에 대한 수신 통화 알림에 발신자 <b>ID</b>(발신자 ID가 구성된 경우), 디렉터리 번호 및 헌트 그룹 파일럿 번호를 표시할 수 있습니다. 헌트 그룹 번호는 레이블 "헌트 그룹" 다음에 표시됩니다.</p> <p>헌트 그룹 및 라우팅 계획에 관한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
착신 통화 알림 타이머	<p>전화기 화면에 착신 통화 알림이 표시되는 시간 길이를 설정할 수 있습니다.</p> <p>착신 통화 알림 타이머를 참조하십시오 <a href="#">제품별 구성, 146 페이지</a>.</p>
Intelligent Proximity	<p>사용자가 블루투스를 사용하여 모바일 장치를 전화기와 페어링하고 전화를 사용하여 모바일 통화를 걸고 받을 수 있습니다.</p> <p><a href="#">Intelligent Proximity 활성화, 209 페이지</a>를 참조하십시오.</p> <p>Cisco IP 전화기 8811, 8841 및 8851NR은 블루투스 또는 Intelligent Proximity를 지원하지 않습니다.</p>
인터콤	<p>프로그램 가능 전화기 버튼을 사용해 인터콤 전화를 걸고 받을 수 있습니다. 인터콤 회선 버튼은 다음과 같이 구성할 수 있습니다.</p> <ul style="list-style-type: none"> <li>특정 인터콤 내선 번호로 직접 전화를 겁니다.</li> <li>인터콤 통화를 시작한 다음, 사용자에게 유효한 인터콤 번호를 입력하라는 메시지가 표시됩니다.</li> </ul> <p>참고 사용자 Cisco Extension Mobility 프로파일을 사용하여 매일 정기적으로 같은 전화기에 로그인하는 경우에는, 인터콤 정보가 들어 있는 전화기 버튼 템플릿을 사용자의 프로파일에 할당하고 해당 전화기를 인터콤 회선의 기본 인터콤 장치로 지정합니다.</p>
IPv6-전용 지원	<p>Cisco IP 전화기의 확장된 IP 주소 지정에 대한 지원을 제공합니다. IPv4 및 IPv6 구성이 권장되고 완전히 지원됩니다. 어떤 기능은 독립형 구성에서 지원되지 않습니다. IPv6 주소만 할당됩니다.</p> <p><a href="#">네트워크 설정 구성, 58 페이지</a>를 참조하십시오.</p>
지터 버퍼	<p>지터 버퍼 기능은 오디오 스트림에 대해 10~1000ms(밀리초)의 지터를 처리합니다.</p> <p>적응형 모드에서 실행되고 동적으로 지터의 크기를 조정합니다.</p>
통화참가	<p>한 회선에서 전화 회의를 시작하고 해당 통화에 남아 있는 2개의 통화를 결합할 수 있습니다.</p>



기능	설명 및 세부 정보
통화 목록 회선 상태	<p>통화 기록 목록에서 모니터링되고 있는 회선 번호의 회선 상태 가용 현황을 확인할 수 있습니다. 회선 상태의 상태는 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>• 오프라인</li> <li>• 대화 가능</li> <li>• 사용 중</li> <li>• 방해사절</li> </ul> <p>통화 목록에 대한 BLF 활성화, 178 페이지를 참조하십시오.</p>
회사 디렉터리의 회선 상태	<p>회사 디렉터리의 연락처 상태 표시를 활성화합니다.</p> <ul style="list-style-type: none"> <li>• 오프라인</li> <li>• 대화 가능</li> <li>• 사용 중</li> <li>• 방해사절</li> </ul> <p>통화 목록에 대한 BLF 활성화, 178 페이지를 참조하십시오.</p>
회선 텍스트 레이블	<p>디렉터리 번호 대신 전화기 회선에 텍스트 레이블을 설정합니다.</p> <p>회선에 대한 레이블 설정, 188 페이지를 참조하십시오.</p>
헌트 그룹 로그아웃	<p>헌트 그룹에서 로그아웃하고, 전화를 받을 수 있는 상태가 아닐 때 전화기로 걸려오는 통화를 일시적으로 차단할 수 있습니다. 헌트 그룹에서 로그아웃해도 헌트 그룹이 아닌 통화로 인해 전화 벨소리가 울릴 수 있습니다.</p> <p>라우팅 계획에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
MCID(장난 전화 발신자 ID)	<p>시스템 관리자에게 걸려온 수상한 전화에 대해 알릴 수 있습니다.</p>
회의개설 전화회의	<p>다른 참가자가 예정된 시간에 미리 지정한 번호로 전화를 거는 회의개설 전화회의를 호스팅할 수 있습니다.</p>
메시지 대기 중	<p>메시지 대기 중 on/off 표시기에 디렉터리 번호를 지정합니다. 직접 연결된 음성 메시지 시스템은 지정된 디렉터리 번호를 사용해 특정 Cisco IP 전화기의 메시지 대기 중 표시를 설정 또는 설정 해제합니다.</p> <p>메시지 대기 중 및 음성 메일에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
메시지 대기 중 표시기	<p>핸드셋의 불빛은 사용자에게 1개 이상의 새 음성 메시지가 있다는 뜻입니다.</p> <p>메시지 대기 중 및 음성 메일에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>

기능	설명 및 세부 정보
최소 벨소리 볼륨	IP 전화기의 최소 벨소리 볼륨 수준을 정합니다.
부재 중 전화 기록	해당 회선 형태(LA)를 위해 부재 중 전화를 부재 중 전화 디렉터리에 기록할지 여부를 지정할 수 있습니다.  디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
모바일 연결	단일 전화 번호를 사용하여 비즈니스 통화를 관리하고, 사무실 전화기 및 휴대폰 같은 원격 장치에서 진행 중인 통화를 당겨받을 수 있습니다. 사용자는 전화 번호 및 시간에 따라 발신자 그룹을 제한할 수 있습니다.  Cisco 유니파이드 Mobility에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
Expressway를 통한 모바일 및 Remote Access	원격 근로자가 VPN(가상 사설망) 클라이언트 터널을 사용하지 않고도 회사 네트워크에 쉽고 안전하게 연결할 수 있습니다.  를 참조하십시오. <a href="#">Expressway를 통한 모바일 및 Remote Access, 181 페이지</a>
모바일 음성 액세스	사용자가 휴대폰 같은 원격 장치에서 통화를 시작할 수 있게 IVR(대화형 음성 응답) 시스템에 액세스할 수 있게 함으로써 모바일 연결 기능을 확장합니다.  Cisco 유니파이드 Mobility에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
모니터링 및 녹음	감독자가 활성 통화를 조용히 모니터링할 수 있습니다. 양쪽 통화자는 감독자의 소리를 들을 수 없습니다. 사용자는 통화가 모니터링되는 경우 통화 중에 모니터링 알림음을 들을 수도 있습니다.  통화에 대한 보안이 이루어지는 경우 통화의 보안 상태가 Cisco IP 전화기에 잠금 아이콘 형태로 표시됩니다. 통화가 연결된 당사자는 통화에 대한 보안이 이루어지고 통화 내용이 모니터링되고 있음을 알리는 알림음을 듣게 될 수도 있습니다.  참고      활성 통화를 모니터링하거나 녹음할 때, 사용자가 인터콤 전화를 받거나 걸 수 있습니다. 그런데 이처럼 사용자가 인터콤 전화를 걸면, 활성 통화가 보류 상태가 되어 녹음 세션이 종료되거나 모니터링 세션이 중단됩니다. 모니터링 세션을 다시 시작하려면 모니터링되던 전화를 건 사람이 통화를 재시작해야 합니다.
MLPP(Multilevel Precedence and Preemption)	군사 기지나 정부 기관 같은 일부 특수 환경에서 긴급 전화나 중요 전화를 걸고 받을 수 있습니다.  <a href="#">MLPP(Multilevel Precedence and Preemption), 198 페이지</a> 를 참조하십시오.

기능	설명 및 세부 정보
회선별 복수 통화 표시	<p>각 회선은 여러 건의 통화를 지원합니다. 기본적으로 전화기는 회선당 두 개의 활성 통화를 지원하고, 회선당 최대 6개의 활성 통화를 지원합니다. 한 번에 하나의 통화만 연결할 수 있으며 다른 통화는 모두 자동으로 보류됩니다.</p> <p>시스템을 사용하여 최대 6/6 이하의 통화/사용 중 트리거를 구성할 수 있습니다. 6/6을 초과하는 구성은 공식적으로 지원되지 않습니다.</p> <p>디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
음악 대기	발신자가 대기 중인 동안 음악을 재생합니다.
음소거	핸드셋 또는 헤드셋 마이크의 음을 소거합니다.
알림 이름 없음	원래 발신자의 전화 번호를 표시하여 최종 사용자가 호전환된 통화를 쉽게 식별할 수 있습니다. 통화는 발신자의 전화 번호 뒤에 알림 통화로 표시됩니다.
온 훅 전화 걸기	오프 훅 상태로 전환하지 않고 전화를 걸 수 있습니다. 이 상태에서는 사용자가 그냥 핸드셋을 들거나 [다이얼]을 누르면 됩니다.
기타 그룹 당겨받기	<p>사용자 그룹과 연결된 다른 그룹의 전화기에서 올리는 전화를 받을 수 있습니다.</p> <p>통화 당겨받기에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
내선 이동 사용자를 위한 전화기 표시 메시지	이 기능은 친숙한 메시지를 제공하여 내선 이동 사용자를 위한 전화기 인터페이스를 개선합니다.
Cisco Unified Communications Manager에서 전화기 신뢰 목록 알림	<p>신뢰 목록(TL)이 업데이트될 때 전화기에서 Cisco Unified Communications Manager로 알림을 보낼 수 있습니다.</p> <p><a href="#">지원 보안 기능, 88 페이지</a>를 참조하십시오.</p>
PLK 대기열 지원 통계	PLK 대기열 지원 통계 기능을 통해 사용자는 힌트 파일럿에 대한 통화 대기열 통계를 쿼리할 수 있고, 정보는 전화기 화면에 표시됩니다.
플러스(+ ) 다이얼	<p>앞에 플러스(+ ) 표시가 있는 E.164 번호로 전화를 걸 수 있습니다.</p> <p>+ 표시 번호로 전화를 걸려면, 별표(*) 키를 최소 1초 정도 누릅니다. 이는 온 훅(편집 모드 포함) 또는 오프 훅 통화를 위해 첫 번째 숫자를 누를 때 적용됩니다.</p>
LLDP에 대한 전원공급 협상	<p>전화기에서 LLDP(Link Level Endpoint Discovery Protocol)와 CDP (Cisco 탐색 프로토콜)를 사용해 전원을 설정할 수 있습니다.</p> <p>전원 협상을 참조하십시오 <a href="#">제품별 구성, 146 페이지</a>.</p>

기능	설명 및 세부 정보
예측 다이얼링	<p>전화 걸기를 간소화합니다. 최근 통화 목록이 다이얼 중인 번호와 유사한 전화 번호만 표시하도록 변경됩니다.</p> <p>고급 회선 모드가 활성화되면 예측 전화 걸기가 활성화됩니다. 예측 전화 걸기 기능을 사용하려면 간소화된 새 통화 UI를 비활성화해야 합니다.</p>
프라이버시	<p>회선을 공유하는 사용자가 통화에 자신을 추가하지 않고 전화기 화면에서 다른 사용자의 통화에 관한 정보를 확인하지 못하게 합니다.</p> <p>참여 및 프라이버시에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
PLAR(Private Line Automated Ringdown)	<p>Cisco Unified Communications Manager 관리자는 핸드셋이 오프 후 상태가 되자마자 Cisco IP 전화기에서 전화를 거는 전화 번호를 구성할 수 있습니다. 비상 전화나 “핫라인” 번호로 전화를 걸도록 지정된 전화기에 유용합니다.</p> <p>관리자는 최대 15초의 지연 시간을 구성할 수 있습니다. 이렇게 하면 전화기가 핫라인 번호로 기본 설정되기 전에 사용자가 전화를 걸 수 있습니다. 타이머는 디바이스 &gt; 디바이스 설정 &gt; SIP 프로파일의 오프 후에서 첫 번째 자릿수 타이머 간격 매개 변수를 통해 구성할 수 있습니다.</p> <p>자세한 내용은 <i>Cisco Unified Communications Manager</i> 기능 구성 설명서를 참조하십시오.</p>
PRT(Problem Report Tool)	<p>관리자에게 전화기 로그를 제출하거나 문제를 보고합니다.</p> <p><a href="#">문제 보고서 도구, 186 페이지</a>를 참조하십시오.</p>
프로그램 가능 기능 버튼	<p>회선 버튼에 전화걸기, 콜백 및 착신 전환 같은 기능을 지정할 수 있습니다.</p> <p>전화기 버튼 템플릿에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
QRT(품질 보고 도구)	<p>버튼을 누르면 문제가 있는 전화기 통화에 관한 정보를 제출할 수 있습니다. QRT는 QRT와의 사용자 상호 작용이 어느 정도 필요한지에 따라 2개의 사용자 모드 중 하나에 구성할 수 있습니다.</p>
최근 통화	<p>사용자는 최근 150통의 개별 통화 및 통화 그룹을 볼 수 있습니다. 최근에 건 번호와 부재 중 통화를 보고 통화 기록을 삭제할 수 있습니다.</p>
재다이얼	<p>버튼을 하나 누르거나 [재다이얼] 소프트키를 눌러 가장 최근에 건 전화 번호로 전화를 걸 수 있습니다.</p>

기능	설명 및 세부 정보
원격 포트 구성	<p>Cisco Unified Communications Manager Administration을 사용해 전화기 이더넷 포트의 전이중/반이중 기능과 속도를 원격에서 구성할 수 있습니다. 이는 구체적인 포트 설정을 사용한 대규모 구축 작업의 성과를 향상합니다.</p> <p>참고 Cisco Unified Communications Manager에서 원격 포트 구성을 위해 포트를 구성하면, 전화기에서 데이터를 변경할 수 없습니다.</p> <p>원격 포트 구성을 참조하십시오 <a href="#">제품별 구성, 146 페이지</a>.</p>
원격 대상에 직접 걸려온 통화를 회사 번호로 재라우팅	<p>사용자의 휴대폰으로 직접 걸려온 통화를 회사 번호(사무실 전화기)로 재라우팅합니다. 원격 대상(휴대폰)으로 전화가 걸려오면 사무실 전화기는 울리지 않으며, 원격 대상에서만 벨소리가 울립니다. 휴대폰에서 수신 전화에 응답하면 사무실 전화기에는 원격 사용 중 메시지가 표시됩니다. 이러한 통화 중에는 휴대폰의 다양한 기능도 사용할 수 있습니다.</p> <p>Cisco 유니파이드 Mobility에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
'통화 종료' 안내 타이머 제거	<p>전화기 화면에서 통화 종료 메시지 표시를 제거하여 통화 종료 응답 시간을 개선합니다.</p>
벨소리 설정	<p>전화에 다른 활성 통화가 있는 경우, 회선에 사용되는 벨소리 유형을 구분합니다. 디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서와 <a href="#">사용자 지정 전화기 벨소리, 117 페이지</a>를 참조하십시오.</p>
SIP를 위한 RTCP 보류	<p>보류 중인 통화를 게이트웨이에서 끊기지 않게 합니다. 게이트웨이는 RTCP 포트의 상태를 확인하여 통화가 활성 상태인지 아닌지를 판단합니다. 전화기 포트를 열어 두면, 게이트웨이에서 보류 중인 통화를 종료하지 않습니다.</p>
보안 전화회의	<p>보안이 이루어진 전화기에서 보안 컨퍼런스 브리지를 사용해 전화회의를 위한 통화를 걸 수 있습니다. [전화회의], [통화참가], [참여] 소프트키나 회의개설 전화회의를 사용해 새로운 참가자가 추가되면, 모든 참가자가 보안 전화기를 사용하는 동안 보안 통화 아이콘이 표시됩니다.</p> <p>전화회의 목록에 각 전화회의 참가자의 보안 수준이 표시됩니다. 게시자는 전화회의 목록에서 보안이 이루어지지 않는 참가자를 삭제할 수 있습니다. 게시자가 아닌 참가자도 고급 임시 전화회의 설정 매개변수가 설정되어 있으면 전화회의 참가자를 추가 또는 삭제할 수 있습니다.</p> <p>전화회의 브리지 및 보안에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서와 <a href="#">지원 보안 기능, 88 페이지</a>를 참조하십시오.</p>
보안 EMCC	<p>원격 사무실에서 자신의 전화기에 로그인하는 사용자에게 강화된 보안을 제공함으로써 EMCC 기능을 개선합니다.</p>

기능	설명 및 세부 정보
서비스	<p>Cisco Unified Communications Manager Administration에서 Cisco IP 전화기 서비스 구성 메뉴를 사용해 사용자가 가입할 수 있는 전화기 서비스 목록을 정의하고 유지할 수 있습니다.</p> <p>서비스에 대한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
서비스 URL 버튼	<p>전화기의 서비스 메뉴를 사용하지 않고 프로그램 가능 버튼에서 서비스에 액세스할 수 있습니다.</p> <p>서비스에 대한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
발신 ID 및 발신 번호 표시	<p>전화기에서 수신 전화의 발신 ID 및 발신 번호 모두를 표시할 수 있습니다. IP 전화기 LCD 화면 크기에 따라 표시되는 발신 ID 및 발신 번호의 길이가 제한됩니다.</p> <p>발신 ID 및 발신 번호 표시 기능은 수신 전화 알림에만 적용되며, 착신 전환 및 헛트 그룹 기능을 변경하지 않습니다.</p> <p>이 표의 “발신자 ID”를 참조하십시오.</p>
Cisco 헤드셋으로 Extension Mobility 로그인 간소화	<p>사용자가 Cisco 헤드셋을 사용하여 Extension Mobility에 로그인할 수 있습니다.</p> <p>전화기가 MRA 모드에 있는 경우 사용자는 헤드셋을 사용하여 전화기에 로그인할 수 있습니다.</p> <p>이 기능을 사용하려면 Cisco Unified Communications Manager(UCM) 릴리스 11.5(1)SU8, 11.5(1)SU.9, 12.5(1)SU3 이상이 필요합니다.</p> <p>자세한 내용은 <i>Cisco Unified Communications Manager</i> 기능 구성 설명서, 릴리스 11.5(1)SU8 이상 또는 릴리스 12.5(1)SU3 이상을 참조하십시오.</p>
단순 태블릿 지원	<p>Android 또는 iOS 태블릿 사용자는 블루투스를 사용하여 태블릿을 전화기에 페어링한 다음 태블릿에서 음성 통화를 하는 데 전화기를 사용할 수 있습니다.</p> <p><a href="#">Intelligent Proximity 활성화, 209 페이지</a>를 참조하십시오.</p> <p>Cisco IP 전화기 8851NR은 블루투스를 지원하지 않습니다.</p>
단축 다이얼	이전에 저장한 특정 번호로 전화를 겁니다.
SSH 액세스	<p>Cisco Unified Communications Manager 관리를 사용하여 SSH 액세스 설정을 활성화하거나 비활성화할 수 있습니다. SSH 서버를 활성화하면 전화기에서 SSH 연결을 수락합니다. 전화기의 SSH 서버 기능을 비활성화하면 전화기에 대한 SSH 액세스가 차단됩니다.</p> <p>SSH 액세스 권한을 참조하십시오. <a href="#">제품별 구성, 146 페이지</a>.</p>

기능	설명 및 세부 정보
시간 기준 라우팅	일정 기간까지 특정 텔레포니 기능에 대한 액세스를 제한합니다. 기간 및 시간 라우팅에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
표준 시간대 업데이트	Cisco IP 전화기의 표준 시간대 변경 기능을 업데이트합니다. 날짜 및 시간에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
호전환	연결된 통화를 자신의 전화기에서 다른 번호로 재전송할 수 있습니다.
호전환 - 직접 호전환	호전환: 첫 번째 호전환 시도는 활성 통화를 대기 중으로 설정한 뒤, 동일한 디렉터리 번호를 사용해 새로운 통화를 시작합니다. 사용자는 활성 통화 호전환 기능을 사용하여 직접 통화를 호전환할 수 있습니다. 일부 JTAPI/TAPI 애플리케이션은 Cisco IP 전화기에서 실행되는 통화참가 및 호연결 기능과 호환되지 않기 때문에, 동일 회선이나 간혹 여러 회선에 걸쳐 통화참가 및 호연결을 비활성화하도록 통화참가 및 호연결 정책을 구성해야 할 수도 있습니다. 디렉터리 번호에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
TVS	TVS(Trust Verification Services)를 사용하면 CTL(Certificate Trust List)의 규모를 확대하거나 전화기에 업데이트된 CTL 파일의 다운로드를 요구하지 않고도 전화기에서 서명 구성을 인증하거나 기타 서버 또는 피어를 인증할 수 있습니다. TVS는 디폴트로 활성화됩니다. TVS 정보는 전화기의 보안 설정 메뉴에 표시됩니다.
UCR 2013	Cisco IP 전화기는 다음과 같은 기능을 제공해 UCR(Unified Capabilities Requirements) 2013을 지원합니다. <ul style="list-style-type: none"> <li>• FIPS(Federal Information Processing Standard) 140-2 지원</li> <li>• 80비트 SRTP 태깅 지원</li> </ul> IP 전화기 관리자는 Cisco Unified Communications Manager Administration에 특정 매개 변수를 설정해야 합니다.
구성되지 않은 기본 회선 알림	기본 회선이 구성되지 않았을 때 사용자에게 알립니다. 전화기 화면에 제공 취소됨 메시지가 나타납니다.
목록, 알림 및 Visual Voicemail에 대한 사용자 인터페이스 업데이트.	애플리케이션 창 크기를 줄여 잘린 문자열을 최소화합니다.

기능	설명 및 세부 정보
비디오 모드	<p>사용자는 시스템에 구성된 모드에 따라, 화상 회의를 보기 위한 비디오 디스플레이 모드를 선택할 수 있습니다.</p> <p>비디오에 대한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p> <p>Cisco IP 전화기 8845, 8865 및 8865NR에서만 사용 가능합니다.</p>
비디오 지원	<p>전화기에서 비디오 지원을 활성화합니다. Cisco Unified Communications Manager 전화기 구성 창에서 영상 통화를 위해 비디오 기능 매개 변수를 활성화해야 합니다. 이 범주는 기본적으로 활성화되어 있습니다.</p> <p>Cisco IP 전화기 8845, 8865 및 8865NR에서만 사용 가능합니다.</p>
PC를 통한 비디오	<p>Cisco 유니파이드 IP 전화기, 개인 컴퓨터 및 외부 비디오 카메라를 사용해 영상 통화를 할 수 있습니다.</p> <p>또한 이 기능을 사용하여 사용자는 Cisco Jabber 또는 Cisco 유니파이드 Video Advantage 제품으로 영상 통화를 할 수 있습니다.</p>
Visual Voicemail	<p>음성 메일 오디오 안내를 그래픽 인터페이스로 대체합니다.</p> <p><a href="http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3">http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3</a>에 있는 <i>Visual Voicemail</i>용 설치 및 구성 안내서를 참조하십시오.</p>
음성 메시지 시스템	<p>전화를 받지 않는 경우 발신자가 메시지를 남길 수 있습니다.</p> <p>음성 메일에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서와 <a href="#">Visual VoiceMail 설정, 195 페이지</a>를 참조하십시오.</p>
VPN	<p>SSL을 사용하면 신뢰된 네트워크 밖에 있을 때 또는 전화기와 Unified Communications Manager 간 네트워크 트래픽이 신뢰되지 않는 네트워크를 지나야 할 때 Cisco 유니파이드 IP 전화기에서 가상 사설망(VPN) 연결을 제공합니다.</p>
기본값으로 비활성화되는 웹 액세스	<p>HTTP 같은 모든 웹 서비스에 대한 액세스를 비활성화하여 보안을 향상합니다. 웹 액세스를 활성화하면 사용자는 오직 웹 서비스에만 액세스할 수 있습니다.</p>

#### 관련 항목

[Cisco Unified Communications Manager 설명서, xvii 페이지](#)

## 기능 단추 및 소프트키

다음 표에서는 소프트키에서 사용할 수 있는 기능, 전용 기능 단추에서 사용할 수 있는 기능, 프로그램 가능 기능 단추로 구성해야 하는 기능에 대해 설명합니다. 표의 “지원됨” 항목은 해당 단추 유형이나 소프트키에 대해 기능이 지원된다는 뜻입니다. 2개의 버튼 유형 및 소프트키 중 프로그램 가능 기능 버튼만 Cisco IP 전화기 Administration에서 구성이 필요합니다.

프로그램 가능 기능 버튼에 관한 자세한 내용은 [전화기 버튼 템플릿, 201 페이지](#)를 참조하십시오.



표 30: 기능 및 해당 버튼 및 소프트키

기능 이름	전용 기능 버튼	프로그램 가능 기능 버튼	소프트키
경고 통화	지원되지 않음	지원됨	지원되지 않음
모든 통화	지원되지 않음	지원됨	지원되지 않음
전화받기	지원되지 않음	지원됨	지원됨
회의끼기	지원되지 않음	지원되지 않음	지원됨
콜백	지원되지 않음	지원됨	지원됨
모든 통화 착신 전환	지원되지 않음	지원되지 않음	지원됨
통화 지정보류	지원되지 않음	지원됨	지원됨
통화 지정보류 회선 상태	지원되지 않음	지원됨	지원되지 않음
통화 당겨받기(당겨받기)	지원되지 않음	지원됨	지원됨
통화 당겨받기 회선 상태	지원되지 않음	지원됨	지원되지 않음
전화회의	지원됨	지원되지 않음	지원됨
전환	지원되지 않음	지원되지 않음	지원됨
DND(Do Not Disturb)	지원되지 않음	지원됨	지원됨
그룹 당겨받기(그룹 당겨받기)	지원되지 않음	지원됨	지원됨
보류	지원됨	지원되지 않음	지원됨
헌트 그룹	지원되지 않음	지원됨	지원되지 않음
인터콤	지원되지 않음	지원됨	지원되지 않음
MCID(장난 전화 ID)	지원되지 않음	지원됨	지원됨
회의개설	지원되지 않음	지원됨	지원됨
병합	지원되지 않음	지원되지 않음	지원됨
모바일 연결(이동성)	지원되지 않음	지원됨	지원됨
음소거	지원됨	지원되지 않음	지원되지 않음

기능 이름	전용 기능 버튼	프로그램 가능 기능 버튼	소프트키
기타 당겨받기	지원되지 않음	지원됨	지원됨
대기열 상태에 대한 PLK 지원	지원되지 않음	지원되지 않음	지원됨
프라이버시	지원되지 않음	지원됨	지원되지 않음
대기열 상태	지원되지 않음	지원됨	지원되지 않음
QRT(품질 보고 도구)	지원되지 않음	지원됨	지원됨
레코드	지원되지 않음	지원되지 않음	지원됨
재다이얼	지원되지 않음	지원됨	지원됨
바로 호출	지원되지 않음	지원됨	지원되지 않음
단축 다이얼 회선 상태	지원되지 않음	지원됨	지원되지 않음
USB 헤드셋의 보류 버튼 지원	지원되지 않음	지원되지 않음	지원됨
호전환	지원됨	지원되지 않음	지원됨

## 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 창의 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 사용자에게 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 사용자에게 대해 페이지 액세스를 활성화할 수 있습니다.

## 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.

## 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.

## 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.

## 제품별 구성

다음 표에서는 [제품별 구성 레이아웃] 창의 필드를 설명합니다.

