



Cisco Unified Communications Manager 기능 구성 설명서, 릴리스 14 및 SU

초판: 2022년 6월 16일

최종 변경: 2023년 4월 25일

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

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

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

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

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

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

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

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

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)

© 2021–2023 Cisco Systems, Inc. 모든 권리 보유.



목 차

장 1	신규 및 변경된 정보 1
	신규 및 변경된 정보 1
부 I:	시작하기 5
장 2	기능 구성 개요 7
	기능 구성 설명서 정보 7
	전화기 기능 목록 생성 7
장 3	□구성도구 9
	기능 구성 설명서 정보 9
	구성 도구 개요 9
	Cisco Unified Communications Manager Administration 9
	Cisco Unified CM 관리에 로그인 10
	Cisco Unified Communications Manager 서비스 가용성 10
	Cisco Unified Communications Manager 서비스 가용성에 로그인 11
	전화기 기능 목록 생성 12
부 II:	원격 작업자 기능 13
장 4	Cisco Unified Mobility 15
	Cisco Unified Mobility 개요 15
	Wi-Fi에서 LTE로 통화 전환 16
	이동성 기능 16

Cisco Unified Mobility 사전 요건	18
Cisco Unified Mobility 구성 작업 흐름	19
이동성 사용자 구성	20
벌크 관리를 통해 이동성 사용자 구성	21
LDAP를 통한 이동성 사용자 프로비저닝	21
IP 전화기에 대한 이동성 구성	22
이동성에 대한 소프트키 템플릿 구성	23
기능 제어 정책 내에서 이동성 활성화	24
이동성을 위한 IP 전화기 구성	25
원격 대상 프로파일 구성	25
원격 대상 구성	26
액세스 목록 구성	27
모바일 음성 액세스 구성	28
Cisco Unified 모바일 음성 액세스 서비스 활성화	29
모바일 음성 액세스 활성화	30
모바일 음성 액세스에 대한 디렉터리 번호 구성	30
Cisco CallManager 서비스 다시 시작	31
원격 액세스를 위한 H.323 또는 SIP 게이트웨이 구성	31
원격 액세스를 위한 새로운 H.323 게이트웨이 구성	33
엔터프라이즈 기능 접근 (EFA) 구성	35
인텔리전트 세션 제어 구성	36
모빌리티 서비스 매개 변수 구성	37
Cisco Jabber 듀얼 모드 구성	37
기타 이중 모드 디바이스 구성	38
모빌리티 프로파일 구성	39
Cisco Jabber에 대한 이중 모드 디바이스 추가	39
이중 모드 디바이스 구성 필드	41
기타 이중 모드 디바이스 추가	41
모빌리티 ID 구성	42
전환 번호 구성	43
Cisco Unified Mobility 통화 흐름	43

스마트 클라이언트가 없는 SIP 트렁크를 통한 FMC	44
통신 사업자 통합 모바일 디바이스에 대한 헛트 그룹 로그인 및 로그아웃	44
Cisco Unified Mobility 상호 작용	45
Cisco Unified Mobility 제한 사항	47
Cisco Unified Mobility 문제 해결	51
데스크톱 전화기에서 통화를 재개할 수 없음	51

장 5

디바이스 모빌리티	53
디바이스 모빌리티 개요	53
디바이스 풀 할당	55
디바이스 모빌리티 그룹 운영 요약	56
디바이스 모빌리티 사전 요건	57
디바이스 모빌리티 설정 작업 흐름	58
디바이스 모빌리티 클러스터 수준 활성화	59
개별 디바이스에 대한 디바이스 모빌리티 활성화	59
물리적 위치 구성	60
디바이스 모빌리티 그룹 구성	60
디바이스 모빌리티를 위한 디바이스 풀 구성	60
디바이스 모빌리티 정보 구성	61
로밍 디바이스풀 매개 변수 보기	62
디바이스 모빌리티 상호 작용	62
디바이스 모빌리티 제한 사항	63

장 6

확장 및 연결	65
확장 및 연결 개요	65
확장 및 연결 사전 요건	66
구성 작업 흐름 확장 및 연결	66
사용자 계정 구성	67
사용자 권한 추가	67
CTI 원격 디바이스 생성	68
디바이스에 디렉터리 번호 추가	69

원격 대상 추가	69
원격 대상 확인	70
사용자를 디바이스에 연결	71
CTIRD (CTI 원격 디바이스) 통화 흐름	71
확장 및 연결 상호 작용	72
확장 및 연결 제한 사항	73

장 7

원격 작업자 비상 통화	75
원격 작업자 비상 통화 개요	75
원격 작업자 비상 통화 사전 요건	75
원격 작업자 비상 통화 구성 작업 흐름	76
사용자를 원격 작업자로 구성	76
비상 통화에 대한 대체 라우팅 지정	77
애플리케이션 서버 구성	77
E911 메시지 구성	78

장 8

모바일 및 원격 액세스 구성	79
모바일 및 원격 액세스 개요	79
모바일 및 원격 액세스 사전 요건	81
모바일 및 원격 액세스 구성 작업 흐름	82
Cisco AXL 웹 서비스 활성화	83
비디오에 대한 최대 세션 비트 레이트 구성	83
모바일 및 원격 액세스를 위한 디바이스폴 구성	84
ICE 구성	85
모바일 및 원격 액세스용 전화기 보안 프로파일 구성	86
Cisco Jabber 사용자에게 대한 모바일 및 원격 액세스 액세스 정책 구성	86
모바일 및 원격 액세스를 위한 사용자 구성	88
모바일 및 원격 액세스를 위한 엔드포인트 구성	88
모바일 및 원격 액세스를 위한 Cisco Expressway 구성	88
경량 Keepalive를 통한 MRA 페일오버	88

부 III:	원격 네트워크 액세스	91
장 9	무선랜	93
	무선 LAN 개요	93
	무선 LAN 구성 작업 흐름	93
	네트워크 액세스 프로파일 구성	94
	무선 LAN 프로파일 구성	94
	무선 LAN 프로파일 그룹 구성	94
	무선 LAN 프로파일 그룹을 디바이스 또는 디바이스폴에 연결	95
	무선 LAN 프로파일 그룹을 디바이스에 연결	95
	무선 LAN 프로파일 그룹을 디바이스폴에 연결합니다.	95
장 10	VPN 클라이언트	97
	VPN 클라이언트 개요	97
	VPN 클라이언트 사전 요건	97
	VPN 클라이언트 구성 작업 흐름	97
	전체 Cisco IOS 사전 요건	99
	IP 전화기를 지원하도록 Cisco IOS SSL VPN 구성	99
	AnyConnect에 대한 전체 ASA 사전 요건	101
	IP 전화기에서 VPN 클라이언트에 대한 ASA 구성	102
	VPN 집중 디바이스 인증서 업로드	104
	VPN 게이트웨이 구성	105
	VPN 클라이언트용 VPN 게이트웨이 필드	105
	VPN 그룹 구성	106
	VPN 클라이언트용 VPN 그룹 필드	106
	VPN 프로파일 구성	107
	VPN 클라이언트용 VPN 프로필 필드	107
	VPN 기능 매개 변수 구성	108
	VPN 기능 파라미터	109
	일반 전화 프로파일에 VPN 세부 정보 추가	110

부 IV: 라이선싱 111

장 11 라이선싱 113

라이선싱 113

Unified Communications Manager 라이선싱 114

라이선스 준수 115

사용자 전용 라이선스 116

디바이스 전용 116

사용자 및 디바이스 116

사용자당 최대 디바이스 수 124

TelePresence Room 라이선스 124

라이선스 대체 125

라이선스 시나리오 125

사용자 추가 125

연결 안 된 디바이스 추가 125

연결된 디바이스와 사용자 추가 126

사용자당 디바이스 수 127

라이선스 사용 보고서 127

Cisco Unified Reporting 128

부 V: 모니터링 및 녹음 131

장 12 사일런트 모니터링 133

사일런트 모니터링 개요 133

자동 모니터링 사전 요건 134

사일런트 모니터링 작업 흐름 구성 134

전화기 클러스터 수준에 빌트-인 브리지(BIB) 활성화 135

전화기의 빌트-인 브리지(BIB) 활성화 136

감독자에 대한 모니터링 권한 활성화 136

발신 검색 공간 모니터링 할당 137

사일런트 모니터링 알람 신호음 구성	137
보안 사일런트 모니터링 구성	138
암호화된 전화기 보안 프로파일 구성	138
전화기에 보안 프로파일 할당	138
Unified Contact Center Express에 대한 사일런트 모니터링 구성	139
사일런트 모니터링 상호 작용	140
사일런트 모니터링 제한 사항	140

장 13

녹음	143
녹음 개요	143
멀티 포크 녹음	144
녹음 미디어 원본 선택	146
녹음 사전 요건	147
녹음 구성 작업 흐름	147
녹음 프로파일 만들기	148
녹음에 대한 SIP 프로파일 구성	148
녹음에 대한 SIP 트렁크 구성	149
녹음을 위한 경로 패턴 구성	149
녹음을 위한 상담사 전화 회선 구성	150
클러스터에 대해 빌트-인 브리지(BIB) 활성화	151
전화기의 빌트-인 브리지(BIB) 활성화	151
녹음을 위한 게이트웨이 활성화	152
녹음 알람 신호음 구성	152
녹음 기능 버튼 구성	153
녹음을 위한 전화기 버튼 템플릿 구성	153
전화기 버튼 템플릿을 전화기와 연결	154
녹음 소프트키 구성	154
녹음을 위한 소프트키 템플릿 구성	154
소프트키 템플릿을 전화기에 연결	155
소프트키 템플릿을 일반 디바이스 구성에 연결	156
녹음 통화 흐름 예	157

녹음 상호 작용 및 제한 사항 157

부 VI: 콜 센터 기능 161

장 14 상담사 인사말 163

상담사 인사말 개요 163

상담사 인사말 사전 요건 163

상담사 인사말 구성 작업 흐름 164

빌트-인 브리지(BIB) 구성 165

상담사 인사말 문제 해결 165

장 15 Auto-Attendant 167

오토 어텐던트 개요 167

Cisco Unity Connection 구성 168

Cisco Unity Connection 구성 작업 흐름 168

CTI 라우트 포인트 구성 170

오토 어텐던트 시스템 통화 처리기 구성 170

발신자 입력 옵션 구성 171

운영자 통화 처리기에 대한 내선 번호 구성 171

운영자에 대한 표준 호 전환 규칙 수정 172

기본 시스템 전송 제한 테이블 업데이트 172

Cisco Unity Connection 오토 어텐던트 문제 해결 172

Cisco Unified CCX 구성 173

Cisco Unified CCX 사전 요건 173

Cisco Unified CCX 오토 어텐던트 작업 흐름 173

Cisco Unified CCX 오토 어텐던트 문제 해결 175

Cisco Unity Express 구성 175

Cisco Unity Express 오토 어텐던트 문제 해결 175

장 16 Manager Assistant 177

Cisco Unified Communications Manager Assistant 개요 177

Manager Assistant 공유 회선 개요	179
Manager Assistant 프록시 회선 개요	179
Manager Assistant 사전 요건	179
프록시 회선에 대한 Manager Assistant 작업 흐름	180
Cisco Unified CM Assistant 구성 마법사 실행	180
프록시 회선의 Manager Assistant 서비스 매개 변수	182
프록시 회선에 대한 관리자 구성 및 보조자 할당	186
프록시 회선에 대한 보조자 회선 표시 구성	187
공유 회선에 대한 Manager Assistant 작업 흐름	188
Manager Assistant 공유 회선 지원을 위한 파티션 구성	190
Manager Assistant 공유 회선 지원을 위한 파티션 이름 지침	191
Manager Assistant 공유 회선 지원에 대한 발신 검색 공간 구성	191
Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수 구성	192
인터콤 설정 구성	192
인터콤 파티션 구성	193
인터콤 발신 검색 공간 구성	193
인터콤 디렉터리 번호 구성	194
인터콤 변환 패턴 구성	194
여러 Manager Assistant 폴 구성	195
Manager Assistant용 CTI에 보안 TLS 연결 구성	196
IPMASecureSysUser 애플리케이션 사용자 구성	196
CAPF 프로파일 구성	197
Cisco WebDialer 웹 서비스 구성	199
CTI 라우트 포인트 구성	200
관리자 및 보조자에 대한 IP 전화 서비스 구성	200
Cisco IP Phone 서비스, 구성 필드	200
관리자, 보조자 및 모든 사용자용 전화 버튼 템플릿 구성	204
Manager Assistant에 대한 전화기 버튼 템플릿 구성	204
Manager Assistant 버튼 템플릿을 전화기와 연결	205
관리자 구성 및 공유 회선 모드에 사용할 보조자 할당	205
공유 회선에 대한 보조자 회선 표시 구성	206

Assistant Console 플러그인 설치	207
Manager Assistant 상호 작용	208
Manager Assistant 제한	211
Cisco Unified Communications Manager Assistant 문제 해결	212
전화하는 사용자에게 다시 걸기 신호음 가져오기	213
필터링이 설정 또는 해제되어 있으면 통화가 라우팅되지 않음	213
Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스에 연결할 수 없음	214
Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스를 초기화할 수 없음	215
웹에서 Assistant Console 설치 실패	216
HTTP 상태 503 —이 애플리케이션은 현재 사용할 수 없습니다.	216
서비스가 계속 실행되는 동안 관리자가 로그아웃됨	217
관리자가 보조 프록시 회선에서 벨이 울리는 통화를 가로챌 수 없음	217
페이지를 찾을 수 없음 오류	218
시스템 오류 - 시스템 관리자에게 문의하십시오.	218
Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스가 다운되면 관리자를 호출할 수 없습니다	219
사용자 인증 실패	220
부 VII:	음성 메시지 기능 221
장 17	음성 메시지 대기 중 표시기 223
	음성 메시지 대기 표시 개요 223
	음성 메시지 대기 표시 사전 요건 223
	음성 메시지 대기 표시 작업 흐름 223
	음성 메시지 대기 표시 서비스 매개 변수 구성 224
	디렉터리 번호에 대한 음성 메시지 대기 표시 구성 224
	SIP 프로파일에 대한 음성 메시지 대기 표시기 구성 225
	음성 메시지 대기 표시 문제 해결 226
	음성 메시지 대기 표시가 전화기에서 들리지 않음 226
	지역화된 AMWI 신호음이 특정 로캘에서 재생되지 않음 226

장 18

지정전환 227

즉시 전환 개요 227

즉시 전환 사전 요건 228

즉시 전환 구성 작업 흐름 228

즉시 전환 서비스 매개 변수 구성 229

즉시 전환에 대한 소프트키 템플릿 구성 230

소프트키 템플릿을 일반 디바이스 구성에 연결 231

소프트키 템플릿을 일반 디바이스 구성에 추가 232

일반 디바이스 구성을 전화기에 연결 233

소프트키 템플릿을 전화기에 연결 233

즉시 전환 상호 작용 233

즉시 전환 제한 사항 235

즉시 전환 문제 해결 236

키가 활성화 상태가 아님 236

일시적 실패 236

통화 중 236

부 VIII:

전화회의 기능 239

장 19

애드-혹 컨퍼런스 241

애드-혹 컨퍼런스 개요 241

애드-혹 컨퍼런스 작업 흐름 241

전화회의용 소프트키 템플릿 구성 242

소프트키 템플릿 일반 디바이스 연결 244

소프트키 템플릿을 일반 디바이스 구성에 추가 244

일반 디바이스 구성을 전화기에 연결 245

소프트키 템플릿을 전화기에 연결 245

애드-혹 컨퍼런스 구성 245

애드-혹 컨퍼런스 서비스 매개 변수 246

회선 간 조인 구성 249

전화회의 상호 작용 250

전화회의 제한 사항 250

장 20

회의개설 컨퍼런싱 255

회의개설 컨퍼런싱 255

회의개설 컨퍼런싱 작업 흐름 255

회의개설 컨퍼런싱용 소프트키 템플릿 구성 256

소프트키 템플릿을 일반 디바이스 구성에 연결 257

소프트키 템플릿을 일반 디바이스 구성에 추가 258

일반 디바이스 구성을 전화기에 연결 258

소프트키 템플릿을 전화기에 연결 259

회의개설 전화회의 번호 구성 259

회의개설 번호 및 패턴 설정 260

회의개설 전화회의 제한 사항 261

장 21

Conference Now 263

Conference Now 개요 263

Conference Now 사전 요건 264

Cisco IP Voice Media Streaming 활성화 264

Conference Now 설정 구성 264

사용자용 Conference Now 활성화 265

LDAP를 통해 Conference Now 활성화 266

Conference Now 상호 작용 267

Conference Now 제한 사항 267

부 IX:

전화 걸기 269

장 22

콜백 271

콜백 개요 271

콜백 사전 요건 272

콜백 구성 작업 흐름 272

콜백에 대한 소프트키 템플릿 구성	273
콜백 소프트키 템플릿을 일반 디바이스 구성에 연결	274
콜백 소프트키 템플릿을 전화기에 연결	276
콜백 버튼 구성	276
콜백에 대한 전화기 버튼 템플릿 구성	276
버튼 템플릿을 전화기와 연결	277
콜백 상호 작용	277
콜백 제한 사항	279
콜백 문제 해결	279
콜백 소프트키를 누른 후 콜백이 발생하기 전에 전화기 분리/재설정	279
발신자가 전화기 재설정 전에 가용성 알람을 보지 못함	280
콜백 오류 메시지	280
콜백이 활성화 상태가 아님	280
콜백이 이미 활성화 상태임	280
콜백을 활성화할 수 없음	281
키가 활성화 상태가 아님	281

장 23

핫라인	283
핫라인 개요	283
핫라인 시스템 요구 사항	284
핫라인 구성 작업 흐름	284
사용자 정의 소프트키 템플릿 만들기	285
전화기에서 핫라인 구성	286
라우트 클래스 신호 처리 작업 흐름 구성	286
클러스터에서 라우트 클래스 신호 처리 활성화	287
트렁크에서 라우트 클래스 신호 처리 활성화	288
게이트웨이에서 라우트 클래스 신호 처리 활성화	288
핫라인 라우트 클래스에 대한 신호 처리 레이블 구성	289
핫라인 라우트 패턴에서 라우트 클래스 구성	289
핫라인 변환 패턴에서 라우트 클래스 구성	290
통화 전용 또는 수신 전용 핫라인 작업 흐름 구성	290

핫라인 통화 전용 수신 전용 파티션 구성	291
핫라인 통화 전용 수신 전용 발신 검색 공간 구성	291
핫라인 전화기에 통화 전용 구성	292
핫라인 전화기에 수신 전용 구성	292
발신 검색 공간과 함께 통화 심사 구성	293
핫라인 통화 심사에 대한 파티션 구성	293
핫라인 통화 심사에 대한 발신 검색 공간 생성	294
통화 심사에 대한 핫라인 전화기 구성	295
핫라인 문제 해결	296

장 24

단축 다이얼	297
단축 다이얼 개요	297
일시 중지가 있는 단축 다이얼 프로그래밍	297
단축 다이얼 구성 작업 흐름	298
단축 다이얼 구성	298

장 25

WebDialer	301
WebDialer 개요	301
WebDialer 사전 요건	301
WebDialer 구성 작업 흐름	302
WebDialer 활성화	303
WebDialer 추적 활성화	303
WebDialer 서블릿 구성	304
Redirector 서블릿 구성	305
WebDialer 애플리케이션 서버 구성	305
CTI에 보안 TLS 연결 구성	306
WDSecureSysUser 애플리케이션 사용자 구성	306
CAPF 프로파일 구성	307
Cisco IP 매니저 어시스턴트 (Cisco IPMA) 구성	308
Webdialer용 언어 로캘 구성	309
WebDialer 알람 구성	309

애플리케이션 다이얼 규칙 구성	310
표준 CCM 최종 사용자 그룹에 사용자 추가	311
프록시 사용자 구성	311
WebDialer 최종 사용자 추가	312
인증 프록시 권한 할당	312
WebDialer 상호 작용	313
WebDialer 제한 사항	314
WebDialer 문제 해결	314
인증 오류	314
일시적으로 서비스를 사용할 수 없음	314
디렉터리 서비스 다운	315
Cisco CTIManager 다운	315
세션이 만료되었습니다. 다시 로그인하십시오	315
어느 디바이스에도 로그인하지 않은 사용자	316
디바이스/회선 열기 실패	316
대상에 연결할 수 없음	317

장 26

페이징	319
페이징 개요	319
InformaCast 기본 페이징	319
InformaCast 고급 알림	319
InformaCast 모바일	320
페이징 사전 요건	320
기본 페이징 작업 흐름에 대해 Cisco Unified Communications Manager 구성	321
페이징을 위한 SNMP 구성	322
SNMP 서비스 활성화	322
InformaCast SNMP 커뮤니티 문자열 생성	323
페이징을 위한 지역 구성	323
기본 코덱을 G.711로 설정	324
페이징에 대한 디바이스폴 구성	324
페이징을 위한 파티션 및 발신 검색 공간 구성	325

InformaCast 페이징을 위한 경로 파티션 구성	325
InformaCast 페이징을 위한 발신 검색 공간 구성	325
페이징을 위한 CTI 포트 구성	326
AXL 액세스를 사용하여 액세스 컨트롤 그룹 구성	327
페이징을 위한 애플리케이션 사용자 구성	327
전화기에 대한 웹 액세스 활성화	328
일반 전화 프로파일에 대한 웹 액세스 활성화	329
엔터프라이즈 전화기 구성에 대한 웹 액세스 활성화	329
인증 URL 구성	330
인증 URL 설정	330
전화기 재설정	331
전화기 테스트	331
고급 알림 페이징 구성 작업 흐름	332
InformaCast 가상 어플라이언스 설치	332
InformaCast에 대한 연결 구성	334
패닉 버튼 구성	336
CallAware 비상 통화 알림 구성	337
페이징 상호 작용	339
고급 알림 페이징 상호 작용	339

장 27

인터콤	341
인터콤 개요	341
인터콤 및 기본 디바이스	341
인터콤 사전 요건	342
인터콤 구성 작업 흐름	342
인터콤 파티션 구성	342
인터콤 발신 검색 공간 구성	343
인터콤 변환 패턴 구성	344
인터콤 디렉터리 번호 구성	344
인터콤 회선 및 단축 다이얼 구성	345
인터콤 상호 작용	346

인터콤 제한 사항	347
인터콤 문제 해결	348
인터콤 회선에서 전화를 걸 때 통화 중 신호음	348
인터콤 통화에서 스피커, 핸드셋 또는 헤드셋과 함께 Talkback를 사용할 수 없음	349
SCCP 문제 해결	349
전화기에 인터콤 회선이 표시되지 않음	349
전화기가 SRST로 폴백할 때 인터콤 회선이 표시되지 않음	349
SIP 문제 해결	350
SIP를 실행하는 전화기 디버그	350
SIP를 실행하는 전화기의 구성	350
Cisco Extension Mobility 사용자가 로그인했지만 인터콤 회선이 표시되지 않음	350
인터콤 회선이 전화기에 표시되지 않음	351

부 X:	통화 수신	353
------	-------	-----

장 28	기본 회선 지원	355
	기본 회선 지원 개요	355
	기본 회선 지원 사전 요건	355
	기본 회선 지원 구성 작업 흐름	355
	클러스터 수준 기본 회선 지원 구성	356
	디바이스에 대한 기본 회선 지원 구성	357
	기본 회선 지원 상호 작용	357
	기본 회선 지원 문제 해결	358
	True로 설정되면 기본 회선 지원이 작동하지 않음	358
	착신 전화에 응답할 수 없음	358
	착신 전화가 자동으로 응답됨	358

장 29	착신 전환	359
	착신 전환 개요	359
	CFA 루프 예방 및 CFA 루프 차단을 포함하여 모두 착신 전환	360
	통화 착신 전환 구성 작업 흐름	361