표 31: 제품별 구성 필드

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
스피커폰 비활성화	확인란	선택 취소됨	전화기의 스피커폰 기능이 해제됩니다.
스피커폰 및 헤드셋 비활성화	확인란	선택 취소됨	전화기의 스피커폰 및 헤드셋 기능이 해제됩니다.
핸드셋 비활성화	확인란	선택 취소됨	전화기의 핸드셋 기능이 해제됩니다.
PC 포트	활성화됨 비활성화됨	활성화됨	PC 포트를 사용하여 컴퓨터의 LAN에 연결하는 기능을 제어합니다.
액세스 설정	비활성화됨 활성화됨 제한됨	활성화됨	설정 앱에서 전화기 구성 설정에 대한 액세스를 활성화, 비활성화 또는 제한합니다. <ul style="list-style-type: none"> <li>비활성화됨 — [설정] 메뉴에 옵션이 표시되지 않습니다.</li> <li>활성화 - [설정] 메뉴의 모든 항목에 액세스할 수 있습니다.</li> <li>제한됨 - 전화기 설정 메뉴에만 액세스할 수 있습니다.</li> </ul>

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
PC 음성 VLAN 액세스	활성화됨 비활성화됨	활성화됨	<p>전화기가 음성 VLAN에 액세스할 수 있도록 PC 포트에 장치를 연결할 수 있게 허용하는지 여부를 보여줍니다.</p> <ul style="list-style-type: none"> <li>• 비활성화됨 —PC가 음성 VLAN 또는 전화기에서 데이터를 송수신할 수 없습니다.</li> <li>• 활성화됨 —PC가 음성 VLAN 또는 전화기에서 데이터를 송수신할 수 있습니다. 애플리케이션이 PC에서 실행되어 전화기 트래픽을 모니터링하는 경우 경우 이 필드를 활성화됨으로 설정합니다. 이러한 애플리케이션은 모니터링과 녹음 애플리케이션을 포함할 수 있으며 네트워크 모니터링 소프트웨어의 용도는 분석 목적입니다.</li> </ul>
비디오 기능	활성화됨 비활성화됨	8845, 8865 및 8865NR: 활성화됨 8811, 8851, 8851NR, 8861: 비 활성화됨	Cisco IP 전화기, 개인 컴퓨터 및 외부 비디오 카메라를 사용해 영상 통화를 할 수 있습니다.
웹 액세스	비활성화됨 활성화됨	비활성화됨	<p>웹 브라우저를 통해 전화기 웹 페이지에 대한 액세스를 활성화 또는 비활성화합니다.</p> <p>주의 이 필드를 활성화하면 전화기에 대한 중요한 정보가 노출될 수 있습니다.</p>
웹 액세스에 대해 TLS 1.0 및 TLS 1.1 비활성화	비활성화됨 활성화됨	비활성화됨	<p>웹 서버 연결에 대해 TLS 1.2 사용을 제어합니다.</p> <ul style="list-style-type: none"> <li>• 비활성화됨—TLS1.0, TLS 1.1 또는 TLS1.2용으로 구성된 전화기는 HTTPS 서버로 작동할 수 있습니다.</li> <li>• 활성화됨—TLS1.2용으로 구성된 전화기만 HTTPS 서버로 작동할 수 있습니다.</li> </ul>

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
Enbloc 전화 걸기	비활성화됨 활성화됨	비활성화됨	전화걸기 방법을 제어합니다. <ul style="list-style-type: none"> <li>• 비활성화됨 - Cisco Unified Communications Manager는 다이얼 플랜 또는 경로 패턴이 중복될 때 interdigit 타이머가 만료될 때까지 대기합니다.</li> <li>• 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.</li> </ul> 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.
디스플레이 비활성화 지정일	요일		[디스플레이 켜기 시간] 필드에 지정된 시간에 디스플레이가 자동으로 켜지지 않는 날을 정의합니다.  드롭다운 목록 상자에서 날짜를 선택합니다. 1일 이상을 선택하려면 <b>Ctrl</b> 키를 누른 채 원하는 날짜를 클릭합니다.
디스플레이 켜기 시간	hh:mm		지정한 각 날짜에 디스플레이가 자동으로 켜지는 시간을 정의합니다([디스플레이를 활성화하지 않는 날짜] 필드에 지정한 날짜는 제외).  이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 00:00은 자정입니다.  예를 들어 오전 07:00시(0700)에 자동으로 디스플레이를 끄고 싶다면 07:00을 입력합니다. 오후 02:00시(1400)에 디스플레이를 켜고 싶다면 14:00을 입력합니다.  이 필드를 공백으로 두면 디스플레이가 자정(0:00)에 자동으로 켜집니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
디스플레이 켜기 지속 시간	hh:mm		<p>[디스플레이 켜기 시간] 필드에 지정된 시간에 디스플레이가 켜진 뒤 유지되는 시간을 정의합니다.</p> <p>예를 들어 자동으로 켜진 뒤 4시간 30분 동안 디스플레이를 켜 상태로 유지하고 싶다면, 04:30을 입력합니다.</p> <p>이 필드를 공백으로 두면 전화기는 자정(0:00)에 켜집니다.</p> <p>[디스플레이 켜기 시간]이 0:00이고 디스플레이 켜기 지속 시간이 공백이거나 24:00으로 되어 있으면, 디스플레이는 꺼지지 않습니다.</p>
디스플레이 유휴 시간 초과	hh:mm	01:00	<p>디스플레이를 끄기 전까지 전화기가 유휴 상태로 유지되는 시간 길이를 정의합니다. 디스플레이가 예정대로 꺼진 때와 사용자가 전화기의 버튼을 누르거나 핸드셋을 들어 올려 디스플레이를 켜 경우에만 적용됩니다.</p> <p>이 필드에 시간:분 형식으로 값을 입력합니다.</p> <p>예를 들어 사용자가 디스플레이를 켜 후 전화기의 유휴 상태가 1시간 30분 동안 지속되었을 때 디스플레이를 끄려면 01:30을 입력합니다.</p> <p>자세한 내용은 <a href="#">유휴 디스플레이 설정, 120 페이지</a>의 내용을 참조하십시오.</p>
전화 수신 시 디스플레이 켜기	비활성화됨 활성화됨	활성화됨	수신 통화가 있는 경우 유휴 디스플레이를 켵니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
절전 플러스 활성화	요일		<p>전화기의 전원을 끄려는 날짜를 정의합니다.</p> <p>드롭다운 목록 상자에서 날짜를 선택합니다. 1일 이상을 선택하려면 <b>Ctrl</b> 키를 누른 채 원하는 날짜를 클릭합니다.</p> <p>절전 플러스 활성화를 설정하면, 긴급 상황(e911)에 대해 경고하는 메시지가 전송됩니다.</p> <p>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.</p> <p>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.</p>
전화 켜기 시간	hh:mm		<p>[절전 플러스 활성화] 필드에 지정된 일 수 동안 전화기를 자동으로 켜는 시간을 정합니다.</p> <p>이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 00:00은 자정입니다.</p> <p>예를 들어 오전 07:00시(0700)에 자동으로 전화기를 켜고 싶다면 07:00을 입력합니다. 오후 02:00(1400)에 전화기를 켜고 싶다면 14:00을 입력합니다.</p> <p>기본값은 공란, 즉 00:00입니다.</p> <p>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.</p>



필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
전화 끄기 시간	hh:mm		<p>[절전 플러스 활성화] 필드에 지정된 일 수 동안 전화기의 전원을 끄는 시간을 식별합니다. [전화 켜기 시간]과 [전화 끄기 시간] 필드에 같은 값이 입력되어 있으면 전화기는 전원을 끄지 않습니다.</p> <p>이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 00:00은 자정입니다.</p> <p>예를 들어 오전 07:00시(0700)에 자동으로 전화기를 끄고 싶다면 7:00을 입력합니다. 오후 02:00(1400)에 전화기를 끄고 싶다면 14:00을 입력합니다.</p> <p>기본값은 공란, 즉 00:00입니다.</p> <p>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.</p>
전화 끄기 유희 시간 초과	20~1440분	60	<p>전화기의 전원을 끄기 전에 전화기가 유희 상태로 머물러야 하는 시간의 길이를 나타냅니다.</p> <p>시간 초과는 다음과 같은 상황에서 발생합니다.</p> <ul style="list-style-type: none"> <li>• 예정대로 전화기가 절전 플러스 모드인 상태에서, 전화기 사용자가 선택 키를 눌러 절전 플러스 모드에서 벗어난 경우</li> <li>• 연결된 스위치에서 전화기의 전원을 다시 켰을 때</li> <li>• 전화 끄기 시간이 되었으나 전화기를 사용 중일 때</li> </ul>
알림음 사용	확인란	선택 취소됨	<p>활성화되면 전화기에 [전화 끄기 시간] 필드에 지정한 시간보다 10분 전에 알림음을 재생하게 합니다.</p> <p>이 확인란은 [절전 플러스 활성화] 목록 상자에서 1일 이상을 선택한 경우에만 적용됩니다.</p>
EnergyWise 도메인	최대 127자		전화기가 소속된 EnergyWise 도메인을 식별합니다.
EnergyWise 비밀번호	최대 127자		EnergyWise 도메인에서 엔드포인트와 통신할 때 사용하는 보안 비밀번호 암호를 식별합니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
EnergyWise 오버라이드 허용	확인란	선택 취소됨	<p>EnergyWise 도메인 컨트롤러 정책에서 전화기로 전력 수준 업데이트를 전송하도록 허용할 것인지 여부를 결정합니다. 다음과 같은 조건이 적용됩니다.</p> <ul style="list-style-type: none"> <li>• [절전 플러스 활성화] 필드에서 1일 이상을 선택해야 합니다.</li> <li>• EnergyWise에서 오버라이드를 전송할 때에도 Cisco Unified Communications Manager Administration의 설정은 실행됩니다.</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>• EnergyWise에서 전화기에 20:00(오후 8:00)에 전화를 끄라고 지시하면, 이러한 지시 사항은 구성된 전화 켜기 시간인 오전 6:00까지 효력이 있습니다(전화에 사용자 개입이 전혀 없다고 가정할 경우).</li> <li>• 오전 6:00시가 되면 전화기가 켜지고 Cisco Unified Communications Manager Administration 설정에서 전력 수준 변경 내용을 수신하여 작동을 시작합니다.</li> <li>• 전화기의 전력 수준을 다시 변경하려면, EnergyWise에서 새로운 전력 수준 변경 명령을 다시 내려야 합니다.</li> </ul> <p>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.</p>

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
참여 및 호연결 정책 설정	동일한 회선, 회선 간 활성화 동일한 회선 활성화만 동일한 회선, 회선 간 비활성화	동일한 회선, 회선 간 활성화	사용자의 참여 및 호전환 호출 기능을 제어합니다. <ul style="list-style-type: none"> <li>동일한 회선, 회선 간 활성화 — 사용자가 직접 호전환하거나 현재 회선의 통화를 다른 회선의 다른 통화에 참가할 수 있습니다.</li> <li>동일한 회선 활성화만 — 양쪽 통화가 동일한 회선에 있는 경우에만 사용자가 직접 호전환하거나 통화에 참가할 수 있습니다.</li> <li>동일한 회선, 회선 간 비활성화 — 동일한 회선에서 사용자가 통화에 참가하거나 호전환할 수 없습니다. 참가 및 호전환 기능이 비활성화되고 사용자가 직접 호전환 또는 통화 참가 기능을 수행할 수 없습니다.</li> </ul>
PC 포트에 연결	비활성화됨 활성화됨	비활성화됨	전화기가 네트워크 포트에서 액세스 포트로 전송되어 수신된 패킷을 착신 전환하는지 보여줍니다.
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 <b>address: &lt;port&gt;@&lt;base=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b> 입니다.
Cisco Discovery Protocol(CDP): 스위치 포트	비활성화됨 활성화됨	활성화됨	전화기의 SW 포트에서 Cisco Discovery Protocol을 제어합니다.
Cisco Discovery Protocol(CDP): PC 포트	비활성화됨 활성화됨	활성화됨	전화기의 PC 포트에서 Cisco Discovery Protocol을 제어합니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
Link Layer Discovery Protocol - 미디어 엔드포인트 검색 (LLDP-MED): 스위치 포트	비활성화됨 활성화됨	활성화됨	SW 포트에서 LLDP-MED를 활성화합니다.
LLDP(Link Layer Discovery Protocol): PC 포트	비활성화됨 활성화됨	활성화됨	SWPC포트에서 LLDP를 활성화합니다.
LLDP 자산 ID	최대 32자의 문자열		인벤토리 관리를 위해 전화기에 할당된 자산 ID를 식별합니다.
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 활성화됨 비활성화됨	사용자 제어됨	802.1x 인증 기능 상태를 지정합니다. <ul style="list-style-type: none"> <li>• 사용자 제어됨 - 사용자가 전화기에서 802.1x를 구성할 수 있습니다.</li> <li>• 비활성화됨 — 802.1x 인증이 사용되지 않습니다.</li> <li>• 활성화됨—802.1x 인증을 사용하고 전화기에 대한 인증을 구성합니다.</li> </ul>
자동 포트 동기화	비활성화됨 활성화됨	비활성화됨	포트를 전화의 포트 간 최저 속도로 동기화하여 패킷 유실을 제거합니다.
스위치 포트 원격 구성	비활성화됨 활성화됨	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.

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
PC 포트 원격 구성	비활성화됨 활성화됨	비활성화됨	원격으로 전화기 PC 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 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.
착신 통화 알림 타이머	0, 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, 60	5	알림을 표시하는 시간(초)을 입력합니다. 시간에는 창이 서서히 나타났다가 사라지는 시간이 포함됩니다.  0은 착신 통화 알림이 비활성화되었음을 의미합니다.
벨소리 로깅	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	통화 로그에 공유 회선 통화를 녹음할지 여부를 지정합니다.
최소 벨소리 볼륨	0-무음 1-15	0-무음	전화기에 대한 최소 벨소리 볼륨을 제어합니다.  벨소리를 해제할 수 없도록 전화기를 설정할 수 있습니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
피어 펌웨어 공유	비활성화됨 활성화됨	활성화됨	<p>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.</p> <p>피어 펌웨어 공유:</p> <ul style="list-style-type: none"> <li>• 중앙의 원격 TFTP 서버로 TFTP 호전환에 따른 혼잡을 제한합니다.</li> <li>• 펌웨어 업그레이드를 수동으로 관리할 필요가 없습니다.</li> <li>• 다수의 전화기를 동시에 재설정할 때 업그레이드를 진행하는 동안 전화기 다운타임이 줄어듭니다.</li> <li>• 대역폭이 제한된 WAN 링크를 실행하는 지점 또는 원격 사무실 구축 시나리오에서 펌웨어 업그레이드하는 데 도움이 됩니다.</li> </ul>
로드 서버	최대 256자의 문자열		<p>전화기가 펌웨어 로드 및 업그레이드를 사용하는 대체 IPv4 서버를 식별합니다.</p> <p>주소의 형식은 <b>address : &lt;port&gt;@@base=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b>입니다.</p>
IPv6 로드 서버	최대 256자의 문자열		<p>전화기가 펌웨어 로드 및 업그레이드를 사용하는 대체 IPv6 서버를 식별합니다.</p> <p>주소의 형식은 <b>[address] : &lt;port&gt;@@base=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b>입니다.</p>
와이드밴드 헤드셋 UI 제어	비활성화됨 활성화됨	활성화됨	아날로그 헤드셋에 대한 와이드밴드 코덱을 사용할 수 있습니다.
와이드밴드 헤드셋	비활성화됨 활성화됨	활성화됨	<p>전화기에서 와이드밴드 헤드셋 사용을 활성화하거나 비활성화합니다. 사용자 제어 와이드밴드 헤드셋과 함께 사용됩니다.</p> <p>자세한 내용은 <a href="#">광대역 코덱 설정, 119 페이지</a>의 내용을 참조하십시오.</p>

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
Wi-Fi	비활성화됨 활성화됨	활성화됨	Cisco IP 전화기 8861 및 8865를 Wi-Fi 네트워크에 연결할 수 있습니다. 이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
뒷면 USB 포트	비활성화됨 활성화됨	8861, 8865 및 8865NR: 활성화됨	Cisco IP 전화기 8861 및 8865의 뒷면 USB 포트를 사용하는 기능을 제어합니다. 이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
측면 USB 포트	비활성화됨 활성화됨	활성화됨	Cisco IP 전화기 8851, 8851NR, 8861, 8865 및 8865NR의 측면 USB 포트를 사용하는 기능을 제어합니다. 이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
콘솔 액세스	비활성화됨 활성화됨	비활성화됨	직렬 콘솔을 활성화 또는 비활성화할지 여부를 지정합니다.
블루투스	비활성화됨 활성화됨	활성화됨	전화기에서 블루투스 옵션을 활성화하거나 비활성화합니다. 비활성화된 경우 전화기에서 블루투스를 사용할 수 없습니다. Cisco IP 전화기 8845, 8851, 8861 및 8865에서 지원됩니다. 이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
블루투스 연락처 가져오기 허용	비활성화됨 활성화됨	활성화됨	블루투스를 사용하여 연결된 모바일 장치에서 연락처를 가져올 수 있습니다. 비활성화된 경우 전화기가 연결된 모바일 장치에서 연락처를 가져올 수 없습니다. Cisco IP 전화기 8845, 8851, 8861 및 8865에서 지원됩니다. 이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
블루투스 모바일 핸드프리 모드 허용	비활성화됨 활성화됨	활성화됨	<p>사용자는 모바일 장치 또는 태블릿으로 전화기의 음향 속성을 이용할 수 있습니다. 사용자는 블루투스를 사용하여 모바일 장치 또는 태블릿을 전화기에 페어링합니다. 비활성화된 경우 사용자는 모바일 장치 또는 태블릿을 전화기에 페어링할 수 없습니다.</p> <p>모바일 장치가 페어링되었으면 사용자는 전화기에서 휴대폰 통화를 걸고 받을 수 있습니다. 태블릿을 사용하여 사용자는 태블릿에서 전화기로 오디오를 라우팅할 수 있습니다.</p> <p>사용자는 다중 모바일 장치, 태블릿 및 블루투스 헤드셋을 전화기에 페어링할 수 있습니다. 그러나 장치 하나와 헤드셋 하나만 동시에 연결할 수 있습니다.</p> <p>이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.</p>
블루투스 프로파일	핸즈프리 HID(Human Interface Device)	핸즈프리	<p>전화기에서 블루투스 프로파일을 활성화할지 또는 비활성화할지 여부를 나타냅니다.</p> <p>이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.</p>
불필요한 ARP	비활성화됨 활성화됨	비활성화됨	<p>Gratuitous ARP에서 MAC 주소를 학습하는 전화기 기능을 활성화 또는 비활성화합니다. 이 기능은 음성 스트림을 모니터링하거나 녹음해야 합니다.</p>
주 회선에서 모든 통화 표시	비활성화됨 활성화됨	비활성화됨	<p>이 전화기로 걸려온 모든 통화를 주 회선에 표시할지 여부를 지정합니다.</p> <p>이 필드의 목적은 최종 사용자가 해당 회선의 통화를 보기 위해 회선을 선택하지 않고도 한 눈에 모든 회선의 모든 통화를 쉽게 볼 수 있도록 하는 것입니다. 즉, 전화기에 여러 회선이 구성된 경우 일반적으로 결합된 디스플레이에 모든 회선의 통화를 모두 표시하는 것이 좋습니다. 이 기능이 활성화된 경우 모든 통화는 주 회선에 표시되지만 해당 특정 회선에 대한 통화만 표시하도록 화면을 특정 회선을 필터링할 수도 있습니다.</p>
HTTPS 서버	HTTP 및 HTTPS 활성화됨 HTTPS만	HTTP 및 HTTPS 활성화됨	<p>전화기에 대한 통신 유형을 제어합니다. HTTPS만을 선택하면 전화 통신은 더 안전합니다.</p>



필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
IPv6 로그 서버	최대 256자의 문자열		IPv6 로그 서버를 식별합니다. 주소의 형식은 <b>[address]:&lt;port&gt;@@base=&lt;0-7&gt;;pfs=&lt;0-1&gt;</b> 입니다.
원격 로그	비활성화됨 활성화됨	비활성화됨	syslog서버에 로그를 전송하는 기능을 제어합니다.
로그 프로파일	기본값 프리셋 텔레포니 SIP UI 네트워크 미디어 업그레이드 액세서리 보안 Wi-Fi VPN EnergyWise MobileRemoteAc	프리셋	미리 정의된 로그 프로파일을 지정합니다. <ul style="list-style-type: none"> <li>• 기본값 - 기본 디버그 로그 수준</li> <li>• 프리셋 - 전화기 로컬 디버그 로깅 설정을 덮어쓰지 않음</li> <li>• 텔레포니 — 텔레포니 또는 통화 기능에 대한 정보를 기록</li> <li>• SIP - SIP 시그널링에 대한 정보를 기록</li> <li>• UI — 전화기 사용자 인터페이스에 대한 정보를 기록</li> <li>• 네트워크 — 네트워크 정보를 기록</li> <li>• 미디어 — 미디어 정보를 기록</li> <li>• 업그레이드 — 업그레이드 정보를 기록</li> <li>• 액세서리 — 액세서리 정보를 기록</li> <li>• 보안 — 보안 정보를 기록</li> <li>• Wi-Fi - Wi-Fi 정보를 기록</li> <li>• VPN — 가상 사설망 정보를 기록</li> <li>• Energywise — 에너지 절약 정보를 기록</li> <li>• MobileRemoteAC — Expressway를 통한 모바일 및 Remote Access 정보를 기록</li> </ul>

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
Advertise G.722 및 iSAC 코덱	시스템 기본값 사용 비활성화됨 활성화됨	시스템 기본값 사용	전화기가 G.722 및 iSAC 코덱을 Cisco Unified Communications Manager에 광고할지 여부를 나타냅니다. <ul style="list-style-type: none"> <li>• 시스템 기본값 사용 - 엔터프라이즈 매개 변수 Advertise G.722 코덱에 지정된 설정을 따릅니다.</li> <li>• 비활성화됨 - G.722를 Cisco Unified Communications Manager에 광고하지 않습니다.</li> <li>• 활성화됨 - G.722를 Cisco Unified Communications Manager에 광고합니다.</li> </ul> <p>자세한 내용은 표 다음의 자료를 참조하십시오.</p>
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. <ul style="list-style-type: none"> <li>• 보통 — Unified CM 연결 실패 감지가 시스템 표준 비율로 발생합니다. Unified CM 연결 실패를 빠르게 감지하려면 이 값을 선택합니다.</li> <li>• 지연됨 — Unified CM 연결 페일오버 감지가 보통보다 약 4배 느리게 발생합니다. 페일오버를 약간 지연시켜 다시 연결할 기회를 제공하려는 경우 이 값을 선택합니다.</li> </ul> <p>보통과 지연됨 연결 오류 감지 사이의 정확한 시간 차이는 계속 변하는 여러 가지 변수에 따라 달라집니다.</p> <p>이 필드는 유선 이더넷 연결에만 적용됩니다.</p>
전원 협상	비활성화됨 활성화됨	활성화됨	전화기에서 LLDP(Link Level Endpoint Discovery Protocol)와 CDP(Cisco 탐색 프로토콜)를 사용해 전원을 설정할 수 있습니다. <p>전화기가 전원공급 협상을 지원하는 스위치에 연결되어 있을 때 전원공급 협상이 비활성화 상태여서는 안 됩니다. 비활성화되면 스위치가 전화기의 전원을 차단할 수 있습니다.</p>

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
해제 버튼에서 신호 음 제공	비활성화됨 활성화됨	비활성화됨	해제 키를 누를 때 들리는 발신음을 제어합니다. <ul style="list-style-type: none"> <li>비활성화됨 - 사용자에게 다이얼 발신음이 들리지 않습니다.</li> <li>활성화됨 - 다이얼 발신음이 들립니다.</li> </ul>
배경 이미지	최대 64자의 문자열		기본 배경 화면 파일을 지정합니다. 기본 배경 화면을 설정하면 사용자 전화기의 배경 화면을 변경할 수 없습니다.
간소화된 새 통화 UI	비활성화됨 활성화됨	비활성화됨	오프 혹은 다이얼에 대한 사용자 인터페이스를 제어합니다. 활성화된 경우 사용자는 최근 통화 목록에서 번호를 선택할 수 없습니다. <p>활성화된 경우 이 필드는 사용자가 전화를 걸 수 있는 간단한 창을 제공합니다. 전화기가 오프 혹은 오프로 전환될 때 표시되는 통화 기록 팝업 창이 표시되지 않습니다. 팝업 창은 간소화된 새 통화 UI를 기본적으로 비활성화하므로 유용한 것으로 간주됩니다.</p>
모든 통화로 되돌리기	비활성화됨 활성화됨	비활성화됨	전화기가 모든 통화를 종료한 후 모든 통화로 돌아갈지 또는 통화에 주 회선, 모든 통화 또는 경고 통화 이외의 필터가 적용된 경우 되돌아가지 않을지 여부를 지정합니다.
선택한 회선의 통화 기록만 표시	비활성화됨 활성화됨	비활성화됨	최근 통화 목록 표시를 제어합니다. <ul style="list-style-type: none"> <li>비활성화됨 — 최근 통화 목록은 모든 회선에 대한 통화 기록을 표시합니다.</li> <li>활성화됨 — 최근 통화 목록은 선택한 회선에 대한 통화 기록을 표시합니다.</li> </ul>
대응 선택 착신 통화 알림	비활성화됨 모든 착신 통화 표시 보이지 않는 착신 통화 표시	모든 착신 통화 표시	전화기 화면에 표시되는 착신 통화 경고의 유형을 제어합니다. 이 필드의 목적은 최종 사용자가 통화에 응답해야 하는 버튼 누름 횟수를 줄이기 위한 것입니다. <ul style="list-style-type: none"> <li>비활성화됨 — 대응 선택 착신 통화 경고가 비활성화되고 기존 착신 통화 팝업 알림이 표시됩니다.</li> <li>모든 착신 통화에 표시 - 가시성과 관계없이 모든 통화에 대해 대응 선택 착신 통화 알림이 표시됩니다.</li> <li>보이지 않는 착신 통화에 표시 - 전화기에 나타나지 않는 통화에 대해 대응 선택 착신 통화 알림이 표시됩니다. 이 매개 변수는 착신 통화 알림 팝업 알림과 유사하게 동작합니다.</li> </ul>

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
DF 비트	0 1	0	<p>네트워크 패킷의 전송 방식을 제어합니다. 패킷을 다양한 크기의 청크(부분)로 전송할 수 있습니다.</p> <p>패킷 헤더에서 DF 비트가 1로 설정된 경우 스위치 및 라우터와 같은 네트워크 장치를 지날 때 네트워크 페이로드가 조각나지 않습니다. 조각을 제거하면 수신 측에서 잘못된 구문 분석을 피하지만, 속도는 약간 더 느려집니다.</p> <p>DF 비트 설정은 ICMP, VPN, VXC VPN 또는 DHCP 트래픽에 적용되지 않습니다.</p>
기본 회선 필터	섬표로 구분된 전화기 장치 이름 목록		<p>기본 필터에 있는 전화기의 목록을 나타냅니다.</p> <p>기본 회선 필터가 구성되면 전화기 설정 &gt; 기본 설정 메뉴의 전화 알림에 일별 일정 필터가 표시됩니다. 이 일별 일정 필터는 미리 설정된 모든 통화 필터에 추가됩니다.</p> <p>기본 회선 필터가 구성되지 않은 경우 전화기는 구축된 회선을 모두 확인합니다. 구성된 경우에는 사용자가 기본 필터를 활성 필터로 선택하거나, 사용자 정의 필터가 없는 경우 전화기가 Cisco Unified Communications Manager에 설정된 회선을 확인합니다.</p> <p>사용자 정의 회선 필터를 사용하면 높은 우선 순위의 회선을 필터링하여 알림 활동을 줄일 수 있습니다. 경고 필터가 적용되는 일부 회선에 대해 통화 알림의 경고 우선 순위를 지정할 수 있습니다. 사용자 정의 필터는 선택된 회선의 수신 통화에 대해 기존의 팝업 경고 또는 대응 선택 경고 중 하나를 표시하도록 선택할 수 있습니다. 각 필터에 대해 포함되는 일부 회선에서만 경고가 표시됩니다. 이 기능은 여러 회선이 있는 사용자에게 높은 우선 순위의 회선에서만 알림을 필터링하고 표시하여 알림 활동을 줄이는 방법을 제공합니다. 최종 사용자가 직접 구성할 수 있습니다. 또는 기본 회선 필터를 프로그래밍하고 전화기에 적용할 수도 있습니다.</p>
가장 낮은 경고 회선 상태 우선 순위	비활성화됨 활성화됨	비활성화됨	<p>공유 회선을 사용하여 알림 상태를 지정합니다.</p> <ul style="list-style-type: none"> <li>• 비활성화됨 — 공유 회선에서 착신 통화 알림이 있을 때 LED/회선 상태 아이콘은 원격 사용 중 대신 알림 상태를 반영합니다.</li> <li>• 활성화됨 - 공유 회선에 착신 통화 알림이 있을 때 원격 사용 중 아이콘이 표시됩니다.</li> </ul>

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
KEM에 대해 1열 표시	비활성화됨 활성화됨	비활성화됨	키 확장 모듈의 표시를 제어합니다. <ul style="list-style-type: none"> <li>• 비활성화됨 — 확장 모듈은 2열 모드를 사용합니다.</li> <li>• 활성화됨 — 확장 모듈은 1열 모드를 사용합니다.</li> </ul> 이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
EEE(Energy Efficient Ethernet): PC 포트	비활성화됨 활성화됨	비활성화됨	PC 포트에서 EEE를 제어합니다.
EEE(Energy Efficient Ethernet): SW 포트	비활성화됨 활성화됨	비활성화됨	스위치 포트에서 EEE를 제어합니다.
비디오 포트 시작			영상 통화에 대한 포트 범위의 시작을 정의합니다. 이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
비디오 포트 중지			영상 통화에 대한 포트 범위의 끝을 정의합니다. 이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
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 오프프레미스에서 공급될 때) 로그인 정보가 로그인 화면에 미리 입력되어 있습니다. 자세한 내용은 <a href="#">Expressway를 통한 모바일 및 Remote Access, 181 페이지</a> 를 참조하십시오.
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 <a href="#">Expressway를 통한 모바일 및 Remote Access, 181 페이지</a> 를 참조하십시오.