착신 전환에 대한 파티션 구성	361
착신 전환에 대한 파티션 이름 지침	362
착신 전환에 대한 발신 검색 공간 구성	363
헌트 목록이 소모되었거나 헌트 타이머가 만료되면 착신 전환 구성	364
착신 전환에 대한 헌트 통화 처리 필드	364
착신 전환(대역폭 없음) 구성	366
착신 전환에 대한 디렉터리 번호 구성 필드	367
착신 전환 대체 대상 구성	367
착신 전환에 대한 MLPP 대체 상대 및 기밀 액세스 수준 설정 필드	368
다른 착신 전환 유형 구성	368
착신 전환 필드	369
통화 착신 전환에 대한 대상 오버라이드 활성화	378
착신 전환 상호 작용	379
착신 전환 제한 사항	383

장 30

통화 당겨받기	385
당겨 받기 개요	385
그룹 당겨받기 개요	385
기타 그룹 당겨받기 개요	385
직접 당겨 받기 개요	386
BLF 당겨받기 개요	386
당겨받기 구성 작업 흐름	387
통화 당겨받기 그룹 구성	389
디렉터리 번호에 통화 당겨받기 그룹 할당	390
당겨받기에 대한 파티션 구성	391
발신 검색 공간 구성	392
헌트 파일럿에 통화 당겨받기 그룹 할당	392
당겨받기 알림 구성	393
그룹 당겨받기에 대한 당겨받기 알림 구성	393
디렉터리 번호에 대한 당겨받기 알림 구성	394
BLF 당겨받기 알림 구성	395

직접 통화 당겨받기 구성	397
기간 구성	397
시간 일정 구성	397
시간 일정을 파티션에 연결	398
자동 통화 응답 구성	398
자동 통화 당겨받기 구성	398
BLF 자동 당겨받기 구성	399
당겨 받기 전화기 버튼 구성	400
당겨받기 전화기 버튼 템플릿 구성	400
당겨받기 버튼 템플릿을 전화기와 연결	401
BLF 당겨받기 이니시에이터에 대한 BLF 단축 다이얼 번호 구성	401
당겨받기에 대한 소프트키 구성	402
통화 당겨 받기에 대한 소프트키 템플릿 구성	402
소프트키 템플릿을 일반 디바이스 구성에 연결	404
소프트키 템플릿을 전화기에 연결	405
당겨받기 상호 작용	405
당겨받기 제한 사항	406

장 31

통화 대기 및 직접 통화	409
통화 대기 개요	409
통화 지정 보류 사전 요건	410
통화 대기 구성 작업 흐름	411
클러스터 수준 통화 대기 구성	412
통화 지정 보류에 대한 파티션 구성	413
통화 지정보류 번호 구성	413
통화 지정보류 구성 필드	415
통화 대기를 위한 소프트키 템플릿 구성	416
소프트키 템플릿을 일반 디바이스 구성에 연결	417
소프트키 템플릿을 일반 디바이스 구성에 추가	418
일반 디바이스 구성을 전화기에 연결	418
소프트키를 전화기와 연결	419

통화 대기 버튼 구성	419
통화 대기를 위한 전화기 버튼 템플릿 구성	419
버튼 템플릿을 전화기와 연결	420
지정보류 모니터링 구성	420
지정보류 모니터링 시스템 타이머 구성	421
헌트 파일럿에 대한 지정보류 모니터링 구성	422
디렉터리 번호에 대한 지정보류 모니터링 구성	423
유니버설 회선 템플릿을 통한 지정보류 모니터링 구성	424
통화 지정 보류 상호 작용	426
통화 대기 제한 사항	427
통화 대기 문제 해결	428
사용자가 통화 대기를 할 수 없음	428
통화 대기 번호가 충분히 길게 표시되지 않음	428
통화 전환 보류 개요	428
통화 전환 보류 사전 요건	429
통화 전환 보류 구성 작업 흐름	429
클러스터 수준 통화 전환 보류 구성	429
통화 전환 보류 번호 구성	430
통화 전환 보류 구성 설정	431
BLF/통화 전환 보류 버튼 구성	431
BLF/통화 전환 보류 구성 필드	432
영향을 받는 디바이스와 통화 전환 보류 동기화	433
통화 전환 보류 상호 작용	433
통화 전환 보류 제한 사항	435
통화 전환 보류 문제 해결	436
사용자가 통화 지정보류를 검색할 수 없음	436
사용자가 통화 대기를 할 수 없음	436
복귀 타이머가 만료된 후 사용자가 다시 걸기 신호음을 수신함	436
사용자가 다시 걸기 신호음 또는 알림 수신	436
사용자가 범위 내의 번호에서 통화를 지정보류할 수 없음	437
통화 지정 보류가 너무 빠르게 복귀함	437

지정보류 슬롯 사용할 수 없음 437

통화 지정보류가 통화 지정보류 번호로 복귀되지 않음 437

번호 또는 범위가 사용 중 이므로 삭제할 수 없음 437

장 32

Extension Mobility 439

Extension Mobility 개요 439

Extension Mobility 사전 요건 439

Extension Mobility 구성 작업 흐름 440

Extension Mobility 서비스 활성화 441

Cisco Extension Mobility 전화 서비스 구성 441

사용자에 대한 Extension Mobility 디바이스 프로파일 생성 442

사용자에 디바이스 프로파일 연결 443

Extension Mobility에 구독 443

인증서 변경 IP 전화 서비스 구성 444

Extension Mobility에 대한 서비스 매개 변수 구성 444

Extension Mobility 서비스 매개 변수 445

Cisco Extension Mobility 상호 작용 449

Cisco Extension Mobility 제한 사항 451

Extension Mobility 문제 해결 452

Extension Mobility 문제 해결 452

인증 오류 452

빈 사용자 ID 또는 PIN 452

통화 중입니다. 다시 시도하십시오. 452

데이터베이스 오류 453

디바이스에 로그인할 수 없음 453

빈 디바이스 이름 453

EMService 연결 오류 453

업그레이드 중 Extension Mobility 성능 453

호스트를 찾을 수 없음 454

HTTP 오류 454

전화기 재설정 454

로그인한 후 전화 서비스를 사용할 수 없음	454
로그아웃한 후 전화 서비스를 사용할 수 없음	454
사용자가 다른 위치에서 로그인	455
사용자 프로필 부재	455
클러스터 간 Extension Mobility	457
Extension Mobility Cross Cluster 개요	457
클러스터 간 Extension Mobility 사전 요건	457
클러스터 간 Extension Mobility 구성 작업 흐름	458
Configure Extension Mobility	459
클러스터 간 Extension Mobility를 위해 서비스 활성화	460
Extension Mobility 전화 서비스 구성	460
클러스터 간 Extension Mobility를 위한 디바이스 프로필 구성	462
사용자에 대해 Extension Mobility 상호 클러스터 활성화	469
디바이스를 Extension Mobility에 구독	469
클러스터 간 Extension Mobility에 대한 인증서 구성	470
Bulk Provisioning Service 활성화	470
벌크 인증서 관리 구성 및 인증서 내보내기	471
인증서 통합	472
클러스터로 인증서 가져오기	472
클러스터 간 Extension Mobility 디바이스 및 템플릿 구성	473
일반 디바이스 구성 만들기	474
클러스터 간 Extension Mobility 템플릿 구성	474
기본 템플릿 설정	474
클러스터 간 Extension Mobility 디바이스 추가	475
클러스터 간 Extension Mobility를 위한 지오로케이션 필터 구성	475
클러스터 간 Extension Mobility에 대한 기능 매개 변수 구성	476
클러스터 간 Extension Mobility에 대한 기능 매개 변수 필드	476
클러스터 간 Extension Mobility에 대한 클러스터 간 SIP 트렁크 구성	479
클러스터 간 Extension Mobility를 위한 클러스터 간 서비스 프로필 구성	480
원격 클러스터 서비스 구성	480

클러스터 간 Extension Mobility 상호 작용	481
클러스터 간 Extension Mobility 제한	482
다양한 클러스터 버전을 위한 익스텐션 모빌리티 크로스 클러스터(EMCC) 및 보안 모드	484
클러스터 간 Extension Mobility 문제 해결	486
Extension Mobility 애플리케이션 오류 코드	486
Extension Mobility 서비스 오류 코드	488

장 34

클러스터 간 Extension Mobility 로밍	493
클러스터 간 Extension Mobility 로밍 개요	493
클러스터 간 Extension Mobility 로밍에 대한 시스템 요구 사항	494
클러스터 간 Extension Mobility 로밍 로그인	494
ILS 상호 작용	497
클러스터 간 Extension Mobility 로밍 작업 흐름	497
전화기 기능 목록 생성	498
Extension Mobility 서비스 활성화	498
Cisco Extension Mobility 전화 서비스 구성	498
사용자에 대한 Extension Mobility 디바이스 프로파일 생성	500
사용자에 디바이스 프로파일 연결	500
Extension Mobility에 구독	501
Extension Mobility 사용자에게 대한 로밍 구성	501
클러스터 간 Extension Mobility 상호 작용 및 제한 사항	502
다른 유형의 Extension Mobility	502
클러스터 간 Extension Mobility 문제 해결	503
인증 오류	503
빈 사용자 ID 또는 PIN	503
통화 중입니다. 다시 시도하십시오.	503
데이터베이스 오류	504
디바이스에 로그인할 수 없음	504
빈 디바이스 이름	504
EMService 연결 오류	504
호스트를 찾을 수 없음	504

HTTP 오류	504
전화기 재설정	505
로그인한 후 전화 서비스를 사용할 수 없음	505
로그아웃한 후 전화 서비스를 사용할 수 없음	505
사용자가 다른 위치에서 로그인	505
사용자 프로파일 부재	506

장 35

보류 복귀	507
보류 복귀 개요	507
보류 복귀 사전 요건	508
보류 복귀 구성 작업 흐름	508
보류 복귀를 위한 통화 포커스 우선 순위 구성	509
클러스터에 대한 보류 복귀 타이머 기본값 구성	509
전화기에 대한 보류 복귀 타이머 설정 구성	510
보류 복귀 상호 작용	511
보류 복귀 제한 사항	512

장 36

헌트 그룹 액세스	515
헌트 그룹 개요	515
헌트 그룹 사전 요건	516
헌트 그룹 구성 작업 흐름	516
헌트 그룹을 위한 소프트키 템플릿 구성	517
소프트키 템플릿을 일반 디바이스 구성에 연결	518
소프트키 템플릿을 일반 디바이스 구성에 추가	519
일반 디바이스 구성을 전화기에 연결	519
소프트키 템플릿을 전화기에 연결	520
헌트 그룹을 위한 전화기 구성	520
헌트 그룹 서비스 매개 변수 구성	521
헌트 그룹 상호 작용	522
헌트 그룹 제한 사항	522

장 37

악성 전화 식별 525

악성 전화 식별 개요 525

악성 전화 식별 525

악성 전화 식별 구성 작업 흐름 526

악성 전화 ID 서비스 매개 변수 설정 527

장난 전화 ID 알람 구성 527

악성 전화 식별을 위한 소프트키 템플릿 구성 528

소프트키 템플릿을 일반 디바이스 구성에 연결 529

소프트키 템플릿을 일반 디바이스 구성에 추가 530

일반 디바이스 구성을 전화기에 연결 530

소프트키 템플릿을 전화기에 연결 531

악성 전화 식별 버튼 구성 531

장난 전화 ID 전화기 버튼 템플릿 구성 531

버튼 템플릿을 전화기와 연결 532

악성 전화 식별 상호 작용 533

악성 전화 식별 제한 사항 535

악성 전화 ID 문제 해결 535

장 38

통화 전환 537

호 전환 개요 537

호 전환 구성 작업 흐름 538

상담 및 비공개 전환 구성 538

전환을 위한 소프트키 템플릿 구성 538

전환 버튼 구성 542

전환 온/오프 구성 543

직접 호전환 구성 543

직접 호전환을 위한 소프트키 템플릿 구성 544

직접 호전환 버튼 구성 547

호 전환 상호 작용 549

호 전환 제한 550

장 39	외부 호전환 제한 551
	외부 호전환 제한 사항 개요 551
	외부 호전환 제한 사항 작업 흐름 구성 552
	외부 호전환 제한을 위한 서비스 매개 변수 구성 552
	수신 통화 작업 흐름 구성 553
	클러스터 수준 서비스 매개 변수 구성 554
	호전환 제한을 위한 게이트웨이 구성 554
	호전환 제한을 위한 트렁크 구성 555
	발신 통화 구성 555
	외부 호전환 제한 상호 작용 556
	외부 호전환 제한 557
부 XI:	프레즌스 및 프라이버시 기능 559
장 40	참여 561
	참여 개요 561
	내장 전화회의 562
	공유 전화회의 562
	내장 및 공유 전화회의의 차이점 562
	참여 구성 작업 흐름 564
	내장 전화회의용 소프트키 템플릿 구성 565
	공유 전화회의용 소프트키 템플릿 구성 566
	소프트키 템플릿을 전화기에 연결 567
	소프트키 템플릿을 일반 디바이스 구성에 연결 567
	소프트키 템플릿을 일반 디바이스 구성에 추가 568
	일반 디바이스 구성을 전화기에 연결 568
	내장 전화회의에 대한 참여 구성 569
	공유 전화회의에 대한 참여 구성 570
	사용자를 디바이스에 연결 570
	참여 상호 작용 571

참여 제한 사항	571
참여 문제 해결	572
사용 가능한 전화회의 브리지 없음	572
오류: 통과 제한	572

장 41

BLF 프리젠스	575
BLF 프리젠스 개요	575
BLF 프리젠스 사전 요건	576
BLF 프리젠스 구성 작업 흐름	576
BLF에 대한 클러스터 수준 엔터프라이즈 매개 변수 구성/동기화	577
BLF에 대한 클러스터 수준 서비스 매개 변수 구성	578
BLF 프리젠스 그룹 구성	579
BLF에 대한 BLF 프리젠스 그룹 필드	580
디바이스 및 사용자와의 BLF 존재 그룹 연결	580
BLF 프리젠스 그룹을 전화기와 연결	581
BLF 프리젠스 그룹을 SIP 트렁크와 연결	582
BLF 프리젠스 그룹을 최종 사용자와 연결	583
BLF 프리젠스 그룹을 애플리케이션 사용자와 연결	583
외부 트렁크 및 애플리케이션에 대한 BLF 프리젠스 요청 수락	584
프레즌스 요청에 대한 발신 검색 공간 구성	585
BLF 및 단축 다이얼 버튼에 대한 전화기 버튼 템플릿 구성	586
버튼 템플릿을 디바이스와 연결	587
사용자 디바이스 프로파일 구성	587
BLF 프리젠스 상호 작용	588
BLF 프리젠스 제한 사항	588

장 42

통화 표시 제한	591
통화 표시 제한 개요	591
통화 표시 제한 구성 작업 흐름	591
통화 표시 제한을 위한 파티션 구성	592
파티션 이름 지침	593

통화 표시 제한 기능에 대한 발신 검색 공간 구성	594
연결된 번호 표시 제한에 대한 서비스 매개 변수 구성	594
변환 패턴 구성	595
통화 표시 제한 기능에 대한 변환 패턴 필드	596
전화기에 통화 표시 제한 구성	597
통화 표시 제한 기능을 위한 PSTN 게이트웨이 구성	598
SIP 트렁크에서 통화 표시 제한 구성	599
통화 표시 제한을 위한 SIP 트렁크 필드	600
통화 표시 제한 상호 작용	601
통화 표시 제한 기능 제한 사항	602

장 43

DND(Do Not Disturb) 603

방해 사절 개요	603
방해 사절 구성 작업 흐름	604
통화 상태 감시(BLF) 상태 구성	605
일반 전화 프로파일에 방해 사절 구성	606
전화기에 방해 사절 설정 적용	606
방해 사절 기능 버튼 구성	607
방해 사절에 대한 전화기 버튼 템플릿 구성	608
버튼 템플릿을 전화기와 연결	608
방해 사절 소프트키 구성	609
방해 사절에 대한 소프트키 템플릿 구성	609
소프트키 템플릿을 일반 디바이스 구성에 연결	610
소프트키 템플릿을 전화기에 연결	612
방해 사절 상호 작용 및 제한 사항	612
상호 작용	612
제한 사항	614
방해 사절 문제 해결	615

장 44

프라이버시 617

프라이버시 개요	617
----------	-----

보류 중 프라이버시	617
프라이버시 구성 작업 흐름	618
프라이버시 클러스터 전체 활성화	618
디바이스에 대한 프라이버시 활성화	619
프라이버시 전화기 버튼 템플릿 구성	619
프라이버시 전화기 버튼 템플릿을 전화기와 연결	620
공유 회선 표시 구성	620
프라이버시 보류 중 구성	621
프라이버시 제한 사항	621

장 45

전용 회선 자동 링다운	623
전용 회선 자동 링다운 개요	623
SCCP 전화기에 대한 전용 회선 자동 링다운 구성 작업 흐름	623
파티션 생성	624
발신 검색 공간에 파티션 할당	624
전용 회선 자동 링다운 대상에 파티션 할당	625
전화기에서 전용 회선 자동 링다운에 대한 변환 패턴 구성	625
SIP 전화기에 대한 전용 회선 자동 링다운 구성 작업 흐름	626
전용 회선 자동 링다운에 대한 SIP 다이얼 규칙 생성	626
SIP 전화기에 전용 회선 자동 링다운 다이얼 규칙 할당	627
전용 회선 자동 링다운 문제 해결	627

장 46

보안 신호음	629
보안 신호음 개요	629
보호된 디바이스 게이트웨이	630
보안 신호음 사전 요건	630
보안 신호음 구성 작업 흐름	630
전화기를 보호된 디바이스로 구성	631
보안 신호음에 대한 디렉터리 번호 구성	632
보안 신호음 서비스 매개 변수 구성	632
MGCP E1 PRI 게이트웨이 구성	632

보안 신호음 상호 작용 633

보안 신호음 제한 사항 633

부 XII:

사용자 정의 기능 635

장 47

브랜딩 사용자 지정 637

브랜드 개요 637

브랜드 필수 조건 637

브랜딩 작업 흐름 638

브랜딩 활성화 638

브랜딩 비활성화 639

Tomcat 서비스 다시 시작 640

브랜딩 파일 요구 사항 640

장 48

클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 645

클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 개요 645

클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 사전 요건 645

클라이언트 매터 코드 및 강제 인증 코드 구성 작업 흐름 646

클라이언트 매터 코드 구성 646

클라이언트 매터 코드(Client Matter Code) 추가 647

클라이언트 매터 코드 활성화 647

강제 인증 코드 구성 648

강제 인증 코드(FAC) 추가 648

강제 인증 코드 활성화 648

클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 상호 작용 649

클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 제한 사항 650

장 49

사용자 지정 전화기 벨소리 및 배경 653

사용자 지정 전화기 벨소리 개요 653

사용자 지정 전화기 벨소리 사전 요건 653

사용자 지정 전화기 벨소리 구성 작업 흐름 654

업로드를 위한 사용자 지정 전화기 벨소리 준비	654
TFTP 서버에 사용자 지정 전화기 벨소리 업로드	655
TFTP 서비스 다시 시작	655
PCM 파일 형식 요구 사항	655
Ringlist.xml 파일 형식 요구 사항	656
사용자 정의 배경	656
사용자 지정 배경 구성 작업 흐름	657
전화기 배경 이미지 만들기	658
List.xml 파일 편집	658
TFTP 서버에 배경 업로드	659
TFTP 서버 다시 시작	660
전화기 사용자에게 대한 전화기 배경 할당	660

장 50

대기 중 음악	663
대기 중 음악 개요	663
발신자별 대기 중 음악	664
IP 음성 미디어 스트리밍 애플리케이션 및 확장된 MOH 오디오 소스의 용량 증가	664
미디어 디바이스와 서비스의 성능 영향	664
용량 수립 계획에 대한 구성 제한	666
외부 멀티캐스트 MOH와 유니캐스트 MOH의 상호 연동	667
대기 중 음악 사전 요건	669
대기 중 음악 구성 작업 흐름	669
Cisco IP Voice Media Streaming 활성화	670
대기 중 음악 서버 구성	670
대기 중 음악용 오디오 파일 업로드	671
대기 중 음악 오디오 소스 구성	672
고정 대기 중 음악 오디오 소스 구성	673
미디어 리소스 그룹에 MOH 추가	673
미디어 리소스 그룹 목록 구성	674
디바이스 풀에 미디어 리소스 추가	674
MOH 서비스 매개 변수 구성	675

대기 중 음악 오디오 파일 보기	675
유니캐스트 및 멀티캐스트 오디오 소스	676
대기 중 음악 상호 작용	678
대기 중 음악 제한 사항	680
대기 중 음악 문제 해결	682
대기 중 음악이 전화기에서 재생되지 않음	682

장 51

셀프 서비스 포털	683
셀프 서비스 포털 개요	683
셀프 서비스 포털 작업 흐름	684
셀프 서비스 포털에 사용자 액세스 권한 부여	684
셀프 서비스 포털 옵션 구성	684
셀프 서비스 포털 상호 작용 및 제한 사항	685

장 52

비상 통화 처리기	687
비상 통화 처리기 개요	687
비상 통화 처리기 사전 요건	688
비상 통화 처리기 작업 흐름	688
비상 통화 처리기 사용	689
비상 위치 그룹 구성	690
비상 위치 그룹에 디바이스폴 추가	691
비상 위치 그룹에 디바이스 추가	691
경로 패턴 및 변환 패턴 활성화	692
비상 위치 그룹 및 전화기의 벌크 관리	693
비상 위치 그룹 및 전화기의 벌크 관리 작업 흐름	693
상호 작용	695
비상 통화 처리기 문제 해결	697
비상 통화 처리기 문제 해결 시나리오 정보	697
Configuration Scenarios	697
비상 통화에 통화 중 신호가 들리고 라우팅되지 않음	697
다시 걸기 신호음을 실행 중인 외부에서 비상 위치 번호로 전화가 걸림	697

Outgoing Calls Scenarios	698
발신 비상 통화에 발신자가 비상 위치 번호로 포함되어 있지 않음	698
발신 비상 통화에 수정된 비상 위치 번호가 포함	698
Incoming Calls Scenarios	698
수신 PSAP 콜백 통화 실패	698
수신 PSAP 콜백 통화가 예상대로 라우팅되지 않음	699

장 53

RedSky로 비상 통화 처리	701
RedSky로 비상 통화 처리 개요	701
비상 통화 처리 구성 작업 흐름	702
RedSky 서버 구성	702
서비스 프로파일 구성	703
서비스 프로파일 할당	704
통화 라우팅에 대한 SIP 경로 패턴 설정	705

장 54

엔터프라이즈 그룹	707
엔터프라이즈 그룹 개요	707
엔터프라이즈 그룹 필수 조건	708
엔터프라이즈 그룹 구성 작업 흐름	709
LDAP 디렉터리에서 그룹 동기화 확인	709
엔터프라이즈 그룹 활성화	709
보안 그룹 활성화	710
보안 그룹 필터 생성	711
LDAP 디렉터리에서 보안 그룹 동기화	711
보안 그룹에 대한 Cisco Jabber 구성	712
사용자 그룹 보기	712
엔터프라이즈 그룹 구축 모델 (Active Directory)	713
엔터프라이즈 그룹 제한 사항	715

부 XIII:

디바이스 관리	719
---------	-----

장 55

헤드셋 및 액세서리 관리	721
헤드셋 및 액세서리 관리 개요	721
헤드셋 및 액세서리 관리를 위한 기능 호환성	721
타사 헤드셋 및 액세서리 지원	723
워크플로: 헤드셋 서비스 가용성 구성	723
Cisco 헤드셋 서비스 활성화	724
헤드셋 COP 파일 준비	725
헤드셋 사용자를 위한 사용자 프로파일 구성	726
최종 사용자에게 사용자 프로파일 적용	727
헤드셋 및 액세서리 템플릿 관리	728
헤드셋 및 액세서리 템플릿 구성	731
펌웨어 관리	732
헤드셋 및 액세서리 재고 목록 관리	733
헤드셋 및 액세서리 재고 목록	733
헤드셋 및 액세서리 재고 목록 관리 작업 흐름	734
헤드셋 및 액세서리 재고 목록 보기	735
전화기 소유자를 헤드셋 또는 액세서리 소유자와 연결	735
헤드셋 및 액세서리 재고 목록 요약	736
구축된 헤드셋 및 액세서리의 집계 요약 가져오기	736
헤드셋 및 액세서리 문제 해결 및 진단	737
Unified CM에서 엔드포인트에 대한 PRT 생성	737
RTMT에서 엔드포인트에 대한 PRT 생성	738