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
웹 관리자	비활성화됨 활성화됨	비활성화됨	웹 브라우저를 통해 전화기 웹 페이지에 대한 관리자 액세스를 활성화 또는 비활성화합니다.  자세한 내용은 <a href="#">관리 페이지에서 전화기 구성, 110 페이지</a> 를 참조하십시오.  이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
관리자 비밀번호	8-127자의 문자열		전화기 웹 페이지에 관리자 권한으로 액세스할 때 관리자 암호를 정의합니다.  이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
WLAN SCEP 서버	최대 256자의 문자열		전화기가 WLAN 인증에 대한 인증서를 얻기 위해 사용하는 SCEP 서버를 지정합니다. 서버의 호스트 이름 또는 IP 주소(표준 IP 주소 지정 형식 사용)를 입력합니다.  이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
WLAN Root CA Fingerprint(SHA256 또는 SHA1)	최대 95자의 문자열		WLAN 인증을 위해 인증서를 발급하는 경우 SCEP 프로세스 동안 유효성 검사를 위해 사용할 Root CA의 SHA256 또는 SHA1 지문을 지정합니다. 인증서 세부 사항을 검사하기 위해 OpenSSL(즉, <code>openssl x509 -in rootca.cer -noout -sha256 -fingerprint</code> ) 또는 웹 브라우저를 사용하여 얻을 수 있는 SHA256 지문을 사용하는 것이 좋습니다.  일반 구분 기호(콜론, 대시, 마침표, 공백)를 사용하거나 구분 기호 없이 SHA256 지문의 경우 64개의 16진수 문자 값 또는 SHA1 지문의 경우 4-개 16진수 문자 값을 입력합니다. 구분 기호를 사용하는 경우 구분 기호는 SHA256의 경우 2, 4, 8, 16 또는 32자 16진수 문자마다 또는 SHA1 지문의 경우 2, 4 또는 8자 16진수 문자마다 일관성 있게 삽입되어야 합니다.  이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
WLAN 인증 시도			이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.
WLAN 프로파일 1 프롬프트 모드	비활성화됨 활성화됨	비활성화됨	이 기능을 지원하지 않는 전화기에는 필드가 표시되지 않습니다.

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
회선 모드	세션 회선 모드 고급 회선 모드	세션 회선 모드	전화기에서 회선 표시를 제어합니다. <ul style="list-style-type: none"> <li>• 세션 회선 모드 — 화면의 한 쪽에 있는 버튼이 회선 키입니다.</li> <li>• 고급 회선 모드 - 전화기 화면의 양면에 있는 버튼이 회선 키입니다. 예측 다이얼링 및 대응 선택 착신 통화 알림은 고급 회선 모드에서 기본적으로 활성화됩니다.</li> </ul>
관리자 구성 가능한 벨소리	비활성화됨 Sunrise Chirp1 Chirp2	비활성화됨	벨소리 및 사용자가 벨소리를 설정하는 기능을 제어합니다. <ul style="list-style-type: none"> <li>• 비활성화됨으로 설정하면 사용자가 전화기에서 기본 벨소리를 구성할 수 있습니다.</li> <li>• 다른 모든 값의 경우 사용자가 벨소리를 변경할 수 없습니다. 설정 메뉴에서 벨소리 메뉴 항목이 회색으로 표시됩니다.</li> </ul>
고객 지원 사용	최대 64자의 문자열	비어 있음	Cisco TAC에만 사용합니다.
TLS 암호화 비활성화	전송 레이어 보안 암호 비활성화, 169 페이지 참조	없음	선택한 TLS 암호화를 비활성화합니다. 컴퓨터 키보드의 <b>Ctrl</b> 키를 누른 채로 둘 이상의 암호화 제품군을 비활성화합니다. 전화기 암호를 모두 선택하는 경우 전화기 TLS 서비스가 영향을 받습니다.
목소리 낮추기 경고	활성화됨 비활성화됨	활성화됨	목소리 낮추기 기능을 제어합니다. <ul style="list-style-type: none"> <li>• 비활성화됨: <ul style="list-style-type: none"> <li>• 전화기의 설정 메뉴에 목소리 낮추기 메뉴 항목이 표시되지 않습니다.</li> <li>• 사용자가 큰 소리로 말하면 화면에 메시지가 표시되지 않습니다.</li> </ul> </li> <li>• 활성화됨: <ul style="list-style-type: none"> <li>• 사용자는 설정 메뉴의 목소리 낮추기 메뉴 항목에서 이 기능을 제어합니다. 이 필드는 기본적으로 켜기로 설정됩니다.</li> </ul> </li> </ul>

필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
통화를 스팸으로 표시	활성화됨 비활성화됨	활성화됨	'통화를 스팸으로 표시' 기능을 제어합니다.  <ul style="list-style-type: none"> <li>• 비활성화됨: <ul style="list-style-type: none"> <li>• 전화기에 스팸으로 표시 소프트웨어가 표시되지 않습니다.</li> <li>• 설정 메뉴의 스팸 목록 항목이 표시되지 않습니다.</li> <li>• 스팸 목록이 있었다면 이 목록이 지워지며 복구는 불가능합니다.</li> </ul> </li> <li>• 활성화됨: <ul style="list-style-type: none"> <li>• 전화기에 스팸으로 표시 소프트웨어가 표시됩니다.</li> <li>• 설정 메뉴의 스팸 목록 항목이 표시됩니다.</li> </ul> </li> </ul>
통화 대기 중인 전용 회선	비활성화됨 활성화됨	활성화됨	통화 지정 보류된 통화가 한 회선을 차지하는지 여부를 제어합니다.  자세한 내용은 Cisco Unified Communications Manager 문서를 참조하십시오.



필드 이름	필드 유형 또는 선택 사항	기본값	설명 및 사용 지침
ELM에서 회선 텍스트 레이블 표시	비활성화됨 활성화됨	활성화됨	<p>고급 회선 모드가 구성되어 있을 때 통화 중 회선 레이블 표시를 제어합니다.</p> <ul style="list-style-type: none"> <li>• 활성화됨 <ul style="list-style-type: none"> <li>• 발신자의 이름이 구성된 경우 통화 세션의 첫 번째 행에 있는 이름과 두 번째 회선의 로컬 회선 레이블을 표시합니다.</li> <li>• 발신자의 이름이 구성되지 않은 경우에는 첫 번째 회선에 원격 번호를 표시하고 두 번째 회선에 로컬 회선 레이블을 표시합니다.</li> </ul> </li> <li>• 비활성화됨 <ul style="list-style-type: none"> <li>• 발신자의 이름이 구성된 경우 통화 세션의 첫 번째 행에 이름이 표시되고 두 번째 회선에 번호가 표시 됩니다.</li> <li>• 발신자의 이름이 구성되지 않은 경우 원격 번호만 표시됩니다.</li> </ul> </li> </ul> <p>이 필드는 필수 항목입니다.</p>



참고 코텍 협상은 두 단계입니다.

1. 전화기는 Cisco Unified Communications Manager에 지원되는 코텍을 광고합니다. 일부 엔드포인트는 동일한 코텍 집합을 지원합니다.
2. Cisco Unified Communications Manager는 지원되는 코텍 목록을 통화 시도에 관련된 모든 전화기에서 가져온 후, 지역 쌍 설정을 포함하여 다음과 같은 다양한 요인을 기준으로 공통적으로 지원되는 코텍을 선택합니다.

## 기능 구성 모범 사례

사용자의 필요에 따라 전화기 기능을 설정할 수 있습니다. 하지만 특정 상황 및 도움이 될 수 있는 구축에 대한 몇 가지 권장 사항이 있습니다.

### 통화량이 높은 환경

통화량이 높은 환경에서 특정 방법으로 일부 기능을 설정하는 것이 좋습니다.

필드	관리 영역	권장 설정
항상 기본 회선 사용	장치 정보	끄기 또는 켜기 자세한 내용은 필드: <a href="#">항상 기본 회선 사용, 169 페이지</a> 의 내용을 참조하십시오.
대응 선택 착신 통화 알림	제품별 구성	모든 착신 통화 표시
주 회선에서 모든 통화 표시	제품별 구성	활성화됨
모든 통화로 되돌리기	제품별 구성	활성화됨

## 복수 회선 환경

복수 회선 환경에서 특정 방법으로 일부 기능을 설정하는 것이 좋습니다.

필드	관리 영역	권장 설정
항상 기본 회선 사용	장치 정보	끄기 자세한 내용은 필드: <a href="#">항상 기본 회선 사용, 169 페이지</a> 의 내용을 참조하십시오.
대응 선택 착신 통화 알림	제품별 구성	모든 착신 통화 표시
주 회선에서 모든 통화 표시	제품별 구성	활성화됨
모든 통화로 되돌리기	제품별 구성	활성화됨

## 세션 회선 모드 환경

고급 회선 모드는 대부분의 통화 환경을 처리하기 위해 선호되는 도구입니다. 그러나 고급 회선 모드가 요구에 적합하지 않으면 세션 회선 모드를 사용할 수 있습니다.

필드	관리 영역	세션 회선 모드에 권장되는 설정
주 회선에서 모든 통화 표시	제품별 구성	비활성화됨
모든 통화로 되돌리기	제품별 구성	비활성화됨
대응 선택 착신 통화 알림	제품별 구성	기본적으로 활성화됨(펌웨어 릴리스 11.5(1) 이상).

관련 항목

[추가 회선 키 설정, 205 페이지](#)

[고급 회선 모드에서 사용할 수 있는 기능, 205 페이지](#)

## 필드: 항상 기본 회선 사용

이 필드는 사용자가 오프 홀스로 전환될 때 IP 전화기의 기본 회선이 선택되었는지 여부를 지정합니다. 이 매개 변수가 True로 설정된 경우 전화기가 오프 홀스 상태로 전환될 때 기본 회선이 선택되고 활성 회선이 됩니다. 통화가 사용자의 두 번째 회선에서 울릴 때도 전화기가 오프 홀스 상태로 전환될 때 첫 번째 회선만 활성 상태가 됩니다. 두 번째 회선에서 착신 전화가 응답하지 않습니다. 이 경우 사용자는 통화에 응답하려면 두 번째 회선을 선택해야 합니다. 기본값은 False입니다.

[항상 기본 회선 사용] 필드의 용도는 이러한 두 가지 기능이 모두 사용되는 경우 기본 회선에서 모든 통화 보기와 모든 통화로 되돌리기 조합과 매우 유사합니다. 그러나 주요한 차이는 항상 기본 회선 사용이 활성화된 경우 착신 전화는 두 번째 회선에서 응답되지 않는다는 것입니다. 기본 회선에는 다 이얼톤만 들립니다. 원하는 사용자 경험인 특정한 높은 통화량 환경이 있습니다. 일반적으로 이 기능을 필요로 하는 높은 통화량 환경의 경우를 제외하고 이 필드를 비활성 상태로 두는 것이 좋습니다.

## 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.

## 공유 회선을 위한 통화 기록 활성화

통화 기록에서 공유 회선 활동을 확인할 수 있습니다. 이 기능의 용도:

- 공유 회선의 부재 중 통화를 기록합니다.

- 공유 회선의 모든 받은 전화 및 발신된 전화를 기록합니다.

#### 시작하기 전에

공유 회선의 통화 기록을 활성화하기 전에 개인 정보 보호를 비활성화하십시오. 그렇지 않으면 통화 기록에 다른 사용자가 응답한 통화가 표시되지 않습니다.

#### 프로시저

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

단계 2 구성할 전화기를 검색합니다.

단계 3 제품 특정 구성 영역의 공유 회선 드롭다운에서 통화 로그 기록으로 이동합니다.

단계 4 드롭다운 목록에서 활성화됨을 선택합니다.

단계 5 저장을 선택합니다.

## 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.

다음은 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.

자세한 내용은 [제품별 구성, 146 페이지](#)의 내용을 참조하십시오.

#### 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 유희 시간 초과

표 32: 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.
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 켜고 싶다면 <b>07:00</b> 을 입력합니다. 오후 02:00시(1400)에 디스플레이를 켜고 싶다면 <b>14:00</b> 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 켜 상태로 유지하고 싶다면, <b>04:30</b> 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 유희 시간 초과	디스플레이를 끄기 전까지 전화기가 유희 상태로 유지되는 시간 길이. 디스플레이가 예정대로 꺼진 때와 사용자가 전화기의 버튼을 누르거나 핸드셋을 들어 올려 디스플레이를 켜는 경우에만 적용됩니다. 이 필드에 시간:분 형식으로 값을 입력합니다. 예를 들어 사용자가 디스플레이를 켜 후 전화기의 유희 상태가 1시간 30분 동안 지속되었을 때 디스플레이를 끄려면 <b>01:30</b> 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 매개 변수는 전화기 화면 구성 매개 변수와 밀접하게 연결됩니다.

EnergyWise가 활성화되고 대기 시간이 설정되면, 전화기는 스위치에 설정한 시간에 전화기를 활성화 하라고 요청을 전송합니다. 스위치는 요청에 대한 수락 또는 거부 메시지를 반환합니다. 스위치가 요청을 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 종료 되면 대기 상태로 전환됩니다.

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

자세한 내용은 [제품별 구성, 146 페이지](#)의 내용을 참조하십시오.

### 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 33: EnergyWise 구성 필드

필드	설명
절전 플러스 활성화	<p>전화기의 전원을 끄려는 날짜를 선택합니다. 일정에 포함할 날짜를 클릭하고, 컨트롤 키를 누른 채로 여러 날짜를 선택합니다.</p> <p>기본적으로는 날짜가 선택되지 않습니다.</p> <p>절전 플러스 활성화를 선택하면, 긴급 상황(e911)에 대해 경고하는 메시지가 전송됩니다.</p> <p>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.</p> <p>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.</p>
전화 켜기 시간	<p>[절전 플러스 활성화] 필드에 지정된 일 수 동안 전화기를 자동으로 켜는 시간을 정합니다.</p> <p>이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 00:00은 자정입니다.</p> <p>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.</p> <p>기본값은 공란, 즉 00:00입니다.</p> <p>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.</p>
전화 끄기 시간	<p>[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.</p> <p>이 필드에 24시간 형식으로 시간을 입력합니다. 따라서 00:00은 자정입니다.</p> <p>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.</p> <p>기본값은 공란, 즉 00:00입니다.</p> <p>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.</p>

필드	설명
전화 끄기 유틸 시간 초과	<p>전화기의 전원을 끄기 전에 전화기가 유틸 상태로 머물러야 하는 시간의 길이.</p> <p>시간 초과는 다음과 같은 상황에서 발생합니다.</p> <ul style="list-style-type: none"> <li>• 예정대로 전화기가 절전 플러스 모드인 상태에서, 전화기 사용자가 선택 키를 눌러 절전 플러스 모드에서 벗어난 경우</li> <li>• 연결된 스위치에서 전화기의 전원을 다시 켰을 때</li> <li>• 전화 끄기 시간이 되었으나 전화기를 사용 중일 때</li> </ul> <p>필드의 범위는 20~1440분입니다.</p> <p>기본값은 60분입니다.</p>
알림음 사용	<p>활성화되면 전화기에 [전화 끄기 시간] 필드에 지정한 시간보다 10분 전에 알림음을 재생하게 합니다.</p> <p>알림음으로는 전화기 벨소리를 사용하며, 경고 시간 10분 동안 몇 차례 짧게 재생됩니다. 알람 벨소리는 사용자가 정한 소리 크기로 재생됩니다. 알림음은 다음과 같은 순서로 울립니다.</p> <ul style="list-style-type: none"> <li>• 전원이 꺼지기 10분 전, 벨소리가 4번 재생됩니다.</li> <li>• 전원이 꺼지기 7분 전, 벨소리가 4번 재생됩니다.</li> <li>• 전원이 꺼지기 4분 전, 벨소리가 4번 재생됩니다.</li> <li>• 전원이 꺼지기 30초 전에 벨소리가 15번 또는 전화기 전원이 꺼질 때까지 재생됩니다.</li> </ul> <p>이 확인란은 [절전 플러스 활성화] 목록 상자에서 1일 이상을 선택한 경우에만 적용됩니다.</p>
EnergyWise 도메인	<p>전화기가 소속된 EnergyWise 도메인입니다.</p> <p>이 필드의 최대 길이는 127자입니다.</p>
EnergyWise 비밀	<p>EnergyWise 도메인에서 엔드포인트와 통신할 때 사용하는 보안 비밀 암호입니다.</p> <p>이 필드의 최대 길이는 127자입니다.</p>



필드	설명
EnergyWise 오버라이드 허용	<p>이 확인란은 EnergyWise 도메인 컨트롤러 정책에서 전화기로 전력 수준 업데이트를 전송하도록 허용할 것인지 여부를 결정합니다. 다음과 같은 조건이 적용됩니다.</p> <ul style="list-style-type: none"> <li>• [절전 플러스 활성화] 필드에서 1일 이상을 선택해야 합니다.</li> <li>• EnergyWise에서 오버라이드를 전송할 때에도 Cisco Unified Communications Manager Administration의 설정은 실행됩니다.</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>• EnergyWise에서 전화기에 20:00(오후 8:00)에 전화를 끄라고 지시하면, 이러한 지시 사항은 구성된 전화 켜기 시간인 오전 6:00까지 효력이 있습니다(전화에 사용자 개입이 전혀 없다고 가정할 경우).</li> <li>• 오전 6:00시가 되면 전화기가 켜지고 Unified Communications Manager Administration 설정에서 전력 수준 변경 내용을 수신하여 작동을 시작합니다.</li> <li>• 전화기의 전력 수준을 다시 변경하려면, EnergyWise에서 새로운 전력 수준 변경 명령을 다시 내려야 합니다.</li> </ul> <p>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.</p>

단계 4 저장을 선택합니다.

단계 5 구성 적용을 선택합니다.

단계 6 전화를 다시 시작합니다.

## 방해사절 설정

방해사절(DND)을 설정하면, 전화벨이 울리는 동안 벨소리가 나지 않거나 어떤 종류의 시각적 또는 청각적 알림도 일어나지 않습니다.

방해사절(DND)을 활성화하면 전화기 화면의 헤더 섹션 색상이 바뀌고 방해사절이 전화기에 표시됩니다.

선택 기능 중 하나인 방해사절이 포함된 전화기 버튼 템플릿으로 전화를 구성할 수 있습니다.

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.

DND가 설정되어 있을 때는 우선 순위(MLPP)가 높은 통화가 이 전화기에서 울리도록 하려면 통화 거부를 선택하지 마십시오.

- 방해사절 착신 전화 알림: 이러한 유형의 알림을 선택하면, 방해사절이 활성화되었을 때 걸려오는 전화에 대해 전화기에서 알림음이 울립니다.

참고 이 매개 변수는 [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](#), xvii 페이지

## 상담사 인사말 활성화

상담사는 상담사 인사말 기능을 사용하여 상담사가 발신자와 대화를 시작하기 전에 고객 통화와 같은 통화 시작 시 재생되는 사전 녹음된 인사말을 만들고 업데이트할 수 있습니다. 상담사는 필요에 따라 하나 또는 여러 개의 인사말을 사전 녹음하고, 인사말을 작성하여 업데이트할 수 있습니다.

고객이 전화를 걸면 상담사와 발신자 모두에게 사전 녹음된 인사말이 들립니다. 인사말이 끝나거나 인사말 도중 전화에 응답할 수 있을 때까지 상담사는 음소거 상태를 유지할 수 있습니다.

전화기에 지원되는 모든 코덱이 상담사 인사말 통화에 지원됩니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서의 참여 및 프라이버시 정보를 참조하십시오.

## 프로시저

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

단계 2 구성할 IP 전화기를 찾습니다.

단계 3 [장치 정보 레이아웃] 창을 스크롤하여 내장 브리지를 켜기 또는 기본 상태로 설정합니다.

단계 4 저장을 선택합니다.

단계 5 브리지 설정을 확인합니다.

- a) 시스템 > 서비스 매개 변수를 선택합니다.
- b) 적절한 서버와 서비스를 선택합니다.
- c) [클러스터 전역 매개 변수(장치 - 전화기)] 창을 스크롤하여 내장 브리지 활성화를 켜기로 설정합니다.
- d) 저장을 선택합니다.

#### 관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## 모니터링 및 녹음 설정

모니터링 및 녹음 기능을 사용하면 감독자가 조용히 활성 통화를 모니터링할 수 있습니다. 통화의 양측 누구도 감독자의 소리를 들을 수 없습니다. 사용자는 통화가 모니터링되는 동안 알림음을 들을 수도 있습니다.

통화에 대한 보안이 이루어지면 잠금 아이콘이 표시됩니다. 발신자는 통화가 모니터링되고 있음을 알리는 알림음을 들을 수도 있습니다. 통화가 연결된 당사자는 통화에 대한 보안이 이루어지고 통화 내용이 모니터링되고 있음을 알리는 알림음을 들을 수도 있습니다.

활성 통화를 모니터링하거나 녹음할 때, 사용자가 인터콤 전화를 받거나 걸 수 있습니다. 그런데 이처럼 사용자가 인터콤 전화를 걸면, 활성 통화가 보류 상태가 됩니다. 그리고 이로 인해 녹음 세션이 종료되거나 모니터링 세션이 중단됩니다. 모니터링 세션을 다시 시작하려면 모니터링되던 사람이 통화를 재시작해야 합니다.

모니터링 및 녹음에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

다음 절차를 수행하면 사용자를 표준 모니터링 사용자 그룹에 추가할 수 있습니다.

#### 시작하기 전에

Cisco Unified Communications Manager는 모니터링 및 녹음 기능을 지원하도록 구성해야 합니다.

#### 프로시저

- 단계 1 Cisco Unified Communications Manager Administration에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.
- 단계 2 [표준 CTI 통화 모니터링 허용 사용자 그룹]과 [표준 CTI 통화 녹음 허용 사용자 그룹]을 선택합니다.
- 단계 3 선택한 항목 추가를 클릭합니다.
- 단계 4 사용자 그룹에 추가를 클릭합니다.
- 단계 5 [애플리케이션 사용자 제어 장치] 목록에 사용자 전화기를 추가합니다.
- 단계 6 저장을 선택합니다.

관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 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.
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.

## 통화 목록에 대한 BLF 활성화

[통화 목록에 대한 BLF] 필드는 [회사 디렉터리 회선 상태] 기능을 제어합니다.

## 프로시저

단계 1 Cisco Unified Communications Manager Administration에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 2 [통화 목록에 대한 BLF] 필드에서 기능을 활성화 또는 비활성화합니다.

이 기능은 기본적으로 비활성화됩니다.

제품별 구성 영역에 설정한 매개 변수는 다양한 장치에 대한 [장치 구성] 창과 [엔터프라이즈 전화기 구성] 창에도 나타날 수 있습니다. 다른 창에도 동일한 매개 변수를 설정하면, 우선 적용되는 설정은 다음 순서에 따라 결정됩니다.

1. [장치 구성] 창 설정
2. [일반 전화기 프로파일] 창 설정
3. [엔터프라이즈 전화기 구성] 창 설정

단계 3 저장을 선택합니다.

## 스위치 및 PC 포트를 위한 EEE(Energy Efficient Ethernet) 설정

IEEE 802.3az EEE(Energy Efficient Ethernet)는 네트워크 인터페이스의 중요한 기능을 제한하지 않고도 에너지 사용을 줄일 수 있는 방법을 제공하는 IEEE 802.3 표준의 확장 버전입니다. 구성 가능한 EEE를 통해 관리자는 개인 컴퓨터 포트 및 스위치 포트의 EEE 기능을 제어할 수 있습니다.



참고 관리자들은 모든 해당 UCM 페이지에서 [무시] 확인란이 선택되었거나 EEE가 기능하지 않음을 확인해야 합니다.

관리자는 다음 두 가지 매개 변수로 EEE 기능을 제어합니다.

- **EEE(Energy Efficient Ethernet):** PC P포트: 개인 컴퓨터와 매끄럽게 연결해 줍니다. 관리자는 [활성화됨] 또는 [비활성화됨] 옵션을 선택하여 기능을 제어할 수 있습니다.
- **EEE(Energy Efficient Ethernet):** 스위치 포트: 개인 컴퓨터와 매끄럽게 연결해 줍니다.

자세한 내용은 다음을 참조하십시오. [제품별 구성, 146 페이지](#)

## 프로시저

단계 1 Cisco Unified Communications Manager Administration에서 다음 창 중 하나를 선택합니다.

- 장치 > 전화기
- 장치 > 장치 설정 > 일반 전화기 프로파일

- 시스템 > 엔터프라이즈 전화기 구성

여러 개의 창에 매개 변수를 구성하는 경우 우선 순위의 순서는 다음과 같습니다.

1. 장치 > 전화기
2. 장치 > 장치 설정 > 일반 전화기 프로파일
3. 시스템 > 엔터프라이즈 전화기 구성

단계 2 필요한 경우 전화기를 검색합니다.

단계 3 **EEE(Energy Efficient Ethernet): PC 포트** 및 **EEE(Energy Efficient Ethernet): 스위치 포트** 필드를 설정합니다.

- EEE(Energy Efficient Ethernet): PC 포트
- EEE(Energy Efficient Ethernet): 스위치 포트

단계 4 저장을 선택합니다.

단계 5 구성 적용을 선택합니다.

단계 6 전화기를 다시 시작합니다.

## RTP/sRTP 포트 범위 설정

SIP 프로파일에 RTP(Real-Time Transport Protocol) 및 sRTP(Real-Time Transport Protocol) 포트 값을 구성합니다. RTP 및 sRTP 포트 값 범위는 2048~65535로, 기본 범위는 16384~32764입니다. RTP 및 sRTP 포트 범위에 속한 일부 포트 값은 다른 전화기 서비스에 지정됩니다. RTP 및 sRTP에는 이러한 포트를 구성할 수 없습니다.

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

프로시저

단계 1 장치 > 장치 설정 > **SIP** 프로파일을 선택합니다.

단계 2 사용할 검색 조건을 선택하고 검색을 클릭합니다.

단계 3 수정할 프로파일을 선택합니다.

단계 4 포트 범위의 시작과 끝이 포함되도록 [미디어 포트 시작]과 [미디어 포트 중지]를 설정합니다.

다음 목록에는 다른 전화기 서비스에서 사용하기 때문에 RTP 및 sRTP에는 사용할 수 없는 UDP 포트가 나와 있습니다.

포트 **4051**

PFS(Peer Firmware Sharing) 기능에 사용함

**포트 5060**

SIP over UDP 전송에 사용함

포트 범위, **49152~53247**

로컬 단기 포트에 사용함

포트 범위, **53248~65535**

VxC 단일 터널 VPN 기능에 사용함

단계 5 저장을 클릭합니다.

단계 6 구성 적용을 클릭합니다.

---

**관련 항목**

[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## 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 Expressway를 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.

Expressway를 통한 모바일 및 Remote Access는 고급 회선 모드를 지원합니다.

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 섹션에는 Expressway를 통한 모바일 및 Remote Access에 대한 다양한 구축 시나리오가 나와 있습니다.

온-프레미스 사용자는 엔터프라이즈 네트워크에 로그인합니다.

Expressway를 통한 모바일 및 Remote Access이 구축된 후에 온-프레미스이면 엔터프라이즈 네트워크에 로그인합니다. 전화기는 네트워크를 감지하고 Cisco Unified Communications Manager에 등록합니다.

오프-프레미스 사용자는 엔터프라이즈 네트워크에 로그인합니다.

사용자가 사무실 밖에 있으면 전화기가 오프-프레미스 모드에 있음을 감지합니다. Expressway를 통한 모바일 및 Remote Access 로그인 창이 나타나고 회사 네트워크에 연결됩니다.

다음에 유의하십시오.

- 사용자가 네트워크에 연결하려면 유효한 서비스 도메인, 사용자 이름 및 암호가 필요합니다.



- 회사 네트워크에 액세스하려면 서비스 모드를 재설정하여 대체 TFTP 설정을 지웁니다. 이렇게 하면 대체 TFTP 서버 설정을 지워 전화기가 오프프레미스 네트워크를 감지하여 전화기가 VPN 연결을 설정하는 것을 중지할 수 있습니다. 처음으로 전화를 구축하는 경우 이 단계를 건너뛰니다.
- 사용자가 네트워크 라우터에 DHCP 옵션 150 또는 옵션 66을 활성화했다면, 회사 네트워크에 로그인하지 못할 수도 있습니다. MRA 모드로 들어가려면 서비스 모드를 재설정합니다.

오프-프레미스 사용자는 **VPN**을 통해 엔터프라이즈 네트워크에 로그인

사용자가 오프-프레미스에 있으면 Expressway를 통한 모바일 및 Remote Access를 구축한 후, VPN을 사용하여 엔터프라이즈 네트워크에 로그인합니다.

전화기에 오류가 발생할 경우 기본 재설정을 수행하여 전화기 구성을 재설정합니다.

사용자는 대체 TFTP 설정을 구성해야 합니다(관리자 설정 > 네트워크 설정 > **IPv4**, 필드 대체 **TFTP 서버 1**).

관련 항목

[기본 재설정](#), 279 페이지

## 미디어 경로 및 상호 연결 설정 지원

상호 연결 설정(ICE)을 구축하여 방화벽이나 네트워크 주소 변환(NAT)을 통과하는 모바일 및 Remote Access(MRA) 호출의 안정성을 향상시킬 수 있습니다. ICE는 NAT 서비스 주위의 릴레이를 사용하여 호출에 가장 적합한 미디어 경로를 선택하는 선택적 구축입니다.

보조 Turn Server 및 Turn Server 장애 조치는 지원되지 않습니다.

MRA 및 ICE에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서, 릴리스 12.0(1) 이상을 참조하십시오. 또한 IETF(Internet Engineering Task Force) 설명 요청 문서에서 추가 정보를 찾을 수 있습니다.