장 56

헤드셋 서비스	739
헤드셋 서비스 개요	739
헤드셋 서비스 사전 요건	740
헤드셋 서비스 관리자 구성 작업 흐름	740
사용자에게 헤드셋 연결	741
최종 사용자 헤드셋 연결 관리	741
헤드셋 기반 Extension Mobility 활성화	742

핀리스 Extension Mobility 로그인 활성화	743
Extension Mobility 헤드셋 로그아웃 타이머 구성	743
헤드셋 서비스 최종 사용자 연결 작업 흐름	744
사용자 헤드셋 연결	745
헤드셋 연결 건너뛰기	745
헤드셋을 사용하여 Extension Mobility 로그인	746
헤드셋을 사용하여 Extension Mobility에서 사용자 로그아웃	746

장 57

IVR 및 전화 서비스를 사용한 기본 전화 마이그레이션	749
IVR 및 전화 서비스를 사용한 기본 전화 마이그레이션 개요	749
전화기 마이그레이션을 위한 엔터프라이즈 매개 변수	750
전화기 마이그레이션 사전 요건	752
셀프 프로비저닝 IVR을 사용하는 전화기 마이그레이션 작업 흐름	753
셀프 프로비저닝 서비스 활성화	754
셀프 프로비저닝을 위한 자동 등록 활성화	754
CTI 라우트 포인트 구성	755
CTI 라우트 포인트에 디렉터리 번호 할당	756
셀프 프로비저닝을 위한 애플리케이션 사용자 구성	756
셀프 프로비저닝을 위한 시스템 구성	757
사용자 프로파일에서 셀프 프로비저닝 활성화	758
전화기 마이그레이션 작업	758
셀프 프로비저닝 IVR을 사용하여 전화기 마이그레이션(관리자)	758
셀프 프로비저닝 IVR을 사용하여 전화기 마이그레이션(전화기 사용자)	759
전화기 마이그레이션 서비스를 사용하여 전화기 마이그레이션 작업 흐름	760
자동 등록 비활성화	760
기본 전화기 로드 설정	761
셀프 프로비저닝 인증 구성	761
전화기 마이그레이션 작업	762
전화기 마이그레이션 서비스를 사용하여 전화기 마이그레이션(관리자)	762
전화기 마이그레이션 서비스를 사용하여 전화기 마이그레이션(전화기 사용자)	763
전화기 마이그레이션 서비스 COP 파일	764

전화기 마이그레이션 보고서 보기	764
Cisco Unified CM 관리 인터페이스를 사용하여 전화기 마이그레이션	764
마이그레이션 시나리오	765
공유 회선을 사용하는 전화기	765
프록시 TFTP에서 실행 중인 전화기 마이그레이션 서비스	765
전화기 마이그레이션 서비스 — 여러 디바이스에 할당된 사용자	766
Unified CM 매개 변수 설정을 기반으로 하는 디바이스 표시	767
Extension Mobility를 사용하는 전화기	768
CTI 제어된 디바이스	768
키 확장 모듈을 사용하는 전화기	768
제품별 구성 매개 변수	769
전화기 버튼 템플릿	770
협업 디바이스 — 실내 시스템, 데스크 및 IP 전화기	770

장 58

비디오 엔드포인트 관리	771
비디오 엔드포인트 관리 개요	771
비디오 엔드포인트 관리 기능 호환성	772
비디오 엔드포인트 프로비저닝을 위한 마이그레이션 고려 사항	773
비디오 엔드포인트 마이그레이션 보고서	774
프로비저닝 및 마이그레이션 시나리오	775
Unified CM에 비디오 엔드포인트 마이그레이션 추가	776

부 XIV:

고급 통화 처리	779
----------	-----

장 59

통화 제어 검색 구성	781
통화 제어 탐색(CCD) 개요	781
통화 제어 탐색(CCD) 사전 요건	781
통화 제어 탐색(CCD) 구성 작업 흐름	782
SAF 보안 프로파일 구성	783
SAF 포워더 구성	784
SIP 또는 H.323 클러스터 간 트렁크 구성	784

호스팅된 DN 그룹 구성	785
호스팅된 DN 패턴 구성	785
광고 서비스 구성	786
통화 제어 탐색(CCD)에 대한 파티션 구성	786
요청 서비스 구성	787
설정된 패턴 차단	787
통화 제어 탐색(CCD) 상호 작용	788
통화 제어 탐색(CCD) 제한 사항	789

장 60

외부 전화 제어 구성	791
외부 전화 제어 개요	791
외부 전화 제어 사전 요건	792
외부 전화 제어 구성 작업 흐름	792
외부 전화 제어를 위한 발신 검색 공간 구성	793
외부 전화 제어 프로파일 구성	794
변환 패턴에 프로파일 할당	794
라우트 서버 인증서를 신뢰할 수 있는 저장소로 가져오기	795
SSC(자가서명 인증서)를 라우트 서버로 내보내기	795
Chaperone 기능 구성	796
사용자 정의된 알림 구성	797
외부 전화 제어 상호 작용	798
외부 전화 제어 제한 사항	800

장 61

통화 대기열 구성	801
통화 대기 개요	801
보안 통화 대기	802
통화 대기 사전 요건	803
통화 대기 작업 흐름	803
알림 구성	803
대기 중 음악 구성	805
대기 중 음악에 대한 오디오 소스 필드	805

헌트 파일럿 대기 구성	808
응답이 없는 경우 헌트 구성원 자동 로그아웃	810
통화 지정 보류 상호 작용	810
통화 대기 제한 사항	811
통화 대기가 포함된 헌트 파일럿의 성능 및 확장성	811

장 62

통화 조절 구성	813
통화 조절 개요	813
통화 조절 구성 작업 흐름	814
통화 조절 구성	814
메모리 조절 구성	815

장 63

논리적 파티션 구성	817
논리적 파티셔닝 개요	817
논리적 파티셔닝 구성 작업 흐름	817
논리적 파티셔닝 활성화	818
지오로케이션 구성	819
지오로케이션 만들기	819
지오로케이션 할당	819
기본 지오로케이션 설정	820
논리적 파티셔닝 기본 정책 구성	820
논리적 파티션 확인을 방지하도록 디바이스를 구성합니다.	821
지오로케이션 필터 구성	821
지오로케이션 필터 규칙 만들기	822
지오로케이션 필터 할당	822
기본 지오로케이션 필터 설정	823
논리적 파티셔닝 정책 레코드 집합 정의	823
위치 전환 활성화	824
논리적 파티셔닝 상호 작용	824
논리적 파티션 제한 사항	826

장 64

위치 인식 구성	829
위치 인식 개요	829
무선 네트워크 업데이트	830
유선 네트워크 업데이트	831
위치 인식을 위해 지원되는 엔드포인트	831
위치 인식 사전 요건	831
위치 인식 구성 작업 흐름	832
무선 인프라 동기화를 위한 서비스 시작	832
무선 액세스 포인트 컨트롤러 구성	833
인프라 디바이스 삽입	834
추적에서 인프라 디바이스 비활성화	835
관련 설명서	835

장 65

유연한 DSCP 표시 및 비디오 프로모션 구성	837
유연한 DSCP 표시 및 비디오 프로모션 개요	837
사용자에 대한 사용자 정의 QoS 설정	838
트래픽 클래스 레이블	839
DSCP 설정 구성 작업 흐름	839
유연한 DSCP 표시 및 비디오 프로모션 정책 구성	840
유연한 DSCP 표시 및 비디오 프로모션 서비스 매개 변수	840
사용자에 대한 사용자 정의 QoS 정책 구성	841
SIP 프로파일에서 사용자 정의 QoS 설정 구성	842
전화기에 사용자 정의 QoS 정책 적용	842
유연한 DSCP 표시 및 비디오 프로모션 상호 작용	843
유연한 DSCP 표시 및 비디오 프로모션 제한 사항	843

장 66

SIP에서 발신자 번호 및 청구 번호 분리	845
외부 표시 이름 및 번호 개요	845
구성 개요	845
통화 처리	846

착신 통화 프로세스	846
발신 통화 프로세스	847
외부 표시 번호 마스크 작업	847
디렉터리 번호 개요	848
디렉터리 번호 구성 작업	848
LDAP에서 최종 사용자 가져오기	848
최종 사용자를 수동으로 추가	849
최종 사용자를 위한 새 전화기 추가	851
최종 사용자에게 기존 전화기 이동	851
DN에 외부 표시 정보 구성	852
SIP 프로파일 개요	853
SIP 프로파일 구성 작업	853
SIP 프로파일 구성	853
SIP 프로파일에 외부 표시 정보 구성	854
SIP 트렁크 개요	855
트렁크 구성 작업	855
SIP 트렁크 보안 프로파일 구성	856
일반 디바이스 설정 구성	857
SIP 트렁크 구성	857
SIP 트렁크에 표시 정보 구성	858
클러스터 간 SME 통화 흐름	860
장 67	SIP OAuth 모드 861
SIP OAuth 모드 개요	861
SIP OAuth 모드 사전 요건	862
SIP OAuth 모드 구성 작업 흐름	862
전화기 옛지 신뢰에 CA 인증서 업로드	863
디바이스에 대한 OAuth 액세스 토큰 활성화	864
새로 고침 로그인 구성	865
OAuth 포트 구성	865
Expressway-C에 대한 OAuth 연결 구성	866

SIP OAuth 모드 활성화	867
Cisco CallManager 서비스 다시 시작	867
전화기 보안 프로파일에서 디바이스 보안 모드 구성	867
MRA 모드에 대해 SIP OAuth 등록 전화기 구성	868

부 XV:

QoS 관리 871

장 68

APIC-EM 컨트롤러를 사용하여 QoS 구성 873

APIC-EM 컨트롤러 개요	873
APIC-EM 컨트롤러 사전 요건	874
APIC-EM 컨트롤러 구성 작업 흐름	874
APIC-EM 컨트롤러 구성	875
APIC-EM 컨트롤러 인증서 업로드	875
APIC-EM 컨트롤러에 대한 HTTPS 연결 구성	876
시스템에 대한 외부 QoS 서비스 활성화	876
SIP 프로파일 수준에서 외부 QoS 서비스 구성	877
SIP 프로파일을 전화기에 할당	877

장 69

AS-SIP 엔드포인트 구성 879

AS-SIP 개요	879
타사 AS-SIP 전화기	880
AS-SIP 컨퍼런싱	881
AS-SIP 사전 요건	882
AS-SIP 엔드포인트 구성 작업 흐름	882
다이제스트 사용자 구성	883
SIP 전화기 보안 포트 구성	884
서비스 다시 시작	884
AS-SIP용 SIP 프로파일 구성	884
AS-SIP에 대한 전화기 보안 프로파일 구성	885
AS-SIP 엔드포인트 구성	886
디바이스를 최종 사용자에게 연결	887

AS-SIP에 대한 SIP 트렁크 보안 프로파일 구성 887

AS-SIP에 대한 SIP 트렁크 구성 888

AS-SIP 기능 구성 889

장 70

MLPP(Multilevel Precedence and Preemption) 구성 893

MLPP(Multilevel Precedence and Preemption) 개요 893

MLPP(Multilevel Precedence and Preemption) 사전 요건 893

MLPP(Multilevel Precedence and Preemption) 작업 흐름 894

도메인 및 도메인 목록 구성 895

MLPP(Multilevel Precedence and Preemption) 도메인 구성 896

리소스 우선 순위 네임스페이스 네트워크 도메인 구성 897

리소스 우선 순위 네임스페이스 네트워크 도메인 목록 구성 897

MLPP(Multilevel Precedence and Preemption)에 대한 일반 디바이스 구성 898

MLPP(Multilevel Precedence and Preemption)에 대한 엔터프라이즈 매개 변수 구성 898

MLPP(Multilevel Precedence and Preemption)에 대한 엔터프라이즈 매개 변수 899

MLPP(Multilevel Precedence and Preemption)에 대한 파티션 구성 900

파티션 이름 지정 지침 900

MLPP(Multilevel Precedence and Preemption)에 대한 발신 검색 공간 구성 901

MLPP(Multilevel Precedence and Preemption)에 대한 경로 패턴 구성 902

MLPP(Multilevel Precedence and Preemption)에 대한 경로 패턴 구성 필드 902

MLPP(Multilevel Precedence and Preemption)에 대한 변환 패턴 구성 903

게이트웨이에 대한 MLPP(Multilevel Precedence and Preemption) 구성 904

전화기에 대한 MLPP(Multilevel Precedence and Preemption) 구성 905

전화기에 대한 MLPP(Multilevel Precedence and Preemption) 설정 906

디렉터리 번호를 구성하여 MLPP(Multilevel Precedence and Preemption) 통화 설정 907

다중 수준 우선 순위 및 선점에 대한 사용자 디바이스 프로파일 구성 908

다중 수준 우선 순위 및 선점에 대한 디폴트 디바이스 프로파일 구성 909

MLPP(Multilevel Precedence and Preemption) 상호 작용 910

MLPP(Multilevel Precedence and Preemption) 제한 사항 911

부 XVI:

SIP 상호 운용성 915

장 71

- SIP 정규화 및 투명성 구성 917**
 - SIP 정규화 및 투명성 개요 917
 - SIP 정규화 및 투명성에 대한 기본 스크립트 918
 - SIP 정규화 및 투명성 사전 요건 918
 - SIP 정규화 및 투명성 구성 작업 흐름 919
 - 새 SIP 정규화 및 투명성 스크립트 만들기 919
 - SIP 트렁크에 정규화 또는 투명성 스크립트 적용 920
 - SIP 디바이스에 정규화 또는 투명성 적용 921

장 72

- SDP 투명성 프로파일 구성 923**
 - SDP 투명성 프로파일 개요 923
 - SDP 투명성 프로파일 제한 사항 923
 - SDP 투명성 프로파일 사전 요건 924
 - SDP 투명성 프로파일 구성 924

장 73

- BFCP를 통한 프레젠테이션 공유 구성 925**
 - Binary Floor Control Protocol 개요 925
 - BFCP 아키텍처 926
 - BFCP 제한 사항 926
 - BFCP 사전 요건을 사용하여 프레젠테이션 공유 927
 - BFCP 구성 작업 흐름을 사용하여 프레젠테이션 공유 927
 - SIP 트렁크에 대한 BFCP 지원 활성화 927
 - 타사 전화기에 대해 BFCP를 사용하여 프레젠테이션 공유 활성화 928

장 74

- 비디오 텔레포니 929**
 - 비디오 전화 통신 개요 929
 - 비디오 전화 통신 지원 930
 - 영상 통화 930
 - MTP 토폴로지에서 실시간 전송 제어 프로토콜 통과 930
 - 비디오 코덱 931

비디오 네트워크	933
비디오 전화 통신 구성 작업 흐름	935
H.323 비디오	935
H.323 통화의 H.239 확장 비디오 채널	936
타사 H.323 디바이스에 대한 지원	936
H.323 디바이스에서 프레젠테이션 기능 호출	937
두 번째 비디오 채널 열기	937
두 번째 비디오 채널의 CAC(Call Admission Control)	938
허용되는 비디오 채널 수	939
H.239 명령 및 표시 메시지	939
토폴로지 및 프로토콜 상호 운용성 제한 사항	940
통화 중 기능 제한	940
비디오 지원	940
스키니 클라이언트 제어 프로토콜 비디오	940
SIP 비디오	940
영상 통화에 대한 SIP 디바이스 구성	941
Cisco 화상 회의 브리지	941
Cisco Telepresence MCU 화상 회의 브리지	941
Cisco TelePresence Conductor 화상 회의 브리지	942
Cisco Meeting Server	942
비디오 암호화	943
VCS를 사용하여 상호 운용성 구성	943
비디오 기능	944
Binary Floor Control Protocol에 대한 엔드포인트 지원	944
암호화된 iX 채널	944
암호화 모드	945
비 암호화 모드	945
종단 카메라 제어 프로토콜 지원	946
비디오 네트워크에 대한 QoS	946
대역폭 관리	946
고급 위치 기반 통화 허용 제어	946

세션 수준 대역폭 한정자	947
SIP 전화기에 대한 비디오 해상도 지원	948
대체 라우팅	949
유연한 DSCP 표시	949
영상 통화에 대한 전화기 구성	949
화상 회의를 위한 전화회의 제어	950
비디오 전화 통신 및 Cisco 통합 서비스 가용성	950
성능 카운터	950
비디오 브리지 카운터	952
CDR(Call Detail Record)	952
통화 관리 기록(CMR)	953

부 XVII:	비상 통화 라우팅 규정	955
---------	--------------	-----

장 75	미국 연방 통신 위원회(FCC) 비상 통화 라우팅 규정	957
	비상 통화 라우팅 규정 개요	957
	비상 통화 라우팅 규정 구성	959



1 장

신규 및 변경된 정보

• [신규 및 변경된 정보, 1 페이지](#)

신규 및 변경된 정보

다음 테이블은 현재 릴리스까지 이 가이드의 주요 기능 변경 사항을 소개합니다. 이 테이블은 가이드에 제공된 모든 변경 사항 또는 이 릴리스의 새 기능에 대한 전체 목록을 제공하지 않습니다.

표 1: **Unified Communications Manager** 및 **IM**과 프레즌스 서비스의 새로운 기능 및 변경된 동작

기능 또는 변경 사항	설명	참고:	날짜
릴리스 14용 문서의 최초 릴리스	—	—	2021년 3월 31일
78xx 및 88xx 전화기용 SIP OAuth 활성화	SIP OAuth는 MRA뿐만 아니라 CAPF 온프레미스 없이 엔드 투 엔드 보안 시그널링 및 미디어 암호화를 제공하며, 기본적으로 TFTP는 SIP OAuth가 활성화된 경우 SIP 전화기에 대해 안전합니다.	<ul style="list-style-type: none"> • SIP OAuth 모드 구성 작업 흐름, 862 페이지 • 디바이스에 대한 OAuth 액세스 토큰 활성화, 864 페이지 	2021년 3월 31일
헤드셋 및 액세서리 재고 목록 다운로드	이 기능을 사용하면 관리자가 배포의 헤드셋 및 액세서리에 대한 상세 보고서를 Unified Communications Manager 사용자 인터페이스의 CSV 파일로 다운로드할 수 있습니다.	헤드셋 및 액세서리 재고 목록, 733 페이지	2021년 3월 31일

기능 또는 변경 사항	설명	참고:	날짜
경량 Keepalive를 통한 MRA 페일오버	엔드포인트 등록에 대한 MRA 고가용성 기능을 통해 Cisco Webex 및 Cisco Jabber 클라이언트는 경로에서 Cisco Expressway-E, Cisco Expressway-C 또는 Unified Communications Manager와 같은 네트워크 요소의 오류를 신속하게 감지하고 새 경로를 사용하여 다시 등록하도록 정정 작업을 수행할 수 있습니다.	경량 Keepalive를 통한 MRA 페일오버, 88 페이지	2021년 3월 31일
IVR 및 전화 서비스를 사용한 기본 전화 마이그레이션	최종 사용자나 관리자는 이 기능을 사용하여 간단한 사용자 인터페이스를 사용하여 이전 전화기의 모든 설정을 새 전화기로 쉽게 마이그레이션할 수 있습니다.	IVR 및 전화 서비스를 사용한 기본 전화 마이그레이션 개요, 749 페이지	2021년 3월 31일
Manager Assistant에서 Oracle JRE 제거	JRE(Oracle Java Runtime Environment)는 더 이상 Cisco Unified Communications Manager Assistant 플러그인에 포함되지 않습니다.	Manager Assistant 사전 요건, 179 페이지	2021년 3월 31일
릴리스 14SU1용 문서의 최초 릴리스	—	—	2021년 10월 27일
Meraki 액세스 포인트 지원	Unified Communications Manager는 Meraki 액세스 포인트를 통해 연결되는 무선 엔드포인트에 대한 위치 인식을 지원합니다.	위치 인식 개요, 829 페이지	2021년 10월 27일
OAuth에 대한 TFTP 프록시 지원	Unified Communications Manager는 SIP OAuth 배포에서 TFTP 프록시를 지원합니다.	SIP OAuth 모드 활성화, 867 페이지	2021년 10월 27일
Wi-Fi에서 LTE로 통화 전환	Unified Communications Manager를 사용하면 사용자가 네트워크를 전환하는 동안 활성 통화를 끊지 않고도 Cisco Webex 사용자가 Wi-Fi 및 LTE 네트워크 간에 전환할 수 있습니다.	Wi-Fi에서 LTE로 통화 전환, 16 페이지	2021년 10월 27일
릴리스 14SU2용 문서의 최초 릴리스	—	—	2022년 6월 16일
RedSky E911 위치 서비스 지원	Unified Communications Manager와 통합된 RedSky 솔루션을 통해 고객은 캠퍼스 내든 원격이든 모든 직원에 대해 9-1-1 비상 통화를 수행할 수 있는 활성 위치 URI를 확보하고 긴급 구조대원에게 통화를 보낼 수 있습니다.	RedSky로 비상 통화 처리, 701 페이지	2022년 6월 16일

기능 또는 변경 사항	설명	참고:	날짜
지정 보류 로트에 대한 보안 통화 지원	Unified Communications Manager는 SRTP 폴백 옵션 상태와 관계 없이 발신 SRTP 전용 통화를 보안 통화로 처리합니다.	보안 통화 대기, 802 페이지	2022년 6월 16일



부

시작하기

- [기능 구성 개요, 7 페이지](#)
- [□구성도구, 9 페이지](#)



2 장

기능 구성 개요

- 기능 구성 설명서 정보, 7 페이지
- 전화기 기능 목록 생성, 7 페이지

기능 구성 설명서 정보

이 설명서는 Unified Communications Manager 시스템에서 기능을 구성하기 위해 완료해야 하는 작업에 대한 정보를 제공합니다. 인바운드 및 아웃바운드 통화, 다이얼 플랜 및 네트워크 리소스와 같은 "1일 구성을 포함하는 통화 제어 시스템을 구성한 후 이 설명서를 사용하십시오. 통화 제어 시스템 구성에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 내용을 참조하십시오.

전화기 기능 목록 생성

구성하려는 기능을 디바이스에서 지원하는지 확인하려면 전화기 기능 목록 보고서를 생성합니다.

프로시저

단계 1 Cisco Unified Reporting Administration에서 시스템 보고서를 선택합니다.

단계 2 보고서 목록에서 **Unified CM Phone** 기능 목록을 클릭합니다.

단계 3 다음 단계 중 하나를 수행합니다.

- 새 보고서 생성(막대 차트 아이콘)을 선택하고 새 보고서를 생성합니다.
- 보고서가 이미 있는 경우 **Unified CM** 전화기 기능 목록을 선택합니다.

단계 4 제품 드롭다운 목록에서 모두를 선택합니다.

단계 5 구성하려는 기능의 이름을 클릭합니다.

단계 6 제출을 클릭하여 보고서를 생성합니다.



3 장

□ 구성 도구

- 기능 구성 설명서 정보, 9 페이지
- 구성 도구 개요, 9 페이지
- 전화기 기능 목록 생성, 12 페이지

기능 구성 설명서 정보

이 설명서는 Unified Communications Manager 시스템에서 기능을 구성하기 위해 완료해야 하는 작업에 대한 정보를 제공합니다. 인바운드 및 아웃바운드 통화, 다이얼 플랜 및 네트워크 리소스와 같은 "1일 구성을 포함하는 통화 제어 시스템을 구성한 후 이 설명서를 사용하십시오. 통화 제어 시스템 구성에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 내용을 참조하십시오.