- 릴레이를 사용한 NAT 주변 탐색: NAT(STUN)에 대한 세션 탐색 유틸리티에 대한 릴레이 확장 (RFC 5766)
- 대화형 연결 설정 (ICE): 제공/응답 프로토콜에 대한 네트워크 주소 변환(NAT) 통과를 위한 프로토콜 (RFC 5245)

## 다음에서 사용 가능한 전화기 기능: Expressway를 통한 모바일 및 Remote Access

Expressway를 통한 모바일 및 Remote Access는 Cisco 모바일 및 원격 사용자를 위해 협업 서비스에 안전하고 VPN이 없는 액세스를 제공합니다. 하지만 이는 네트워크 보안을 유지하기 위해 몇 가지 전화기 기능에 대한 액세스를 제한합니다.

다음 목록은 Expressway를 통한 모바일 및 Remote Access와 함께 사용할 수 있는 전화기 기능을 나타낸 것입니다.

다음에서 사용 가능한 전화기 기능: **Expressway**를 통한 모바일 및 **Remote Access**

표 34: 기능 지원 및 **Expressway**를 통한 모바일 및 **Remote Access**

전화기 기능	전화기 펌웨어 릴리스
단축 다이얼	10.3(1) 이상
가장 오래된 전화에 응답	11.5(1)SR1 이상
지원된 직접 통화 지정보류	10.3(1) 이상
자동 응답	11.5(1)SR1 이상
참여 및 회의끼기	11.5(1)SR1 이상
BLF(통화 중 램프 필드)	10.3(1) 이상
BLF(통화 중 램프 필드) 당겨받기	10.3(1) 이상
BLF(통화 중 램프 필드) 단축 다이얼	10.3(1) 이상
콜백	10.3(1) 이상
통화 착신 전환	10.3(1) 이상
통화 착신 전환 알림	10.3(1) 이상
통화 지정보류	10.3(1) 이상
통화 당겨받기	10.3(1) 이상
Cisco 통합 서비스 가용성	11.5(1)SR1 이상
클라이언트 액세스 라이선스(CAL)	11.5(1)SR1 이상
전화회의	10.3(1) 이상
전화회의 목록/참가자 제거	11.5(1)SR1 이상
회사 디렉터리	11.5(1)SR1 이상
CTI 애플리케이션(CTI 제어됨)	11.5(1)SR1 이상
호연결	10.3(1) 이상
통화 전환 보류	10.3(1) 이상
벨소리 구분	11.5(1)SR1 이상
전환	10.3(1) 이상
고급 회선 모드	12.1(1) 이상
전환	10.3(1) 이상

전화기 기능	전화기 펌웨어 릴리스
강제 액세스 코드 및 클라이언트 매터 코드	11.5(1)SR1 이상
그룹 통화 당겨받기	10.3(1) 이상
보류/보류해제	10.3(1) 이상
보류 복귀	10.3(1) 이상
지정전환	10.3(1) 이상
참가	10.3(1) 이상
MCID(장난 전화 발신자 ID)	11.5(1)SR1 이상
회의개설 전화회의	10.3(1) 이상
메시지 대기 중 표시기	10.3(1) 이상
모바일 연결	10.3(1) 이상
모바일 음성 액세스	10.3(1) 이상
MLPP(Multilevel Precedence and Preemption)	11.5(1)SR1 이상
복수 회선	11.5(1)SR1 이상
대기 중 음악	10.3(1) 이상
음소거	10.3(1) 이상
네트워크 프로필(자동)	11.5(1)SR1 이상
오프 훅 다이얼링	10.3(1) 이상
온 훅 전화걸기	10.3(1) 이상
플러스(+) 다이얼	10.3(1) 이상
프라이버시	11.5(1)SR1 이상
PLAR(Private Line Automated Ringdown)	11.5(1)SR1 이상
재다이얼	10.3(1) 이상
단축 다이얼(일시 중지를 지원하지 않음)	10.3(1) 이상
서비스 URL 버튼	11.5(1)SR1 이상
호전환	10.3(1) 이상
URI(Uniform Resource Identifier) 전화 걸기	10.3(1) 이상

## 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 매개 변수를 활성화하면, 이 정보를 다시 입력할 필요가 없도록 사용자 로그인 자격 증명이 저장됩니다. 이 매개 변수는 기본적으로 비활성화되어 있습니다.

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

관련 항목

[전화기 기능 구성](#), 144 페이지

[제품별 구성](#), 146 페이지

## MRA 로그인용 QR 코드 생성

카메라가 있는 전화기를 사용하는 사용자는 수동으로 서비스 도메인 및 사용자 이름을 입력하는 대신, QR 코드를 스캔하여 MRA에 로그인할 수 있습니다.

프로시저

---

**단계 1** QR 코드 생성자를 사용하여 서비스 도메인 또는 쉼표로 구분한 서비스 도메인과 사용자 이름을 포함하는 QR 코드를 생성합니다. 예: mra.example.com 또는 mra.example.com,username.

**단계 2** QR 코드를 인쇄하고 사용자에게 제공합니다.

---

## 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 매개 변수와 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 매개 변수를 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 URL을 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.
- 

## 듀얼 बैं크 정보 설정

듀얼 बैं크 정보를 설정하려면 다음 단계를 따르십시오.

### 프로시저

- 
- 단계 1 Cisco Unified Communications Manager Administration에서 장치 > 장치 기본값을 선택합니다.

단계 2 [비활성 로드 정보] 필드의 로드 정보를 확인합니다.

단계 3 벌크 관리 > 가져오기/내보내기 > 내보내기 > 장치 기본값을 선택하고 내보내기 작업을 예약합니다.

단계 4 내보낸 tar 파일을 다운로드하고 압축 해제(untar)합니다.

단계 5 내보낸 CSV 파일의 파일 형식을 확인하고 CSV 파일에 올바른 값을 포함한 [비활성 로드 정보] 열이 있는지 확인합니다.

참고 CSV 파일 값은 Cisco Unified Communications Manager Administration 창의 장치 기본값 값과 일치해야 합니다.

## 지정보류 모니터링

지정보류 모니터링은 Cisco IP 전화기에서 통화를 지정보류할 때만 지원됩니다. 그런 다음 지정보류 모니터링에서 지정보류된 통화를 모니터링합니다. 지정보류 모니터링 통화 버블은 지정보류된 통화가 지정보류된 통화를 검색하거나 중단할 때까지 지워지지 않습니다. 이 지정보류된 통화는 통화를 지정보류한 전화기에서 동일한 통화 버블을 사용하여 검색할 수 있습니다.

### 지정보류 모니터링 타이머 설정

Cisco Unified Communications Manager Administration은 지정보류 모니터링에 대한 세 가지 클러스터 수준 서비스 타이머 매개 변수인 지정보류 모니터링 복귀 타이머, 지정보류 모니터링 정기 복귀 타이머 및 지정보류 모니터링 착신 전환 검색 없음 타이머를 제공합니다. 각 서비스 매개 변수에는 기본 값이 포함되며 특별한 구성이 필요하지 않습니다. 이러한 타이머 매개 변수는 지정보류 모니터링에만 적용되며, 통화 지정보류 표시 타이머 및 통화 지정보류 복귀 타이머는 지정보류 모니터링에 사용되지 않습니다. 해당 매개 변수에 대한 설명은 다음 표를 참조하십시오.

Cisco Unified Communications Manager 서비스 매개 변수 페이지에서 타이머를 구성합니다.

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 시스템 > 서비스 매개 변수를 선택합니다.

단계 2 [클러스터 수준 매개 변수](기능 - 일반) 창에서 [지정보류 모니터링 복귀 타이머], [지정보류 모니터링 정기 복귀 타이머] 및 [지정보류 모니터링 착신 전환 검색 없음 타이머] 필드를 업데이트합니다.

표 35: 지정보류 모니터링 서비스 매개 변수

필드	설명
지정보류 모니터 복귀 타이머	기본값은 60초입니다. 이 매개 변수는 Cisco Unified Communications Manager에서 사용자 지정보류한 통화를 검색하라는 메시지를 표시하기 전까지 대기하는 시간(초)을 결정하는 데 사용됩니다. 이 타이머는 사용자가 전화기에서 [지정보류]를 누르면 시작되고, 타이머가 만료되면 링이 발행됩니다.  [디렉터리 번호 구성] 창의 [지정보류 모니터링] 섹션에서 이 서비스 매개 변수가 회선당 지정하는 값을 재지정할 수 있습니다(Cisco Unified Communications Manager Administration > 통화 라우팅 > 디렉터리 번호를 선택함). 지정보류 모니터링 정기 복귀 타이머 서비스 매개 변수 지정하는 정기 복귀 간격을 즉시 사용하려면 값을 0으로 지정합니다. (다음에 나타난 설정 하십시오) 예를 들어 이 매개 변수를 0으로 설정하고 지정보류 모니터링 정기 복귀 타이머를 설정하면, 사용자에게 지정보류된 통화에 대해 즉시 알리고 이후 지정보류 모니터링 착신 검색 없음 타이머(다음의 설명 참조)가 만료될 때까지 15초마다 알립니다.
지정보류 모니터링 정기 복귀 타이머	기본값은 30초입니다. 이 매개 변수는 Cisco Unified Communications Manager에서 사용자가 지정보류되었음을 알리기 전에 대기하는 간격(초)을 결정합니다. 사용자가 지정보류된 통화에 연결하려면 이러한 메시지가 표시될 때 오프 hook 상태로 전환하기만 하면 됩니다. Cisco Unified Communications Manager는 지정보류된 통화가 남아 있는 경우 지정보류 모니터링 착신 검색 없음 타이머(다음의 설명 참조)가 지정하는 시간이 만료될 때까지 사용자에게 지정보류된 통화에 대해 계속 알립니다. 지정보류된 통화에 대한 메시지가 정기적으로 표시되지 않도록 하려면 0으로 지정합니다.
지정보류 모니터링 착신 전환 검색 없음 타이머	기본값은 300초입니다. 이 매개 변수는 지정보류 [디렉터리 번호 구성] 창에서 지정한 지정보류 모니터링 착신 전환 검색 없음 대상으로 지정보류된 통화를 착신 전환하기 전에 지정보류된 통화를 통지할 시간(초)을 결정합니다(Cisco Unified Communications Manager 관리에 착신 전환 검색 없음 경우에는 통화를 지정보류한 회선으로 반환). 이 매개 변수는 지정보류 모니터링 복귀 서비스 매개 변수가 지정하는 시간이 만료될 때 시작됩니다. 지정보류 모니터링 착신 검색 없음 타이머가 만료되면 통화를 지정보류에서 제거하고 지정된 대상으로 착신 전환하여 회선으로 반환합니다.

## 디렉터리 번호에 대한 지정보류 모니터링 매개 변수 설정

디렉터리 번호 구성 창에는 세 가지 매개 변수를 구성할 수 있는 지정보류 모니터링 영역이 있습니다.

### 프로시저

**단계 1** Cisco Unified Communications Manager Administration에서 통화 라우팅 > 디렉터리 번호를 선택합니다.

**단계 2** 다음 표에 설명된 대로 지정보류 모니터링 필드를 설정합니다.



표 36: 지정보류 모니터링 매개 변수

필드	설명
지정보류 모니터 착신 전환 검색 없음 외부 대상	피지정보류자가 외부인이면 지정보류의 [지정보류 모니터링 착신 전환 외부 검색 대상 없음] 매개 변수에 지정된 대상으로 통화를 착신 전환합니다. [착신 전환 외부 검색 대상 없음] 필드 값이 비어 있는 경우에는 피지정보류자가 지정보류 회선으로 재전송됩니다.
지정보류 모니터 착신 전환 검색 없음 내부 대상	피지정보류자가 내부 통화자이면 지정보류의 [지정보류 모니터링 착신 전환 내부 검색 대상 없음] 매개 변수에 지정된 대상으로 통화를 착신 전환합니다. [착신 전환 내부 검색 대상 없음]이 비어 있는 경우에는 피지정보류자가 지정보류 회선으로 재전송됩니다.
지정보류 모니터 복귀 타이머	이 매개 변수는 Cisco Unified Communications Manager에서 사용자에게 지정보류한 통화를 검색하라는 메시지를 표시하기 전까지 대기하는 시간(초)을 결정하는 데 사용됩니다. 이 타이머는 사용자가 전화기에서 [지정보류]를 누르면 시작되고, 타이머가 만료되면 미리 알림이 발행됩니다.  기본값: 60초  0이 아닌 값을 구성하면 이 값이 [서비스 파라미터] 창에서 설정한 이 파라미터 값을 오버라이드합니다. 그러나 여기서 값을 0으로 구성하면 [서비스 파라미터] 창에 있는 값이 사용됩니다.

## 헌트 목록에 대한 지정보류 모니터링 설정

헌트 목록을 통해 전송된 통화가 지정보류되면 지정보류 모니터링 착신 전환 검색 없음 타이머가 만료될 때 헌트 파일럿 지정보류 모니터링 착신 전환 검색 대상 없음 매개 변수 값(비어 있지 않은 경우)이 사용됩니다.

### 프로시저

**단계 1** Cisco Unified Communications Manager Administration에서 통화 라우팅 > 경로/헌트 > 헌트 파일럿을 선택합니다.

**단계 2** 헌트 파일럿 지정보류 모니터링 착신 전환 검색 대상 없음 매개 변수를 설정합니다.

헌트 파일럿 지정보류 모니터링 착신 전환 검색 대상 없음 매개 변수 값이 비어 있는 경우에는 지정보류 모니터링 착신 전환 검색 없음 타이머가 만료될 때 통화가 [디렉터리 번호 구성] 창에 구성되어 있는 대상으로 착신 전환됩니다.

## 오디오 및 비디오 포트 범위 설정

QoS(Quality of Service)를 향상시키기 위해 오디오 및 비디오 트래픽을 다른 RTP 포트 범위로 보낼 수 있습니다.

다음 필드는 Cisco Unified Communications Manager Administration의 포트 범위를 제어합니다.

- 오디오 포트
  - 미디어 포트 시작(기본값:16384)
  - 미디어 포트 중지(기본값:32766)
- 비디오 포트
  - 비디오(비디오 시작 포트 설정)를 시작합니다.
    - 최소값: 2048
    - 최대값: 65535
  - 비디오(비디오 중지 포트 설정)를 중지합니다.
    - 최소값: 2048
    - 최대값: 65535

비디오 포트 필드를 구성할 때 다음 규칙이 적용됩니다.

비디오 RTP 포트 시작과 비디오 RTP 포트 중지가 구성되면 전화기는 비디오 트래픽에 대한 비디오 포트 범위 내 포트를 사용합니다. 오디오 트래픽은 미디어 포트를 사용합니다.

오디오 및 비디오 포트 범위가 겹칠 경우 중첩된 포트는 오디오 및 비디오 트래픽을 모두 전달합니다. 비디오 포트 범위가 올바르게 구성되지 않으면 전화기는 오디오 및 비디오 트래픽 모두에 대해 구성된 오디오 포트를 사용합니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

### 프로시저

단계 1 Cisco Unified Communications Manager Administration에서 장치 > 장치 설정 > SIP 프로파일을 선택합니다.

단계 2 오디오 포트 범위에 대한 [미디어 포트 시작]과 [미디어 포트 중지] 필드를 설정합니다.

단계 3 저장을 선택합니다.

단계 4 다음 창 중 하나를 선택합니다.

- 시스템 > 엔터프라이즈 전화기 구성
- 장치 > 장치 설정 > 일반 전화기 프로파일
- 장치 > 전화기 > 전화기 구성

단계 5 필요한 포트 범위에 대해 비디오 RTP 포트 시작 및 비디오 RTP 포트 중지 필드를 설정합니다.

비디오 포트 필드를 구성할 때 다음 규칙이 적용됩니다.

- 비디오 RTP 포트 중지 필드의 값은 비디오 RTP 포트 시작 필드의 값보다 커야 합니다.
- 비디오 RTP 포트 시작 필드와 비디오 RTP 포트 중지 필드의 차이는 16 이상이어야 합니다.

단계 6 저장을 선택합니다.

관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## Cisco IP Manager Assistant 설정

Cisco IPMA(Cisco IP Manager Assistant)에서는 관리자와 보조자가 통화를 보다 효율적으로 처리할 수 있도록 도와주는 통화 라우팅 기능 및 기타 통화 관리 기능을 제공합니다.

사용자가 IPMA 서비스를 사용하려면 Cisco Unified Communications Manager에 이러한 서비스를 구성해야 합니다. IPMA 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서를 참조하십시오.

IPMA에는 다음과 같은 3가지 주요 구성 요소가 있습니다.

관리자

관리자에게 통화 라우팅 서비스에 의해 차단된 통화가 있습니다.

보조자

도우미가 관리자를 대신하여 통화를 처리합니다.

**Assistant Console**

어시스턴트 콘솔은 보조자가 작업을 수행하고 대부분의 기능을 관리하는 데 사용할 수 있는 데스크톱 애플리케이션입니다.

IPMA는 프록시 회선 지원 및 공유 회선 지원의 두 가지 작동 모드를 지원합니다. 두 모드 모두 관리자에 대해 회선당 다중 통화를 지원합니다. IPMA 서비스는 클러스터에서 프록시 회선과 공유 회선 지원을 모두 지원합니다.

공유 회선 모드에서 관리자와 보조자는 디렉터리 번호를 공유하고 통화를 공유 회선에서 처리합니다. 공유 회선으로 전화가 수신되면 관리자 전화기와 보조자 전화기에 벨이 울립니다. 공유 회선 모드는 기본 보조자 선택, 보조자 시계, 통화 필터링 또는 모든 통화 전환을 지원하지 않습니다.

공유 회선 모드에서 Cisco IPMA를 구성할 경우 관리자와 보조자는 디렉터리 번호(예: 1701)를 공유합니다. 보조자는 관리자를 위해 공유된 디렉터리 번호에서 통화를 처리합니다. 관리자가 디렉터리 번호 1701에서 전화를 받으면 관리자 전화기와 보조자 전화기가 모두 울립니다.

공유 회선 모드에서는 기본 보조자 선택, 보조자 감시, 통화 필터링 및 모든 통화 전환을 포함하여 일부 IPMA 기능을 사용할 수 없습니다. 보조자는 Assistant Console 애플리케이션에서 이러한 기능을 보거나 액세스할 수 없습니다. 보조자 전화기에는 모두 전환 기능을 위한 소프트키가 없습니다. 관리자 전화기에는 보조자 감시, 통화 차단 또는 모두 전환 기능을 위한 소프트키가 없습니다.

사용자 장치에서 공유 회선 지원에 액세스하려면 먼저 Cisco Unified Communications Manager Administration을 사용하여 Cisco IP Manager Assistant 서비스를 구성하고 시작해야 합니다.

프록시 회선 모드에서 보조자는 프록시 번호를 사용하여 관리자 대신 통화를 처리합니다. 프록시 회선 모드는 모든 IPMA 기능을 지원합니다.

Cisco IPMA를 프록시-회선 모드로 구성하는 경우 관리자와 보조자가 디렉터리 번호를 공유하지 않습니다. 보조자는 프록시 번호를 사용하여 관리자의 통화를 처리합니다. 프록시 번호는 관리자의 디렉터리 번호입니다. 시스템에서 선택한 대체 번호이며 보조자가 관리자 통화를 처리하는 데 사용됩니다. 프록시-회선 모드에서 관리자와 보조자는 기본 보조자 선택, 보조자 감시, 통화 필터링, 모두 전환 등을 비롯해 IPMA에서 사용 가능한 모든 기능에 액세스할 수 있습니다.

사용자 장치에서 프록시 회선 지원에 액세스하려면 먼저 Cisco Unified Communications Manager Administration을 사용하여 Cisco IP Manager Assistant 서비스를 구성하고 시작해야 합니다.

소프트키 및 전화기 서비스를 통해 IPMA 기능에 액세스합니다. 소프트키 템플릿은 Cisco Unified Communications Manager에서 구성됩니다. IPMA는 다음 표준 소프트키 템플릿을 지원합니다.

#### 표준 관리자

프록시 모드에 대해 관리자를 지원합니다.

#### 표준 공유 모드 관리자

공유 모드에 대해 관리자를 지원합니다.

#### 표준 보조자

프록시 또는 공유 모드에서 보조자를 지원합니다.

다음 표에서는 소프트키 템플릿에서 사용할 수 있는 소프트키를 설명합니다.

표 37: IPMA 소프트키

소프트키	통화 상태	설명
재전송	벨울림, 연결됨, 보류 중	선택한 통화를 미리 구성된 대상으로 전환합니다.
차단	모든 상태	보조자 전화기의 전호를 관리자의 전화기로 전환하여 자동 응답합니다.
감시 설정	모든 상태	보조자가 처리 중인 통화의 상태를 봅니다.
전환(VM)	벨울림, 연결됨, 보류 중	선택한 통화를 관리자의 음성 메일로 재전송합니다.
모두 전환	모든 상태	관리자에게 전송된 모든 통화를 미리 구성된 대상으로 전환합니다.



참고 차단, 감시설정 및 모두 전환은 프록시 회선 모드에서 관리자 전화기에 대해서만 구성되어야 합니다.

다음 절차는 필수 단계에 대한 개요입니다.

프로시저

- 단계 1 전화기와 사용자를 구성합니다.
- 단계 2 전화기를 사용자에게 연결합니다.
- 단계 3 [서비스 활성화] 창에서 Cisco IP Manager Assistant 서비스를 활성화합니다.
- 단계 4 시스템 관리 매개 변수를 구성합니다.
- 단계 5 필요한 경우, IPMA 클러스터 수준 서비스 매개 변수를 구성합니다.
- 단계 6 (선택 사항) 사용자 CAPF 프로파일을 구성합니다.
- 단계 7 (선택 사항) 보안을 위한 IPMA 서비스 매개 변수를 구성합니다.
- 단계 8 IPMA 서비스를 중지하고 다시 시작합니다.
- 단계 9 소프트키 템플릿을 구성하여 전화기 매개 변수, 관리자 및 보조자 설정을 구성합니다.
- 단계 10 Cisco Unified Communications Manager Assistant 애플리케이션을 구성합니다.
- 단계 11 다이얼 규칙을 구성합니다.
- 단계 12 Assistant Console 애플리케이션을 설치합니다.
- 단계 13 관리자 및 보조자 콘솔 애플리케이션을 구성합니다.

## Visual VoiceMail 설정

Visual Voicemail은 Cisco Unified Communications Manager Administration에서 모든 Cisco IP 전화기 또는 개별 사용자 또는 사용자 그룹에 대해 구성됩니다.



참고 구성 정보는 <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>에 있는 Cisco Visual Voicemail 설명서를 참조하십시오.

Visual Voicemail 클라이언트는 Cisco IP 전화기 8800 전화기의 MIDlet으로 지원되지 않습니다.

프로시저

- 단계 1 Cisco Unified Communications Manager Administration에서 장치 > 장치 설정 > 전화 서비스를 선택합니다.
- 단계 2 새로 추가를 선택하여 Visual Voicemail에 대한 새 서비스를 만듭니다.

단계 3 IP Phone 서비스 구성 창에서 각 필드에 다음 정보를 입력합니다.

- 서비스 이름—**VisualVoiceMail**을 입력합니다.
- ASCII 서비스 이름—**VisualVoiceMail**을 입력합니다.
- 서비스 URL—**Application: Cisco/VisualVoiceMail**로 입력합니다.
- 서비스 범주—폴다운 메뉴에서 **XML** 서비스를 선택합니다.
- 서비스 유형—폴다운 메뉴에서 메시지를 선택합니다.

단계 4 활성화를 선택하고 저장을 클릭합니다.

참고 엔터프라이즈 가입은 선택하지 마십시오.

단계 5 서비스 매개 변수 정보 창에서 새 매개 변수를 클릭하고 각 필드에서 다음 정보를 입력합니다.

- 매개 변수 이름. `voicemail_server`를 입력합니다.
- 매개 변수 표시 이름. `voicemail_server`를 입력합니다.
- 기본값. 기본 Unity Server의 호스트 이름을 입력합니다.
- 매개 변수 설명

단계 6 매개 변수가 필요합니다.를 선택하고 저장을 클릭합니다.

참고 매개 변수가 암호(마스크 내용)입니다.를 선택하지 마십시오.

단계 7 창을 닫고 전화 서비스 구성 창에서 저장을 다시 선택합니다.

## 특정 사용자용 Visual VoiceMail 설정

다음 절차를 사용하여 특정 사용자에 대한 Visual Voicemail을 구성할 수 있습니다.



참고 구성 정보는 <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>에 있는 Cisco Visual 음성 메일 설명서를 참조하십시오.

### 프로시저

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

단계 2 검색 중인 사용자에게 할당된 장치를 선택합니다.

단계 3 관련 링크 드롭다운에서 서비스 가입/가입 해지를 선택하고 이동을 클릭합니다.

단계 4 사용자가 만든 VisualVoiceMail 서비스를 선택한 다음, 다음 > 가입을 선택합니다.

## 사용자 그룹용 Visual Voicemail 설정

Cisco IP 전화기 배치를 Visual Voicemail에 가입한 Cisco Unified Communications Manager에 추가하려면 각 전화기 유형에 대한 BAT 도구 및 각 전화기 템플릿에서 전화기 템플릿을 만드십시오. 그런 다음 Visual Voicemail 서비스에 가입하고 템플릿을 사용하여 전화기를 삽입할 수 있습니다.

Cisco IP 전화기를 이미 등록했고 전화기에서 Visual Voicemail 서비스에 가입하려면 BAT에서 전화기 템플릿을 만들고 템플릿에서 Visual Voicemail 서비스에 가입한 다음 BAT 도구를 사용하여 전화기를 업데이트하십시오.

자세한 내용은 <http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html>의 내용을 참조하십시오.

## 보증된 서비스 SIP

보증된 서비스 SIP(AS-SIP)은 Cisco IP 전화기 및 타사 전화기에 대해 매우 안전한 통화 흐름을 제공하는 기능 및 프로토콜 모음입니다. 다음과 같은 기능 및 AS-SIP 통칭:

- MLPP(Multilevel Precedence and Preemption)
- DSCP(Differentiated Services Code Point)
- TLS(Transport Layer Security) 및 SRTP(Secure Real-time Transport Protocol)
- IPv6(인터넷 프로토콜 버전 6)

AS-SIP은 대개 Multilevel Precedence and Preemption(MLPP)과 함께 사용되어 긴급 상황 중 통화 우선 순위를 지정합니다. MLPP를 사용하여 발신 통화에 우선 순위 수준을 수준 1(낮음)부터 수준 5(높음)까지 할당합니다. 전화를 받으면 통화 우선 순위를 보여주는 우선 순위 아이콘이 전화기에 표시됩니다.

AS-SIP을 구성하려면 Cisco Unified Communications Manager에서 다음 작업을 완료하십시오.

- 다이제스트 사용자 구성 - SIP 요청에 대해 다이제스트 인증을 사용하도록 최종 사용자를 구성합니다.
- SIP 전화기 보안 포트 구성 - Cisco Unified Communications Manager는 이 포트를 사용하여 TLS를 통한 SIP 회선 등록을 위한 SIP 전화를 수신합니다.
- 서비스 다시 시작 - 보안 포트를 구성한 후 Cisco Unified Communications Manager 및 Cisco CTL Provider 서비스를 다시 시작합니다. AS-SIP에 대한 SIP 프로파일 구성 - AS-SIP 엔드포인트와 SIP 트렁크를 위한 SIP 설정을 사용하여 SIP 프로파일을 구성합니다. 전화기 특정 매개 변수는 타사 AS-SIP 전화기에 다운로드되지 않으며, Cisco 유니파이드 Manager에만 사용됩니다. 타사 전화기에서는 동일한 설정을 로컬로 구성해야 합니다.
- AS-SIP용 전화기 보안 프로파일 구성 - 전화기 보안 프로파일을 사용하여 TLS, SRTP 및 다이제스트 인증과 같은 보안 설정을 할당할 수 있습니다.
- AS-SIP 엔드포인트 구성 — Cisco IP 전화기 또는 타사 엔드포인트 및 AS-SIP 지원을 구성합니다.

- 장치를 최종 사용과 연결 - 엔드포인트를 사용자와 연결합니다.
- AS-SIP용 SIP 트렁크 보안 프로파일 구성 - SIP 트렁크 보안 프로파일을 사용하여 TLS 또는 다이제스트 인증과 같은 보안 기능을 SIP 트렁크에 할당할 수 있습니다.
- AS-SIP용 SIP 트렁크 구성 - AS-SIP 지원을 사용하여 SIP 트렁크를 구성합니다.
- AS-SIP 기능 구성 - MLPP, TLS, V.150 및 IPv6과 같은 추가 AS-SIP 기능을 구성합니다.

AS-SIP 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager*용 시스템 구성 안내서의 "AS-SIP 엔드포인트 구성" 장을 참조하십시오.

## 전화기를 다중 플랫폼 전화기로 직접 마이그레이션

전환 펌웨어 로드를 사용하지 않고도 한 번에 회사 전화기를 다중 플랫폼 전화기로 쉽게 마이그레이션할 수 있습니다. 서버에서 마이그레이션 라이선스를 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-iphone.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-iphone.html)을 참조해 주십시오.

## MLPP(Multilevel Precedence and Preemption)

MLPP(Multilevel Precedence and Preemption)를 사용하면 응급 상황이나 기타 위기 상황에서 전화 우선 순위를 지정할 수 있습니다. 1~5 범위에 있는 발신 통화에 우선 순위를 할당합니다. 수신 통화에는 통화 우선 순위를 표시하는 아이콘이 표시됩니다. 인증된 사용자는 대상 기지국에 대한 통화 또는 완전히 가입된 TDM 트렁크를 통한 통화를 선점할 수 있습니다.