구성 도구 개요

이 설명서의 절차에서는 다음 두 가지 구성 도구를 사용해야 합니다.

- Cisco 통합 커뮤니케이션 매니저 관리
- Cisco 유니파이드 Serviceability

이 장에서는 도구에 대한 간략한 설명과 이러한 도구에 액세스하는 방법에 대해 설명합니다.

Cisco Unified Communications Manager Administration

Cisco 통합 커뮤니케이션 매니저 관리 관리는 Unified Communications Manager 서비스 노드에 대한 개별 구성 변경을 수동으로 수행할 수 있게 해주는 웹 기반 애플리케이션입니다. 이 설명서의 절차에서는 이 애플리케이션을 사용하여 기능을 구성하는 방법에 대해 설명합니다.

벌크 구성 작업을 수행해야 하고 구성 프로세스를 자동화하려는 경우 Unified Communications Manager BAT(벌크 관리 도구)를 사용하여 많은 수의 구성을 동시에 변경할 수 있습니다. 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서](#)의 내용을 참조하십시오.

Cisco Unified CM 관리에 로그인

다음 절차에 따라 Cisco Unified Communications Manager 관리에 로그인합니다. Cisco Unified Communications Manager 관리에 로그인하면 Unified Communications Manager에 대한 라이선스의 현재 상태를 나타내는 메시지가 주 창에 표시될 수 있습니다. 예를 들어 Unified Communications Manager에서 다음과 같은 경우를 식별할 수 있습니다.

- Unified Communications Manager가 현재 스타터(데모) 라이선스로 작동하고 있으므로 적절한 라이선스 파일을 업로드하십시오.
- Unified Communications Manager가 현재 부족한 수의 라이선스로 작동하고 있으므로 라이선스 파일을 추가로 업로드하십시오.
- Unified Communications Manager가 현재 올바른 소프트웨어 기능 라이선스를 사용하고 있지 않습니다. 이 경우 적절한 소프트웨어 버전 라이선스를 업로드하고 Cisco CallManager 서비스를 다시 시작하기 전까지 Cisco CallManager 서비스가 중지되고 시작되지 않습니다.

다음 절차에 따라 서버를 찾고 Cisco Unified CM 관리에 로그인합니다.

프로시저

단계 1 기본 운영 체제 브라우저를 시작합니다.

단계 2 웹 브라우저의 주소 표시줄에 다음 URL을 대/소문자를 구분하여 입력합니다.

`https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do`

여기서: <Unified CM-server-name>은 서버의 이름 또는 IP 주소입니다.

참고 선택적으로 포트 번호를 지정할 수 있습니다.

단계 3 [보안 경고] 대화 상자가 표시됩니다. 해당하는 버튼을 클릭합니다.

단계 4 주 Cisco Unified CM 관리 창에서 Unified Communications Manager 설치 시 지정한 사용자 이름과 암호를 입력하고 로그인을 클릭합니다. (두 필드의 내용을 모두 지우려면 재설정을 클릭합니다.)

참고 보안을 위해 사용하지 않고 30분이 지나면 Cisco 통합 커뮤니케이션 매니저 관리에서 로그아웃되며 다시 로그인해야 합니다.

Cisco Unified Communications Manager 서비스 가용성

이 설명서의 일부 절차에서는 Cisco 유니파이드 Serviceability 애플리케이션을 사용하여 Unified Communications Manager 노드에서 서비스를 시작하거나 다시 시작해야 합니다.

Cisco 유니파이드 Serviceability 다음과 같은 기능을 제공하는 웹 기반 문제 해결 도구입니다.

- 문제 해결에 대한 정보 및 이벤트를 저장하고 정보 메시지 정의를 제공합니다.
- 문제 해결에 대한 로그 파일에 추적 정보를 저장합니다.

- Cisco Unified 실시간 모니터링 도구(Unified RTMT)를 통해 구성 요소의 실시간 동작을 모니터링합니다.
- 사용자가 시스템에 구성 변경 사항을 기록하거나 사용자 작업의 결과로 인해 감사 기능을 제공합니다. 이 기능은 Unified Communications Manager 및 Cisco Unity Connection의 정보 보증 기능을 지원합니다.
- 서비스 활성화 창을 통해 활성화 및 비활성화하고 볼 수 있는 기능 서비스를 제공합니다.
- 경보 요약 또는 서버 통계 보고서와 같은 일별 보고서를 생성하고 아카이브합니다.
- Unified Communications Manager, IM and Presence 서비스 및 Cisco Unity Connection이(가) SNMP(Simple Network Management Protocol) 원격 관리 및 문제 해결을 위해 관리되는 디바이스로 작동하는 것을 허용합니다.
- 노드(또는 클러스터의 모든 노드)에서 로그 파티션의 디스크 사용을 모니터링합니다.
- 시스템에서 스레드 및 프로세스 수를 모니터링하고, 캐시를 사용하여 성능을 향상시킵니다.
- **Unified Communications Manager**만 해당: Cisco Unified Communications Manager CDR 분석 및 보고를 통한 서비스 품질, 트래픽 및 청구 정보에 대한 Unified Communications Manager 보고서를 생성합니다.

Cisco Unified Communications Manager 서비스 가용성에 로그인

다음 절차를 사용하여 Cisco 유니파이드 Serviceability에 로그인합니다.

프로시저

단계 1 기본 운영 체제 브라우저를 시작합니다.

단계 2 웹 브라우저의 주소 표시줄에 다음 URL을 대/소문자를 구분하여 입력합니다.

`https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do`

여기서: <Unified CM-server-name>은 서버의 이름 또는 IP 주소입니다.

단계 3 [보안 경고] 대화 상자가 표시됩니다. 해당하는 버튼을 클릭합니다.

단계 4 탐색 드롭다운 목록 상자에서 **Cisco Unified Serviceability**를 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.하고 이동을 클릭합니다.

단계 5 Unified Communications Manager 설치 중 지정한 사용자 이름과 암호를 입력하고 로그인을 클릭합니다.

참고 보안을 위해 30분 동안 사용하지 않으면 시스템이 사용자를 로그아웃하며 다시 로그인해야 합니다.

전화기 기능 목록 생성

구성하려는 기능을 디바이스에서 지원는지 확인하려면 전화기 기능 목록 보고서를 생성합니다.

프로시저

단계 1 Cisco Unified Reporting Administration에서 시스템 보고서를 선택합니다.

단계 2 보고서 목록에서 **Unified CM Phone** 기능 목록을 클릭합니다.

단계 3 다음 단계 중 하나를 수행합니다.

- 새 보고서 생성(막대 차트 아이콘)을 선택하고 새 보고서를 생성합니다.
- 보고서가 이미 있는 경우 **Unified CM** 전화기 기능 목록을 선택합니다.

단계 4 제품 드롭다운 목록에서 모두를 선택합니다.

단계 5 구성하려는 기능의 이름을 클릭합니다.

단계 6 제출을 클릭하여 보고서를 생성합니다.



II 부

원격 작업자 기능

- [Cisco Unified Mobility, 15 페이지](#)
- [디바이스 모빌리티, 53 페이지](#)
- [확장 및 연결, 65 페이지](#)
- [원격 작업자 비상 통화, 75 페이지](#)
- [모바일 및 원격 액세스 구성, 79 페이지](#)



4 장

Cisco Unified Mobility

- Cisco Unified Mobility 개요, 15 페이지
- Cisco Unified Mobility 사전 요건, 18 페이지
- Cisco Unified Mobility 구성 작업 흐름, 19 페이지
- Cisco Unified Mobility 통화 흐름, 43 페이지
- 스마트 클라이언트가 없는 SIP 트렁크를 통한 FMC, 44 페이지
- 통신 사업자 통합 모바일 디바이스에 대한 헌트 그룹 로그인 및 로그아웃, 44 페이지
- Cisco Unified Mobility 상호 작용, 45 페이지
- Cisco Unified Mobility 제한 사항, 47 페이지
- Cisco Unified Mobility 문제 해결, 51 페이지

Cisco Unified Mobility 개요

Cisco Unified Mobility 는 사용자가 어디에서든지, 또는 사용 중인 디바이스에 상관 없이 통합 커뮤니케이션 애플리케이션에 대한 상호 작용을 허용하는 이동성 관련 기능을 제공합니다. 사용 중인 디바이스가 홈 오피스 전화기, WiFi 연결을 통해 iPhone 또는 Android 클라이언트의 듀얼 모드 Cisco Jabber 또는 다른 셀룰러 공급업체의 휴대폰인지 여부에 상관 없이, 여전히 통합 커뮤니케이션 기능에 액세스하여 엔터프라이즈에 통화를 앵커링할 수 있습니다.

예를 들어, 구성된 전화기에서 엔터프라이즈 번호로 전송되는 통화로 응답한 다음 통화를 휴대폰으로 호 전환할 수 있으므로 사무실 외부에서도 진행 중인 대화를 계속할 수 있습니다.

Cisco Unified Mobility의 이점

대부분의 이동성 기능은 엔터프라이즈 내에서 통화 앵커를 제공합니다. 통화는 모바일 디바이스에서 발신되거나 모바일 디바이스에서 전송되더라도 통화는 엔터프라이즈 게이트웨이를 통해 라우팅됩니다.

이렇게 하면 다음과 같은 이점이 있습니다.

- 사용 중인 디바이스와 사무실 외부에 있는지 여부와 관계 없이 모든 비즈니스 통화로 대한 단일 엔터프라이즈 전화 번호 및 음성 메일
- 모바일 디바이스에 대한 비즈니스 통화를 확장하고 사무실 전화기인 것처럼 통화를 계속 처리할 수 있습니다.

- 모바일 디바이스에서 발신된 통화는 엔터프라이즈에 앵커링되고 엔터프라이즈 게이트웨이를 통해 라우팅됩니다. 이를 통해 UC 통화 중 기능에 액세스, 중앙 집중식 청구 및 통화 세부 정보 레코드 및 값비싼 셀룰러 네트워크를 피하는 잠재적인 비용 절감을 제공합니다.
- 한 네트워크에서 다른 네트워크로 로밍하고 통화가 삭제되지 않도록 할 수 있습니다.

Wi-Fi에서 LTE로 통화 전환

이 기능을 사용하면 소프트웨어 클라이언트 최종 사용자가 네트워크를 전환하는 동안 활성 통화를 끊지 않고 Wi-Fi와 LTE 네트워크 간에 또는 그 반대로 전환할 수 있도록 유연성을 제공합니다. Wi-Fi에서 LTE로 통화 전환 기능은 자동으로 활성화되지만 Unified Communications Manager 릴리스 14SU1 이상이 필요합니다.

통화 중에 소프트웨어 클라이언트가 네트워크의 변화를 감지하고 등록을 전환한 다음 스위치에 대한 시청각 표시와 함께 활성 통화를 최종 사용자에게 다시 연결합니다. 그러나 사용자는 통화 시 원활한 오디오 및 비디오 환경을 계속 유지합니다.



참고 이 기능은 활성 통화 핸드오버만 지원합니다. 통화 녹음이 활성 상태이면 녹음이 중지되고 핸드오버 후 계속되지 않습니다. 또한, 네트워크 핸드오버는 통화 도중 기능(예: 보류 또는 전송), 화면 공유, 전화 회의, 콜 센터 기능을 지원하지 않습니다. 자세한 내용은 [Webex의 통화 구축 가이드\(Unified CM\)](#)에서 'Webex의 통화 환경 준비(Unified CM)' 장을 참조하십시오.

Cisco Desktop 및 최신 Webex Mobile(WebexApp 41.8) 버전은 이 기능을 지원합니다. 자세한 내용은 [Webex 통화 구축 가이드\(Unified CM\)](#)에서 'Webex(Unified CM) 통화 시 알려진 문제 및 제한 사항' 섹션을 참조하십시오.

이동성 기능

Cisco Unified Mobility에서는 다음과 같은 이동성 관련 기능을 제공합니다.

이동성 기능	설명
단일 전화번호 연결	사무실에 있든 사무실 외부에 있든 관계 없이 통화자에게 연락할 수 있는 단일 엔터프라이즈 전화 번호 및 음성 메일을 제공합니다. 다른 사용자가 사용자의 엔터프라이즈 번호로 전화를 걸면 데스크폰 또는 구성된 원격 대상(예: 자택 사무용 전화기, iPhone 또는 Android 클라이언트의 이중 모드 Cisco Jabber 및 다른 공급업체의 휴대폰)에서 전화를 받을 수 있습니다.

이동성 기능	설명
모바일로 이동	<p>데스크폰에서 Cisco IP 전화기의 이동성 소프트웨어를 눌러 원격 대상으로 구성된 모바일 디바이스로 활성 통화를 호 전환할 수 있습니다. 이는 원격 대상 구성의 일부로 단일 번호 연락에 연결되어 있습니다.</p> <p>모바일로 이동 옵션과 마찬가지로 데스크 당겨받기 옵션도 있습니다. 이 옵션은 모바일 통화 중이며 사무실에 막 도착하는 경우에 적합합니다. 모바일 디바이스의 통화를 끊고 데스크 당겨받기의 최대 대기 시간이 만료되기 전에 사무실 전화를 당겨받아 통화를 즉시 재개할 수 있습니다(기본값은 10초). 이 옵션은 단일 전화번호 연결 구성의 일부로 활성화됩니다.</p> <ul style="list-style-type: none"> • 보류 중인 통화에 프라이버시 설정 적용 서비스 매개 변수를 False로 설정해야 합니다. • 엔터프라이즈 기능 액세스 코드 및 세션 핸드오프 코드를 사용하여 원격 대상 및 데스크폰 간에 통화를 호전환할 수도 있습니다.
모바일 음성 액세스	<p>원격 전화기에서 전화를 걸고 사무실 전화에서 전화를 건 것처럼 전화가 엔터프라이즈에 고정되어 수신자에게 표시되도록 할 수 있습니다. 이 기능을 사용하는 경우 모바일 디바이스에서 대화형 음성 응답 시스템으로 전화를 걸어야 합니다. 사용자를 인증하고 통화 대상에게 메시지를 표시하면 시스템은 사용자가 엔터프라이즈 전화기에서 전화를 건 것처럼 통화를 배치합니다.</p> <p>모바일 음성 액세스 프롬프트를 사용하여 원격 대상에 대한 단일 번호 연락을 활성화하거나 비활성화할 수도 있습니다.</p>
엔터프라이즈 기능 액세스	<p>구성된 원격 대상에서 2단계 다이얼링을 제공합니다. 또한, 착신자에게 건 전화가 데스크폰에서 시작된 것처럼 나타나도록 합니다. 모바일 음성 액세스와 달리 엔터프라이즈 기능 액세스를 사용하려면 구성된 원격 대상 중 하나에서 전화를 걸어야 합니다.</p> <p>엔터프라이즈 기능 액세스를 사용하면 원격 대상에서 통화하는 동안 통화 중 기능에 액세스할 수 있습니다. 보류, 배타적 보류, 호 전환 등의 다양한 기능에 대한 코드를 나타내는 DTMF 숫자를 전송하여 통화 중 기능에 액세스할 수 있습니다.</p>
인텔리전트 세션 제어	<p>구성된 원격 대상 번호(예: 원격 대상으로 구성된 휴대폰 번호에 대한 엔터프라이즈 기반 호출)에 직접 배치되는 엔터프라이즈 기반 호출에 대해 자동 통화 앵커링을 활성화합니다. 서비스 매개 변수를 구성하면 시스템에서 해당 통화를 연결된 엔터프라이즈 번호로 자동 재전송하여 비용 절감 및 추가 UC 기능을 제공할 수 있습니다.</p>

이동성 기능	설명
듀얼 모드 전화기	<p>iPhone 및 Android 클라이언트의 Cisco Jabber를 이중 모드 디바이스로 프로비저닝할 수 있습니다. 듀얼 모드 전화기에는 Wi-Fi 또는 셀룰러 네트워크를 통해 연결할 수 있는 기능이 있습니다. 클라이언트가 엔터프라이즈 네트워크 내에 있는 경우 Cisco Jabber가 Wi-Fi를 통해 Unified Communications Manager에 등록하고 UC 통화 및 인스턴트 메시징 기능을 가질 수 있습니다. 모바일 디바이스의 전화 번호를 사용하여 모바일 ID를 구성하는 경우 엔터프라이즈 네트워크를 떠나는 경우 Jabber에서 셀룰러 디바이스로 통화를 전송할 수 있습니다.</p> <p>참고 Cisco Jabber 모바일 클라이언트에서 사용할 수 있는 추가 기능은 모바일 및 원격 액세스가 가능하며, 이를 통해 Cisco Jabber 클라이언트가 네트워크 외부에 있을 때 데이터 네트워크에 연결할 수 있습니다. 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서의 "모바일 및 원격 액세스 구성" 섹션을 참조하십시오.</p>

Cisco Unified Mobility 사전 요건

다음 사전 요건을 참조하십시오.

- 이동성 기능을 활성화하려면 다이얼 플랜 및 통화 라우팅 구성에서 구축 요구 사항을 처리할 수 있는지 확인하기 위한 적절한 계획이 필요합니다. 자세한 내용은 *Cisco Collaboration System Solution Reference Network Designs* 설명서의 "모바일 협업" 섹션을 참조하십시오.
- 이동성 기능을 지원하는 Cisco IP 전화기에 대한 자세한 내용은 [전화기 기능 목록 생성, 7 페이지](#)의 내용을 참조하십시오.
 - 이동성 소프트웨어를 지원하는 Cisco IP 전화기 목록을 보려면 이동성 기능에 대한 보고서를 실행합니다.
 - 지원되는 이중 모드 전화기 목록을 보려면 이중 모드 기능에 대한 보고서를 실행합니다.
- 모바일 음성 액세스를 구축하고 있고 시스템에서 추가 로컬을 사용할 수 있도록 하려면(영어 이외의 전화기 로컬 또는 국가별 신호음을 사용하려는 경우) [cisco.com](#)에서 로컬 설치 관리자를 다운로드하여 Cisco Unified OS 관리 인터페이스를 통해 설치할 수 있습니다. 로케일 설치에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 및 IM and Presence Service 설치 설명서](#)의 내용을 참조하십시오.
- 전화기 사용자가 자신의 Cisco Jabber 클라이언트 및 원격 대상을 프로비저닝할 수 있도록 셀프 프로비저닝을 구성합니다. 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "셀프 프로비저닝 구성" 및 "최종 사용자 프로비저닝" 섹션을 참조하십시오.



주의 Cisco 이동성 솔루션은 Cisco 장비로만 검증됩니다. 이 솔루션은 기타 타사 PSTN 게이트웨이 및 SBC(세션 보더 컨트롤러)에서도 작동할 수 있지만 기능이 여기에서 설명하는 대로 작동하지 않을 수 있습니다. 타사 PSTN 게이트웨이 또는 SBC와 함께 이 솔루션을 사용하는 경우 Cisco 기술 지원에서 사용자에게 발생한 문제를 해결하지 못할 수도 있습니다.

Cisco Unified Mobility 구성 작업 흐름

구축에 대한 이동성 기능을 구성하려면 이러한 작업을 완료합니다.

프로시저

	명령 또는 동작	목적
단계 1	다음 중 하나를 수행합니다. <ul style="list-style-type: none"> • 이동성 사용자 구성, 20 페이지 • 벌크 관리를 통해 이동성 사용자 구성, 21 페이지 • LDAP를 통한 이동성 사용자 프로비저닝, 21 페이지 	<p>개별 최종 사용자에게 대한 이동성 기능을 추가합니다.</p> <p>많은 수의 기존 최종 사용자에게 대한 이동성 기능을 구성합니다. 벌크 관리 도구를 사용합니다.</p> <p>이동성 기능을 사용하여 새 사용자를 프로비저닝하면 기능 그룹 템플릿과 LDAP 동기화를 사용할 수 있습니다.</p>
단계 2	IP 전화기에 대한 이동성 구성, 22 페이지	SNR(단일 번호 연락) 및 모바일로 이동 기능 설정을 포함하여 이동성을 위해 Cisco IP 전화기를 구성합니다. 이를 통해 엔터프라이즈 전화기 사용자는 홈 오피스 전화기 또는 휴대폰을 포함하여 광범위한 모바일 디바이스로 엔터프라이즈 통화를 확장할 수 있습니다.
단계 3	모바일 음성 액세스 구성, 28 페이지	선택 사항. 모바일 사용자가 모바일 디바이스에서 전화를 걸고 발신자가 엔터프라이즈 사무실 전화기에서 전화를 거는 것처럼 착신자에게 전화를 걸 수 있도록 시스템 IVR을 제공합니다.
단계 4	엔터프라이즈 기능 접근 (EFA) 구성, 35 페이지	선택 사항. 구성된 원격 대상에서 2단계 다이얼링을 제공하고 데스크폰에서 시작된 것처럼 착신자에게 전화를 걸 수 있습니다. 이 기능을 사용하면 원격 대상에서 통화하는 동안 통화 중 기능에 액세스할 수 있습니다.
단계 5	인텔리전트 세션 제어 구성, 36 페이지	원격 대상에 대한 인바운드 통화가 사용 가능한 경우 연결된 엔터프라이즈로 재전송되도록

	명령 또는 동작	목적
		록 시스템을 구성합니다. 이 기능은 엔터프라이즈 내 이동성 통화에 대한 자동 통화 앵커를 제공하여 비용 절감을 제공하고 통합 커뮤니케이션 기능을 추가합니다.
단계 6	모빌리티 서비스 매개 변수 구성, 37 페이지	선택 사항. Cisco Unified Mobility의 동작을 변경하려는 경우 선택적 이동성 관련 서비스 매개 변수를 구성합니다.
단계 7	Cisco Jabber 듀얼 모드 구성, 37 페이지	사용자가 스마트폰의 Jabber 클라이언트를 통해 엔터프라이즈 통신 기능에 액세스할 수 있도록 Cisco Jabber에 이동성을 구성합니다.
단계 8	기타 이중 모드 디바이스 구성, 38 페이지	Wi-Fi를 통해 연결할 수 있는 FMC 또는 IMS 클라이언트와 같은 다른 이중 모드 디바이스를 구축하려는 경우 이 작업 흐름을 완료합니다.

이동성 사용자 구성

이 절차를 사용하여 이동성 기능을 지원하는 최종 사용자를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 찾기 및 나열 창에서 다음 작업 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 사용자를 선택하여 설정을 수정합니다.
- 새로 추가를 클릭하여 새 사용자를 구성합니다.

단계 3 다음 필수 필드에 대한 값을 구성합니다.

- 사용자 ID
- 성

단계 4 이동성 정보 영역에서 다음 필드를 완성합니다.

- 이동성 활성화 확인란을 선택합니다.
- 선택 사항. 이 사용자가 모바일 음성 액세스를 사용할 수 있도록 하려면 모바일 음성 액세스 활성화 확인란을 선택합니다.
- 데스크 당겨받기 최대 대기 시간 필드에 값(밀리초)을 입력합니다. 원격 대상에서 전화를 끊은 후에 이 타이머는 사용자가 데스크폰에서 통화를 재개하는 옵션이 여전히 있는 시간을 나타냅니다.
- 원격 대상 제한 필드에 사용자에게 SNR(단일 번호 연락) 대상에 대해 허용되는 원격 대상의 수를 입력합니다.

단계 5 최종 사용자 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

별크 관리를 통해 이동성 사용자 구성

이 절차를 사용하여 별크 관리의 사용자 업데이트 메뉴를 사용하여 이동성 기능을 기존 최종 사용자에게 별크 방식으로 추가할 수 있습니다.



참고 별크 관리에는 별크를 사용하여 기존 사용자를 업데이트할 수 있는 다른 기능이 포함되어 있습니다. 예를 들어, 내보내기 및 가져오기 기능을 사용하여 새 이동성 설정을 사용하여 CSV 파일을 가져올 수 있습니다. 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 별크 관리 지침서](#)를 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 별크 관리 > 사용자 > 사용자 업데이트 > 쿼리.

단계 2 필터를 적용하고 찾기를 클릭하여 이동성 사용자로 할당하려는 사용자를 선택합니다.

단계 3 다음을 클릭합니다.

단계 4 이동성 정보 영역에서 먼저 왼쪽의 확인란을 선택하여 이 필드를 업데이트할 것을 표시한 다음 오른쪽의 설정을 구성하여 다음 4개의 필드를 수정합니다.

- 이동성 활성화 - 이 템플릿으로 프로비저닝된 사용자에게 이동성 기능을 활성화하려면 이 확인란을 선택합니다.
- 모바일 음성 액세스 활성화 - 프로비저닝된 사용자가 모바일 음성 액세스를 사용할 수 있게 하려면 이 확인란을 선택합니다.
- 사무실 당겨 받기에 대한 최대 대기 시간 - 이 필드는 휴대폰에서 통화를 끊은 후 데스크폰에서 통화를 재개해야 하는 시간을 나타냅니다.
- 원격 대상 제한 - 이 필드는 이 템플릿을 통해 설정된 사용자에게 할당할 수 있는 원격 대상 및 모바일 ID의 수를 나타냅니다.

단계 5 작업 정보 아래에서 즉시 실행을 선택합니다.

단계 6 제출을 클릭합니다.

LDAP를 통한 이동성 사용자 프로비저닝

LDAP 디렉토리를 아직 동기화하지 않은 경우 이 절차를 사용하여 기능 그룹 템플릿 구성을 통해 이동성 기능을 사용하여 동기화된 최종 사용자를 구성할 수 있습니다. 새로 동기화된 사용자는 템플릿에서 이동성 설정을 상속합니다.



참고 이 방법은 LDAP 디렉터리를 아직 동기화하지 않은 경우에만 작동합니다. 초기 동기화가 발생한 후에는 새 기능 그룹 템플릿 구성을 LDAP 디렉터리 동기화에 할당할 수 없습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 사용자/전화기 추가 > 기능 그룹 템플릿.

단계 2 기능 그룹 템플릿 찾기 및 나열 창에서 다음 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 템플릿을 구성합니다.
- 찾기를 클릭하고 기존 템플릿을 선택하여 구성합니다.

단계 3 템플릿에 이름을 할당합니다.

단계 4 다음 이동성 필드를 구성합니다.

- 이동성 활성화 - 이 템플릿으로 프로비저닝된 사용자에게 이동성 기능을 활성화하려면 이 확인란을 선택합니다.
- 모바일 음성 액세스 활성화 - 프로비저닝된 사용자가 모바일 음성 액세스를 사용할 수 있게 하려면 이 확인란을 선택합니다.
- 사무실 당겨 받기에 대한 최대 대기 시간 - 이 필드는 휴대폰에서 통화를 끊은 후 데스크폰에서 통화를 재개해야 하는 시간(밀리초)을 나타냅니다.
- 원격 대상 제한 - 이 필드는 이 템플릿을 통해 설정된 사용자에게 할당할 수 있는 원격 대상 및 모바일 ID의 수를 나타냅니다.

단계 5 기능 그룹 템플릿 구성 창에서 나머지 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

참고 구성된 기능 그룹 템플릿을 아직 동기화되지 않은 LDAP 디렉터리에 할당합니다. 새로 동기화된 사용자는 이동성이 활성화됩니다. LDAP를 통한 사용자 프로비저닝에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "최종 사용자 프로비저닝" 장을 참조하십시오.

IP 전화기에 대한 이동성 구성

이러한 작업을 완료하여 Cisco IP 전화기에 대한 이동성 기능을 구성합니다. 여기에는 SNR(단일 번호 연락) 및 모바일으로 이동 기능 설정이 포함됩니다. 따라서 사용자는 단일 엔터프라이즈 번호로 모든 디바이스에서 울릴 뿐만 아니라 어떤 디바이스에서 벨소리가 울리더라도 연결할 수 있는 엔터프라이즈 수준의 음성 메일도 사용할 수 있습니다. 그리고 사용자는 자신의 데스크폰 및 모바일 디바이스 간에 활성 통화를 전송할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	이동성에 대한 소프트키 템플릿 구성, 23 페이지	이동성 소프트키를 포함하는 Cisco IP 전화기에 대한 이동성 소프트키 템플릿을 구성합니다. 사용자는 소프트키를 눌러 해당 데스크폰에서 모바일폰으로 통화를 전송할 수 있습니다.
단계 2	이동성을 위한 IP 전화기 구성, 25 페이지	엔터프라이즈 번호에 대한 수신 통화가 원격 대상으로 확장되도록 이동성에 대한 IP 전화를 구성합니다.
단계 3	원격 대상 프로파일 구성, 25 페이지	사용자의 모든 원격 대상 번호에 적용하려는 일반 설정을 구성합니다.
단계 4	원격 대상 구성, 26 페이지	사용자에게 연락할 수 있는 모바일 디바이스 (예: 홈 오피스 전화기, 셀룰러 네트워크의 휴대폰)를 나타내는 가상 디바이스인 원격 대상을 구성합니다. 원격 대상에서 사용자의 데스크폰과 동일한 설정을 많이 수행합니다.
단계 5	액세스 목록 구성, 27 페이지	선택 사항. 어떤 통화가 어떤 원격 대상에서 하루 중 어느 시간에 벨이 울릴 수 있는지 제어합니다. 액세스 목록은 발신자 ID를 기반으로 발신자를 필터링하고 해당 원격 대상의 벨 소리 일정 동안 발신자의 통화를 허용하거나 통화를 차단할 수 있습니다.

이동성에 대한 소프트키 템플릿 구성

이 절차를 사용하여 이동성 소프트키를 포함하는 소프트키 템플릿을 구성합니다. 이 템플릿을 사용하는 모든 전화기에 대해 소프트키가 활성화됩니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 만들려면 다음을 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- 새로 추가를 클릭합니다.
 - 기본 템플릿을 선택하고 복사를 클릭합니다.
 - 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - 저장을 클릭합니다.
- 단계 3 기존 템플릿에 이동성 소프트키를 추가합니다.
- 검색 기준을 입력하고 찾기를 클릭합니다.

b) 기존 템플릿을 선택합니다.

단계 4 (선택 사항) 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.

참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.

단계 5 저장을 클릭합니다.

단계 6 관련 링크 드롭다운 목록에서 소프트키 레이아웃 구성을 선택하고 이동을 클릭합니다.

단계 7 구성할 통화 상태 선택 드롭다운 목록에서 소프트키를 추가할 통화 상태를 선택합니다. 일반적으로 온훅및 연결됨 통화 상태 모두에 대해 소프트키를 추가합니다.

단계 8 선택되지 않은 소프트키 목록에서 이동성 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.

단계 9 추가 통화 상태로 소프트키를 표시하려면 이전 단계를 반복합니다.

단계 10 저장을 클릭합니다.

참고 새 소프트키 템플릿을 만든 경우 전화기 구성 창 또는 벌크 관리의 전화기 업데이트 메뉴를 통해 전화기 그룹에 템플릿을 할당할 수 있습니다.

프로비저닝 중에는 전화기에 소프트키 템플릿을 할당하는 몇 가지 방법이 있습니다. 예를 들어, 범용 디바이스 템플릿 구성을 사용하거나 특정 모델에 대한 기본 디바이스 프로파일로 할당할 수 있습니다.

기능 제어 정책 내에서 이동성 활성화

Cisco IP 전화기에 대한 기능을 활성화하거나 비활성화하도록 기능 제어 정책을 구성한 경우에는 Cisco IP 전화기에서 사용하는 정책 내에서 이동성도 활성화해야 합니다. 전화기에서 사용하는 기능 제어 정책 구성 내에서 이 기능을 비활성화하면 해당 정책을 사용하는 모든 Cisco IP 전화기에 대해 이동성 소프트키가 비활성화됩니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 기능 제어 정책.

단계 2 찾기를 클릭하고 해당 정책을 선택합니다.

참고 전화기에 할당하여 다른 관련 기능과 함께 이동성을 활성화하는 새 기능 제어 정책을 만들려는 경우 새로 추가를 선택할 수도 있습니다. 전화기 구성 창 또는 일반 전화 프로파일 구성을 통해 전화기 세트에 정책을 할당할 수 있습니다. 또한 정책을 프로비전할 때 전화기에 할당하도록 정책을 범용 디바이스 템플릿에 할당할 수 있습니다.

- 단계 3 이름 필드에 기능 제어 정책의 이름을 입력합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다. 각 기능 제어 정책 이름은 시스템에서 고유해야 합니다.
- 단계 4 설명 필드에 기능 제어 정책에 대한 간단한 설명을 입력합니다. 이 설명은 최대 50자의 영숫자를 포함하고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.
- 단계 5 기능 제어 영역에서 이동성 소프트키에 해당하는 기본값 무시 확인란과 설정 활성화 확인란을 모두 선택합니다.
- 단계 6 저장을 클릭합니다.

이동성을 위한 IP 전화기 구성

단일 번호 연락 또는 이동성으로 이동을 구성한 경우 이 절차를 사용하여 엔터프라이즈 통화를 원격 대상으로 재전송하도록 이동성 기능을 사용하여 데스크폰을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 다음 작업 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 전화기를 선택하여 설정을 수정합니다.
- 새로 추가를 클릭하고 전화기 유형 드롭다운 목록에서 전화기를 선택하여 새 전화기를 추가합니다.

단계 3 다음을 클릭합니다.

단계 4 소프트키 템플릿 드롭다운 목록에서 구성된 모빌리티 소프트키 템플릿을 선택합니다.

단계 5 소유자 사용자 ID 드롭다운 목록에서 이동성을 활성화한 사용자 계정을 선택합니다.

참고 소유자 사용자 ID 또는 이동성 사용자 ID 필드를 구성할 수 있습니다. 이동성 사용자는 이동성 활성화 디바이스에 대해 구성되고 소유자 사용자는 비 이동성 디바이스에 대해 구성됩니다. 동일한 디바이스에 대해 두 사용자를 구성하는 것은 권장되지 않습니다.

단계 6 (선택 사항) 기능 제어 정책을 사용하여 기능을 활성화하는 경우 드롭다운 목록에서 정책을 선택합니다.

단계 7 저장을 클릭합니다.

원격 대상 프로파일 구성

사용자의 모든 원격 대상 번호에 적용하려는 일반 설정을 구성합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 프로파일 > 원격 대상 프로파일.
 - 단계 2 새로 추가를 클릭합니다.
 - 단계 3 프로파일의 이름을 입력합니다.
 - 단계 4 사용자 ID 드롭다운 목록에서 이 프로파일이 적용되는 최종 사용자를 선택합니다.
 - 단계 5 디바이스폴 드롭다운 목록에서 이 프로파일이 상주해야 하는 디바이스폴을 선택합니다.
 - 단계 6 원격 대상 프로파일 구성 창에서 나머지 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
 - 단계 7 저장을 클릭합니다.
 - 단계 8 연결 정보에서 새 DN 추가를 클릭합니다.
 - 단계 9 디렉터리 번호 필드에 사용자의 데스크폰 디렉터리 번호를 추가합니다.
-

원격 대상 구성

원격 대상은 사용자에게 연락할 수 있는 모바일 디바이스(예: 홈 오피스 전화기, 셀룰러 네트워크의 휴대폰 또는 PSTN 전화기)를 나타내는 가상 디바이스입니다. 원격 대상에서 사용자의 데스크폰과 동일한 설정을 많이 수행합니다.



참고

- 엔터프라이즈 사용자가 원격 대상에서 Cisco Jabber로 통화를 시작하는 경우, Unified Communications Manager은 Cisco TelePresence Video Communication Server(VCS)에 INVITE 메시지를 전송하여 Cisco Jabber를 사용하여 데이터 통화를 설정하려고 시도합니다. 통화는 VCS에서 응답을 수신하는 것과 관계 없이 설정됩니다.
 - 셀프 프로비저닝 기능이 활성화된 경우 최종 사용자는 셀프 서비스 포털에서 자신의 전화기를 프로비저닝할 수 있습니다. 셀프 프로비저닝을 위한 시스템 구성에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#) 및 "셀프 프로비저닝 구성" 장을 참조하고 사용자 프로파일의 일부로 셀프 프로비저닝 활성화에 대한 자세한 내용은 "최종 사용자 프로비저닝" 부분을 참조하십시오.
-

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 원격 대상.
 - 단계 2 새로 추가를 클릭합니다.
 - 단계 3 대상 필드에 원격 대상 번호를 입력합니다. 예를 들어, 이 값은 셀룰러 번호 또는 PSTN 번호일 수 있습니다.
 - 단계 4 이동성 사용자 ID 필드에서 이 원격 대상을 사용하는 이동성 사용 최종 사용자를 선택합니다.

- 단계 5 **Unified Mobility** 활성화 기능 확인란을 선택합니다.
- 단계 6 원격 대상 프로파일 드롭다운 목록에서 이 원격 대상을 소유하는 사용자에게 대해 설정할 프로파일을 선택합니다.
- 단계 7 단일 번호 연락 음성 메일 정책 드롭다운 목록을 사용하여 음성 메일 정책을 구성합니다.
- 단일 번호 연락 활성화 확인란을 선택합니다.
 - 사용자가 데스크폰에서 이동성 소프트웨어를 누를 때 이 원격 대상을 사용 가능한 대상 목록에 포함하려면 휴대폰으로 이동 활성화 확인란을 선택합니다.
- 단계 8 (선택 사항) 이 원격 대상에 대한 엔터프라이즈 통화를 근무 시간과 같은 특정 기간으로 제한하려면 벨소리 일정을 구성합니다.
- 단계 9 위의 벨소리 일정 중에 전화를 받을 때 영역에서 이 원격 대상에 대해 구성된 목록을 적용합니다.
- 단계 10 원격 대상 구성 창에서 나머지 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 11 저장을 클릭합니다.

액세스 목록 구성

액세스 목록은 어떤 원격 대상에서 어떤 시간에 어떤 통화에서 벨소리를 울릴 수 있는지 제어하려는 경우 선택할 수 있는 원격 대상 구성입니다. 액세스 목록은 발신자 ID를 기반으로 발신자를 필터링하고 해당 원격 대상의 벨소리 일정 동안 통화를 허용하거나 통화를 차단할 수 있습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 액세스 목록.
- 단계 2 새로 추가를 클릭하여 액세스 목록을 만듭니다.
- 단계 3 새 액세스 목록을 식별할 이름과 설명을 입력합니다.
- 단계 4 소유자 드롭다운 목록에서 ID를 선택하여 액세스 목록을 사용자와 연결합니다.
- 단계 5 다음 옵션 중 하나를 선택합니다.
- 허용됨 - 액세스 목록에 있는 모든 번호가 허용됩니다.
 - 차단됨 - 액세스 목록에 있는 모든 번호가 차단됩니다.
- 단계 6 저장을 클릭합니다.
- 단계 7 필터 마스크 드롭다운 목록에서 액세스 목록에 적용할 필터를 선택합니다.
- 사용할 수 없음 - 사용할 수 없음 상태를 광고하는 모든 발신자가 액세스 목록에 추가됩니다.
 - 프라이빗 - 프라이빗 상태를 광고하는 모든 발신자가 액세스 목록에 추가됩니다.
 - 디렉터리 번호 — 사용자가 지정하는 모든 디렉터리 번호 또는 디렉터리 문자열이 액세스 목록에 추가됩니다. 이 옵션을 선택하는 경우 **DN** 마스크 필드에 번호 또는 숫자 문자열을 추가합니다.
- 단계 8 저장을 선택합니다.
- 단계 9 원격 대상에 액세스 목록을 적용합니다.

- a) Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 원격 대상 그리고 생성한 원격 대상을 다시 엽니다.
- b) 이 액세스 목록에 대한 벨소리 일정을 구성하고 다음 중 하나를 수행합니다.
 - 허용된 액세스 목록을 만든 경우 발신자가 있는 경우에만 이 대상에 벨소리 올리기 라디오 버튼을 클릭하고 드롭다운 목록에서 만든 액세스 목록을 선택합니다.
 - 차단된 액세스 목록을 만든 경우 발신자가 있는 경우 이 대상에 벨소리 올리지 않기 라디오 버튼을 클릭하고 드롭다운 목록에서 만든 액세스 목록을 선택합니다.
- c) 저장을 클릭합니다.

모바일 음성 액세스 구성

다음 작업을 완료하여 모바일 음성 액세스를 위한 시스템을 구성하면 사용자가 모든 디바이스에서 엔터프라이즈에 앵커된 전화를 걸 수 있습니다. 사용자가 인증을 위해 시스템 IVR로 전화를 걸면 전화가 사무실 전화기에서 전송된 것처럼 최종 사용자에게 표시되는 엔터프라이즈 통화로 전송됩니다.

시작하기 전에

모바일 음성 액세스를 사용하려면:

- 최종 사용자 구성 내에서 모바일 음성 액세스 활성화 옵션을 선택하여 사용자를 모바일 사용자로 활성화해야 합니다. 자세한 내용은 [이동성 사용자 구성, 20 페이지](#)의 내용을 참조하십시오.
- 대화형 음성 응답 서비스는 활성 상태여야 하며 트렁크가 사용하는 미디어 리소스 그룹 목록에 포함되어야 합니다.

프로시저

	명령 또는 동작	목적
단계 1	Cisco Unified 모바일 음성 액세스 서비스 활성화, 29 페이지	Cisco 유니파이드 Serviceability에서 Cisco Unified 모바일 음성 액세스 기능 서비스가 활성화되어 있는지 확인합니다.
단계 2	모바일 음성 액세스 활성화, 30 페이지	모바일 음성 액세스 기능을 활성화하고 사용자가 엔터프라이즈에 연결하기 위해 전화를 걸 수 있는 디렉터리 번호를 지정합니다.
단계 3	모바일 음성 액세스에 대한 디렉터리 번호 구성, 30 페이지	엔터프라이즈 외부에서 전화를 거는 사용자에게 대한 지역화된 프롬프트 집합을 할당하도록 MVA(모바일 음성 액세스)를 구성합니다.
단계 4	Cisco CallManager 서비스 다시 시작, 31 페이지	모바일 음성 액세스를 활성화한 후에는 Cisco CallManager 서비스를 다시 시작합니다.

	명령 또는 동작	목적
단계 5	<p>다음 작업 중 하나를 수행하여 레거시 MVA 또는 엔터프라이즈 기능 접근 (EFA)에 대한 게이트웨이를 구성합니다.</p> <ul style="list-style-type: none"> 원격 액세스를 위한 H.323 또는 SIP 게이트웨이 구성, 31 페이지 원격 액세스를 위한 새로운 H.323 게이트웨이 구성, 33 페이지 	<p>참고</p> <p>게이트웨이 구성은 더 이상 모바일 음성 액세스에 필요하지 않습니다. 이는 선택적 구성으로, ISR G2 라우터를 통해 레거시 모바일 음성 액세스를 구성하려는 경우에만 해당 됩니다.</p> <p>시스템 요구 사항에 따라 새 게이트웨이를 추가하거나 기존 게이트웨이를 구성하여, MVA 또는 EFA를 통해 엔터프라이즈 외부에서 수신되는 통화를 처리할 수 있습니다.</p> <p>시스템에 기존 H.323 또는 SIP PSTN 게이트웨이가 있는 경우 MVA에 대해 이를 구성할 수 있습니다. H.323 또는 SIP VoiceXML(VXML) 게이트웨이가 응답하고 처리하는 시스템 구성의 DID 번호로 전화를 걸어 이 기능에 액세스합니다. 게이트웨이를 구성한 후에 퍼블리셔 노드에서 vxml 스크립트를 사용하여 MVA 사용자에게 재생되는 IVR(대화형 음성 응답) 프롬프트를 가져옵니다. 이러한 프롬프트는 사용자가 전화기 키패드에서 전화를 걸어야 하는 번호의 사용자 인증 및 입력을 요청합니다.</p> <p>기존 H.323 또는 SIP PSTN 게이트웨이가 없고 모바일 음성 액세스를 구성하려는 경우 헤어 피닝 방법을 사용하여 새 H.323 게이트웨이를 추가하고 MVA 기능에 맞게 구성해야 합니다. 기술적인 관점에서 이 방법은 두 번째 게이트웨이를 사용하여 인바운드 통화를 받고, MVA 서비스를 적용하고, 시스템에서 MVA 서비스를 적용한 후에는 인바운드 통화 레그가 PSTN 게이트웨이(원래 소스)로 반환됨을 나타냅니다.</p>

Cisco Unified 모바일 음성 액세스 서비스 활성화

다음 절차를 사용하여 퍼블리셔 노드에서 이 서비스를 활성화합니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. 도구 > 서비스 활성화.

단계 2 서버 드롭다운 목록에서 게시자 노드를 선택합니다.

단계 3 이동을 클릭합니다.

단계 4 CM 서비스에서 **Cisco Unified** 모바일 음성 액세스 서비스 확인란을 선택합니다.

단계 5 저장을 클릭합니다.

모바일 음성 액세스 활성화

서비스 매개 변수를 구성하여 MVA(모바일 음성 액세스)를 활성화하고 사용자가 IVR에 도달하기 위해 사용자가 전화를 걸 수 있는 디렉터리 번호 또는 PSTN의 번호를 지정합니다.

시작하기 전에

모바일 음성 액세스가 작동하려면 Cisco Unified 모바일 음성 액세스 기능 서비스를 활성화해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 퍼블리셔 노드를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 다음 서비스 매개 변수를 구성합니다.

- 모바일 음성 액세스 활성화 - 이 매개 변수를 **True**로 설정합니다.
- 모바일 음성 액세스 번호 - 사용자가 엔터프라이즈에 액세스할 때 사용자가 전화를 걸 번호를 입력합니다.

단계 5 저장을 클릭합니다.

모바일 음성 액세스에 대한 디렉터리 번호 구성

엔터프라이즈 외부에서 전화를 거는 사용자에게 대한 지역화된 프롬프트 집합을 할당하도록 MVA(모바일 음성 액세스)를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.미디어 리소스 > 모바일 음성 액세스.

단계 2 모바일 음성 액세스 디렉터리 번호에서 게이트웨이로부터 모바일 음성 액세스 통화를 수신하는 DN(내부 디렉터리 번호)을 입력합니다.

1-24자리의 값을 입력합니다. 유효한 값은 0-9입니다.

단계 3 지역화 창에서 선택할 로케일을 이 창으로 또는 이 창에서 이동합니다.

참고 모바일 음성 액세스에서는 모바일 음성 액세스 창의 선택한 로캘 창에 표시되는 첫 번째 로캘을 사용합니다. 예를 들어 English United States가 선택한 로캘 창에서 첫 번째로 표시되는 경우 Cisco Unified Mobility 사용자는 통화 중 IVR이 사용될 때 영어를 듣게 됩니다.

단계 4 저장을 클릭합니다.

Cisco CallManager 서비스 다시 시작

모바일 음성 액세스 기능을 활성화한 후에는 Cisco CallManager 서비스를 다시 시작합니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. 도구 > 제어 센터 - 기능 서비스.

단계 2 서버 드롭다운 목록에서 Cisco Unified Communications Manager 퍼블리셔 노드를 선택합니다.

단계 3 CM 서비스에서 **Cisco CallManager** 서비스에 해당하는 라디오 버튼을 선택합니다.

단계 4 재시작을 클릭합니다.

다음에 수행할 작업

이제 기본 모바일 음성 액세스 지원을 사용하여 Unified Communications Manager를 구성하는 데 필요한 모든 작업을 완료했습니다. 그러나, ISR G2 라우터가 IVR 및 음성 프롬프트를 제공하는 레거시 모바일 음성 액세스를 구성하려면 다음 두 가지 옵션 작업 중 하나를 수행할 수 있습니다.