이 기능은 중요한 조직 및 개인에 대한 높은 순위의 개인 통신을 보장합니다.

MLPP는 주로 보증된 서비스 SIP(AS-SIP)과 함께 사용됩니다. MLPP 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager*용 시스템 구성 안내서의 "MLPP(Multilevel Precedence and Preemption) 구성" 장을 참조하십시오.

## 소프트키 템플릿 설정

*Cisco Unified Communications Manager Administration*을 사용하면 최대 18개의 소프트키를 전화기에서 지원하는 애플리케이션과 연결할 수 있습니다. *Cisco Unified Communications Manager*는 표준 사용자 및 표준 기능 소프트키 템플릿을 지원합니다.

소프트키를 지원하는 애플리케이션에는 이와 관련된 1개 이상의 표준 소프트키 템플릿이 있습니다. 표준 소프트키 템플릿을 복사하고, 이름을 바꾼 후 새 템플릿을 업데이트하여 이 템플릿을 수정합니다. 비표준 소프트키 템플릿을 수정할 수도 있습니다.

소프트키 제어 매개 변수는 전화기의 소프트키가 소프트키 템플릿 기능으로 제어되는 경우 표시됩니다. 소프트키 제어 매개 변수는 필수 필드입니다.

이 기능의 구성에 관한 자세한 내용은 해당 *Cisco Unified Communications Manager* 릴리스용 문서를 참조하십시오.



Cisco IP 전화기가 Cisco Unified Communications Manager Administration의 Softkey Template Configuration(소프트키 템플릿 구성)에서 구성할 수 있는 모든 소프트키를 지원하는 것은 아닙니다. Cisco Unified Communications Manager를 사용하여 제어 정책 구성 설정에서 일부 소프트키를 활성화 하거나 비활성화할 수 있습니다. 다음 표는 소프트키 템플릿에 구성할 수 있는 기능과 소프트키를 나열하고, Cisco IP 전화기에서 지원 여부를 식별합니다.



참고 Cisco Unified Communications Manager를 통해 소프트키 템플릿에 소프트키를 구성할 수 있습니다. 그러나 지원되지 않는 소프트키는 전화기에 표시되지 않습니다.

표 38: 구성 가능한 소프트키

기능	소프트키 템플릿 구성에 구성할 수 있는 소프트키	소프트키로 지원됨
전화받기	전화받기(전화받기)	지원됨
콜백	콜백(콜백)	지원됨
모든 통화 착신 전환	착신 전환(착신전환)	지원됨
통화 지정보류	통화 지정보류(지정보류)	지원됨
통화 당겨받기	당겨받기(당겨받기)	지원됨
참여	참여	지원됨
회의끼기	전화회의 참여	지원됨
전화회의	전화회의(전화회의)	지원됨
전화회의 목록	전화회의 목록(회의인원)	지원됨
전환	지정전환(전환)	지원됨
DND(Do Not Disturb)	방해사절(DND) 전환	지원됨
통화종료	통화 종료(통화종료)	지원됨
그룹 당겨받기	그룹 당겨받기(그룹픽업)	지원됨
보류	보류(보류)	지원됨
힌트 그룹	힌트로그(힌트로그)	지원됨
참가	통화 참가(통화참가)	지원되지 않음

기능	소프트키 템플릿 구성에 구성할 수 있는 소프트키	소프트키로 지원됨
악성 전화 식별	MCID(장난 전화 식별) 전환	지원됨
회의개설	회의개설(회의개설)	지원됨
모바일 연결	이동성(이동성)	지원됨
전화걸기	새 통화(전화걸기)	지원됨
기타 당겨받기	기타 당겨받기(기타픽업)	지원됨
PLK 대기열 지원 통계	대기열 상태	지원되지 않음
QRT(Quality Reporting Tool)	QRT(품질 보고 도구)	지원됨
재다이얼	재다이얼(재다이얼)	지원됨
마지막 전화회의 참가자 제거	마지막 전화회의 참가자 제거(제거)	지원되지 않음
보류해제	보류 해제(보류해제)	지원됨
선택	선택(선택)	지원되지 않음
바로 호출	단축 다이얼(단축 다이얼)	지원됨
호전환	호전환(호전환)	지원됨
비디오 모드 명령	비디오 모드 명령(비디오)	지원되지 않음

### 프로시저

**단계 1** Cisco Unified Communications Manager Administration에서 다음 창 중 하나를 선택합니다.

- 소프트키 템플릿을 구성하려면 장치 > 장치 설정 > 소프트키 템플릿을 선택합니다.
- 소프트키 템플릿을 전화기에 할당하려면 장치 > 전화기를 선택하고 [소프트키 템플릿] 필드를 구성합니다.

**단계 2** 변경 내용을 저장합니다.

### 관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## 전화기 버튼 템플릿

전화기 버튼 템플릿을 사용하면 프로그램 가능 버튼에 단축 다이얼과 통화 처리 기능을 지정할 수 있습니다. 버튼에 할당할 수 있는 통화 처리 기능으로는 응답, 이동 및 모든 통화가 있습니다.

네트워크에 전화기를 등록하기 전에 템플릿을 수정하는 것이 가장 좋습니다. 이렇게 하면 등록 중에 Cisco Unified Communications Manager에서 사용자 정의된 전화기 버튼 템플릿 옵션에 액세스할 수 있습니다.

## 전화기 버튼 템플릿 수정

IP 전화기 서비스 및 회선 버튼 구성에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

프로시저

- 단계 1 Cisco Unified Communications Manager Administration에서 장치 > 장치 설정 > 전화기 버튼 템플릿을 선택합니다.
- 단계 2 찾기를 클릭합니다.
- 단계 3 전화기 모델을 선택합니다.
- 단계 4 복사를 선택하고, 새 템플릿의 이름을 입력한 다음, 저장을 선택합니다.  
[전화기 버튼 템플릿 구성] 창이 열립니다.
- 단계 5 할당하려는 버튼을 확인하고, 해당 회선과 관련된 기능 드롭다운 목록에서 서비스 URL을 선택합니다.
- 단계 6 저장을 선택하여 서비스 URL을 사용하는 새로운 전화기 버튼 템플릿을 작성합니다.
- 단계 7 장치 > 전화기를 선택하고, 전화기의 [전화기 구성] 창을 엽니다.
- 단계 8 [전화기 버튼 템플릿] 드롭다운 목록에서 새 전화기 버튼 템플릿을 선택합니다.
- 단계 9 저장을 선택하여 변경 사항을 저장한 다음, 구성 적용을 선택하여 변경 사항을 구현합니다.  
전화기 사용자는 이제 [셀프 서비스 포털]에 액세스해 전화기 버튼과 서비스를 연결할 수 있습니다.

관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## 모든 통화에 대한 전화기 버튼 템플릿 할당

다중 공유 회선을 사용하는 사용자의 전화기 템플릿에 모든 통화 버튼을 할당합니다.

전화기에 모든 통화 버튼을 구성할 때 사용자는 [모든 통화] 버튼을 사용하여 다음 작업을 수행할 수 있습니다.

- 전화기의 모든 회선에서 현재 통화 통합 목록을 봅니다.
- 전화기의 모든 회선에서 (통화 기록 아래) 모든 부재 중 전화 목록을 봅니다.
- 사용자가 오프 훅할 때 사용자의 기본 회선으로 전화를 겁니다. 모든 통화는 발신 통화에 대해 자동으로 사용자 기본 회선으로 기본 지정됩니다.

#### 프로시저

단계 1 모든 통화 버튼을 포함하려면 전화기 버튼 템플릿을 수정하십시오.

단계 2 전화기에 템플릿을 할당합니다.

## IP 전화기 서비스에 PAB 또는 단축 다이얼 설정

프로그램 가능 버튼과 서비스 URL을 연결하도록 전화기 버튼 템플릿을 수정할 수 있습니다. 이렇게 하면 사용자에게 PAB 및 단축 다이얼에 대한 단일 버튼 액세스 기능이 제공됩니다. 전화기 버튼 템플릿을 수정하기 전에 먼저 PAB 및 단축 다이얼을 IP 전화기 서비스로 구성해야 합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

PAB 및 단축 다이얼을 IP 전화기 서비스로 구성하려면(아직 서비스로 구성되어 있지 않은 경우), 다음 단계를 따르십시오.

#### 프로시저

단계 1 Cisco Unified Communications Manager Administration에서 장치 > 장치 설정 > 전화 서비스를 선택합니다.

[IP Phone 서비스 찾기 및 나열] 창이 표시됩니다.

단계 2 새로 추가를 클릭합니다.

[IP PHone 서비스 구성] 창이 표시됩니다.

단계 3 다음과 같은 설정을 입력합니다.

- 서비스 이름: 개인 주소록을 입력합니다.
- 서비스 설명: 서비스에 대한 선택적 설명을 입력합니다.
- 서비스 URL

PAB의 경우는 다음 URL을 입력합니다.

**http://<Unified CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**

고속 다이얼의 경우는 다음 URL을 입력합니다.

**http://<Unified-CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**

- 보안 서비스 URL

PAB의 경우는 다음 URL을 입력합니다.

**https://<Unified CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab**

고속 다이얼의 경우는 다음 URL을 입력합니다.

**https://<Unified-CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd**

- 서비스 범주: **XML** 서비스를 선택합니다.
- 서비스 유형: 디렉터리를 선택합니다.
- 활성화: 확인란을 선택합니다.

*http://<IP\_address>* 또는 *https://<IP\_address>* (Cisco IP 전화기가 지원하는 프로토콜에 따라 달라짐)

단계 4 저장을 선택합니다.

참고 서비스 URL을 변경하거나 IP 전화기 서비스 매개 변수를 제거하거나 사용자가 가입한 전화기 서비스의 전화기 서비스 매개 변수 이름을 변경하는 경우, 가입 업데이트를 클릭하여 현재 가입한 모든 사용자를 변경 내용으로 업데이트해야 합니다. 그렇지 않으면 사용자가 서비스에 다시 가입하여 정확한 URL을 다시 구축해야 합니다.

관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## PAB 또는 고속 다이얼에 대한 전화기 버튼 템플릿 수정

프로그램 가능 버튼과 서비스 URL을 연결하도록 전화기 버튼 템플릿을 수정할 수 있습니다. 이렇게 하면 사용자에게 PAB 및 단축 다이얼에 대한 단일 버튼 액세스 기능이 제공됩니다. 전화기 버튼 템플릿을 수정하기 전에 먼저 PAB 및 단축 다이얼을 IP 전화기 서비스로 구성해야 합니다.

IP 전화기 서비스 및 회선 버튼 구성에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 장치 > 장치 설정 > 전화기 버튼 템플릿을 선택합니다.

단계 2 찾기를 클릭합니다.

단계 3 전화기 모델을 선택합니다.

단계 4 복사를 선택하고, 새 템플릿의 이름을 입력한 다음, 저장을 선택합니다.

[전화기 버튼 템플릿 구성] 창이 열립니다.

- 단계 5 할당하려는 버튼을 확인하고, 해당 회선과 관련된 기능 드롭다운 목록에서 서비스 **URL**을 선택합니다.
- 단계 6 저장을 선택하여 서비스 URL을 사용하는 새로운 전화기 버튼 템플릿을 작성합니다.
- 단계 7 장치 > 전화기를 선택하고, 전화기의 [전화기 구성] 창을 엽니다.
- 단계 8 [전화기 버튼 템플릿] 드롭다운 목록에서 새 전화기 버튼 템플릿을 선택합니다.
- 단계 9 저장을 선택하여 변경 사항을 저장한 다음, 구성 적용을 선택하여 변경 사항을 구현합니다.
- 전화기 사용자는 이제 [셀프 서비스 포털]에 액세스해 전화기 버튼과 서비스를 연결할 수 있습니다.

#### 관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## VPN 구성

Cisco VPN 기능은 사용자에게 회사 네트워크에 연결하기 위한 안전하고 믿을 수 있는 방법을 제공하면서 네트워크 보안을 보존하는 데 도움을 줍니다. 다음과 같은 경우 이 기능을 사용합니다.

- 전화기가 신뢰된 네트워크 외부에 있는 경우
- 전화기와 Cisco Unified Communications Manager 간의 네트워크 트래픽이 신뢰할 수 없는 네트워크를 지나는 경우

VPN에서는 클라이언트 인증을 위한 세 가지 일반적인 접근 방식이 있습니다.

- 디지털 인증서
- 암호
- 사용자 이름 및 암호

각 방법은 이점을 가지고 있습니다. 그러나 회사 보안 정책에서 허용할 경우, 인증서는 사용자 조정 없이 매끄러운 로그인을 허용하므로 인증서 기반 접근 방식을 권장합니다. LSC 및 MIC 인증서가 모두 지원됩니다.

VPN 기능을 구성하려면 먼저 장치 온프레미스를 구축한 다음 장치 오프프레미스를 구축할 수 있습니다.

VPN 네트워크에서 인증서 인증 및 작업에 대한 자세한 내용은 ASA 구성에 인증서를 포함한 *AnyConnect VPN Phone* 예 기술 자료를 참조하십시오. 이 문서의 URL은 <http://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html>입니다.

암호 또는 사용자 이름과 암호 접근 방식을 사용하면 사용자에게 로그인 자격 증명을 묻습니다. 회사 보안 정책에 따라 사용자 로그인 자격 증명을 설정합니다. 또한 사용자 암호가 전화기에 저장되도록 암호 지속성 활성화 설정을 구성할 수 있습니다. 실패한 로그인 시도가 발생하거나, 사용자가 수동으로 암호를 지우거나, 전화기가 재설정되거나, 전화기 전원이 유실될 때까지 사용자 암호가 전화기에 저장됩니다.

다른 유용한 도구는 자동 네트워크 탐지 활성화 설정입니다. 이 확인란을 활성화할 때 VPN 클라이언트가 회사 네트워크 외부에 있다는 것을 감지하는 경우에만 실행될 수 있습니다. 이 설정은 기본적으로 비활성화되어 있습니다.

Cisco 전화기는 클라이언트 유형으로 Cisco SVC IPPhone 클라이언트 v1.0을 지원합니다.

VPN을 포함한 가상 사설망의 유지 보수, 구성 및 작동에 대한 추가 정보는 *Cisco Unified Communications Manager* 보안 설명서, "가상 사설망 설정" 장을 참조하십시오. 이 문서의 URL은 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>입니다.

Cisco VPN 기능은 SSL(Secure Sockets Layer)을 사용하여 네트워크 보안을 보존합니다.



참고 내장된 클라이언트를 사용하여 ASA에 대한 SSL VPN의 오프프레미스 전화기를 구성할 때 대체 TFTP 서버 설정을 입력하십시오.

## 추가 회선 키 설정

고급 회선 모드를 활성화하여 전화기 화면의 양면에 있는 버튼을 회선 키로 사용할 수 있습니다. 예측 다이얼링 및 대응 선택 착신 통화 알림은 고급 회선 모드에서 기본적으로 활성화됩니다.

시작하기 전에

새로운 사용자 지정된 전화기 버튼 템플릿을 만들어야 합니다.

프로시저

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

단계 2 설정할 전화기를 검색합니다.

단계 3 [제품별 구성 영역]으로 이동하고 회선 모드 필드를 고급 회선 모드로 설정합니다.

단계 4 장치 정보 영역으로 이동하고 전화기 버튼 템플릿 필드를 사용자 지정된 템플릿으로 설정합니다.

단계 5 구성 적용을 선택합니다.

단계 6 저장을 선택합니다.

단계 7 전화기를 다시 시작합니다.

관련 항목

[세션 회선 모드 환경](#), 168 페이지

## 고급 회선 모드에서 사용할 수 있는 기능

고급 회선 모드(ELM)는 Expressway를 통한 모바일 및 Remote Access와 함께 사용할 수 있습니다.

ELM은 또한 초기 공유 회선이 사용 중일 때 다른 공유 회선으로 통화를 전달하는 착신 전환 구성인 롤오버 회선과 함께 사용할 수 있습니다. 롤오버 회선과 함께 ELM을 사용할 경우, 공유 회선에 대한 최근 통화가 단일 디렉터리 번호로 통합됩니다. 롤오버 회선에 대한 자세한 내용은 Cisco Unified Communications Manager 릴리스 12.0(1) 이상의 경우 *Cisco Unified Communications Manager* 기능 구성 설명서를 참조하십시오.

ELM은 대부분의 기능을 지원합니다. 기능의 활성화는 지원을 의미하지 않습니다. 다음 표를 읽고 기능이 지원되지 않는지 확인합니다.

표 39: 기능 지원 및 고급 회선 모드

기능	지원됨	펌웨어 릴리스
전화받기	예	11.5(1) 이상
자동으로 전화받기	예	11.5(1) 이상
참여/회의끼기	예	11.5(1) 이상
BLF와 직접 통화 지정정보류	예	12.0(1) 이상
블루투스 스마트폰 통합	아니요	-
블루투스 USB 헤드셋	예	11.5(1) 이상
콜백	예	11.5(1) 이상
Call Chaperone	아니요	-
모든 통화 착신 전환	예	11.5(1) 이상
통화 지정정보류	예	12.0(1) 이상
통화 지정정보류 회선 상태	예	12.0(1) 이상
통화 당겨받기	예	11.5(1) 이상
통화 당겨받기 회선 상태	예	11.5(1) 이상
복수 회선에서 모두 착신 전환	예	11.5(1) 이상
Cisco Extension Mobility Cross Cluster	예	12.0(1) 이상이 이 기능을 지원합니다.
Cisco IP Manager Assistant(IPMA)	아니요	-
Cisco Unified Communications Manager Express	아니요	-
전화회의	예	11.5(1) 이상



기능	지원됨	펌웨어 릴리스
CTI(Computer Telephony Integration) 애플리케이션	예	11.5(1) 이상
거부	예	11.5(1) 이상
장치 호출 녹음	예	11.5(1)SR1 이상
DND(Do Not Disturb)	예	11.5(1) 이상
Enhanced SRST	아니요	-
Extension Mobility	예	11.5(1) 이상
그룹 당겨받기	예	12.0(1) 이상이 이 기능을 지원합니다.
보류	예	11.5(1) 이상
헌트 그룹	예	12.0(1) 이상
구성 가능한 타이머를 사용한 착신 통화 알림	아니요	-
인터콥	예	11.5(1) 이상
키 확장 모듈	Cisco IP 전화기 8851/8861 키 확장 모듈 및 Cisco IP 전화기 8865 키 확장 모듈에서 고급 회선 모드 지원	12.0(1) 이상
MCID(장난 전화 ID)	예	11.5(1) 이상
회의개설	예	11.5(1) 이상
모바일 연결	예	11.5(1) 이상
MLPP(Multilevel Precedence and Preemption)	아니요	-
음소거	예	11.5(1) 이상
기타 당겨받기	예	12.0(1) 이상
대기열 상태에 대한 PLK(Programmable Line Key) 지원	예	11.5(1) 이상
프라이버시	예	11.5(1) 이상
대기열 상태	예	11.5(1) 이상

기능	지원됨	펌웨어 릴리스
QRT(품질 보고 도구)	예	11.5(1) 이상
오른쪽에서 왼쪽으로 로컬 지원	아니요	-
재다이얼	예	11.5(1) 이상
무성 모니터링 및 녹음	예	11.5(1)SR1 이상
바로 호출	예	11.5(1) 이상
SRST(Survivable Remote Site Telephony)	예	11.5(1) 이상
호 전환	예	11.5(1) 이상
URI(Uniform Resource Identifier) 전화 걸기	예	11.5(1) 이상
영상 통화	예	11.5(1) 이상
Visual Voicemail	예	11.5(1) 이상
음성 메일	예	11.5(1) 이상

관련 항목

[세션 회선 모드 환경](#), 168 페이지

## TLS 재개 타이머 설정

TLS 세션 재개를 사용하면 전체 TLS 인증 프로세스를 반복하지 않고 TLS 세션이 재개할 수 있습니다. 이렇게 하면 TLS 연결이 데이터를 교환하는 데 걸리는 시간을 크게 줄일 수 있습니다.

전화기가 TLS 세션을 지원하더라도, 모든 TLS 세션은 TLS 재개를 지원하지 않습니다. 다음 목록은 다른 세션 및 TLS 재개 지원을 설명합니다.

- SIP 시그널링에 대한 TLS 세션: 재개를 지원합니다.
- HTTP 클라이언트: 재개를 지원합니다.
- CAPF: 재개를 지원합니다.
- TVS: 재개를 지원합니다.
- EAP-TLS: 재개를 지원하지 않습니다.
- EAP-FAST: 재개를 지원하지 않습니다.
- VPN 클라이언트: 재개를 지원하지 않습니다.

자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

프로시저

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

**단계 2** TLS 재개 타이머 매개 변수를 설정합니다.

타이머에 대한 범위는 0~3600초입니다. 기본값은 3600입니다. 필드가 0으로 설정되면 TLS 세션 재개가 비활성화됩니다.

관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## Intelligent Proximity 활성화



**참고** 이 절차는 블루투스 활성화 전화기에만 적용됩니다. Cisco IP 전화기 8811, 8841, 8851NR 및 8865NR은 블루투스를 지원하지 않습니다.

사용자는 Intelligent Proximity를 사용하여 모바일 장치 또는 태블릿으로 전화기의 음향 속성을 이용할 수 있습니다. 사용자는 블루투스를 사용하여 모바일 장치 또는 태블릿을 전화기에 페어링합니다.

모바일 장치가 페어링되었으면 사용자는 전화기에서 휴대폰 통화를 걸고 받을 수 있습니다. 태블릿을 사용하여 사용자는 태블릿에서 전화기로 오디오를 라우팅할 수 있습니다.

사용자는 다중 모바일 장치, 태블릿 및 블루투스 헤드셋을 전화기에 페어링할 수 있습니다. 그러나 장치 하나와 헤드셋 하나만 동시에 연결할 수 있습니다.

프로시저

**단계 1** Cisco Unified Communications Manager Administration에서 전화기 > 장치를 선택합니다.

**단계 2** 수정할 전화기를 찾습니다.

**단계 3** 블루투스 필드를 찾고 필드를 활성화됨으로 설정합니다.

**단계 4** [블루투스 모바일 핸드프리 모드 허용] 필드를 찾고 필드를 활성화됨으로 설정합니다.

**단계 5** 변경 사항을 저장하고 전화기에 적용합니다.

## 비디오 전송 해상도 설정

Cisco IP 전화기 8845, 8865 및 8865NR은 다음 비디오 형식을 지원합니다.

- 720p (1280x720)
- WVGA (800x480)
- 360p (640x360)
- 240p (432x240)
- VGA (640x480)
- CIF (352x288)
- SIF (352x240)
- QCIF (176x144)

비디오 기능이 있는 Cisco IP 전화기는 전화기 구성 또는 해상도 제한을 기준으로 하여 대역폭에 대한 최상의 해상도를 설정합니다. 예: 직접 88x5 대 88x5 통화 시, 전화기는 실제 720p를 전송하지 않고, 800x480을 전송합니다. 이 제한 사항은 순전히 800 x 480으로 되는 88x5의 5인치 WVGA 화면 해상도로 인한 것입니다.

비디오 유형	비디오 해상도	초당 프레임 수(fps)	비디오 비트율 범위
720p	1280 x 720	30	1360–2500 kbps
720p	1280 x 720	15	790-1359 kbps
WVGA	800 x 480	30	660-789 kbps
WVGA	800 x 480	15	350-399 kbps
360p	640 x 360	30	400-659 kbps
360p	640 x 360	15	210–349kbps
240p	432 x 240	30	180–209kbps
240p	432 x 240	15	64–179kbps
VGA	640 x 480	30	520–1500kbps
VGA	640 x 480	15	280–519kbps
CIF	352 x 288	30	200-279 kbps
CIF	352 x 288	15	120-199 kbps
SIF	352 x 240	30	200-279 kbps
SIF	352 x 240	15	120-199 kbps
QCIF	176 x 144	30	94-119 kbps
QCIF	176 x 144	15	64-93 kbps

# 이전 버전의 Cisco Unified Communications Manager에서 헤드셋 관리

12.5(1) SU1 이전 버전의 Cisco Unified Communications Manager를 사용하는 경우 온프레미스 전화기와 함께 사용할 Cisco 헤드셋 설정을 원격으로 구성할 수 있습니다.

Cisco Unified Communication Manager 버전 10.5(2), 11.0(1), 11.5(1), 12.0(1) 및 12.5(1)에서 원격 헤드셋을 구성하려면 [Cisco 소프트웨어 다운로드](#) 웹 사이트에서 파일을 다운로드하고 파일을 편집한 다음 Cisco Unified Communications Manager TFTP 서버에서 파일을 업로드해야 합니다. 파일은 JSON(JavaScript Object Notification) 파일입니다. 업데이트된 헤드셋 구성이 10~30분의 시간 프레임을 초과하는 엔터프라이즈 헤드셋에 적용되어 TFTP 서버의 트래픽 백로그가 방지됩니다.



**참고** Cisco Unified Communications Manager 관리 버전 11.5(1) SU7을 통해 헤드셋을 관리하고 구성할 수 있습니다.

JSON 파일 작업시 다음 사항에 유의하십시오.

- 코드에 대괄호가 없는 경우 설정이 적용되지 않습니다. JSON Formatter와 같은 온라인 도구를 사용하여 형식을 확인합니다.
- **updatedTime** 설정을 현재 epoch 시간으로 설정하십시오. 그렇지 않으면 구성이 적용되지 않습니다. 또는 **updatedTime** 값을 +1로 증가시켜 이전 버전보다 크게 설정할 수도 있습니다.
- 매개 변수 이름을 변경하지 마십시오. 변경하면 설정이 적용되지 않습니다.

TFTP 서비스에 대한 자세한 내용은 *Cisco Unified Communications Manager* 및 *IM and Presence* 서비스용 관리 가이드의 "장치 펌웨어 관리" 장을 참조하십시오.

defaultheadsetconfig.json 파일을 적용하기 전에 전화기를 최신 펌웨어 릴리스로 업그레이드합니다. 다음 표에서는 JSON 파일을 사용하여 조정할 수 있는 기본 설정에 대해 설명합니다.

## 기본 헤드셋 설정 파일 다운로드

헤드셋 매개 변수를 원격으로 구성하기 전에 먼저 최신 JSON(JavaScript Object Notation) 샘플 파일을 다운로드해야 합니다.

프로시저

단계 1 다음 URL로 이동합니다. <https://software.cisco.com/download/home/286320550>

단계 2 헤드셋 500 시리즈를 선택합니다.

단계 3 헤드셋 시리즈를 선택합니다.

단계 4 릴리스 폴더를 선택하고 zip 파일을 선택합니다.

단계 5 다운로드 또는 장바구니에 추가 단추를 클릭하고 지시를 따릅니다.

단계 6 PC의 디렉터리에 파일의 압축을 풉니다.

다음에 수행할 작업

[기본 헤드셋 설정 파일 수정, 212 페이지](#)

## 기본 헤드셋 설정 파일 수정

JSON(JavaScript Object Notation) 파일을 작업하면서 다음 사항에 유의하십시오.

- 코드에 대괄호가 없는 경우 설정이 적용되지 않습니다. JSON Formatter와 같은 온라인 도구를 사용하여 형식을 확인합니다.
- **"updatedAt"** 설정을 현재 epoch 시간으로 설정하십시오. 그렇지 않으면 구성이 적용되지 않습니다.
- **firmwareName**이 LATEST인지 확인합니다. 그렇지 않으면 구성이 적용되지 않습니다.
- 매개 변수 이름을 변경하지 마십시오. 변경하면 설정이 적용되지 않습니다.

프로시저

단계 1 텍스트 편집기를 사용하여 defaultheadsetconfig.json 파일을 엽니다.

단계 2 **UpdatedTime** 및 수정할 헤드셋 매개 변수 값을 편집합니다.

샘플 스크립트는 아래와 같습니다. 이 스크립트는 참조용으로만 제공됩니다. 헤드셋 매개 변수를 구성할 때 지침으로 사용하십시오. 펌웨어 로드에는 포함된 JSON 파일을 사용합니다.

```
{
  "headsetConfig": {
    "templateConfiguration": {
      "configTemplateVersion": "1",
      "updatedAt": 1537299896,
      "reportId": 3,
      "modelSpecificSettings": [
        {
          "modelSeries": "530",
          "models": [
            "520",
            "521",
            "522",
            "530",
            "531",
            "532"
          ],
          "modelFirmware": [
            {
              "firmwareName": "LATEST",
              "latest": true,
              "firmwareParams": [
                {

```

```

        "name": "Speaker Volume",
        "access": "Both",
        "usageId": 32,
        "value": 7
    },
    {
        "name": "Microphone Gain",
        "access": "Both",
        "usageId": 33,
        "value": 2
    },
    {
        "name": "Sidetone",
        "access": "Both",
        "usageId": 34,
        "value": 1
    },
    {
        "name": "Equalizer",
        "access": "Both",
        "usageId": 35,
        "value": 3
    }
    ]
}
],
{
    "modelSeries": "560",
    "models": [
        "560",
        "561",
        "562"
    ],
    "modelFirmware": [
        {
            "firmwareName": "LATEST",
            "latest": true,
            "firmwareParams": [
                {
                    "name": "Speaker Volume",
                    "access": "Both",
                    "usageId": 32,
                    "value": 7
                },
                {
                    "name": "Microphone Gain",
                    "access": "Both",
                    "usageId": 33,
                    "value": 2
                },
                {
                    "name": "Sidetone",
                    "access": "Both",
                    "usageId": 34,
                    "value": 1
                },
                {
                    "name": "Equalizer",
                    "access": "Both",
                    "usageId": 35,
                    "value": 3
                }
            ],
        }
    ]
}

```





## Cisco TFTP 서버 다시 시작

defaultheadsetconfig.json 파일을 TFTP 디렉터리에 업로드한 후에 Cisco TFTP 서버를 다시 시작하고 전화기를 재설정합니다. 약 10 - 15분 후에 다운로드 프로세스가 시작되고 새 구성이 헤드셋에 적용됩니다. 설정을 적용하려면 10~30분이 추가로 소요됩니다.