- [원격 액세스를 위한 H.323 또는 SIP 게이트웨이 구성, 31 페이지](#)
- [원격 액세스를 위한 새로운 H.323 게이트웨이 구성, 33 페이지](#)

원격 액세스를 위한 H.323 또는 SIP 게이트웨이 구성

시스템에 기존 H.323 또는 SIP PSTN 게이트웨이가 있는 경우 MVA에 대해 이를 구성할 수 있습니다. H.323 또는 SIP VoiceXML(VXML) 게이트웨이가 응답하고 처리하는 시스템 구성의 DID 번호로 전화를 걸어 이 기능에 액세스합니다. 게이트웨이를 구성한 후에 퍼블리셔 노드에서 vxml 스크립트를 사용하여 MVA 사용자에게 재생되는 IVR(대화형 음성 응답) 프롬프트를 가져옵니다. 이러한 프롬프트는 사용자가 전화기 키패드에서 전화를 걸어야 하는 번호의 사용자 인증 및 입력을 요청합니다.

시작하기 전에

[모바일 음성 액세스에 대한 디렉터리 번호 구성, 30 페이지](#)

프로시저

단계 1 PSTN에서 PRI에 대한 T1/E1 컨트롤러를 구성합니다.

예제:

```
controller T1 1/0
framing esf
linecode b8zs
pri-group timeslots 1-24
```

단계 2 PRI에 대한 직렬 인터페이스를 구성합니다(T1/E1).

예제:

```
interface Serial 1/0:23
ip address none
logging event link-status none
isdn switch-type primary 4ess
isdn incoming-voicevoice
isdn bchan-number-order ascending
no cdp enable
```

단계 3 퍼블리셔 노드에서 VXML 애플리케이션을 로드합니다.

예제:

IOS 버전 12.3(13) 이상에 대한 샘플 구성:

```
application service CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

예제:

IOS 버전 12.3(12) 이전의 샘플 구성:

```
call application voice Unified CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

주의 VXML이 버전 12.2(11)에 추가되었지만 버전 12.3(8), 12.3(9), 12.3(14)T1 및 12.2(15)에는 VXML 문제가 있습니다.

단계 4 Cisco Unified Mobility 애플리케이션을 시스템 원격 액세스에 연결하도록 다이얼 피어를 구성합니다.

예제:

IOS 버전 12.3(13) 이상에 대한 샘플 구성:

```
dial-peer voice 58888 pots
service CCM (Cisco Unified Mobility VXML application)
incoming called-number 58888
```

예제:

IOS 버전 12.3(12) 이전에 대한 샘플 구성:

```
dial-peer voice 100 pots
application CCM (Cisco Unified Mobility VXML application)
incoming called-number 58888
```

(58888은 MVA(모바일 음성 액세스) 번호를 나타냅니다.)

단계 5 다이얼 피어를 추가하여 통화를 MVA DN으로 호 전환합니다.

예제:

주 Unified Communications Manager의 샘플 구성:

```
dial-peer voice 101 voip
preference 1
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.3
codec g711ulaw
dtmf-relay h245-alphanumeric
no vad
```

예제:

보조 Unified Communications Manager의 샘플 구성(필요한 경우):

```
dial-peer voice 102 voip
preference 2
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.4
codec g711ulaw
dtmf-relay h245-alphanumeric
no vad
```

참고 일반 다이얼 피어가 통화를 종료하도록 이미 구성되어 있고 MVA DN과 일치하면 이 단계를 수행할 필요가 없습니다.

예제:

SIP 게이트웨이 VoIP 다이얼 피어에 대한 샘플 구성:

```
dial-peer voice 80 voip
destination-pattern <Mobile Voice Access DN>
rtp payload-type nse 99
session protocol sipv2
session target ipv4:10.194.107.80
incoming called-number .T
dtmf-relay rtp-nte
codec g711ulaw
```

원격 액세스를 위한 새로운 H.323 게이트웨이 구성

기존 H.323 또는 SIP PSTN 게이트웨이가 없고 모바일 음성 액세스를 구성하려는 경우 헤어피닝 방법을 사용하여 새 H.323 게이트웨이를 추가하고 MVA 기능에 맞게 구성해야 합니다. 기술적인 관점에서 이 방법은 두 번째 게이트웨이를 사용하여 인바운드 통화를 받고, MVA 서비스를 적용하고, 시스템에서 MVA 서비스를 적용한 후에는 인바운드 통화 레그가 PSTN 게이트웨이(원래 소스)로 반환됨을 나타냅니다.



참고 헤어피닝 기능과 함께 모바일 음성 액세스를 사용하는 경우 시스템에 전화를 거는 사용자는 발신자 ID로 자동 식별되지 않습니다. 대신에 사용자는 PIN을 입력하기 전에 원격 대상 번호를 수동으로 입력해야 합니다. 그 이유는 PSTN 게이트웨이가 먼저 Unified Communications Manager에 대한 통화를 라우팅해야 헤어피닝 모바일 음성 액세스 게이트웨이에 연결할 수 있기 때문입니다. 이 라우트 경로로 인해 모바일 음성 액세스 게이트웨이가 통화를 처리하기 전에 전화 번호를 모바일 번호에서 엔터프라이즈 디렉터리 번호로 변환합니다. 그 결과 게이트웨이가 구성된 원격 대상과 호출 번호를 일치시킬 수 없으므로 시스템에서 사용자에게 원격 대상 번호를 입력하라는 메시지를 표시합니다.

시작하기 전에

[모바일 음성 액세스에 대한 디렉터리 번호 구성, 30 페이지](#)

프로시저

단계 1 퍼블리셔 노드에서 VXML 애플리케이션을 로드합니다.

예제:

IOS 버전 12.3(13) 이상에 대한 샘플 구성:

```
application service CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

예제:

IOS 버전 12.3(12) 이전의 샘플 구성:

```
call application voice CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

주의 VXML이 버전 12.2(11)에 추가되었지만 버전 12.3(8), 12.3(9), 12.3(14)T1 및 12.2(15)에는 VXML 문제가 있습니다.

단계 2 Cisco Unified Mobility 애플리케이션을 시스템 원격 액세스에 연결하도록 다이얼 피어를 구성합니다.

예제:

IOS 버전 12.3(13) 이상에 대한 샘플 구성:

```
dial-peer voice 1234567 voip
service CCM
incoming called-number 1234567
codec g711u
session target ipv4:<ip_address of call manager>
```

예제:

IOS 버전 12.3(12) 이전에 대한 샘플 구성:

```
dial-peer voice 1234567 voip
application CCM
incoming called-number 1234567
codec g711u
session target ipv4:<ip_address of call manager>
```

단계 3 모바일 음성 액세스(MVA) DN으로 호 전환하기 위한 다이얼 피어를 추가합니다.

예제:

주 Unified Communications Manager의 샘플 구성:

```
dial-peer voice 101 voip
preference 1
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.3
voice-class h323 1
codec g711ulaw
dtmf-relay h245-alphanumeric
novad
```

예제:

보조 Unified Communications Manager의 샘플 구성(필요한 경우):

```
dial-peer voice 102 voip
preference 2
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.4
voice-class h323 1
codec g711ulaw
dtmf-relay h245-alphanumeric
novad
```

참고 일반 다이얼 피어가 통화를 종료하도록 이미 구성되어 있고 MVA DN과 일치하면 이 단계를 수행할 필요가 없습니다.

단계 4 헤어핀을 구성합니다.

```
voice service voip
allow-connections h323 to h323
```

단계 5 Unified Communications Manager에서 수신 MVA 번호를 vxml 스크립트가 로드되어 있는 H.323 게이트웨이로 재전송하기 위한 새 경로 패턴을 생성합니다. 게이트웨이의 수신 CSS에서 새 경로 패턴이 생성되는 파티션에 액세스할 수 있는지 확인합니다.

엔터프라이즈 기능 접근 (EFA) 구성

다음 절차를 사용하여 원격 대상에서 엔터프라이즈 기능 액세스를 구성합니다.

- 2단계 전화걸기를 사용하여 구성된 원격 대상에서 엔터프라이즈 전화를 겁니다. 통화가 연결된 데스크폰에서 가져온 것처럼 착신자에게 표시됩니다.
- 원격 대상에서 전송된 DTMF 숫자를 사용하여 전송되는 EFA 코드를 통해 통화 중 기능에 대한 원격 대상 액세스입니다.



참고 모바일 음성 액세스와 달리, 엔터프라이즈 기능 액세스의 경우에는 구성된 원격 대상에서 통화해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 이동성 > 엔터프라이즈 기능 액세스 구성.

단계 2 번호 필드에 모바일 사용자가 엔터프라이즈 기능 액세스 기능에 액세스하기 위해 원격 대상에서 전화를 걸 수 있는 고유한 DID 번호를 입력합니다.

단계 3 라우트 파티션 드롭다운 목록에서 DID가 있는 파티션을 선택합니다.

단계 4 (선택 사항) 이 EFA 번호를 이 시스템의 기본값으로 설정하려면 기본 엔터프라이즈 기능 액세스 번호 확인란을 선택합니다.

단계 5 저장을 클릭합니다.

단계 6 엔터프라이즈 기능 액세스 서비스 매개 변수를 구성합니다.

- a) Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- b) 서버 드롭다운 목록에서 게시자 노드를 선택합니다.
- c) 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- d) 엔터프라이즈 기능 액세스 활성화 서비스 매개 변수를 **True**로 설정합니다.
- e) (선택 사항) 클러스터 수준 매개 변수(시스템 - 이동성) 영역에서 엔터프라이즈 기능 액세스를 통해 통화 중 기능에 액세스하기 위해 입력해야 하는 DTMF 숫자를 편집합니다. 예를 들어 기본값 *81이 있는 보류에 대한 엔터프라이즈 기능 액세스 코드 서비스 매개 변수를 편집할 수 있습니다. 기본값은 다음과 같습니다.

- 보류: *81
- 단독 보류: *82
- 재개: *83
- 전환: *84
- 전화회의: *85
- 세션 핸드오프: *74
- 선택적 녹음 시작: * 86
- 선택적 녹음 중지: *87
- 힌트 그룹 로그인 - 새 코드 입력
- 힌트 그룹 로그아웃 - 새 코드 입력

- f) 저장을 클릭합니다.

인텔리전트 세션 제어 구성

원격 대상에 대한 인바운드 통화가 사용 가능한 경우 연결된 엔터프라이즈 번호로 재전송되도록 시스템을 구성합니다. 이 기능은 엔터프라이즈 내 이동성 통화에 대한 자동 통화 앵커를 제공하여 비용 절감을 제공하고 통합 커뮤니케이션 기능을 추가합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 Cisco Unified Communications Manager 노드를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 클러스터 수준 매개 변수(기능 - 엔터프라이즈 번호로 원격 대상 통화 재전송)에서 다음 서비스 매개 변수를 설정합니다.

- 엔터프라이즈 번호로 원격 대상 통화 재전송—인텔리전트 세션 제어를 활성화하려면 이 매개 변수를 **True**로 설정합니다.
- 모든 공유 회선 벨울림 - 매개 변수의 값을 **True**로 설정합니다. 인텔리전트 세션 제어가 활성화되고 이 서비스 매개 변수도 활성화된 경우 시스템 앵커가 엔터프라이즈 내의 원격 대상으로 호출되고 사용자의 모든 공유 회선에도 전화벨이 울립니다.
- 엔터프라이즈 DN에서 모두 착신 전환 무시 -이 매개 변수는 지능형 세션 제어가 활성화되어 있을 때 원격 대상에 대한 발신 통화에만 적용됩니다. 기본적으로 이 매개 변수는 **True**로 설정됩니다.

단계 5 저장을 클릭합니다.

모빌리티 서비스 매개 변수 구성

이 절차를 사용하여 선택적 이동성 관련 서비스 매개 변수를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 게시자 노드를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 편집할 서비스 매개 변수를 구성합니다. 이동성 관련 매개 변수는 다음 제목 아래에 나열됩니다. 도움말에 대한 설명을 보려면 매개 변수 이름을 클릭합니다.

- 클러스터 수준 매개 변수(시스템 - 이동성)
- 클러스터 수준 매개 변수(시스템 - 이동성 단일 번호 연락 음성 메일)
- 클러스터 수준 매개 변수(기능 - 엔터프라이즈 번호로 원격 대상 통화 재전송)

단계 5 저장을 클릭합니다.

Cisco Jabber 듀얼 모드 구성

이 작업을 완료하여 iPhone 또는 Android에서 Cisco Jabber를 WiFi를 통해 연결할 수 있는 듀얼 모드 모바일 디바이스로 구성합니다. Cisco Jabber는 WiFi를 통해 Unified Communications Manager에 등록되며, 사용자의 모바일 ID에서 단일 번호 연락을 활성화한 경우 엔터프라이즈 번호를 통해 연결할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	모빌리티 프로파일 구성, 39 페이지	사무실 통화를 통해 전화를 거는 Jabber 모바일 클라이언트에 일관된 발신자 ID를 전송하도록 이동성 프로파일을 구성합니다.
단계 2	Cisco Jabber에 대한 이중 모드 디바이스 추가, 39 페이지	iPhone 또는 Android 클라이언트에서 Cisco Jabber에 대한 이중 모드 디바이스 유형을 구성합니다.
단계 3	모빌리티 ID 구성, 42 페이지	Jabber가 WiFi 범위 밖으로 로밍할 때 통화를 제공할 수 있도록 디바이스 전화 번호(즉, iPhone 번호)를 가리키는 Jabber 모바일 클라이언트에 이동성 ID를 추가합니다. 모바일 ID에 단일 번호 연락 대상을 활성화합니다.
단계 4	필수: 전환 번호 구성, 43 페이지	엔터프라이즈를 종료하는 이중 모드 디바이스에 대한 전환 번호를 구성합니다. 엔터프라이즈 WiFi 네트워크에서 디바이스 연결을 끊으면 원격 모바일 또는 셀룰러 네트워크에 다시 연결하여 해당 통화를 중단 없이 유지할 수 있습니다.

기타 이중 모드 디바이스 구성

셀룰러 네트워크를 통해 전화를 걸 수 있는 기타 듀얼 모드 모바일 디바이스를 구성하기 위해 이러한 작업을 완료하고 WiFi를 통해 연결할 수도 있습니다. 예:

- FMC(Fixed Mobile Convergence) 네트워크를 통해 연결되는 통신업체 통합 모바일 디바이스.
- IP 멀티미디어 네트워크를 통한 IMS 통합 모바일 디바이스

프로시저

	명령 또는 동작	목적
단계 1	Cisco Jabber에 대한 이중 모드 디바이스 추가, 39 페이지	IMS 또는 FMC 이중 모드 디바이스를 구성합니다.
단계 2	모빌리티 ID 구성, 42 페이지	실제 디바이스의 전화 번호를 가리키는 이동성 ID를 추가합니다.
단계 3	필수: 전환 번호 구성, 43 페이지	엔터프라이즈에서 나가는 이중 모드 디바이스에 대한 전환 번호를 구성합니다. 엔터프라이즈 WiFi 네트워크에서 디바이스 연결을 끊으면 원격 모바일 또는 셀룰러 네트워크에 다시 연결하여 해당 통화를 중단 없이 유지할 수 있습니다.

	명령 또는 동작	목적
		시 연결하여 해당 통화를 중단 없이 유지할 수 있습니다.

모빌리티 프로파일 구성

iPhone 및 Android 클라이언트에서 이중 모드 Cisco Jabber에 대한 모빌리티 프로파일을 구성합니다. 프로파일은 사무실 전화기를 통해 전화를 걸 수 있는 일관된 발신자 ID로 클라이언트를 구성합니다.



참고 기술적인 관점에서 이 발신자 ID는 모빌리티 ID 또는 대체 콜백 번호로 통화의 DVO-R(Dial Via Office 리버스콜백) 콜백 부분을 통해 전송됩니다. DVO-R 통화 기능은 Enbloc 전화걸기를 사용합니다. 모빌리티 ID에 할당된 이동성 프로파일이 없거나 콜백 발신자 ID 필드를 공백으로 둘 경우 시스템은 기본 엔터프라이즈 기능 액세스 번호를 전송합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 이동성 > 이동성 프로파일.

단계 2 새로 추가를 클릭합니다.

단계 3 프로파일의 이름을 입력합니다.

단계 4 모바일 클라이언트 통화 옵션 드롭다운 목록에서 Dial Via Office 리버스콜백을 선택합니다.

참고 필드 옵션에도 불구하고 DVO-F(Dial via Office 착신전환)를 사용할 수 없습니다.

단계 5 Dial Via Office 리버스콜백에 대한 콜백 발신자 ID를 구성합니다.

단계 6 모빌리티 프로파일 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 7 저장을 클릭합니다.

Cisco Jabber에 대한 이중 모드 디바이스 추가

다음 절차를 사용하여 iPhone 또는 Android 클라이언트에서 Cisco Jabber에 대한 이중 모드 디바이스 유형을 구성합니다.

시작하기 전에

최종 사용자가 이동성을 지원하는지 확인합니다. 또는, Jabber 클라이언트에 원격 대상을 추가하려는 경우에는 이동성 소프트웨어가 포함된 소프트웨어 템플릿이 있는지 확인하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하여 기존 디바이스를 편집합니다.
- 새로 추가를 클릭하고 **Android**용 **Cisco** 듀얼 모드 또는 **iPhone**용 **Cisco** 듀얼 모드를 전화기 모델로 선택하여 새 디바이스를 추가합니다. 다음을 클릭합니다.

단계 3 전화기 구성 창에서 필드를 구성합니다.

제품별 구성 레이아웃 필드에 대한 자세한 내용은 <http://www.cisco.com/go/jabber>에서 Jabber 클라이언트 설명서를 참조하십시오.

단계 4 다음 필수 필드를 구성합니다.

- 디바이스 이름
- 디바이스 풀
- 소프트키 템플릿
- 소유자 사용자 ID — 사용자가 이동성을 활성화해야 합니다.
- 이동성 사용자 ID - 사용자가 이동성을 활성화해야 합니다.
- 디바이스 보안 프로파일
- SIP 프로파일

단계 5 저장을 클릭합니다.

단계 6 새 디렉터리 번호 추가:

- a) 왼쪽 연결 영역에서 새 **DN** 추가를 클릭합니다.
- b) 디렉터리 번호를 입력하고 저장을 클릭합니다.
- c) 디렉터리 번호 구성 창에서 원하는 필드를 완성하고 저장을 클릭합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- d) 최종 사용자 연결을 클릭합니다.
- e) 찾기를 클릭하고 이 DN을 소유하는 이동성 사용 최종 사용자를 선택합니다.
- f) 선택한 항목 추가를 클릭합니다.
- g) 저장을 클릭합니다.

다음에 수행할 작업

iPhone 또는 Android 디바이스의 전화 번호를 가리키는 모빌리티 ID를 추가합니다. 이렇게 하면 Wi-Fi 범위 밖으로 이동하는 경우 통화를 전화기로 호 전환할 수 있습니다. 디바이스를 단일 번호 연락 대상으로 추가할 수도 있습니다. 자세한 내용은 [모빌리티 ID 구성, 42 페이지](#)의 내용을 참조하십시오.

선택적으로, 원격 대상 및 단일 번호를 Cisco Jabber 클라이언트에 추가합니다. 누군가가 Jabber 클라이언트에 전화를 걸 때 원격 대상에서도 벨소리가 울립니다. [원격 대상 구성, 26 페이지](#).

이중 모드 디바이스 구성 필드

표 2: 이중 모드 디바이스 구성 필드

필드	설명
소프트키 템플릿	이동성 소프트키 템플릿을 선택합니다.
소유자 사용자 ID	할당된 전화기 사용자의 사용자 ID를 선택합니다. 이 디바이스에서 발신한 모든 통화의 사용자 ID가 CDR(통화 세부 정보 레코드)에 기록됩니다.
이동성 사용자 ID	이 듀얼 모드 전화기가 할당된 사람의 사용자 ID를 선택합니다.
디바이스 보안 프로파일	디바이스에 적용할 보안 프로파일을 선택합니다. 보안 프로파일을 Cisco 통합 커뮤니케이션 매니저 관리에 구성된 모든 전화기에 적용해야 합니다. 전화기에 보안 기능을 사용하려면 디바이스 유형 및 프로토콜에 대한 새 보안 프로파일을 구성하여 전화기에 적용해야 합니다.
채라우팅 발신 검색 공간	구성된 원격 대상 및 이 디바이스에 대해 구성된 이동성 ID로 통화를 라우팅하는 발신 검색 공간을 선택합니다.
SIP 프로파일	모바일 디바이스에 대한 표준 SIP 프로파일을 선택합니다.

기타 이중 모드 디바이스 추가

이 절차를 사용하여 다른 이중 모드 디바이스(예: 네트워크 기반 **FMC**용 통신업체 통합 모바일 디바이스 또는 **IMS** 통합 모바일 디바이스)를 추가합니다.

시작하기 전에

최종 사용자가 이동성을 지원하는지 확인합니다. 사용자에게 이동성을 활성화하는 방법에 대한 자세한 내용은 이 장의 앞부분에 있는 항목을 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 전화기

단계 2 새로 추가를 클릭합니다.

단계 3 전화기 모델 드롭다운 목록 통신업체-통합 모바일 디바이스 또는 **IMS** 통합 모바일 디바이스에서

단계 4 다음 필수 필드를 구성합니다.

- 디바이스 이름
- 디바이스 풀
- 소유자 사용자 ID — 사용자가 이동성을 활성화해야 합니다.
- 이동성 사용자 ID - 사용자가 이동성을 활성화해야 합니다.

단계 5 전화기 구성 창에서 나머지 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

단계 7 새 디렉터리 번호 추가:

- a) 왼쪽 연결 영역에서 새 **DN** 추가를 클릭합니다.
- b) 디렉터리 번호를 입력하고 저장을 클릭합니다.
- c) 디렉터리 번호 구성 창에서 원하는 필드를 완성하고 저장을 클릭합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- d) 최종 사용자 연결을 클릭합니다.
- e) 찾기를 클릭하고 이 DN을 소유하는 이동성 사용 최종 사용자를 선택합니다.
- f) 선택한 항목 추가를 클릭합니다.
- g) 저장을 클릭합니다.

모빌리티 ID 구성

엔터프라이즈 번호를 통해 연락할 수 있는 단일 번호 연락으로 디바이스를 활성화하려는 경우 디바이스의 전화 번호를 가리키는 모빌리티 ID를 추가합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 필요한 경우 검색 기준을 입력하고 찾기를 클릭한 다음 생성한 이중 모드 디바이스를 선택합니다.

단계 3 새 모빌리티 ID 추가를 클릭합니다.

단계 4 대상 필드에 모바일 디바이스의 전화 번호를 입력합니다. 예를 들어 iPhone 클라이언트의 Cisco Jabber의 경우 이것은 iPhone의 전화 번호입니다.

단계 5 Cisco Jabber만 해당. 구성된 이동성 프로파일을 선택합니다.

단계 6 이 모바일 ID를 엔터프라이즈 전화 번호에서 사용할 수 있게 하려면 다음을 수행합니다.

- a) 단일 번호 연락 활성화 확인란을 선택합니다.
- b) 단일 번호 연락(SNR) 보이스메일 정책을 구성합니다.

단계 7 DVO-R(Dial-via-Office Reverse) 보이스메일 정책을 구성합니다.

단계 8 모빌리티 ID 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 9 저장을 클릭합니다.

참고 벨소리 일정 및 액세스 목록을 적용하여 이 모바일 ID에 대한 통화를 특정 시간 및 사용자로 제한하려면 **액세스 목록 구성, 27 페이지**.

전환 번호 구성

사용자가 엔터프라이즈 밖으로 이동하는 동안 시스템에서 통화를 유지하도록 하려면 듀얼 모드 전화기에 대한 전환 이동성을 구성합니다. 사용자의 디바이스가 엔터프라이즈 WiFi 네트워크에서 연결을 끊고 모바일 음성 또는 셀룰러 네트워크에 다시 연결하는 경우에도 진행 중인 통화는 중단 없이 유지됩니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 이동성 > 전환 구성

단계 2 전환 번호 필드에 Wi-Fi와 모바일 음성 또는 셀룰러 네트워크 사이의 전환을 위한 직접 내부 다이얼링(DID) 번호를 입력합니다.

국제 이스케이프 문자+로 시작하는 번호의 경우+앞에 백슬래시(\)를 입력해야 합니다. 예:\+15551234.

단계 3 라우트 파티션 드롭다운 목록에서 전환 DID 번호가 속한 파티션을 선택합니다.

단계 4 저장을 클릭합니다.

Cisco Unified Mobility 통화 흐름

이 섹션에서는 일반적으로 SNR(단일 번호 연락)로 알려진 Cisco Unified Mobility의 수신 및 발신 통화 흐름에 대해 설명합니다. Unified Communications Manager는 사용자가 데스크폰에서 모바일 디바이스로 통화를 확장하는 것을 허용하도록 설정된 경우 별도의 발신자 번호 및 청구 번호 기능을 지원합니다.

예를 들어, 사용자 A가 PSTN 네트워크에서 디렉터리 번호가 SNR로 구성된 사용자-B로 전화를 겁니다. SIP 프로파일에서 외부 표시 이름 및 번호 활성화 확인란이 선택되고 외부 표시 이름 및 번호 표시 서비스 매개 변수 값이 *True*로 설정된 경우 Unified Communications Manager는 사용자-B의 데스크폰과 구성된 원격 대상 디바이스 모두에 FROM 헤더 정보를 표시합니다. 동일한 방식으로, 하나의 옵션이 비활성화 된 경우 Unified Communications Manager에는 착신 디바이스에서 P-Asserted-Identity(PAID) 헤더 정보를 표시합니다.

마찬가지로, 발신 통화 시나리오 사용자 B(SNRD 회선)에서 디렉터리 번호 구성 페이지의 외부 표시 정보를 사용하여 구성되는 경우 SIP 트렁크를 통해 PSTN 네트워크에 대한 통화를 시작합니다. 외부 표시 이름 및 번호 활성화가 SIP 프로파일에 구성되어 있으면 Unified Communications Manager는 발신 SIP 메시지의 FROM 헤더에 있는 외부 표시 정보를 전송하여 착신 디바이스에 표시할 수 있습니다.

외부 표시 이름 및 번호 활성화 확인란을 비활성화하지 않은 경우 Unified Communications Manager는 FROM 및 PAID의 디렉터리 번호 정보를 보내 X-Cisco-Presentation 헤더의 착신 디바이스와 구성된 외부 표시 정보를 표시합니다.

익명 외부 표시 확인란을 선택하면 구성된 외부 표시 이름과 외부 표시 번호가 해당 필드 및 착신 디바이스에 익명으로 표시된 외부 표시에서 제거됩니다.

외부 표시 정보 구성에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 디렉터리 번호 구성을 참조하십시오.

스마트 클라이언트가 없는 SIP 트렁크를 통한 FMC

Unified Communications Manager에서는 서비스 공급자가 모바일의 스마트 클라이언트 없이도 엔터프라이즈 전화걸기, SNR, 단일 VM, 통화 이동 및 통화 중 기능 등 PBX 내선 기반 기능을 제공할 수 있습니다. SNR, 사무실 전화 받기, 휴대폰으로 통화 보내기, 모바일 음성 액세스 및 통화 중 DTMF 기능 같은 기본 모바일 기능이 지원됩니다. 내선 전화걸기가 네트워크에 구현되어 있거나 네트워크가 Unified Communications Manager에 통합되어 있는 경우 내선 전화걸기가 지원됩니다. 이러한 기능은 모든 유형의 트렁크에서 제공될 수 있습니다.

Unified Communications Manager의 모든 공유 회선 벨올림(Ring All Shared Lines) 서비스 매개 변수를 구성하여 모바일 DN으로 전화를 걸 때 공유 회선에서 전화벨이 울리도록 할 수 있습니다.



참고 모든 공유 회선에 벨올림을 적용하려면 [원격 대상 통화를 엔터프라이즈 번호로 재전송] 기능을 활성화해야 합니다. [원격 대상 통화를 엔터프라이즈 번호로 재전송]은 기본적으로 비활성화되어 있습니다.

IMS 공유 회선에서는 모든 공유 회선 벨올림(Ring All Shared Lines) 매개 변수 값에 따라서만 벨이 울립니다.

또한 이전 버전에 사용된 원격 대상 기능에서 이 새로운 디바이스 유형으로 마이그레이션할 수도 있습니다.

통신 사업자 통합 모바일 디바이스에 대한 헌트 그룹 로그인 및 로그아웃

디바이스 유형인 통신사업자 통합 모바일을 구성할 때는 소유자 사용자 ID 값을 모바일 사용자 ID로 설정합니다. 모바일 사용자 ID는 구성 페이지에 표시되지 않습니다. 이동성이 활성화된 사용자만 최종 사용자 페이지의 소유자 사용자 ID 드롭다운에 나타납니다. 사용자는 모바일 ID를 FMC와 연결해야 합니다. 이러한 연결을 디바이스를 추가한 후 [FMC 디바이스 구성] 페이지에서 수행할 수 있습니다. 모바일 ID 번호로 통화를 확장하려면 사용자가 모바일 ID 창에서 Cisco Unified Mobility를 활성화해야 합니다.

엔터프라이즈 기능 액세스 코드를 통해 헌트 그룹 로그인 및 로그아웃을 지원하도록 통신업체 통합 모바일 디바이스를 구성할 수 있습니다. 다음을 구성했는지 확인합니다.

- 엔터프라이즈 기능 액세스는 통화 라우팅 > 이동성 > 엔터프라이즈 기능 액세스 번호 구성에서 구성해야 합니다.
- 서비스 매개 변수의 헌트 그룹 로그인에 대한 엔터프라이즈 기능 액세스 번호 및 헌트 그룹 로그아웃에 대한 엔터프라이즈 기능 액세스 번호 값을 할당해야 합니다.

이러한 값을 구성한 후에는 구성된 엔터프라이즈 기능 액세스 번호에 전화를 걸어 통신사업자 통합 모바일 디바이스의 헌트 그룹에 로그인하거나 로그아웃할 수 있습니다. 사용자가 지정된 헌트 로그인 액세스 코드 번호로 전화를 걸면, 통신사업자 통합 모바일 디바이스를 사용하여 헌트 그룹 목록의 일부가 될 수 있습니다. 헌트 로그아웃 액세스 코드에 전화를 걸 경우 사용자는 헌트 그룹 목록 밖으로 이동되고 통화에 연결되지 않습니다.



참고 통신사업자 통합 모바일 디바이스를 사용하는 사용자는 엔터프라이즈 기능 액세스 코드를 통해 통화 중 기능을 호출할 수 있습니다. 엔터프라이즈 기능 액세스를 구성하고 사용하는 방법에 대한 자세한 내용은 [엔터프라이즈 기능 접근 \(EFA\) 구성](#) 섹션을 참조하십시오.

Cisco Unified Mobility 상호 작용

표 3: Cisco Unified Mobility 상호 작용

기능	상호 작용
자동 통화 당겨받기	<p>Cisco Unified Mobility는 서비스 매개 변수를 구성한 방법에 따라 자동 통화 당겨받기와 상호 작용합니다. 자동 통화 당겨받기 활성화 서비스 매개 변수가 True로 설정된 경우 사용자는 통화를 당겨받을 때 당겨받기 소프트웨어를 눌러야 합니다.</p> <p>이 서비스 매개 변수가 False로 설정된 경우 사용자는 당겨받기, 그룹당겨받기 또는 기타픽업 소프트웨어를 누른 다음 전화받기 소프트웨어를 눌러야 합니다.</p>
AAR(Automatic Alternate Routing)	<p>Cisco Unified Mobility는 이제 다음과 같이 AAR(Automatic Alternate Routing)을 지원합니다.</p> <ul style="list-style-type: none"> • 위치 기반 서비스에 대한 대역폭 부족으로 인해 거부가 발생하는 경우 거부는 AAR을 트리거하고 PSTN을 통해 통화를 재전송하므로 발신자가 전화를 끊고 재다이얼할 필요가 없습니다. • 거부는 RSVP(리소스 예약 프로토콜)로 인해 발생하지만 원격 대상 통화에 대해 AAR이 트리거되지 않고 통화가 중지됩니다.
확장 및 연결	<p>Cisco Unified Mobility와 확장 및 연결 기능이 모두 필요한 사용자는, 두 디바이스 유형의 소유자 ID가 동일한 경우, 원격 디바이스 프로파일 및 CTI 원격 디바이스 유형에서 동일한 원격 대상을 구성할 수 있습니다. 이렇게 구성하면 Cisco Unified Mobility 기능을 확장 및 연결과 동시에 사용할 수 있습니다.</p> <p>자세한 내용은 “확장 및 연결” 장을 참조하십시오.</p>

기능	상호 작용
외부 전화 제어	<p>외부 전화 제어가 구성된 경우 Unified Communications Manager는 다음 Cisco Unified Mobility 기능을 위해 보조 라우트 서버의 라우트 결정을 따릅니다.</p> <ul style="list-style-type: none"> • Cisco Unified Mobility • 모바일 음성 액세스 • 엔터프라이즈 기능 액세스 • DVO(Dial Via Office) <p>Unified Communications Manager에서는 다음 Cisco Unified Mobility 기능에 대한 라우팅 쿼리를 전송하지 않습니다.</p> <ul style="list-style-type: none"> • 휴대폰 당겨받기 • 사무실 전화 당겨받기 • 세션 전환
인텔리전트 세션 제어 및 세션 전환	<p>엔터프라이즈 번호로 앵커링되는 원격 대상 직접 통화의 경우, 모바일 사용자는 세션 전환 기능을 사용하여 통화를 데스크폰으로 전환할 수 있습니다.</p> <p>인텔리전트 세션 제어를 구현하기 전에 Cisco Unified Mobility를 활성화해야 합니다.</p>
라이선싱	Cisco Unified Mobility는 Basic부터 Professional까지 모든 사용자 기반 라이선스에 포함됩니다.
로컬 경로 그룹	<p>원격 대상에 대한 단일 번호 연결(SNR) 통화의 경우 시작한 발신자의 디바이스폴에 따라 표준 로컬 라우트 그룹 선택이 결정됩니다.</p> <p>참고 빌트-인 브리지(BIB)를 사용하는 AgentGreeting이 호출되는 경우 로컬 라우트 그룹이 지원되지 않습니다.</p>

기능	상호 작용
지원되는 통화 수	<p>각 원격 대상은 최대 2개의 활성 통화를 지원합니다. 그러나 지원 되는 통화 수는 Unified Communications Manager configuration 구성에 따라 달라집니다.</p> <p>예를 들어 사용자가 원격 대상에 대한 6개의 통화가 이미 있거나 사용자가 DTMF를 사용하여 원격 대상에서 통화를 호 전환하거나 전화회의를 하는 동안 Cisco Unified Mobility 사용자는 통화를 수신합니다.</p> <p>수신된 통화는 다음과 같은 경우 엔터프라이즈 음성 메일로 전송됩니다.</p> <ul style="list-style-type: none"> • 사용자와의 통화 수가 통화 중 트리거 구성을 초과하는 경우 • CFB가 구성된 경우 • 모든 공유 회선이 통화 중인 경우 <p>참고 엔터프라이즈 음성 메일로 전송되는 통화는 지원되는 최대 통화를 기반으로 하지 않습니다.</p>
Cisco Unified Border Element 사용 SIP 트렁크	Cisco Unified Mobility는 CUBE(Cisco Unified Border Element) 사용 SIP 트렁크를 통한 통화 중 기능을 제외하고 Cisco Unified Mobility 기능을 지원합니다.

Cisco Unified Mobility 제한 사항

표 4: Cisco Unified Mobility 상호 작용

제한 사항	설명
자동 응답	<p>자동 응답을 활성화하면 원격 대상 통화가 작동하지 않습니다.</p> <p>참고 듀얼 모드 전화기에서는 자동 응답이 지원되지 않습니다.</p>
등록되지 않은 착신 전환	<p>iPhone 및 Android에서 Cisco Jabber에 대한 CFUR(등록되지 않은 착신 전환) 지원은 다음과 같습니다.</p> <ul style="list-style-type: none"> • iPhone 또는 Android의 Cisco Jabber에 모바일 ID 또는 원격 대상이 구성되어 있지 않은 경우 CFUR이 지원됩니다. • 원격 대상이 구성된 경우 CFUR이 지원되지 않으며 작동하지 않습니다. • 모바일 ID가 휴대폰 번호를 사용하여 구성되고 단일 번호 연락이 활성화된 경우 CFUR이 지원되지 않으며 작동하지 않습니다. <p>모바일 ID 또는 원격 대상이 구성된 경우 대신 통화 중 착신 전환 및 무응답 번호 착신 전환을 사용합니다.</p>

제한 사항	설명
통화 대기시키기	Unified Communications Manager는 Cisco Unified Mobility를 사용한 통화 대기를 지원하지 않습니다.
전화회의	<p>사용자는 모바일 음성 액세스를 사용하여 미팅시작 전화회의를 전화회의 컨트롤러로 시작할 수 없지만 미팅시작 전화회의에 참가할 수는 있습니다.</p> <p>기존의 전화회의 통화가 공유 회선 IP 전화기나 듀얼 모드 전화기 또는 원격 대상에 해당하는 스마트폰에서 시작되는 경우, 통화가 휴대폰으로 전송되거나 듀얼 모드 핸드오프 동작이 발생하고 난 후에는 새로운 전화회의 상대를 기존의 전화회의에 추가할 수 없습니다.</p> <p>새로운 전화회의 상대를 추가하도록 허용하려면 고급 애드-혹 컨퍼런스 사용(Advanced Ad Hoc Conference Enabled) 서비스 매개 변수를 사용하십시오.</p>
휴대폰에서 + 문자 다이얼	<p>휴대폰에서 DTMF(복합 주파수 부호)를 통해 + 기호를 다이얼하여 국제 이스케이프 문자를 지정할 수 있습니다.</p> <p>Cisco Unified Mobility는 IVR로 휴대폰에서, 디렉터리 번호에 + 문자가 포함되어 있는 기업 IP 전화기로 발신 전화를 걸기 위한 DTMF를 통한 + 다이얼링을 지원하지 않습니다.</p> <p>Cisco Unified Mobility는 2단계 다이얼링으로 휴대폰에서, 디렉터리 번호에 + 문자가 포함되어 있는 기업 IP 전화기로 발신 전화를 걸기 위한 DTMF를 통한 + 다이얼링을 지원하지 않습니다.</p>
데스크폰의 방해 사절 및 원격 대상으로의 직접 통화	<p>데스크폰에서 DND(방해사절)가 활성화되어 있으면 사무실 전화기가 원격 사용 중 상태로 전환될 수 없으므로 다음 시나리오에서는 통화가 앵커링되지 않습니다.</p> <ul style="list-style-type: none"> • DND가 통화 거부 옵션으로 활성화된 경우 • 사무실 전화기에서 DND 소프트웨어를 눌러 DND가 활성화된 경우 <p>DND가 벨소리 꺼짐 옵션으로 활성화된 경우에도 통화는 앵커링되지 않습니다.</p>

제한 사항	설명
듀얼 모드 전화기	<p>듀얼 모드 핸드오프 및 발신자 ID</p> <p>듀얼 모드 전환의 전환 DN 방법에는 셀룰러 네트워크에서 발신자 ID가 필요합니다. 이동성 소프트웨어 방법에는 발신자 ID가 필요하지 않습니다.</p> <p>듀얼 모드 전화기 및 CTI 애플리케이션</p> <p>듀얼 모드 전화기가 Wi-Fi 엔터프라이즈 모드에 있는 경우 CTI 애플리케이션에서 그러한 전화기를 제어할 수 없으며 모니터링할 수도 없습니다.</p> <p>듀얼 모드 전화기가 WLAN 범위를 벗어나는 경우 WLAN으로 공유 회선으로 통화 중인 듀얼 모드 전화기에 대한 원격 사용 중 표시기는 사라집니다.</p> <p>듀얼 모드 전화기 및 SIP 등록 기간</p> <p>듀얼 모드 전화기에서 Unified Communications Manager는 SIP Station 킵 얼라이브 간격 서비스 매개 변수에 지정된 값이 아니라, 전화기와 연결된 SIP 프로파일의 등록 만료 타이머(초) 필드 값을 사용하여 등록 기간을 결정합니다. 모바일 디바이스에 대한 표준 SIP 프로파일은 해당 프로파일의 등록 만료 시간 필드에 정의된 등록 기간을 결정합니다.</p>
셀룰러 네트워크의 엔터프라이즈 기능	<p>셀룰러 네트워크의 엔터프라이즈 기능을 사용하려면 대역 외 DTMF가 필요합니다.</p> <p>SIP 트렁크(클러스터 간 트렁크 또는 게이트웨이)를 통해 IP 전화기의 원격 대상으로 클러스터 간 DN을 사용하는 경우 IP 전화기를 구성할 때 DTMF 수신 필요 확인란을 선택하십시오. 이렇게 하면 대역 외에서 DTMF 숫자를 받을 수 있는데, 이는 엔터프라이즈 기능 액세스 통화 중 기능에서 매우 중요합니다.</p>
게이트웨이 및 포트	<p>모바일 음성 액세스에는 H.323 및 SIP VoIP 게이트웨이가 모두 지원됩니다.</p> <p>T1 CAS, FXO, FXS 및 BRI에는 Cisco Unified Mobility 기능이 지원되지 않습니다.</p> <p>SNR(단일 번호 연락)은 MGCP(미디어 게이트웨이 제어 프로토콜)에서 지원되지 않습니다.</p>
Jabber 디바이스	<p>처음 구성하는 경우 Jabber 디바이스는 등록된 디바이스로 계산됩니다. 이러한 디바이스는 최대 등록된 디바이스 수 서비스 매개 변수에 의해 설정된, 노드에 등록된 디바이스 수를 증가시킵니다.</p>

제한 사항	설명
지역	<p>Cisco Unified Mobility 최대 9개의 로캘을 지원합니다. 9개가 넘는 로캘이 설치된 경우 이들 로캘이 사용 가능한 로캘 창에 나타나지만 선택한 로캘 창에는 로캘을 9개까지만 저장할 수 있습니다.</p> <p>Cisco Unified Mobility에서 로캘을 10개 이상 구성하려고 하면 다음 메시지가 나타납니다. “업데이트에 실패했습니다. 제약 조건 (informix.cc_ivruserlocale_orderindex)이 실패했는지 확인하십시오.”</p>
데스크톱 통화 당겨받기의 최대 대기 시간	<p>사용자가 원격 대상(스마트폰 또는 다른 전화기)에서 *81 DTMF 코드를 눌러 전화를 보류하는 경우 사용자 사무실 전화기에는 보류해제 소프트키가 표시되지 않습니다. 그러나 사무실 전화기는 데스크톱 통화 당겨받기에 타이머를 적용하지 않습니다. 통화를 당겨받는 최종 사용자에게 대해 구성된 제한 시간이 경과한 후에도 보류해제 키는 계속 표시되며 통화가 끊기지 않습니다.</p> <p>대신, 사용자가 원격 전화기의 전화를 끊어야 합니다. 그러면 사무실 전화기에서 데스크톱 통화 당겨받기에 대한 타이머가 적용되게 됩니다. (이 설정을 변경하려면 최종 사용자 구성 창의 통화 당겨받기의 최대 대기 시간 필드를 사용합니다.)</p>
MLPP(Multilevel Precedence and Preemption)	Cisco Unified Mobility은 MLPP(Multilevel Precedence and Preemption)와 함께 작동하지 않습니다. 통화가 MLPP에서 선점되는 경우 그 통화에 대해 Cisco Unified Mobility 기능은 비활성화됩니다.
중복 송신	인텔리전트 세션 제어 기능에는 중복 송신 패턴이 지원되지 않습니다.
Q 신호 처리	이동성은 QSIG(Q 신호 처리)를 지원하지 않습니다.
QSIG 경로 대체	QSIG 경로 대체는 지원되지 않습니다.
서비스 매개 변수	엔터프라이즈 기능 액세스 서비스 매개 변수는 표준 전화기 및 스마트폰에 적용됩니다. 그러나 스마트폰은 일반적으로 원터치 키를 사용하여 해당 코드를 보냅니다. 사용자는 Cisco Unified Mobility와 함께 사용할 스마트폰을 모두, 엔터프라이즈 기능 액세스를 위한 기본 코드 또는 스마트폰 설명서에 지정된 코드를 사용하도록 구성해야 합니다.
세션 전환	<p>세션 전환 기능에 적용되는 제한 사항은 다음과 같습니다.</p> <ul style="list-style-type: none"> 휴대폰에서 데스크폰에 대한 세션 전환만 이루어질 수 있습니다. 데스크폰에서 휴대폰으로의 세션 전환을 사용하려면 현재 원격 대상 당겨받기 방법에서 휴대폰으로 통화 보내기를 사용하도록 지정합니다. 음성 통화 세션 전환만 지원됩니다.

제한 사항	설명
SNR(단일 번호 연락)과 헌트 그룹	헌트 그룹이 구성되어 있고 헌트 그룹이 가리키는 하나 이상의 디렉터리 번호에 SNR(단일 번호 도달)이 또한 활성화되어 있는 경우, 헌트 그룹의 모든 디바이스가 로그인되어 있지 않으면 통화는 SNR 원격 대상으로 확장되지 않습니다. 헌트 그룹 내의 각 디바이스의 경우, 해당 디바이스에 대한 전화기 설정 창에서 헌트 그룹에 로그인됨 확인란에 체크 표시가 되어 있어야만 합니다.
SIP 트렁크	Cisco Unified Mobility 기능은 PRI(Primary Rate Interface)의 PSTN(Public Switched Telephone Network) 연결에만 지원됩니다. SIP 트렁크의 경우 Cisco Unified Mobility는 IOS 게이트웨이 또는 클러스터 간 트렁크를 통해 지원됩니다.
SIP URI 및 원격 대상으로 의 직접 통화	인텔리전트 세션 제어 기능은 직접 URI 전화걸기를 지원하지 않습니다. 따라서 SIP URI로 걸린 통화는 엔터프라이즈 번호로 앵커링될 수 없습니다.
Unified Communications Manager 게시자 종속 기 능	클러스터 환경에서는 단일 번호 연락을 활성화 또는 비활성화하기 위해 게시자에 연결할 수 있어야 합니다. 게시자가 현재 실행되고 있지 않으면 일부 기능이 작동하지 않을 수 있습니다. 모바일 음성 액세스는 퍼블리셔 노드에 연결할 수 없는 경우에는 사용할 수 없습니다. 모바일 음성 액세스에 대한 IVR 프롬프트는 게시자에만 저장됩니다.
영상 통화	Cisco Unified Mobility 서비스는 영상 통화로 확장되지 않습니다. 사무실 전화기로 수신된 영상 통화는 휴대폰에서 당겨받을 수 없습니다.
모바일 음성 액세스 (MVA)	Cisco 4000 Series Integrated Services Routers는 Voice XML(VXML)을 지원하지 않습니다. 따라서 이러한 라우터가 Cisco Unified Communications Manager를 사용하여 통합 커뮤니케이션 게이트웨이로 작동하는 경우에는 MVA(Mobile Voice Access) 애플리케이션을 지원하지 않습니다.

관련 항목

[애드-혹 컨퍼런스 서비스 매개 변수](#), 246 페이지

Cisco Unified Mobility 문제 해결

데스크톱 전화기에서 통화를 재개할 수 없음

문제 원격 대상(휴대폰)이 스마트폰이고 이 휴대폰에 대한 통화가 Cisco Unified Communications Manager를 통해 앵커링되면 사용자는 휴대폰을 끊고 사용자 데스크톱 전화기에서 다시 시작 소프트웨어를 표시하여 통화를 재개할 수 있습니다. 사용자는 사용자 데스크톱 전화기에서 이 통화를 재개할 수 없습니다.