프로시저

- 
- 단계 1 Cisco Unified Serviceability에 로그인하고 도구 > 제어 센터 - 기능 서비스를 선택합니다.
  - 단계 2 **Server** 드롭다운 목록 상자에서 Cisco TFTP 서비스가 실행 중인 서버를 선택합니다.
  - 단계 3 **Cisco TFTP** 서비스에 해당하는 무선 단추를 클릭합니다.
  - 단계 4 재시작을 클릭합니다.
-





# 10 장

## 회사 및 개인 디렉터리

- 회사 디렉터리 설정, 217 페이지
- 개인 디렉터리 설정, 217 페이지
- 사용자 개인 디렉터리 항목 설정, 218 페이지

### 회사 디렉터리 설정

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

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

Cisco IP 전화기는 클라이언트와 서버 모두에서 SecureApp에 동적 할당을 사용합니다. 이렇게 하면 전화기가 4KB를 초과하는 인증서를 읽을 수 있고 사용자가 해당 디렉터리에 액세스 할 때 호스트를 찾을 수 없음 오류 메시지 빈도가 줄어 듭니다.

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](#), xvii 페이지

### 개인 디렉터리 설정

개인 디렉터를 사용하면 사용자가 개인 번호를 저장할 수 있습니다.

개인 디렉터리는 다음과 같은 기능으로 구성됩니다.

- PAB(개인 주소록)

- 바로 호출
- 주소록 동기화 도구(TABSynch)

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.
- Microsoft Windows 애플리케이션에서 사용자는 TABSynch 도구를 사용하여 사용자의 PAB를 Microsoft Windows 주소록(WAB)과 동기화할 수 있습니다. Microsoft Outlook 주소록(OAB)을 사용하려면 데이터를 OAB에서 WAB로 가져와서 시작해야 합니다. 그래야 TabSynch를 사용하여 WAB와 개인 디렉터리를 동기화할 수 있습니다. TABSynch에 대한 지침은 [Cisco IP 전화기 Address Book Synchronizer 다운로드, 219 페이지](#) 및 [Synchronizer 설정, 220 페이지](#)를 참조하십시오.

Cisco IP 전화기는 클라이언트와 서버 모두에서 SecureApp에 동적 할당을 사용합니다. 이렇게 하면 전화기가 4KB를 초과하는 인증서를 읽을 수 있고 사용자가 해당 디렉터리에 액세스 할 때 호스트를 찾을 수 없음 오류 메시지 빈도가 줄어 듭니다.

Cisco IP 전화기 Address Book Synchronizer 사용자가 최종 사용자 데이터에만 액세스하는지 확인하려면, [Cisco Unified 서비스 가용성]에서 [Cisco UXL 웹 서비스]를 활성화합니다.

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

## 사용자 개인 디렉터리 항목 설정

사용자는 Cisco IP 전화기에 개인 디렉터리 항목을 구성할 수 있습니다. 개인 디렉터리를 구성하려면, 사용자에게 다음에 대한 액세스 권한이 있어야 합니다.

- 셀프 서비스 포털: 사용자가 셀프 서비스 포털에 액세스하는 방법을 알고 있는지 확인합니다. 자세한 내용은 [셀프 서비스 포털에 사용자 액세스 설정, 84 페이지](#)를 참조하십시오.
- Cisco IP 전화기 Address Book Synchronizer: 사용자에게 설치 프로그램을 제공해야 합니다. [Cisco IP 전화기 Address Book Synchronizer 다운로드, 219 페이지](#) 참조



참고 Cisco IP 전화기 주소록 동기화 도구는 지원되지 않는 버전의 Windows(예: Windows XP 및 이전 버전)에서만 지원됩니다. 새 버전의 Windows에서는 이 도구가 지원되지 않습니다. 나중에 이 항목이 Cisco Unified Communications Manager 플러그인 목록에서 제거될 예정입니다.

## Cisco IP 전화기 Address Book Synchronizer 다운로드

사용자에게 전송할 Synchronizer 사본을 다운로드하려면, 다음 단계를 수행합니다.

프로시저

- 단계 1 설치 프로그램을 확보하려면 Cisco 통합 커뮤니케이션 매니저 관리에서 애플리케이션 > 플러그인을 선택합니다.
- 단계 2 Cisco IP 전화기 Address Book Synchronizer 플러그인 이름 옆에 있는 다운로드를 선택합니다.
- 단계 3 [파일 다운로드] 대화 상자가 나타나면 저장을 선택합니다.
- 단계 4 이 애플리케이션을 요청한 모든 사용자에게 TabSyncInstall.exe 파일과 [Cisco IP 전화기 주소록 동기화 도구 구축, 219 페이지](#)에 나온 지침을 전송합니다.

## Cisco IP 전화기 주소록 동기화 도구 구축

Cisco IP 전화기 주소록 동기화 도구는 Microsoft Windows 주소록에 저장된 데이터를 Cisco Unified Communications Manager 디렉터리 및 셀프 서비스 포털 주소록과 동기화합니다.



- 팁 Windows 주소록과 개인 주소록을 성공적으로 동기화하려면 다음 절차를 수행하기 전에 Windows 주소록에 모든 Windows 주소록 사용자를 입력해야 합니다.

## Synchronizer 설치

Cisco IP 전화기 Address Book Synchronizer를 설치하려면 다음 단계를 수행하십시오.

프로시저

- 단계 1 시스템 관리자에게 Cisco IP 전화기 Address Book Synchronizer 설치 프로그램 파일을 요청합니다.
- 단계 2 관리자가 제공한 TabSyncInstall.exe 파일을 두 번 클릭합니다.
- 단계 3 실행을 선택합니다.
- 단계 4 다음을 선택합니다.
- 단계 5 라이선스 계약 정보를 읽고, 동의함을 선택합니다. 다음을 선택합니다.
- 단계 6 애플리케이션을 설치할 디렉터리를 선택하고 다음을 선택합니다.
- 단계 7 설치를 선택합니다.
- 단계 8 마침을 선택합니다.
- 단계 9 프로세스를 완료하려면 [Synchronizer 설정, 220 페이지](#)에 나와 있는 단계를 수행하십시오.

## Synchronizer 설정

Cisco IP 전화기 Address Book Synchronizer를 구성하려면 다음 단계를 수행합니다.

프로시저

**단계 1** Cisco IP 전화기 Address Book Synchronizer를 엽니다.

기본 설치 디렉터리를 허용한 경우에는 시작 > 모든 프로그램 > **Cisco** 시스템 > **TabSync**를 선택하여 애플리케이션을 엽니다.

**단계 2** 사용자 정보를 구성하려면 사용자를 선택합니다.

**단계 3** Cisco IP 전화기 사용자 이름과 암호를 입력한 후 확인을 선택합니다.

**단계 4** Cisco Unified Communications Manager 서버 정보를 구성하려면 서버를 선택합니다.

**단계 5** Cisco Unified Communications Manager 서버의 IP 주소나 호스트 이름 및 포트 번호를 입력하고 확인을 선택합니다.

이 정보를 알지 못하는 경우에는 시스템 관리자에게 문의하십시오.

**단계 6** 디렉터리 동기화 과정을 시작하려면 동기화를 선택합니다.

[동기화 상태] 창은 주소록 동기화 상태를 보여줍니다. 중복 항목 규칙에 사용자에게 물어보기(user intervention)를 선택한 상태에서 중복 주소록 항목이 있는 경우, "중복 선택" 창이 표시됩니다.

**단계 7** 개인 주소록에 포함시킬 항목을 선택한 후 확인을 선택합니다.

**단계 8** 동기화가 완료되면 종료를 선택하여 Cisco Unified CallManager Address Book Synchronizer를 닫습니다.

**단계 9** 동기화가 제대로 이루어졌는지 확인하려면, 셀프 서비스 포털에 로그인한 다음 개인 주소록을 선택합니다. Windows 주소록의 사용자가 표시되어야 합니다.



## IV 부

### Cisco IP 전화기 문제 해결

- 전화기 시스템 모니터링, 223 페이지
- 문제 해결, 259 페이지
- 유지 보수, 279 페이지
- 국제 사용자 지원, 285 페이지







# 11 장

## 전화기 시스템 모니터링

- [Cisco IP 전화기 상태, 223 페이지](#)
- [Cisco IP 전화기 웹 페이지, 239 페이지](#)
- [전화기의 정보를 XML로 요청, 256 페이지](#)

### Cisco IP 전화기 상태

이 섹션에서는 Cisco IP 전화기 8800 시리즈에서 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.

문제 해결에 대한 자세한 내용은 [문제 해결, 259 페이지](#)를 참조하십시오.

### [전화기 정보] 창 표시

모델 정보 화면을 표시하려면 다음 단계를 수행하십시오.

프로시저

단계 1 애플리케이션  을 누릅니다.

단계 2 전화기 정보를 선택합니다.

사용자가 보안 또는 인증된 서버에 연결되어 있으면, 서버 옵션 오른쪽의 [전화기 정보 화면]에 해당 아이콘(잠금 또는 인증서)이 표시됩니다. 사용자가 보안 또는 인증된 서버에 연결되어 있지 않으면, 어떤 아이콘도 표시되지 않습니다.

단계 3 [모델 정보] 화면을 종료하려면 종료를 누릅니다.

## 전화기 정보 필드

다음 표에서는 전화기 정보 설정에 대해 설명합니다.

표 40: 전화기 정보 설정

옵션	설명
모델 번호	전화기의 모델 번호
IPv4 주소	전화기의 IP 주소입니다.
호스트 이름	전화기의 호스트 이름입니다.
활성 로드	전화기에 현재 설치된 펌웨어의 버전입니다. 자세한 내용은 상세정보를 눌러 볼 수 있습니다.
비활성 로드	비활성 로드는 다운로드가 진행 중인 경우에만 나타납니다. 다운로드 아이콘과 “업그레이드 진행 중” 또는 “업그레이드 실패” 상태도 표시됩니다. 업그레이드 도중 사용자가 상세정보를 누르면 다운로드 파일 이름 및 구성 요소가 나열됩니다.  유지 보수 창에 앞서 새 펌웨어 이미지를 다운로드하도록 설정할 수 있습니다. 따라서 모든 전화기가 펌웨어를 다운로드할 때까지 기다리지 않고, 시스템이 기존 로드를 비활성 상태로 재설정하는 동작과 새 로드를 설치하는 동작 간에 더 빨리 전환합니다.  다운로드가 완료될 때 아이콘이 변경되어 완료됨 상태를 나타내고, 성공적인 다운로드에 대해 체크 표시가 표시되거나, 실패한 다운로드에 대해 “X”가 표시됩니다. 가능한 경우 나머지 로드는 계속 다운로드됩니다.
마지막 업그레이드	최신 펌웨어 업그레이드 날짜입니다.
활성 서버	전화기가 등록된 서버의 도메인 이름입니다.
대기 서버	대기 서버의 도메인 이름입니다.

## 상태 메뉴 표시


상태 메뉴는 전화기 및 전화기 작업에 대한 정보를 제공하는 다음 옵션을 포함합니다.

- 상태 메시지: 중요한 시스템 메시지 로그를 나타내는 상태 메시지 화면을 표시합니다.
- 이더넷 통계: 이더넷 트래픽 통계를 나타내는 이더넷 통계 화면을 표시합니다.

- 무선 통계: 해당되는 경우, 무선 통계 화면을 표시합니다.
- 통화 통계: 현재 통화에 대한 카운터 및 통계를 표시합니다.
- 현재 액세스 지점: 해당되는 경우, 현재 액세스 지점 화면을 표시합니다.

상태 메뉴를 표시하려면, 다음 단계를 수행합니다.

프로시저

단계 1 상태 메뉴를 표시하려면 애플리케이션  을 누릅니다.


단계 2 관리 설정 > 상태를 선택합니다.

단계 3 [상태] 메뉴를 종료하려면 종료를 누릅니다.

## 상태 메시지 창 표시

[상태 메시지] 창은 전화기가 생성한 최근 30개의 상태 메시지를 표시합니다. 전화기가 시작을 마치지 않았더라도, 언제든지 이 화면에 액세스할 수 있습니다.

프로시저

단계 1 애플리케이션  을 누릅니다.

단계 2 관리 설정 > 상태 > 상태 메시지를 선택합니다.

단계 3 현재 상태 메시지를 제거하려면 지우기를 누릅니다.

단계 4 상태 메시지 화면을 종료하려면 종료를 누릅니다.

## 상태 메시지 필드

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

표 41: Cisco 유니파이드 IP 전화기의 상태 메시지

메시지	설명	가능한 설명 및 조치
CFG TFTP 크기 오류	전화기의 파일 시스템에 비해 구성 파일이 너무 큽니다.	전화기 전원을 껐다가 다시 켜십시오.
체크섬 오류	다운로드한 소프트웨어 파일이 손상되었습니다.	전화기 펌웨어에서 새 사본을 디렉터리에 저장합니다. TFTP 서버가 실패하면 이 디렉터리에 파일을 다운로드하지 않으면 파일이 손상될 수 있습니다.

메시지	설명	가능한 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 할 수 있는지 확인합니다.
CTL 및 ITL 설치됨	CTL 및 ITL 파일이 전화기에 설치되었습니다.	없음 이 메시지는 정보 제공용일 ITL 파일이 모두 이전에 설치되
CTL 설치됨	인증서 신뢰 목록(CTL) 파일이 전화기에 설치되었습니다.	없음 이 메시지는 정보 제공용일 이전에 설치되지 않았습니다.
CTL 업데이트 실패	전화기가 인증서 신뢰 목록(CTL) 파일을 업데이트할 수 없습니다.	TFTP 서버의 CTL 파일에 문제가
DHCP 시간 초과	DHCP 서버가 응답하지 않았습니다.	네트워크 사용 중: 네트워크 로드는 자체적으로 해결됩니다. DHCP 서버와 전화기 사이의 네트워크 연결을 확인하십시오. DHCP 서버 중단: DHCP 서버 구성 오류 지속: 고정 IP 주소 할당을
DNS 시간 초과	DNS 서버가 응답하지 않았습니다.	네트워크 사용 중: 네트워크 로드는 자체적으로 해결됩니다. DNS 서버와 전화기 사이의 네트워크 연결을 확인하십시오. DNS 서버 중단: DNS 서버 구성
DNS 알 수 없는 호스트	DNS에서 TFTP 서버나 Cisco Unified Communications Manager의 이름을 확인할 수 없습니다.	DNS에 TFTP 서버나 Cisco Unified Communications Manager의 호스트 이름이 적절히 구성되어 있는지 확인합니다. 호스트 이름이 아닌 IP 주소 사용
중복 IP	또 다른 장치에서 해당 전화기에 할당된 IP 주소를 사용하고 있습니다.	전화기에 고정 IP 주소가 있다면 해당하지 않았는지 확인합니다. DHCP를 사용 중이라면 DHCP 서버를 재설정하십시오.
CTL 및 ITL 파일 지우기	CTL이나 ITL 파일이 지워집니다.	없음 이 메시지는 정보 제공용일

메시지	설명	가능한 설명 및 조치
로케일 업데이트 오류	TFTPath 디렉터리에서 1개 이상의 현지화 파일을 찾을 수 없거나 파일이 유효하지 않습니다. 로케일이 변경되지 않았습니다.	<p>Cisco Unified Operating System 파일 관리의 하위 디렉터리에서 하는지 확인합니다.</p> <ul style="list-style-type: none"> <li>• 네트워크 로케일과 동일한 디렉터리에 저장된 파일: <ul style="list-style-type: none"> <li>• tones.xml</li> </ul> </li> <li>• 사용자 로케일과 동일한 디렉터리에 저장된 파일: <ul style="list-style-type: none"> <li>• glyphs.xml</li> <li>• dictionary.xml</li> <li>• kate.xml</li> </ul> </li> </ul>
파일을 찾을 수 없음 <Cfg File>	TFTP 서버에 이름 기반의 기본 구성 파일이 없습니다.	<p>Cisco Unified Communications Manager 전화기가 추가되면 전화기에 해당 파일이 생성됩니다. 그런데 Cisco Unified Communications Manager 데이터베이스에 전화기가 존재하지만 서버 <b>CFG</b> 파일을 찾을 수 없습니다.</p> <ul style="list-style-type: none"> <li>• 전화기가 Cisco Unified Communications Manager에 등록되어 있지 않습니다. 전화기의 자동 등록을 하거나 Cisco Unified Communications Manager에 전화기를 추가해야 합니다. <a href="#">자동 등록 방식, 73 페이지</a>를 참조하십시오.</li> <li>• DHCP를 사용하고 있다면 DHCP 서버를 지정하고 있는지 확인하십시오.</li> <li>• 고정 IP 주소를 사용하고 있다면 고정 IP 주소를 확인하십시오.</li> </ul>
파일을 찾을 수 없습니다. <CTLFile.tlv>	이 메시지는 Cisco Unified Communications Manager 클러스터가 보안 모드가 아닐 때 전화기에 표시됩니다.	별 다른 영향은 없습니다. Cisco Unified Communications Manager에 전화기가 추가되면 이 메시지는 사라집니다.
IP 주소 해제됨	전화기가 IP 주소를 해제하도록 구성되어 있습니다.	전원을 껐다 켜거나 DHCP 주소를 사용하여 유휴 상태로 남아 있습니다.
ITL 설치됨	ITL 파일이 전화기에 설치되었습니다.	없음 이 메시지는 정보 제공용입니다. 전화기가 이전에 설치되지 않았습니다.

메시지	설명	가능한 설명 및 조치
거부된 HC 로드	다운로드된 애플리케이션이 전화기 하드웨어와 호환되지 않습니다.	전화기의 하드웨어 변경 사항을 웨어 버전을 전화기에 설치하려면 전화기에 할당된 로드 ID를 확인 Communications Manager에서 전화기에 표시되는 로드를 다시 업로드합니다.
기본 라우터 없음	DHCP 또는 고정 구성에서 기본 라우터를 지정하지 않았습니다.	전화기에 고정 IP 주소가 있다면, 이를 확인합니다. DHCP를 사용하고 있다면, DHCP 서버를 제공하지 않은 것입니다. DHCP 서버를 확인합니다.
DNS 서버 IP 없음	이름이 지정되었으나, DHCP 또는 고정 IP 구성에서 DNS 서버 주소를 지정하지 않은 경우입니다.	전화기에 고정 IP 주소가 있다면, 이를 확인합니다. DHCP를 사용하고 있다면, DHCP 서버를 제공하지 않은 것입니다. DHCP 서버를 확인합니다.
설치된 신뢰 목록이 없음	전화기에 CTL 파일이나 ITL 파일이 설치되어 있지 않습니다.	Cisco Unified Communications Manager 구성되어 있지 않아서, 디폴트로 설치됩니다.
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 Manager 구성 변경을 했을 가능성이 높을 경우, 영향을 적용하기 위해 적용이 필요합니다.
TFTP 액세스 오류	TFTP 서버에서 존재하지 않는 디렉토리를 지정하고 있습니다.	DHCP를 사용하고 있다면, DHCP 서버를 지정하고 있는지 확인합니다. 고정 IP 주소를 사용하고 있다면, 이를 확인합니다.
TFTP 오류	전화기에서 TFTP 서버가 제공한 오류 코드를 인식하지 못합니다.	Cisco TAC에 문의하십시오.
TFTP 시간 초과	TFTP 서버가 응답하지 않았습니다.	네트워크가 버스임: 네트워크 로드를 재시도하는 자체적으로 해결됩니다. TFTP 서버와 전화기 사이의 네트워크 연결을 확인합니다. TFTP 서버 중단: TFTP 서버 구성을 확인합니다.

메시지	설명	가능한 설명 및 조치
시간 초과	802.1X 트랜잭션을 시도했으나 인증자의 부재로 시간이 초과되었습니다.	스위치에 802.1X가 구성되어 시간이 초과됩니다.
신뢰 목록 업데이트 실패	CTL 및 ITL 파일 업데이트에 실패했습니다.	전화기에 CTL 및 ITL 파일이 ITL 파일을 업데이트하는 데 가능한 실패 이유: <ul style="list-style-type: none"> <li>• 네트워크 문제가 발생했</li> <li>• TFTP 서버가 중단되었습</li> <li>• CTL 파일을 서명하는 데 ITL 파일을 서명하는 데 개되었지만, 현재 전화기 제공되지 않습니다.</li> <li>• 내부 전화기 문제가 발생</li> </ul> 가능한 해결 방법: <ul style="list-style-type: none"> <li>• 네트워크 연결을 확인합</li> <li>• TFTP 서버가 활성화되었 있는지 확인합니다.</li> <li>• Cisco Unified Communic TVS(Transactional Vsam 면, TVS 서버가 활성화되 지 확인합니다.</li> <li>• 보안 토큰과 TFTP 서버</li> </ul> 앞의 모든 해결 방법이 실패 수동으로 삭제한 다음 전화기
신뢰 목록 업데이트	CTL 파일이나 ITL 파일 또는 두 파일 모두 업데이트 되었습니다.	없음 이 메시지는 정보 제공-
버전 오류	전화기 로드 파일의 이름이 잘못되었습니다.	전화기 로드 파일의 이름이
XmlDefault.cnf.xml 또는 전화기 장치 이름에 해당하는 .cnf.xml	구성 파일의 이름입니다.	없음 이 메시지는 전화기를 표시됩니다.

관련 항목


[Cisco Unified Communications Manager 설명서](#), xvii 페이지

## 네트워크 통계 화면 표시

네트워크 정보 화면에 표시되는 정보를 사용하여 전화기의 연결 문제를 해결합니다.

사용자에게 전화기 네트워크에 연결하는 데 문제가 있는 경우 전화기에 메시지가 표시됩니다.


### 프로시저

- 
- 단계 1 상태 메뉴를 표시하려면 애플리케이션  을 누릅니다.
  - 단계 2 관리 설정 > 상태 > 상태 메시지를 선택합니다.
  - 단계 3 네트워크 정보를 선택합니다.
  - 단계 4 네트워크 정보를 종료하려면 종료를 누릅니다.
- 

## 네트워크 통계 화면 표시

네트워크 통계 화면은 전화기 및 네트워크 성능에 대한 정보를 표시합니다.  
네트워크 통계 화면을 표시하려면, 다음 단계를 수행하십시오.

### 프로시저

- 
- 단계 1 애플리케이션  을 누릅니다.
  - 단계 2 관리 설정>상태>네트워크 통계를 선택합니다.
  - 단계 3 Rx 프레임, Tx 프레임 및 Rx 브로드캐스트 통계치를 0으로 재설정하려면, 지우기를 누릅니다.
  - 단계 4 이더넷 통계 화면을 종료하려면 종료를 누릅니다.
- 

## 이더넷 통계 정보

다음 표에서는 이더넷 통계 화면에 포함되어 있는 정보에 관해 설명합니다.

표 42: 이더넷 통계 정보

항목	설명
Rx Frames	전화기에서 수신한 패킷 수입입니다.
Tx Frames	전화기에서 송신한 패킷 수입입니다.
Rx Broadcasts	전화기에서 수신한 브로드캐스트 패킷 수입입니다.



항목	설명
재시작 원인	<p>전화기를 가장 최근에 재설정 한 이유입니다. 다음 값 중 하나를 지정합니다.</p> <ul style="list-style-type: none"> <li>• 초기화됨</li> <li>• TCP-시간 초과</li> <li>• CM-TCP-종료됨</li> <li>• TCP-Bad-ACK</li> <li>• CM-reset-TCP</li> <li>• CM-aborted-TCP</li> <li>• CM-NAKed</li> <li>• KeepaliveTO</li> <li>• 장애 복구</li> <li>• 전화 키패드</li> <li>• 전화-IP-재구성</li> <li>• 재설정-재설정</li> <li>• 재설정-재시작</li> <li>• 전화-등록-거부</li> <li>• 거부된 HC 로드</li> <li>• CM-ICMP-연결 못 함</li> <li>• 통화 중단</li> </ul>
경과시간	전화기를 마지막으로 재부팅한 후 경과한 시간입니다.
포트 1	네트워크 포트의 연결 및 링크 상태입니다. <b>Auto 100 Mb Full-Duplex</b> 는 네트워크 포트가 연결 상태고, 자동 설정된 전이 중, 100-Mbps 연결 상태라는 뜻입니다.
포트 2	PC 포트의 연결 및 링크 상태입니다.
DHCP 상태(IPv4 / IPv6)	<ul style="list-style-type: none"> <li>• IPv4 전용 모드에서는 DHCP BOUND와 같은 DHCPv4 상태만 표시합니다.</li> <li>• IPv6 모드에서는 ROUTER ADVERTISE와 같은 DHCPv6 상태만 표시합니다.</li> <li>• DHCPv6 상태 정보가 표시됩니다.</li> </ul>

다음 표는 DHCPv4 및 DHCPv6 상태에 대해 나타나는 메시지에 대해 설명합니다.

표 43: DHCPv4 이더넷 통계 메시지

DHCPv4 상태	설명
CDP INIT	CDP가 바운드되지 않거나 WLAN이 서비스 중이 아닙니다.
DHCP BOUND	DHCPv4가 바운드(BOUND)됩니다.
DHCP DISABLED	DHCPv4가 비활성화되었습니다.
DHCP INIT	DHCPv4가 INIT입니다.
DHCP INVALID	DHCPv4가 유효하지 않습니다(INVALID). 이것이 초기 상태입니다.
DHCP RENEWING	DHCPv4가 재개 중(RENEWING)입니다.
DHCP REBINDING	DHCPv4가 리바인딩(REBINDING)입니다.
DHCP REBOOT	DHCPv4가 초기 재부팅(init-reboot)됩니다.
DHCP REQUESTING	DHCPv4가 요청 중입니다.
DHCP RESYNC	DHCPv4가 재동기화(RESYNCH)됩니다.
DHCP WAITING COLDBOOT TIMEOUT	DHCPv4가 부팅 중입니다.
DHCP UNRECOGNIZED	인식되지 않는 DHCPv4 상태
DISABLED DUPLICATE IP	중복된 IPv4 주소
DHCP TIMEOUT	DHCPv4 시간 초과
IPV4 STACK TURNED OFF	전화기가 IPv4 스택이 꺼진 IPv6 전용 모드에 있습니다.
ILLEGAL IPV4 STATE	부적합한 IPv4 상태이며 일어나면 안 됩니다.

표 44: DHCPv6 이더넷 통계 메시지

DHCPv6 상태	설명
CDP INIT	CDP가 초기화 중입니다.
DHCP6 BOUND	DHCPv6이 바운드(BOUND)됩니다.
DHCP6 DISABLED	DHCPv6이 비활성화되었습니다.
DHCP6 RENEW	DHCPv6이 재개 중입니다.
DHCP6 REBIND	DHCPv6이 리바인딩입니다.


DHCPv6 상태	설명
DHCP6 INIT	DHCPv6이 초기화 중입니다.
DHCP6 SOLICIT	DHCPv6이 권유되고 있습니다.
DHCP6 REQUEST	DHCPv6이 요청 중입니다.
DHCP6 RELEASING	DHCPv6이 해제 중입니다.
DHCP6 RELEASED	DHCPv6이 해제되었습니다.
DHCP6 DISABLING	DHCPv6이 비활성화 중입니다.
DHCP6 DECLINING	DHCPv6이 거부되고 있습니다.
DHCP6 DECLINED	DHCPv6이 거부되었습니다.
DHCP6 INFOREQ	DHCPv6이 INFOREQ입니다.
DHCP6 INFOREQ DONE	DHCPv6이 INFOREQ DONE입니다.
DHCP6 INVALID	DHCPv6이 유효하지 않습니다(INVALID). 이것이 초기 상태입니다.
DISABLED DUPLICATE IPV6	DHCP6이 비활성화(DISABLED)되었지만, 중복 IPV6이 탐지되었습니다.
DHCP6 DECLINED DUPLICATE IP	DHCP6이 거부(DECLINED)되었지만, 중복 IPV6이 탐지되었습니다.
ROUTER ADVERTISE., (DUPLICATE IP)	자동 구성된 IPv6 주소가 중복되었습니다.
DHCP6 WAITING COLDBOOT TIMEOUT	DHCPv6이 부팅 중입니다.
DHCP6 TIMEOUT USING RESTORED VAL	플래시 메모리에 저장된 값을 사용하는 데 DHCPv6 시간 초과가 발생했습니다.
DHCP6 TIMEOUT CANNOT RESTORE	DHCP6 시간 초과가 발생했고 플래시 메모리에서 백업이 없습니다.
IPV6 STACK TURNED OFF	전화기가 IPv6 스택이 꺼진 IPv4 전용 모드에 있습니다.
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY	IPv6 주소가 라우터 또는 DHCPv6 서버에서 제공되지 않습니다.
ILLEGAL IPV6 STATE	부적합한 IPv6 상태이며 일어나면 안 됩니다.

## 무선 통계 화면 표시

이 절차는 무선 Cisco IP 전화기 8861에만 적용됩니다.

무선 통계 화면을 표시하려면, 다음 단계를 수행하십시오.

프로시저

- 
- 단계 1 애플리케이션  을 누릅니다.
- 단계 2 관리 설정 > 상태 > 통화 통계를 선택합니다.
- 단계 3 무선 통계를 0으로 재설정하려면 지우기를 누릅니다.
- 단계 4 무선 통계 화면을 종료하려면 종료를 누릅니다.
- 

## WLAN 통계

다음 표는 전화기의 WLAN 통계에 대해 설명합니다.

표 45: Cisco 유니파이드 IP 전화기의 WLAN 통계

항목	설명
tx 바이트	전화기에서 송신한 바이트 수입입니다.
rx 바이트	전화기에서 수신한 바이트 수입입니다.
tx 패킷	전화기에서 송신한 패킷 수입입니다.
rx 패킷	전화기에서 수신한 패킷 수입입니다.
tx 패킷 중단	송신 중 중단된 패킷 수입입니다.
rx 패킷 중단	수신 중 중단된 패킷 수입입니다.
tx 패킷 오류	전화기에서 송신한 오류 패킷 수입입니다.
rx 패킷 오류	전화기에서 수신한 오류 패킷 수입입니다.
Tx 프레임	성공적으로 송신된 MSDU 수입입니다.
tx 멀티캐스트 프레임	성공적으로 수신된 멀티캐스트 MSDU 수입입니다.
tx 재시도	한 번 이상 재송신 후 성공적으로 송신된 MSDU 수입입니다.
tx 멀티 재시도	한 번 이상 재송신 후 성공적으로 송신된 멀티캐스트 MSDU 수입입니다.
tx 실패	송신 시도 횟수가 재시도 제한을 초과하여 성공적으로 송신되지 않은 MSDU 수입입니다.

항목	설명
rts 성공	이 카운터는 CTS가 RTS에 대한 응답으로 수신될 때 증분됩니다.
rts 실패	이 카운터는 CTS가 RTS에 대한 응답으로 수신되지 않을 때 증분됩니다.
ack 실패	이 카운터는 예상될 때 ACK가 수신되지 않으면 증분됩니다.
rx 중복 프레임	시퀀스 제어 필드가 나타내는 수신된 프레임 수가 중복입니다.
rx 조각 패킷	데이터 또는 관리 유형의 성공적으로 수신된 MPDU 수입니다.
로밍 수	성공적인 로밍 수입니다.

## 통화 통계 창 표시


전화기에서 가장 최근 통화의 카운터, 통계 및 음질 메트릭을 표시하는 [통화 통계] 화면에 액세스할 수 있습니다.



**참고** 웹 브라우저를 사용해 스트리밍 통계 웹 페이지에 액세스하면, 통화 통계 정보를 원격에서 확인할 수 있습니다. 이 웹 페이지에는 전화기에는 제공되지 않는 추가 RTCP 통계가 포함되어 있습니다.

단일 통화에서 여러 개의 음성 스트림을 사용할 수 있지만, 데이터가 캡처되는 것은 최종 음성 스트림뿐입니다. 음성 스트림은 두 엔드포인트 간의 패킷 스트림입니다. 한 엔드포인트가 보류 상태가 되면, 통화가 연결된 상태라도 음성 스트림이 중단됩니다. 통화를 재개하면 새로운 음성 패킷 스트림이 시작되고, 새 통화 데이터가 이전 통화 데이터를 덮어씁니다.

### 프로시저

- 단계 1 애플리케이션  을 누릅니다.
- 단계 2 관리 설정 > 상태 > 통화 통계를 선택합니다.
- 단계 3 통화 통계 화면을 종료하려면 종료를 누릅니다.

### 통화 통계 필드

다음 표에서는 통화 통계 화면에 포함되어 있는 항목에 대해 설명합니다.

표 46: Cisco 유니파이드 Phone의 통화 통계 항목


항목	설명
수신자 코덱	수신된 음성 스트림의 유형(코덱으로부터의 RTP 스트리밍 오디오): <ul style="list-style-type: none"> <li>• G.729</li> <li>• G.722</li> <li>• G722.2 AMR-WB</li> <li>• G.711 mu-law</li> <li>• G.711 A-law</li> <li>• iLBC</li> <li>• Opus</li> <li>• iSAC</li> </ul>
송신자 코덱	전송한 음성 스트림의 유형(코덱으로부터의 RTP 스트리밍 오디오): <ul style="list-style-type: none"> <li>• G.729</li> <li>• G.722</li> <li>• G722.2 AMR-WB</li> <li>• G.711 mu-law</li> <li>• G.711 A-law</li> <li>• iLBC.</li> <li>• Opus</li> <li>• iSAC</li> </ul>
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.

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

## 현재 액세스 지점 창 표시

현재 액세스 지점 화면은 Cisco IP 전화기 8861이 무선 통신을 위해 사용하는 액세스 지점에 대한 통계를 표시합니다.

## 프로시저

단계 1 애플리케이션  을 누릅니다.

단계 2 관리 설정 > 상태 > 현재 액세스 지점을 선택합니다.

단계 3 현재 액세스 지점 화면을 종료하려면 종료를 누릅니다.

## 현재 액세스 지점 필드

다음 표에서는 현재 액세스 지점 화면의 필드에 대해 설명합니다.

표 47: 현재 액세스 지점 항목

항목	설명
AP 이름	CCX 규격을 준수할 경우 AP의 이름이며, 그렇지 않으면 MAC 주소가 여기에 표시됩니다.
MAC 주소	AP의 MAC 주소입니다.
빈도	이 AP가 관찰된 최신 빈도입니다.
현재 채널	이 AP가 관찰된 최신 채널입니다.
마지막 RSSI	이 AP가 관찰된 최신 RSSI입니다.
표지 간격	표지 간 시간 단위 수입니다. 시간 단위는 1.024ms입니다.
기능	이 필드는 요청되거나 광고된 선택적 기능을 나타내는 데 사용되는 다양한 하위 필드를 포함합니다.
기본 속도	AP에 필요한 데이터 속도 및 스테이션이 작동할 수 있어야 하는 AP입니다.
선택 속도	AP가 지원하는 데이터 속도 및 스테이션이 작동하는 선택적 AP입니다.
지원되는 VHT(rx) 속도	VHT는 AP에서 수신한 RX MCS 세트를 지원합니다.
지원되는 VHT(tx) 속도	VHT는 AP에서 수신한 TX MCS 세트를 지원합니다.
지원되는 HT MCS	HT는 AP에서 수신한 MCS 세트를 지원합니다.
DTIM 기간	n번째 표지마다 dtime 기간입니다. 각 DTIM 표지 후, AP는 절전 장치용으로 대기열에 있는 브로드캐스트 또는 멀티캐스트 패킷을 보냅니다.
국가 코드	두 자릿수 국가 코드입니다. 국가 정보 요소(IE)가 표지에 없는 경우에는 국가 정보를 표시할 수 없습니다.



항목	설명
채널	(국가 IE에서) 지원되는 채널 목록입니다.
전력 제약 조건	관리 도메인 제한에서 최대 전송 전력을 줄여야 하는 전력량입니다.
전력 제한	해당 채널에 대해 허용되는 최대 전송 전력(dBm)입니다.
채널 활용도	물리적 또는 가상 CS(Carrier Sense) 메커니즘에 나타난 대로, AP에서 매체가 사용 중임을 감지한 시간의 백분율(255로 정규화됨)입니다.
스테이션 수	이 AP와 현재 연결된 총 STA 수입니다.
승인 수용 능력	초당 32ms 초 단위로, 명시적 승인 제어를 통해 사용할 수 있는 남은 매체 시간을 지정하는 부호 없는 정수입니다. 값이 0이면 AP가 이 정보 요소를 지원하지 않고 수용 능력을 알 수 없습니다.
WMM 지원됨	Wi-Fi 멀티미디어 확장을 지원합니다.
UAPSD 지원됨	AP는 UAPSD(Unscheduled Automatic Power Save Delivery)를 지원합니다. WMM이 지원되는 경우에만 사용할 수 있습니다. 이 기능은 통화 시간과 무선 IP 전화기에서 최대 통화 밀도에 도달하는 데 중요합니다.
프록시 ARP	CCX 준수 AP는 연결된 스테이션 대신 IP ARP 요청에 대한 응답을 지원합니다. 이 기능은 무선 IP 전화기에서의 대기 시간에 중요합니다.
CCX 버전	AP가 CCX를 준수하는 경우 이 필드는 CCX 버전을 나타냅니다.
Best Effort	Best Effort 대기열과 관련된 정보를 포함합니다.
배경	배경 대기열과 관련된 정보를 포함합니다.
영상	영상 대기열과 관련된 정보를 포함합니다.
음성	음성 대기열과 관련된 정보를 포함합니다.

## 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 표시됩니다.
- 네트워크 통계: 네트워크 트래픽에 관한 정보를 제공하는 하이퍼링크가 표시됩니다.
- 장치 로그: 문제 해결에 참조할 수 있는 정보를 제공하는 하이퍼링크가 표시됩니다.

- 스트리밍 통계: 다양한 스트리밍 통계를 표시하는 하이퍼링크가 표시됩니다.
- 시스템: 전화기를 다시 시작하는 하이퍼링크가 표시됩니다.

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 웹 페이지 액세스


전화기의 웹 페이지에 액세스하려면, 다음 단계를 수행합니다.



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.

- 장치 > 전화기를 선택하여 Cisco 통합 커뮤니케이션 매니저 관리에서 전화기를 검색합니다. Cisco Unified Communications Manager에 등록된 전화기는 전화기 찾기 및 나열 창과 전화기 구성 창 상단에 IP 주소를 표시합니다.
- Cisco IP 전화기에서 애플리케이션  을 누르고 관리자 설정 > 네트워크 설정 > 이더넷 설정 > IPv4 설정을 선택한 다음, IP 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

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



참고 다음 표의 일부 항목은 일부 전화기 모델에만 적용됩니다.

장치 정보 영역을 표시하려면 [전화기 웹 페이지 액세스, 240 페이지](#)에 설명된 대로, 전화기의 웹 페이지에 액세스한 다음, 장치 정보 하이퍼링크를 클릭합니다.

표 48: 장치 정보 항목

항목	설명
서비스 모드	전화기에 대한 서비스 모드입니다.
서비스 이름	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	전화기에서 실행되는 애플리케이션 펌웨어 버전입니다.
부트 로드 ID	부트 펌웨어 버전입니다.
버전	전화기에서 실행되는 펌웨어 식별자
키 확장 모듈 1	해당되는 경우 첫 번째 키 확장 모듈에 대한 식별자입니다. Cisco IP 전화기 8851, 8851NR, 8861, 8865 및 8865NR에 적용할 수 있습니다.
키 확장 모듈 2	해당되는 경우 두 번째 키 확장 모듈에 대한 식별자입니다. Cisco IP 전화기 8851, 8851NR, 8861, 8865 및 8865NR에 적용할 수 있습니다.
키 확장 모듈 3	해당되는 경우 세 번째 키 확장 모듈에 대한 식별자입니다. Cisco IP 전화기 8851, 8851NR, 8861, 8865 및 8865NR에 적용할 수 있습니다.
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. <ul style="list-style-type: none"> <li>• 장치 유형 - 하드웨어 유형을 표시합니다. 예: 모든 전화기 모델의 전화기 디스플레이</li> <li>• 장치 설명 - 표시된 모델 유형과 관련 있는 전화기의 이름을 표시합니다.</li> <li>• 제품 식별자 - 전화기 모델을 지정합니다.</li> <li>• 버전 ID(VID) - 주요 하드웨어 버전 번호를 지정합니다.</li> <li>• 일련 번호 - 전화기의 고유한 일련 번호를 표시합니다.</li> </ul>

항목	설명
키 확장 모듈 UDI	키 확장 모듈의 Cisco UDI(Unique Device Identifier)입니다. Cisco IP 전화기 8851, 8851NR, 8861, 8865 및 8865NR에 적용할 수 있습니다.
헤드셋 이름	왼쪽 열에 연결된 Cisco 헤드셋의 이름이 표시됩니다. 오른쪽 열에 표시되는 정보는 다음과 같습니다. <ul style="list-style-type: none"> <li>• 포트 - 헤드셋을 전화기에 연결하는 방법을 표시합니다. <ul style="list-style-type: none"> <li>• USB</li> <li>• 보조 장치</li> </ul> </li> <li>• 버전 - 헤드셋 펌웨어 버전을 표시합니다.</li> <li>• 무선 범위 - DECT 라디오에 대해 구성된 강도를 표시합니다. Cisco 헤드셋 560 시리즈에만 해당합니다.</li> <li>• 대역폭 - 헤드셋이 광대역 또는 협대역을 사용하는지 여부를 표시합니다. Cisco 헤드셋 560 시리즈에만 해당합니다.</li> <li>• 블루투스 - 블루투스가 활성화 또는 비활성화되었는지 표시합니다. Cisco 헤드셋 560 시리즈에만 해당합니다.</li> <li>• 전화 회의 - 전화 회의 기능이 활성화 또는 비활성화되었는지 여부를 표시합니다. Cisco 헤드셋 560 시리즈에만 해당합니다.</li> <li>• 펌웨어 소스 — 허용되는 펌웨어 업그레이드 방법을 표시 합니다. <ul style="list-style-type: none"> <li>• UCM만 제한</li> <li>• UCM 또는 Cisco Cloud에서 허용</li> </ul> </li> </ul> <p>Cisco 헤드셋 560 시리즈에만 해당합니다.</p>
시간	전화기가 속한 날짜/시간 그룹의 시간. 이 정보는 Cisco Unified Communications Manager에서 제공합니다.
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 가능한 메모리	전화기에서 사용하지 않은 메모리의 양
Java 힙 사용 가능한 메모리	가능한 내부 Java 힙 메모리의 양

항목	설명
Java 풀 사용 가능한 메모리	가능한 내부 Java 풀 메모리의 양
FIPS 모드 사용	FIPS(Federal Information Processing Standard) 모드의 활성화 여부를 표시합니다.

## 네트워크 설정

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

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



참고 다음 표의 일부 항목은 일부 전화기 모델에만 적용됩니다.

네트워크 설정 영역을 표시하려면 [전화기 웹 페이지 액세스, 240 페이지](#)에 설명된 대로, 전화기의 웹 페이지에 액세스한 다음, 네트워크 설정 하이퍼링크를 클릭합니다.

표 49: 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 주소입니다.
BOOTP 서버	전화기가 BootP(Bootstrap Protocol) 서버에서 구성을 받는지 알려줍니다.
DHCP	전화기에서 DHCP를 사용하는지를 알려줍니다.
IP 주소	전화기의 IPv4(인터넷 프로토콜) 주소입니다.
서브넷 마스크	전화기가 사용하는 서브넷 마스크입니다.
기본 라우터	전화기가 사용하는 기본 라우터입니다.
DNS 서버 1-3	전화기가 사용하는 기본 DNS 서버 (DNS Server 1)와 옵션 항목인 백업 DNS 서버(DNS Server 2 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.

항목	설명
DHCP 주소 해제됨	전화기의 [네트워크 구성] 메뉴에서 [DHCP 주소 해제됨] 옵션의 설정을 나타냅니다.
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.
CUCM 서버 1-5	<p>전화기가 등록할 수 있는 Cisco Unified Communications Manager 서버의 호스트 이름 또는 주소(우선 순위 순서)입니다. 또한 제한된 Cisco Unified Communications Manager 기능을 사용할 수 있는 SRST 라우터의 IP 주소가 항목에 표시될 수도 있습니다(해당 라우터가 제공되는 경우).</p> <p>사용 가능한 서버의 경우 Cisco Unified Communications Manager 서버 IP 주소와 다음 중 하나가 항목에 표시됩니다.</p> <ul style="list-style-type: none"> <li>• 활성 - 전화기가 현재 통화 처리 서비스를 받고 있는 Cisco Unified Communications Manager 서버</li> <li>• 대기 - 현재 서버가 서비스를 제공하지 못하는 경우 전화기가 대신 연결하는 Cisco Unified Communications Manager 서버</li> <li>• 공란 - Cisco Unified Communications Manager 서버에 현재 연결되어 있지 않음</li> </ul> <p>또한 SRST(Survivable Remote Site Telephony) 지정 사항이 항목에 포함될 수 있습니다. 사항을 통해 제한된 기능 집합으로 Cisco Unified Communications Manager 기능을 제공하는 SRST 라우터를 파악할 수 있습니다. 모든 기타 Cisco Unified Communications Manager 서버에 연결할 수 없게 되면 이 라우터가 통화 처리를 제어합니다. SRST Cisco Unified Communications Manager는 항상 서버 목록의 마지막에 표시됩니다(활성 상태인 경우도 마찬가지임). SRST 라우터 주소는 [Cisco Unified Communications Manager Configuration] 창의 [장치 풀] 섹션에서 생성할 수 있습니다.</p>
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 유니파이드 IP 전화기 서비스를 가져오는 서버의 URL입니다.
유휴 URL	[유휴 URL 시간] 필드에 지정한 시간 동안 전화기가 유휴 상태일 때 전화기에서 표시되는 URL입니다. 그리고 이 시간 동안 열리는 메뉴는 없습니다.
유휴 URL 시간	URL에서 지정한 XML 서비스가 활성화되기 전에 전화기가 유휴 상태로 메뉴가 열리는 시간(초 단위)입니다.
프록시 서버 URL	전화기의 HTTP 클라이언트를 대신해 비로컬 호스트 주소에 HTTP 요청을 하고, 비로컬 주소에서 전화기의 HTTP 클라이언트로 응답을 전송하는 프록시 서버의 URL입니다.
인증 URL	전화기에서 전화기 웹 서버에 생성되는 요청을 확인하는 데 사용하는 URL입니다.

항목	설명
SW 포트 설정	스위치 포트의 속도 및 전이중/반이중: <ul style="list-style-type: none"> <li>• A = 자동 설정</li> <li>• 10H = 10-BaseT/반이중</li> <li>• 10F = 10-BaseT/전이중</li> <li>• 100H = 100-BaseT/반이중</li> <li>• 100F = 100-BaseT/전이중</li> <li>• 1000F = 1000-BaseT/전이중</li> <li>• 링크 없음= 스위치 포트에 대한 연결 없음</li> </ul>
PC 포트 설정	PC 포트의 속도 및 전이중/반이중: <ul style="list-style-type: none"> <li>• A = 자동 설정</li> <li>• 10H = 10-BaseT/반이중</li> <li>• 10F = 10-BaseT/전이중</li> <li>• 100H = 100-BaseT/반이중</li> <li>• 100F = 100-BaseT/전이중</li> <li>• 1000F = 1000-BaseT/전이중</li> <li>• 링크 없음= PC 포트에 대한 연결 없음</li> </ul>
PC 포트 비활성화됨	전화기의 PC 포트의 활성화 상태를 알려줍니다.
사용자 로캘	전화기 사용자와 관련된 사용자 로케일입니다. 언어, 글꼴, 날짜 및 시간 서식, 영숫 텍스트 정보 등 자세한 사용자 지원 정보를 식별합니다.
네트워크 로케일	전화기 사용자와 관련된 네트워크 로케일입니다. 전화기에서 사용하는 신호음 및 소리에 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.
GARP 사용	전화기가 Gratuitous ARP 응답에서 MAC 주소를 확보하는지를 보여줍니다.
PC 포트에 연결	전화기가 네트워크 포트에서 액세스 포트로 전송되어 수신된 패킷을 착신 전환하는지 여부를 알려줍니다.
비디오 기능 사용	전화기가 적절한 장비를 갖춘 카메라에 연결되었을 때 영상 통화에 참여할 수 있는지를 알려줍니다.
음성 VLAN 사용	전화기가 음성 VLAN에 액세스할 수 있도록 PC 포트에 장치를 연결할 수 있게 허용 여부를 보여줍니다.
PC VLAN 사용	PC로 전송된 패킷의 802.1P/Q 태그를 식별하고 삭제하는 VLAN입니다.

항목	설명
자동 회선 선택 사용	전화기가 오프 후 상태로 전환될 때 전화기는 자동으로 회선 선택할지 식별합니다.
DSCP 프로토콜 제어	통화 제어 신호 처리를 위한 DSCP IP 분류입니다.
구성에 대한 DSCP	전화 구성 호전환을 위한 DSCP IP 분류입니다.
서비스에 대한 DSCP	전화 기반 서비스를 위한 DSCP IP 분류입니다.
보안 모드(비보안)	전화기에 설정된 보안 모드입니다.
웹 액세스 사용	웹 액세스가 활성화(예) 상태인지 비활성(아니요) 상태인지를 알려줍니다.
SSH 액세스 사용	SSH 포트가 활성화되었거나 비활성화되었는지를 나타냅니다.
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 포트의 활성화합니다. 전화기가 Cisco 스위치에 연결했을 때 스위치 포트의 CDP를 활성화합니다. Cisco Unified Communications Manager에서 CDP가 비활성화되면, 전화기가 Cisco 제품 스위치에 연결된 경우에만 스위치 포트의 CDP를 비활성화해야 한다는 내용의 경고가 나옵니다. 설정 메뉴에 현재 PC와 스위치 포트 CDP 값이 표시됩니다.
CDP: PC 포트	PC 포트에서 CDP가 지원되는지를 알려줍니다(기본값은 활성화). Cisco Unified Communications Manager에서 CDP가 비활성화되면, PC 포트의 CDP를 비활성화하면 CVTA가 작동하지 않는다는 내용의 경고가 표시됩니다. 설정 메뉴에 현재 PC와 스위치 포트 CDP 값이 표시됩니다.
LLDP-MED: SW 포트	스위치 포트에 LLDP-MED(Link Layer Discovery Protocol Media Endpoint Discovery)가 활성화되어 있는지를 알려줍니다.
LLDP-MED:PC 포트	PC 포트에서 LLDP-MED의 활성화 여부를 나타냅니다.
LLDP 전원 우선 순위	전화기에 전원을 공급할 수 있게 하는 스위치에 대한 전화기 전원 우선 순위입니다. 설정 메뉴와 같습니다. <ul style="list-style-type: none"> <li>• 알 수 없음: 기본값입니다.</li> <li>• 낮음</li> <li>• 높음</li> <li>• 중요</li> </ul>
LLDP 자산 ID	인벤토리 관리를 위해 전화기에 할당된 자산 ID입니다.
CTL 파일	CTL 파일의 MD5 해시입니다.



항목	설명
ITL 파일	초기 신뢰 목록이 포함된 ITL 파일입니다.
ITL 서명	ITL 파일의 MD5 해시입니다.
CAPF 서버	사용 중인 CPF 서버입니다.
TVS	기본적인 주요 보안 구성 요소입니다. TVS(Trust Verification Services)는 HTTPS가 있는 동안 Cisco 유니파이드 IP 전화기에서 EM 서비스, 디렉터리 및 MIDlet 같은 애플리케이션 서버를 인증하게 합니다.
TFTP 서버	전화기에서 사용하는 TFTP 서버의 이름입니다.
TFTP 서버	전화기에서 사용하는 TFTP 서버의 이름입니다.
자동 포트 동기화	전화기가 포트 속도를 자동으로 동기화하여 패킷 손실을 제거하는지를 나타냅니다.
전환 포트 원격 구성	SW 포트가 원격으로 제어되는지 여부를 나타냅니다.
PC 포트 원격 구성	PC 포트가 원격으로 제어되는지 여부를 나타냅니다.
IP 주소 지정 모드	주소 지정 모드를 식별합니다. <ul style="list-style-type: none"> <li>• IPv4 전용</li> <li>• IPv4 및 IPv6</li> <li>• IPv6 전용</li> </ul>
IP 기본 설정 모드 제어	전화기에 IPv4 및 IPv6가 모두 제공될 때, Cisco Unified Communications Manager로 연결하는 동안 전화기가 사용하는 IP 주소 버전을 보여줍니다.
미디어용 IP 기본 설정 모드	
IPv6 자동 구성	미디어를 위해 장치에서 IPv4 주소를 사용해 Cisco Unified Communications Manager로 연결하고 있음을 보여줍니다.
IPv6 중복 주소 보호	
IPv6 재전송 메시지 허용	전화기에서 대상 번호에 사용되는 것과 동일한 라우터의 재전송 메시지를 수락하는지 여부를 나타냅니다.
IPv6 Reply 멀티캐스트 에코 요청	IPv6 전용 주소로 전송된 에코 요청 메시지에 응답하여 전화기에서 에코 회신 메시지를 수신하는지 여부를 알려줍니다.
IPv6 로드 서버	전화기 펌웨어 업그레이드를 위한 설치 시간을 최적화하고 이미지를 로컬로 저장하여 WAN 링크를 이동할 필요가 없도록 하여 WAN을 오프로드하는 데 도움이 됩니다.

항목	설명
IPv6 로그 서버	
IPv6 CAPF 서버	전화기가 로그 메시지를 보내는 원격 로깅 시스템의 IP 주소 및 포트를 보여줍니다.
DHCPv6	전화기가 IPv6-전용 주소를 가져오기 위해 사용하는 방법을 나타냅니다. DHCPv6가 활성화되었을 때 전화기는 DHCPv6 서버 또는 IPv6 사용 가능 라우터가 보 SLAAC에서 IPv6 주소를 가져옵니다. 그리고 DHCPv6가 비활성화된 경우 전화기는 상 (DHCPv6 서버에서) 또는 비상대유지(SLAAC에서) IPv6 주소를 가지지 않습니다. 참고 DHCPv4와 달리, DHCPv6는 비활성화되었다더라도 자동 구성이 활성화되면 는 여전히 SLAAC 주소를 생성할 수 있습니다.
IPv6 주소	전화기의 현재 IPv6 전용 주소를 표시합니다. 두 가지 주소 형식이 지원됩니다. <ul style="list-style-type: none"> <li>• 콜론으로 구분된 16진수 숫자의 8개 세트 X:X:X:X:X:X:X:X</li> <li>• 연속 0 그룹의 1회 연속을 이중 콜론으로 나타난 단일 그룹으로 축소하는 압축 형</li> </ul>
IPv6 접두사 길이	서브넷에 대한 현재 IPv6 전용 접두사 길이를 표시합니다.
IPv6 기본 라우터	전화기에서 사용되는 기본 IPv6 라우터를 표시합니다.
IPv6 DNS 서버 1-2	전화기에서 사용되는 기본 및 보조 DNSv6 서버를 표시합니다.
IPv6 대체 TFTP	보조 IPv6 TFTP 서버가 사용되는지 여부를 표시합니다.
IPv6 TFTP 서버 1-2	전화기에서 사용되는 기본 및 보조 IPv6 TFTP 서버를 표시합니다.
IPv6 주소 해제됨	사용자가 IPv6 관련 정보를 해제했는지 여부를 표시합니다.
Energywise 전력 레벨	전화기가 대기 중일 때 사용되는 전원 수준입니다.
EnergyWise 영역	전화기가 소속된 EnergyWise 도메인입니다.
DF_BIT	패킷에 대한 DF 비트 설정을 나타냅니다.

## 네트워크 통계

전화기 웹 페이지의 다음 [네트워크 통계] 하이퍼링크에서는 전화기의 네트워크 트래픽에 관한 정보를 제공합니다.

- 이더넷 정보: 이더넷 트래픽에 관한 정보를 표시합니다.
- 액세스: 전화기의 PC 포트를 오가는 네트워크 트래픽에 관한 정보를 표시합니다.
- 네트워크: 전화기의 네트워크 포트를 오가는 네트워크 트래픽에 관한 정보를 표시합니다.

[네트워크 통계] 영역을 표시하려면 전화기의 웹 페이지에 액세스한 다음, 이더넷 정보, 액세스 또는 네트워크 하이퍼링크를 클릭합니다.

### 이더넷 정보 웹 페이지

다음 표에서는 이더넷 정보 웹 페이지의 콘텐츠에 대해 설명합니다.

표 50: 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

### 액세스 및 네트워크 웹 페이지

다음 표에서는 액세스 및 네트워크 웹 페이지에 포함되어 있는 정보에 대해 설명합니다.

표 51: 액세스 및 네트워크 필드

항목	설명
Rx totalPkt	전화기에서 수신한 총 패킷 수
Rx crcErr	CRC가 실패했을 때 수신한 총 패킷 수
Rx alignErr	잘못된 FCS(Frame Check Sequence)가 있을 때 수신된 64바이트 및 1522바이트 길이의 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 shortErr	64바이트보다 작은 수신된 FCS 오류 패킷이나 Align 오류 패킷의 총 수

항목	설명
Rx shortGood	64바이트보다 작은 올바른 수신 패킷의 총 수
Rx longGood	1522바이트보다 큰 올바른 수신 패킷의 총 수
Rx longErr	1522바이트보다 큰 수신된 FCS 오류 패킷이나 Align 오류 패킷의 총 수
Rx size64	잘못된 패킷을 포함해 크기가 0에서 64바이트 사이의 수신 패킷의 총 수
Rx size65to127	잘못된 패킷을 포함해 크기가 65에서 127바이트 사이의 수신 패킷의 총 수
Rx size128to255	잘못된 패킷을 포함해 크기가 128에서 255바이트 사이의 수신 패킷의 총 수
Rx size256to511	잘못된 패킷을 포함해 크기가 256에서 511바이트 사이의 수신 패킷의 총 수
Rx size512to1023	잘못된 패킷을 포함해 크기가 512에서 1023바이트 사이의 수신 패킷의 총 수
Rx size1024to1518	잘못된 패킷을 포함해 크기가 1024에서 1518바이트 사이의 수신 패킷의 총 수
Rx tokenDrop	리소스 부족(예: FIFO 오버플로)으로 인해 중단된 총 패킷 수
Tx excessDefer	미디어 사용량이 많아 전송 중에 지연된 총 패킷 수
Tx lateCollision	패킷 전송을 시작한 이후 512비트 시간보다 늦게 충돌이 발생한 횟수
Tx totalGoodPkt	전화기에서 수신한 올바른 패킷(멀티캐스트, 브로드캐스트 및 유니캐스트)의 총 수
Tx Collisions	패킷이 전송되는 동안 발생한 총 충돌 횟수
Tx excessLength	패킷이 16번의 전송 시도를 경험하여 전송되지 못한 총 패킷 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

항목	설명
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 IPv6 주소	CDP 프로토콜이 발견한 인접 장치의 IP 주소
CDP 인접 포트	CDP 프로토콜이 발견한 전화기에 연결된 인접 장치 포트
LLDP 인접 장치 ID	LLDP가 발견한 이 포트에 연결된 장치 식별자
LLDP 인접 IPv6 주소	LLDP 프로토콜이 발견한 인접 장치의 IP 주소
LLDP 인접 포트	LLDP 프로토콜이 발견한 전화기에 연결된 인접 장치 포트
포트 정보	속도 및 전이중/반이중 정보

## 장치 로그

전화기 웹 페이지의 다음 장치 로그 하이퍼링크에서는 전화기를 모니터링하고 문제 해결에 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 켜 후 현재까지 전화기가 생성한 10개의 가장 최신 상태 메시지가 표시됩니다. 이 정보는 전화기의 [상태 메시지] 화면에도 표시됩니다.
- 디버그 표시: 문제 해결에 도움이 필요할 경우, Cisco TAC에게 유용할 수도 있는 디버그 메시지를 표시합니다.

## 스트리밍 통계

Cisco 유니파이드 IP 전화기는 최대 3개의 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.

다음 표에서는 스트리밍 통계에 포함되어 있는 항목에 관해 설명합니다.

표 52: 스트리밍 통계 항목

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 전송 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 전용으로 설정되면 값은 0입니다.
송신자 옥텟	연결을 시작한 이후 전화기가 RTP 데이터 패킷으로 전송한 총 페이로드 옥텟 수. 이 수신 전용 모드로 설정되면 값은 0입니다.
송신자 코덱	전송된 스트리밍을 위한 오디오 인코딩 유형
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 지연되거나 중복된 모든 패킷이 포함됩니다. 연결이 송신 전용 모드로 설정되면 값은 0으로 표시됩니다.
평균 지터	밀리초 단위로 측정되는 RTP 데이터 패킷 도착 간격 시간의 표준 편차 추정치. 연결이 송신 전용 모드로 설정되면 값은 0으로 표시됩니다.
수신자 코덱	수신된 스트리밍에 사용된 오디오 인코딩 유형
수신자 보고서 전송 (설명 참조)	RTCP 수신자 보고서가 전송된 횟수
수신자 보고 시간 전송 (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. 통화기 캐스트 통화인 경우 다양한 소스에서 수신한 패킷이 포함됩니다. 연결이 송신 전용으로 설정되면 값은 0으로 표시됩니다.

항목	설명
수신자 옥텟	연결을 시작한 이후 장치가 RTP 데이터 패킷으로 수신한 총 페이로드 옥텟 수 멀티캐스트 통화인 경우 다양한 소스에서 수신한 패킷이 포함됩니다. 연결이 모드로 설정되면 값은 0으로 표시됩니다.
MOS LQK	청취 품질(LQK)에 대한 평균 평가점(MOS)의 객관적인 측정 점수입니다. 5(홀 1(나쁨)로 평가됩니다. 이 점수는 음성 스트림의 선행 8초 간격에서 유실된 프 가청 은닉 이벤트에 기반합니다. 자세한 내용은 <a href="#">음질 모니터링, 282 페이지</a> 의 조하십시오.  참고 MOS LQK 점수는 Cisco 유니파이드 IP 전화기가 사용하는 코덱 유 인해 달라질 수 있습니다.
평균 MOS LQK	전체 음성 스트림에 관찰되는 평균 MOS LQK 점수입니다.
최소 MOS LQK	음성 스트림 시작부터 관찰되는 최저 MOS LQK 점수입니다.
최대 MOS LQK	음성 스트림 시작부터 관찰되는 기준선 또는 최고 MOS LQK 점수입니다.  이러한 코덱은 프레임 유실 없이 정상적인 조건에서 다음 최대 MOS LQK 점 합니다.  • G.711은 4.5를 생성합니다. • G.729 A /AB는 3.7을 생성합니다.
MOS LQK 버전	MOS LQK 점수를 계산하는 데 사용되는 Cisco의 독점적 알고리즘 버전입니다
누적 숨김률	음성 스트림을 시작하고 수신한 총 스피치 프레임(speech frame) 수로 숨긴 전 의 수를 나눈 값
간격 숨김률	활성 스피치 앞의 3초 간격 동안 스피치 프레임에 포함된 숨김 프레임 비율. V activity detection)가 사용되면, 3초의 활성 스피치를 모으는 데 더 긴 시간이 필 있습니다.
최대 숨김률	음성 스트림을 시작한 이후 가장 높은 간격 숨김률
숨김(초)	음성 스트림을 시작한 이후 숨김 이벤트가 발생한 시간(초 단위, 엄격하게 숨 이 포함됨)
엄격한 숨김(초)	음성 스트림을 시작한 이후 5%가 넘는 숨김 이벤트(손실 프레임)가 발생한 시 위)
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)

항목	설명
송신자 보고서 수신 (설명 참조)	RTCP 송신자 보고서가 수신된 횟수
송신자 보고 시간 수신 (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
수신자 보고서 수신 (설명 참조)	RTCP 수신자 보고서가 수신된 횟수
수신자 보고 시간 수신 (설명 참조)	RTCP 수신자 보고서가 수신된 가장 최근 시간
수신자 암호화됨	수신자가 암호화를 사용하는 경우를 나타냅니다.
송신자 암호화됨	송신자가 암호화를 사용하는 경우를 나타냅니다.
송신자 프레임	전송된 프레임 수입니다.
송신자 부분 프레임	전송된 부분 프레임 수입니다.
송신자 i 프레임	전송된 I 프레임 수입니다. I 프레임은 비디오 전송에 사용됩니다.
송신자 IDR 프레임	전송된 즉석 디코더 새로 고침(IDR) 프레임 수입니다. IDR 프레임은 비디오 전송에 사용됩니다.
송신자 프레임 비율	송신자가 프레임을 전송하는 비율입니다.
송신자 대역폭	송신자의 대역폭입니다.
송신자 해상도	송신자의 비디오 해상도입니다.
수신자 프레임	수신된 프레임 수입니다.
수신자 부분 프레임	수신된 부분 프레임 수입니다.
수신자 i 프레임	수신된 I 프레임 수입니다.
수신자 IDR 프레임	수신된 IDR 프레임 수입니다.
수신자 IFrame 필요	수신된 요청 IDR 프레임 수입니다.
수신자 프레임 비율	수신자가 프레임을 수신하는 비율입니다.
수신자 프레임 손실	수신되지 않은 프레임 수입니다.



항목	설명
수신자 프레임 오류	수신되지 않은 프레임 수입니다.
수신자 대역폭	수신자의 대역폭입니다.
수신자 해상도	수신자의 비디오 해상도입니다.
도메인	전화기가 있는 도메인입니다.
송신자 참가	송신자가 참가한 횟수입니다.
수신자 참가	수신자가 참가한 횟수입니다.
작별인사	“작별 인사” 프레임 수입니다
송신자 시작 시간	송신자가 시작한 시간입니다.
수신자 시작 시간	수신자가 시작한 시간입니다.
행 상태	전화기 스트리밍 여부
송신자 도구	스트림에 사용되는 오디오 인코딩 유형
송신자 보고서	RTCP 송신자 보고서
송신자 보고 시간	RTCP 송신자 보고서가 전송된 마지막 시간입니다.
수신자 지터	스트림의 최대 지터
수신자 도구	스트림에 사용되는 오디오 인코딩 유형
수신자 보고서	웹 페이지에서 이 스트리밍 통계 보고서에 액세스한 횟수입니다.
수신자 보고 시간	이 스트리밍 통계 보고서가 생성될 때를 나타내는 내부 타임 스탬프입니다.
비디오	통화가 영상 통화인지 또는 오디오 전용인지 나타냅니다.
통화 ID	통화의 ID입니다.
그룹 ID	전화기가 있는 그룹의 ID입니다.



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

## 문제 해결

- 일반 문제 해결 정보, 259 페이지
- 시작 문제, 260 페이지
- 전화기 재설정 문제, 265 페이지
- 전화기가 LAN에 접속할 수 없음, 267 페이지
- Cisco IP 전화기 보안 문제, 267 페이지
- 영상 통화 문제, 269 페이지
- 일반적인 전화기 통화 문제, 271 페이지
- 문제 해결 절차, 272 페이지
- Cisco Unified Communications Manager의 디버그 제어 정보, 276 페이지
- 추가 문제 해결 정보, 277 페이지

## 일반 문제 해결 정보

다음 표에서는 Cisco IP 전화기의 일반적인 문제 해결 정보를 제공합니다.

표 53: Cisco IP 전화기 문제 해결

요약	설명
Cisco IP 전화기와 다른 Cisco IP 전화기 연결	Cisco는 PC 포트를 통해 IP 전화기를 다른 IP 전화기에 연결하는 것을 지원하지 않습니다. 각 IP 전화기는 스위치 포트에 직접 연결해야 합니다. 서로 PC 포트를 사용하여 서로 연결된 여러 전화기는 작동하지 않습니다.
장기적인 브로드캐스트 스톰으로 인해 IP 전화기가 재설정되거나 전화를 걸거나 받을 수 없게 됨	음성 VLAN 상에서 장기적인 레이어 2 브로드캐스트 스톰(몇 분간 발생하여 IP 전화기가 재설정되거나, 진행 중인 통화가 중단되거나, 하거나 전화를 받을 수 없게 될 수 있습니다. 전화기는 브로드캐스트 끝날 때까지 작동하지 않을 수도 있습니다.

요약	설명
전화기에서 워크스테이션으로 네트워크 연결 이동	<p>네트워크 연결을 통해 전화기에 전원을 공급한다면, 전화기의 네트워크 케이블을 뽑아 데스크톱 컴퓨터에 꽂을 때 주의해야 합니다.</p> <p>주의      컴퓨터의 네트워크 카드는 네트워크 연결을 통해 전원을 얻을 수 없습니다. 따라서 전원이 이 연결을 통해 공급된다면 워크 카드가 손상될 수 있습니다. 네트워크 카드를 보호하는 전화기에서 케이블을 뽑아 컴퓨터에 꽂을 때까지 10초 기다리십시오. 이렇게 하면 스위치에서 해당 회선에 전화기 이상 존재하지 않음이 인식되고 케이블에 대한 전원 공급할 충분한 시간을 줄 수 있습니다.</p>
전화기 구성 변경	<p>기본적으로 네트워크 구성 옵션은 사용자가 네트워크 연결에 영향을 있는 변경 작업을 수행하지 못하도록 잠겨 있습니다. 따라서 네트워크 구성을 구성하려면 설정 잠금을 해제해야 합니다. 자세한 내용은 <a href="#">전화기 용, 50 페이지</a>를 참조하십시오.</p> <p>참고      일반 전화기 프로파일에 관리자 암호가 설정되어 있지 않거나 사용자가 네트워크 설정을 수정할 수 있습니다.</p>
전화기와 기타 장치 간의 코덱 불일치	<p>RxType 및 TxType 통계는 이 Cisco IP 전화기와 기타 장치 간의 대화에 코덱을 보여줍니다. 이 통계값은 일치해야 합니다. 만약 이 값이 일치 않으면, 기타 장치에서 코덱 대화를 처리할 수 있는지 또는 트랜스코더기를 처리할 준비가 되어 있는지 확인합니다.</p>
전화기와 기타 장치 간의 사운드 샘플 불일치	<p>RxSize 및 TxSize 통계는 이 Cisco IP 전화기와 기타 장치 간의 대화에 음성 패킷의 크기를 보여줍니다. 이 통계값은 일치해야 합니다.</p>
루프백 조건	<p>루프백 조건은 다음 조건이 만족하면 발생합니다.</p> <ul style="list-style-type: none"> <li>• 전화기의 [네트워크 구성] 메뉴에 있는 SW 포트 구성 옵션이 10 (10-BaseT/반이중)으로 설정되어 있을 때</li> <li>• 전화기가 외부 부전원 공급 장치에서 전원을 공급받을 때</li> <li>• 전화기의 전원을 끈 상태일 때(전원 공급 장치 연결이 끊어짐)</li> </ul> <p>이 경우 전화기의 스위치 포트는 비활성화될 수 있고, 스위치 콘솔 로그와 같은 메시지가 표시됩니다.</p> <p>HALF_DUX_COLLISION_EXCEED_THRESHOLD</p> <p>이 문제를 해결하려면 스위치에서 포트를 다시 활성화합니다.</p>

## 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](#), 66 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 활성화 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 컵니다.
- 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](#), 66 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, 272 페이지](#)를 참조하십시오.

### 전화기에 오류 메시지 표시

#### 문제

시작하는 동안 상태 메시지에서 오류를 표시합니다.

#### 해결 방법

시작 프로세스를 통해 전화기가 전원을 켜다 켜기 때문에, 문제의 원인에 관한 정보를 제공할 수도 있는 상태 메시지에 액세스할 수 있습니다.

#### 관련 항목

[상태 메시지 창 표시](#), 225 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](#), 273 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.

## 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.

## 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, 276 페이지](#)의 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.

## 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, 73 페이지](#)에서 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, 72 페이지](#)를 참조하십시오.

이미 Cisco Unified Communications Manager 데이터베이스에 전화기가 존재한다면 구성 파일이 손상되었을 수도 있습니다. 자세한 내용은 [구성 파일 변조, 263 페이지](#)를 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 등록되지 않음

### 문제

전화기 화면에 "활성화 코드 또는 서비스 도메인 입력"이라는 프롬프트가 표시됩니다.

### 해결 방법

전화기에 TFTP 주소가 없습니다. 옵션 150이 DHCP 서버에서 제공되는지 또는 대체 TFTP가 수동으로 구성되었는지 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.

### 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 애플리케이션  을 누르고 관리자 설정 > 상태 > 네트워크 통계를 선택하면 Cisco IP 전화기가 Cisco Unified Communications Manager로부터 재설정 명령을 받았는지 확인할 수 있습니다.

- [재시작 원인] 필드에 재설정-재설정이라고 표시되면, 전화기는 Cisco 통합 커뮤니케이션 매니저 관리에서 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, 273 페이지](#)에 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.

## 영상 통화 문제

### 두 Cisco IP Video Phone 간의 영상 없음

#### 문제

두 Cisco IP video phone 간에 비디오가 스트리밍되지 않습니다.

### 해결 방법

MTP(Media Termination Point)가 통화 흐름에 사용되고 있는지 확인합니다.

## 비디오 화면이 끊기거나 프레임이 손실됨

### 문제

영상 통화 중일 때 비디오가 버퍼링되거나 프레임이 손실됩니다.

### 해결 방법

이미지 품질은 통화의 대역폭에 따라 다릅니다. 비트 전송률을 높이면 비디오 품질이 향상되지만 추가 네트워크 리소스가 필요합니다. 항상 비디오 유형에 가장 적합한 비트 전송률을 사용하십시오. 720p 및 초당 15 프레임의 영상 통화에는 790kbps 이상의 비트 전송률이 필요합니다. 720p 및 초당 30 프레임의 영상 통화에는 1360kbps 이상의 비트 전송률이 필요합니다.

대역폭에 대한 자세한 내용은 "전화기 기능 및 설정" 장의 비디오 전송 해상도 설정 섹션을 참조하십시오.

### 해결 방법

영상 통화 매개 변수에 대한 최대 세션 비트 전송률이 최소 비디오 비트 전송률 범위로 구성되었는지 확인합니다. Cisco Unified Communications Manager에서 시스템 > 지역 정보 > 지역으로 이동합니다.

## 영상 통화를 호전환할 수 없습니다

### 문제

사무실 전화기에서 휴대폰으로 영상 통화를 호전환할 수 없습니다.

### 해결 방법

Cisco 유니파이드 Mobility는 영상 통화로 확장되지 않습니다. 사무실 전화기로 수신된 영상 통화는 휴대폰에서 당겨받을 수 없습니다.

## 전화회의 동안 영상 없음

### 문제

통화에 두 명 이상의 통화자를 추가하면 영상 통화가 음성 통화로 전환됩니다.

임시 및 Meet-Me 화상 회의에 대해 화상 회의 브리지를 사용해야 합니다.



## 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) 소프트웨어가 전화기에서 생성하는 것과 동일한 정보가 생성됩니다.

문제 보고서에는 전화기와 헤드셋에 대한 정보가 포함되어 있습니다.

프로시저

- 
- 단계 1 Cisco Unified CM 관리에서 장치 > 전화를 선택합니다.
  - 단계 2 찾기를 클릭하고 하나 이상의 Cisco IP 전화를 선택합니다.
  - 단계 3 선택한 Cisco IP 전화기에 사용된 헤드셋에 대한 PRT 로그를 수집하려면 선택 항목에 대한 **PRT** 생성을 클릭합니다.
- 


### 전화기에서 콘솔 로그 만들기

전화기가 네트워크에 연결되지 않고 PRT(문제 보고서 도구)에 액세스할 수 없는 경우 콘솔 로그를 생성합니다.

시작하기 전에


전화기의 뒤쪽에 있는 보조 포트에 콘솔 케이블을 연결합니다.

프로시저

- 
- 단계 1 전화기에서 애플리케이션  을 누릅니다.
  - 단계 2 관리 설정 > Aux 포트에 이동합니다.
  - 단계 3 콘솔 로그 수집을 선택하여 장치 로그를 수집합니다.
-

## TFTP 설정 확인

프로시저

- 단계 1 Cisco IP 전화기에서 애플리케이션  을 누르고 관리 설정 > 네트워크 설정 > 이더넷 설정 > IPv4 설정 > TFTP Server 1을 선택합니다.
- 단계 2 전화기에 고정 IP 주소를 지정했다면, TFTP Server 1 옵션에 대한 설정을 수동으로 입력해야 합니다.
- 단계 3 DHCP를 사용하고 있다면, 전화기는 DHCP 서버에서 TFTP 서버에 대한 주소를 확보합니다. 옵션 150에 IP 주소가 구성되어 있는지 확인합니다.
- 단계 4 전화기에서 대체 TFTP 서버를 사용하도록 할 수도 있습니다. 그러한 설정은 최근 전화기가 원래 위치에서 다른 곳으로 이동한 경우 특히 유용합니다.
- 단계 5 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

[기본 재설정](#), 279 페이지

[전화기 MAC 주소 결정](#), 72 페이지

## DHCP 설정 확인

프로시저

단계 1 전화기에서 애플리케이션  을 누릅니다.

단계 2 **Wi-Fi** > 네트워크 설정 > **IPv4** 설정을 선택하고, 다음 옵션을 확인합니다.

- DHCP 서버: 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.

[http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod\\_tech\\_notes\\_list.html](http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html)

- IP 주소, 서브넷 마스크, 기본 라우터: 전화기에 고정 IP 주소를 할당했다면, 이 옵션에 대한 설정을 수동으로 입력해야 합니다.

단계 3 DHCP를 사용 중이라면, DHCP 서버에서 배포한 IP 주소를 확인합니다.

다음 URL에서 *Catalyst* 스위치나 엔터프라이즈 네트워크에서의 *DHCP* 문제 해결 문서를 참조하십시오.

[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a00800f0804.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml)

## 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

[Cisco Unified Communications Manager 설명서](#), xvii 페이지  
[전화기 추가 방식](#), 73 페이지

## 802.1X 인증 문제 식별

### 프로시저

단계 1 필수 구성 요소를 적절하게 구성했는지 확인하십시오.


단계 2 공유 비밀이 전화기에 구성되었는지 확인하십시오.

- 공유 비밀이 구성된 경우 인증 서버에 동일한 공유 비밀이 있는지 확인하십시오.
- 공유 비밀이 전화기에 구성되지 않은 경우 공유 비밀을 입력하고 이것이 인증 서버의 공유 비밀과 일치하는지 확인하십시오.

## DNS 설정 확인

DNS 설정을 확인하려면 다음 단계를 수행하십시오.

### 프로시저

단계 1 애플리케이션  을 누릅니다.

단계 2 관리자 설정 > 네트워크 설정 > IPv4 설정 > DNS 서버 1을 선택합니다.

단계 3 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 제어판이 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, 텔레포니, SIP, UI, 네트워크, 미디어, 업그레이드, 액세스 서버, 보안, Wi-Fi, VPN, Energywise, MobileRemoteAccess

참고      파라미터의 멀티 레벨 및 멀티 섹션 지원을 구현하려면 [로그 프로파일] 확인란을 선택합니다.

- 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




- 기본 재설정, 279 페이지
- 네트워크 구성 재설정 수행, 281 페이지
- 사용자 네트워크 구성 재설정 수행, 281 페이지
- CTL 파일 삭제, 281 페이지
- 품질 보고서 도구, 282 페이지
- 음질 모니터링, 282 페이지
- Cisco IP 전화기 청소, 284 페이지

## 기본 재설정

Cisco IP 전화기의 기본 재설정을 수행하면 전화기에 오류가 발생한 경우 이를 복구하고, 다양한 구성 및 보안 설정을 재설정 또는 복구할 수 있습니다.

다음 표에서는 기본 재설정 수행 방식에 대해 설명합니다. 전화기가 시작된 후 이러한 작업을 수행하면 전화기를 재설정할 수 있습니다. 상황에 작업을 선택합니다.

표 54: 기본 재설정 방식

작업	동작	설명
전화기 재시작	애플리케이션  을 누릅니다. 관리 설정 > 설정 재설정 > 장치 재설정으로 이동합니다.	변경 메모
설정 재설정	설정을 재설정하려면, 애플리케이션  을 누르고 관리자 설정 > 설정 재설정 > 네트워크를 선택합니다.	사용합니다.
	CTL 파일을 재설정하려면, 애플리케이션  을 누르고 관리자 설정 > 설정 재설정 > 보안을 선택합니다.	CTL

## 전화기 키패드에서 초기 설정으로 전화기 재설정

전화기를 초기 설정으로 재설정할 수 있습니다. 재설정하면 모든 전화기 매개 변수가 지워집니다.

## 프로시저

단계 1 다음 방법 중 하나로 전화기에서 전원을 제거합니다.

- 전원 어댑터 코드를 뽑습니다.
- LAN 케이블을 뽑습니다.

단계 2 5초 동안 기다립니다.

단계 3 #을 누른 상태에서 전화기를 다시 켜줍니다. 헤드셋과 스피커 버튼이 켜져 있을 때만 #에서 손을 뺍니다.

참고 일부 하드웨어 버전에서는 전화기를 다시 연결하면 헤드셋 및 스피커 버튼과 함께 음소거 버튼이 켜집니다. 그런 경우에는 헤드셋과 스피커 버튼이 다시 켜질 때에만 모두가 #에서 손을 뺍니다.

단계 4 다음 키 시퀀스를 입력합니다.

**123456789\*0#**

1 키를 누르면 헤드셋 버튼의 표시등이 꺼집니다. 키 시퀀스를 입력하면 음소거 버튼이 켜집니다.


주의 초기 재설정 프로세스가 완료될 때까지 전화기의 전원을 끄지 마십시오. 프로세스가 완료되면 기본 화면이 나타납니다.

전화기가 재설정됩니다.

## [전화기에서 모든 설정 재설정] 메뉴 수행

사용자 및 네트워크 설정을 기본값으로 재설정하려면 이 작업을 수행합니다.

## 프로시저

단계 1 애플리케이션  을 누릅니다.

단계 2 관리자 설정 > 설정 재설정 > 모든 설정을 선택합니다.

필요한 경우 전화기 옵션을 잠금 해제합니다.

## 백업 이미지에서 전화기 재부팅

Cisco IP 전화기에는 기본 이미지가 손상되었을 때 전화기를 복구할 수 있는 보조 백업 이미지가 있으며,

백업 이미지에서 전화기를 재부팅하려면 다음 절차를 수행하십시오.

### 프로시저

- 
- 단계 1 전원 공급 장치를 분리합니다.
  - 단계 2 별표(\*) 키를 길게 누릅니다.
  - 단계 3 전원을 다시 연결합니다. 음소거 LED가 꺼질 때까지 계속 별표 키를 누릅니다.
  - 단계 4 별표 키를 놓습니다.  
전화기가 백업 이미지로 재부팅됩니다.
- 

## 네트워크 구성 재설정 수행

네트워크 구성 설정을 기본값으로 재설정하고 전화기를 다시 설정합니다. 이 방법을 사용하면 DHCP가 전화기의 IP 주소를 다시 구성합니다.

### 프로시저

- 
- 단계 1 관리자 설정 메뉴에서 필요할 경우 전화기 옵션을 잠금 해제합니다.
  - 단계 2 설정 재설정 > 네트워크 설정을 선택합니다.
- 

## 사용자 네트워크 구성 재설정 수행

변경한 사용자 및 네트워크 구성 변경 사항을 재설정합니다. 그러나 전화기가 플래시 메모리의 이전에 저장한 설정에 이를 기록하지 않기 때문에 전화기를 재시작합니다.

### 프로시저

- 
- 단계 1 관리자 설정 메뉴에서 필요할 경우 전화기 옵션을 잠금 해제합니다.
  - 단계 2 설정 재설정 > 장치 재설정을 선택합니다.
- 

## CTL 파일 삭제

전화기에서 CTL 파일만 삭제합니다.

## 프로시저

단계 1 관리자 설정 메뉴에서 필요할 경우 전화기 옵션을 잠금 해제합니다.

단계 2 설정 재설정 > 보안 설정을 선택합니다.

## 품질 보고서 도구

QRT(품질 보고서 도구)는 Cisco IP 전화기를 위한 음질 및 일반 문제 보고 도구입니다. QRT는 Cisco Unified Communications Manager 설치 중에 설치됩니다.

사용자 Cisco IP 전화기에 QRT를 구성할 수 있습니다. QRT를 구성하면, [보고서 품질]을 눌러 통화 문제를 보고할 수 있습니다. 이 소프트키나 버튼은 Cisco IP 전화기가 [연결], [전화회의 연결], [호전화 연결] 또는 [온훅] 상태일 때만 제공됩니다.

사용자가 [보고서 품질]을 누르면, 문제 범주 목록이 나타납니다. 사용자가 적절한 문제 범주를 선택하면, 이 피드백이 XML 파일로 기록됩니다. 기록된 실제 정보는 사용자 선택 및 대상 장치가 Cisco IP 전화기인지에 따라 달라집니다.

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

### 관련 항목

[Cisco Unified Communications Manager 설명서, xvii 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 55: 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.	<ul style="list-style-type: none"> <li>• 에코 또는 오디오 수준 같은 오디오 채널의 잡음 또는 왜곡</li> <li>• 셀룰러 네트워크나 전화 카드 네트워크에 대한 통화처럼 여러 개의 인코딩/디코딩을 거치는 탠덤 통화</li> <li>• 스피커폰, 핸드프리 휴대폰 또는 무선 헤드셋으로 인해 발생하는 음향 문제</li> </ul> <p>패킷 전송(TxCnt)과 패킷 수신(RxCnt) 카운터를 확인하여 음성 패킷이 잘 전달되는지 확인합니다.</p>
MOS LQK 지수가 크게 감소합니다.	<p>패킷 손실이나 높은 지터 수준으로 인한 네트워크 손상</p> <ul style="list-style-type: none"> <li>• 평균 MOS LQK 감소는 광범위하면서 확실적인 손상을 의미할 수 있습니다.</li> <li>• 개별 MOS LQK 감소는 버스티 손상을 의미할 수 있습니다.</li> </ul> <p>숨김률과 숨김(초)을 대조 검토하여 패킷 손실 및 지터의 증거를 찾습니다.</p>
MOS LQK 지수가 크게 증가합니다.	<ul style="list-style-type: none"> <li>• 전화기가 예상했던 것과는 다른 코덱을 사용하고 있지 않은지 확인합니다(RxType 및 TxType).</li> <li>• 펌웨어 업그레이드 후에 MOS LQK 버전이 변경되었는지 확인합니다.</li> </ul>



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, 285 페이지
- [국제 통화 로깅 지원](#), 285 페이지
- [언어 제한 사항](#), 286 페이지

## 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.

털리스에 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 털리스용 문서를 참조하십시오.



참고 최신 로케일 설치 관리자가 곧바로 제공되지 않을 수도 있으므로 웹 사이트에서 수시로 업데이트를 확인하십시오.

관련 항목

[Cisco Unified Communications Manager 설명서](#), xvii 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(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.

중국어 입력은 PC와 휴대폰에서 비슷하게 작동합니다. 중국어 입력이 작동하려면 중국어 로캘 설치 프로그램이 필요합니다.



## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.