가능한 원인 휴대폰에서 전화를 끊을 때 발신자가 통화 중, 다시 걸기 또는 연결 끊기 신호음을 수신하는 경우, 휴대폰 공급자가 미디어를 연결 해제하지 않았을 수 있습니다. 공급자로부터 연결 끊기 신호를 수신하지 못했습니다. 이 가능성을 확인하려면 발신자가 45초 동안 대기하도록 합니다. 이 대기 시간이 지나면 서비스 공급자가 시간 초과하여 연결 끊김 신호를 전송하고, 이때 Cisco Unified Communications Manager가 통화를 재개하는 재개 소프트웨어를 제공할 수 있습니다.

- 게이트웨이에 다음 명령을 추가합니다.

```
voice call disc-pi-off
```

- Cisco CallManager 서비스의 경우 활성 통화를 위해 **PI**로 연결 끊김 시 미디어 유지 매개 변수를 **False**로 설정합니다.



5 장

디바이스 모빌리티

- 디바이스 모빌리티 개요, 53 페이지
- 디바이스 모빌리티 사전 요건, 57 페이지
- 디바이스 모빌리티 설정 작업 흐름, 58 페이지
- 디바이스 모빌리티 상호 작용, 62 페이지
- 디바이스 모빌리티 제한 사항, 63 페이지

디바이스 모빌리티 개요

디바이스 모빌리티를 사용하면 모바일 사용자가 사이트 간에 로밍하면서 로컬 사이트의 사이트별 설정을 사용할 수 있습니다. 이 기능이 구성되면 Cisco Unified Communications Manager는 로밍 디바이스의 IP 주소를 디바이스 모빌리티 구성의 IP 서브넷에 일치시켜 적절한 디바이스폴을 할당할 수 있도록 디바이스의 실제 위치를 확인합니다. 이 동적으로 할당된 디바이스폴의 설정은 해당 디바이스에 대한 전화기 구성의 설정을 무시하고, 새 전화기 위치에 대한 음성 품질과 리소스 할당이 적절한지 확인합니다.

로밍 모바일 디바이스의 경우 이 기능을 사용하면 네트워크 리소스를 더 효율적으로 사용할 수 있습니다.

- 휴대폰 사용자가 다른 위치로 이동할 경우 CAC(통화 허용 제어)는 해당 위치에 적절한 대역폭이 할당된 비디오 및 오디오 품질을 보장할 수 있습니다.
- 모바일 사용자가 PSTN 통화를 걸 경우 전화기는 로컬 게이트웨이로 라우팅됩니다. 그렇지 않으면, PSTN 통화가 먼저 IP WAN 연결을 통해 홈 사이트로 다시 라우팅된 다음 홈 사이트의 PSTN 게이트웨이로 라우팅됩니다.
- 모바일 사용자가 홈 위치로 발신할 경우 Cisco Unified Communications Manager가 해당 지역에 적절한 코덱을 할당할 수 있습니다.

사이트별 설정

로밍 디바이스의 경우 Cisco Unified Communications Manager는 디바이스 구성의 다음 디바이스폴 매개 변수를 동적으로 할당된 디바이스 폴의 값으로 덮어씁니다.

- 날짜/시간 그룹

- 지역
- 위치
- 네트워크 로깅
- SRST 참조
- 연결 모니터 지속 시간
- 물리적 위치
- 디바이스 모빌리티 그룹
- 미디어 자원 그룹 목록

네트워크의 지오로케이션이 미국 밖까지 연결되는 경우 디바이스 모빌리티 그룹을 구성하여 전화기 사용자가 로밍 위치와 상관없이 구성된 다이얼 플랜을 사용할 수 있도록 할 수 있습니다. 디바이스가 로밍하면서 동일한 디바이스 모빌리티 그룹에 있는 경우에도 Cisco Unified Communications Manager가 다음 디바이스폴 매개 변수를 덮어씁니다.

- AAR 그룹
- AAR 발신 검색 공간
- 디바이스 발신 검색 공간

전화기가 홈 위치로 돌아오면 시스템이 로밍 디바이스폴의 연결을 해제하고 홈 위치의 구성 설정을 다운로드한 다음 디바이스를 재설정합니다. 디바이스가 홈 위치 구성 설정으로 등록됩니다.



참고 Cisco Unified Communications Manager는 항상 전화기 레코드의 Communications Manager Group 설정을 사용합니다. 디바이스는 로밍할 때 언제나 홈 위치의 Cisco Unified Communications Manager로 등록합니다. 전화기가 로밍 중일 때에는 대역폭 할당, 미디어 리소스 할당, 지역 구성, AAR 그룹 등의 네트워크 위치 설정만 변경됩니다.

구성

이 기능은 시스템 수준 및 디바이스 수준에서 활성화되어야 합니다. 시스템 수준에서 이 기능은 다음 구성 요소를 사용합니다.

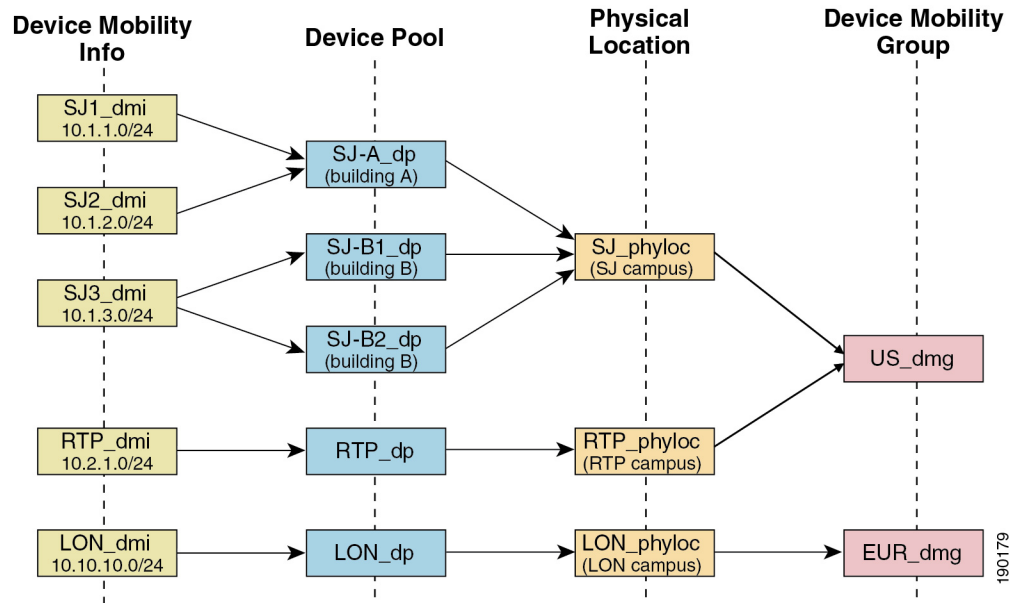
- 물리적 위치 — 디바이스폴의 물리적 위치를 정의합니다. 등록하는 동안 시스템은 디바이스 등록 위치를 디바이스 모빌리티 정보의 서브넷에 일치시켜 적절한 디바이스폴을 할당합니다.
- 디바이스폴 - 미디어 리소스, 지역 및 SRST 참조와 같은 위치 특정 디바이스 설정입니다. 로밍 디바이스의 경우 시스템에서 해당 디바이스의 물리적 위치와 일치하는 디바이스폴을 할당합니다.
- 디바이스 모빌리티 그룹 - 비슷한 전화걸기 패턴을 사용하는 사이트의 논리적 그룹입니다. 예를 들어, 전세계 네트워크를 사용하는 기업에서는 개별 국가를 나타내는 그룹을 설정할 수 있습니다.

다. 디바이스 모빌리티 그룹 설정에 따라 같은 지리적 엔티티 내에서 주로 사용자가 자체 다이얼 플랜을 유지할 수 있도록 디바이스를 이동할지 여부가 결정됩니다.

- 디바이스 모빌리티 정보 - 이 정보에는 시스템이 로밍 디바이스를 위해 제공하는 서브넷과 시스템에서 이러한 서브넷 중 하나에 등록하는 로밍 디바이스에 할당할 수 있는 디바이스풀이 포함됩니다.

디바이스 수준에서 이 기능을 사용하려면 디바이스에 대해 이 기능이 설정되어 있어야 합니다.

그림 1: 디바이스 모빌리티 관련 구성



190179

디바이스 풀 할당

이 섹션에서는 Unified Communications Manager가 디바이스 모빌리티를 활성화할 경우 디바이스풀을 할당하는 방법에 대해 설명합니다. 디바이스가 로밍 중인지 여부에 따라 디바이스에 로컬 사이트에서 디바이스풀을 할당할 수도 있고, 홈 사이트에서 디바이스풀을 사용할 수도 있습니다.

초기화 이후, 디바이스 모빌리티 기능은 다음 프로세스에 따라 작동합니다.

1. 모바일로 프로비저닝되는 IP 전화기에 대해 전화기 디바이스 레코드가 생성되고 전화기가 디바이스풀에 할당됩니다. 전화기가 Unified Communications Manager에 등록되고 등록 프로세스 중 IP 주소가 할당됩니다.
2. Unified Communications Manager가 디바이스의 IP 주소를 디바이스 모빌리티 정보 구성 창에서 디바이스 모빌리티에 대해 구성된 서브넷과 비교합니다. 가장 정확한 일치 항목은 IP 서브넷 마스크에서 가장 많은 비트 수를 사용합니다(가장 긴 일치 규칙). 예를 들어 IP 주소 9.9.8.2는 서브넷 9.9.0.0/16이 아니라 서브넷 9.9.8.0/24와 일치합니다.
3. 전화기 레코드의 디바이스풀이 일치하는 서브넷의 디바이스풀과 일치하는 경우 시스템은 전화기가 홈 위치에 있는 것으로 간주하고 전화기는 홈 디바이스풀의 매개 변수를 유지합니다.

4. 전화기 레코드의 디바이스폴이 일치하는 서브넷의 디바이스폴과 일치하지 않는 경우 전화기가 로밍하는 것으로 간주됩니다. 다음 표는 디바이스 모빌리티 및 시스템 응답에 대해 가능한 시나리오를 설명합니다.

표 5: 디바이스 모빌리티 시나리오

시나리오	시스템 응답
전화기 디바이스폴의 물리적 위치 설정이 일치하는 서브넷과 연결된 디바이스폴의 물리적 위치 설정과 일치합니다. 참고 전화기가 서브넷 사이를 이동했을 수 있지만, 물리적 위치 및 연결 서비스는 변경되지 않았습니다.	시스템은 전화기가 로밍하는 것으로 간주하지 않고 홈 위치 디바이스폴의 설정을 사용합니다.
일치하는 서브넷에 단일 디바이스폴이 할당되어 있습니다. 서브넷 디바이스폴은 홈 위치 디바이스폴과 다르며 물리적 위치가 다릅니다.	전화기가 로밍하는 것으로 간주되고 일치하는 서브넷에 대한 디바이스폴의 매개 변수로 다시 등록됩니다.
물리적 위치가 다르며 일치하는 서브넷에 여러 디바이스폴이 할당되어 있습니다.	전화기가 로밍하는 것으로 간주되고 라운드 로빈 규칙에 따라 새 디바이스폴이 할당됩니다. 로밍 디바이스가 서브넷에 등록하려고 할 때마다 사용 가능한 디바이스폴 집합의 다음 디바이스폴이 할당됩니다.
물리적 위치가 홈 디바이스폴에 대해 정의되지만 일치하는 서브넷과 연결된 디바이스폴에 대해서는 정의되지 않습니다.	물리적 위치가 변경되지 않았기 때문에 전화기가 홈 디바이스폴에 계속 등록된 상태를 유지합니다.
홈 디바이스폴에 정의되지 않은 물리적 위치가 일치하는 서브넷과 연결된 디바이스폴에 대해 정의됩니다.	시스템은 전화기가 정의된 물리적 위치로 로밍하는 것으로 간주하고 일치하는 서브넷에 대한 디바이스폴의 매개 변수로 등록합니다.
서브넷이 업데이트 또는 제거됩니다.	나머지 서브넷을 사용하여 디바이스폴의 로밍 및 할당 규칙이 적용됩니다.



참고 디바이스 모빌리티 정보 항목이 디바이스 IP 주소와 일치할 경우 디바이스는 홈 위치의 디바이스폴 설정을 사용합니다.

디바이스 모빌리티 그룹 운영 요약

디바이스 모빌리티 그룹을 사용하여 디바이스가 지리적 엔티티 내에서 다른 위치로 이동했는지 확인할 수 있으므로 사용자가 자신만의 다이얼 플랜을 사용할 수 있습니다. 예를 들어, 미국에 대한 디

바이스 모빌리티 그룹을 구성하고 영국에 대해 다른 그룹을 구성할 수 있습니다. 전화기가 다른 이동성 그룹으로 이동할 경우(예: 미국에서 영국으로) Unified Communications Manager는 로밍 위치가 아닌 전화기 레코드에서 발신 검색 공간, AAR 그룹, AAR CSS를 사용합니다.

디바이스가 동일한 이동성 그룹의 다른 위치로 이동할 경우(예: 미국 리처드슨에서 미국 볼더로) 로밍 디바이스 풀 설정의 CSS 정보를 가져옵니다. 이 방식에서 사용자가 PSTN 대상으로 다이얼할 경우 사용자가 로컬 게이트웨이에 연결됩니다.

다음 표는 시스템이 다양한 시나리오를 위해 사용하는 디바이스 풀 매개 변수에 대해 설명합니다.

표 6: 디바이스 모빌리티 그룹 시나리오

시나리오	사용되는 매개 변수
로밍 디바이스가 동일한 디바이스 모빌리티 그룹에서 다른 위치로 이동하는 경우	로밍 디바이스 풀: 예 위치: 로밍 디바이스 풀 설정 지역: 로밍 디바이스 풀 설정 미디어 리소스 그룹 목록: 로밍 디바이스 풀 설정 디바이스 CSS: 로밍 디바이스 풀 설정(디바이스 모빌리티 CSS) AAR 그룹: 로밍 디바이스 풀 설정 AAR CSS: 로밍 디바이스 풀 설정
로밍 디바이스가 다른 디바이스 모빌리티 그룹에서 다른 위치로 이동하는 경우	로밍 디바이스 풀: 예 위치: 로밍 디바이스 풀 설정 지역: 로밍 디바이스 풀 설정 미디어 리소스 그룹 목록: 로밍 디바이스 풀 설정 디바이스 CSS: 홈 위치 설정 AAR 그룹: 홈 위치 설정 AAR CSS: 홈 위치 설정
디바이스가 로밍하고 홈 또는 로밍 디바이스 풀에 대해 디바이스 모빌리티 그룹이 정의되지 않은 경우	디바이스가 로밍하기 때문에 디바이스 모빌리티 발신 검색 공간, AAR 발신 검색 공간, AAR 그룹 등의 로밍 디바이스 풀 설정을 사용합니다.

디바이스 모빌리티 사전 요건

- 전화기가 디바이스 모빌리티를 이용하려면 동적 IP 주소가 있어야 합니다. 정적 IP 주소를 사용하는 전화기가 로밍할 경우 Unified Communications Manager는 홈 위치의 구성 설정을 사용합니다.

- 디바이스 모빌리티 기능을 사용하려면 사이트 특정 설정을 사용하여 디바이스폴을 설정해야 합니다. 이 장에서는 디바이스 모빌리티에 관련된 디바이스폴 설정에 대해서만 설명합니다. 디바이스폴 구성에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "디바이스폴 구성" 장을 참조하십시오.
- Cisco Database Layer Monitor 서비스가 Cisco CallManager 서비스와 동일한 노드에서 실행 중이어야 함
- Cisco TFTP 서비스가 클러스터에 있는 하나 이상의 노드에서 실행 중이어야 합니다.
- Cisco Unified Communications Manager 로컬 설치 관리자(영어 이외의 전화기 로컬 또는 국가별 번호를 사용하고자 하는 경우)
- SCCP 또는 SIP를 실행하는 전화기입니다.

디바이스 모빌리티 설정 작업 흐름

디바이스 모빌리티를 구성하려면 이 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 1	다음 작업 중 하나를 완료하여 디바이스 수준에서 디바이스 모빌리티를 활성화합니다. <ul style="list-style-type: none"> • 디바이스 모빌리티 클러스터 수준 활성화, 59 페이지 • 개별 디바이스에 대한 디바이스 모빌리티 활성화, 59 페이지 	클러스터 수준 서비스 매개 변수를 통해 디바이스를 지원하거나 개별 디바이스의 전화기 구성 창 내에서 디바이스 지원을 활성화합니다.
단계 2	물리적 위치 구성, 60 페이지	디바이스폴에 할당할 실제 위치를 설정합니다.
단계 3	디바이스 모빌리티 그룹 구성, 60 페이지	디바이스 모빌리티 그룹은 비슷한 전화걸기 패턴을 사용하는 사이트의 논리적 그룹입니다.
단계 4	디바이스 모빌리티를 위한 디바이스 폴 구성, 60 페이지	디바이스 모빌리티에 사용될 디바이스폴에 실제 위치, 디바이스 모빌리티 그룹 및 기타 디바이스 모빌리티 관련 정보를 할당합니다.
단계 5	디바이스 모빌리티 정보 구성, 61 페이지	로밍 디바이스를 등록할 수 있는 IP 서브넷과 이러한 로밍 디바이스에 할당할 수 있는 디바이스폴을 할당합니다.

디바이스 모빌리티 클러스터 수준 활성화

다음 절차를 사용하여 전화기의 전화기 구성에 다시 정의된 구성이 있는 경우를 제외하고 모든 전화기 클러스터 수준에 대해 기본 디바이스 모빌리티 설정을 켜기로 설정하는 서비스 매개 변수를 구성합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 노드를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager** 서비스를 선택합니다.
- 단계 4 클러스터 수준 매개 변수(디바이스 - 전화기)에서 디바이스 모빌리티 모드 서비스 매개 변수를 켜기로 설정합니다.
- 단계 5 저장을 클릭합니다.

이미 등록된 디바이스에 대해 이 새 설정을 활성화하려면 **Cisco CallManager** 서비스를 다시 시작해야 합니다.

다음에 수행할 작업

개별 디바이스에 대한 디바이스 모빌리티 설정을 구성하려면 [개별 디바이스에 대한 디바이스 모빌리티 활성화, 59 페이지](#)(으)로 이동합니다.

그렇지 않으면 디바이스 모빌리티를 위해 시스템 구성을 시작할 수 있습니다. [물리적 위치 구성, 60 페이지](#)로 이동합니다.

개별 디바이스에 대한 디바이스 모빌리티 활성화

이 절차를 사용하여 개별 디바이스에 대한 디바이스 모빌리티를 활성화합니다. 이 구성은 디바이스 모빌리티 모드 클러스터 수준 서비스 매개 변수의 설정을 무시합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 구성할 디바이스를 선택합니다.
- 단계 3 디바이스 모빌리티 모드 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
 - 켜기—디바이스 모빌리티가 이 디바이스에 대해 활성화됩니다.
 - 끄기 - 디바이스 모빌리티가 이 디바이스에 대해 비활성화됩니다.
 - 기본값—디바이스가 디바이스 모빌리티 모드 클러스터 수준 서비스 매개 변수의 설정을 사용합니다. 이 값이 기본 설정입니다.

단계 4 저장을 클릭합니다.

물리적 위치 구성

이 절차를 사용하여 디바이스폴에 할당할 물리적 위치를 구성합니다. 디바이스 모빌리티는 디바이스 등록의 위치를 사용하여 적절한 디바이스폴을 할당합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 물리적 위치.

단계 2 새로 추가를 클릭합니다.

단계 3 위치에 대한 이름을 입력합니다.

단계 4 위치에 대한 설명을 입력합니다.

단계 5 저장을 클릭합니다.

디바이스 모빌리티 그룹 구성

다음 절차에 따라 다이얼링 패턴이 비슷한 사이트의 논리적 그룹인 디바이스 모빌리티 그룹을 구성합니다. 예를 들어, 전세계 네트워크를 사용하는 회사에서는 개별 국가를 나타내는 디바이스 모빌리티 그룹을 설정하고자 할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 디바이스 모빌리티 > 디바이스 모빌리티 그룹.

단계 2 새로 추가를 클릭합니다.

단계 3 디바이스 모빌리티 그룹을 식별하기 위한 이름을 입력합니다.

단계 4 디바이스 모빌리티 그룹에 대한 설명을 입력합니다.

단계 5 저장을 클릭합니다.

디바이스 모빌리티를 위한 디바이스 폴 구성

이 절차를 사용하여 디바이스 모빌리티에 대해 구성된 매개 변수를 사용하여 디바이스폴을 설정합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 디바이스폴.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 디바이스폴을 선택합니다.
- 새로 추가를 클릭하여 새 디바이스 폴을 만듭니다.

단계 3 로밍 감도 설정 아래에서 이전 디바이스 모빌리티 작업에 설정된 매개 변수를 할당합니다.

- 실제 위치 - 드롭다운 목록에서 이 디바이스폴에 대해 설정하는 실제 위치를 선택합니다. 디바이스 모빌리티는 이 위치를 사용하여 로밍 디바이스에 대한 디바이스폴을 할당합니다.
- 디바이스 모빌리티 그룹 - 드롭다운 목록에서 이 디바이스폴에 대해 설정하는 디바이스 모빌리티 그룹을 선택합니다.

단계 4 디바이스 모빌리티 관련 정보 아래에서 다음 디바이스 모빌리티 관련 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

- 디바이스 모빌리티 발신 검색 공간 - 이 디바이스폴을 사용하는 로밍 디바이스에서 사용할 CSS를 선택합니다.
- AAR 발신 검색 공간 - AAR(자동 우회 라우팅)이 수행될 때 디바이스에서 사용하기에 적합한 발신 검색 공간을 선택합니다.
- AAR 그룹 - AAR이 구성된 경우 이 디바이스에 대한 AAR 그룹을 선택합니다.
- 발신자 변환 CSS - 이 디바이스폴을 사용하는 로밍 디바이스에 대한 발신자 변환 CSS를 선택합니다.

참고

- 전화기 구성 창에서 디바이스폴 발신자 변환 CSS 사용 확인란이 선택되지 않은 경우에도 발신자 변환 CSS는 로밍 디바이스에 대해 디바이스 수준 구성을 무시합니다.
- 착신자 변환 CSS 설정이 로밍 디바이스 대신 게이트웨이에 적용됩니다.

단계 5 디바이스폴 구성 창의 나머지 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

디바이스 모빌리티 정보 구성

이 절차를 사용하여 로밍 디바이스가 등록할 수 있는 IP 서브넷과 시스템이 로밍 디바이스에 할당할 수 있는 해당 디바이스폴을 나타내는 디바이스 모빌리티 정보를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 디바이스 모빌리티 > 디바이스 모빌리티 정보.

단계 2 새로 추가를 클릭합니다.

단계 3 디바이스 모빌리티 정보에 대한 이름을 입력합니다.

단계 4 로밍 디바이스 등록에 대한 IP 서브넷 세부 정보를 입력합니다.

- 모바일 디바이스에 대해 IPv4 주소를 사용하는 경우 IPv4 서브넷 정보를 입력합니다.
- 모바일 디바이스에 대해 IPv6 주소를 사용하는 경우 IPv6 서브넷 정보를 입력합니다.

단계 5 시스템에서 이러한 서브넷 중 하나에 등록하는 로밍 디바이스에 할당할 디바이스폴을 선택합니다. 화살표를 사용하여 선택한 디바이스폴 목록 상자에서 사용 가능한 디바이스폴 목록 상자로 적절한 디바이스폴을 이동합니다.

단계 6 저장을 클릭합니다.

필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

로밍 디바이스폴 매개 변수 보기

다음 절차를 사용하여 디바이스에 대한 현재 디바이스 모빌리티 설정을 보고 확인합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 검색 기준을 입력하고 찾기를 클릭하여 디바이스 모빌리티 모드가 활성화된 디바이스를 찾습니다.

단계 3 디바이스 모빌리티 모드 필드 옆에 있는 현재 디바이스 모빌리티 설정 보기를 클릭합니다.

로밍 디바이스폴 설정이 표시됩니다. 디바이스가 로밍되고 있지 않은 경우 홈 위치 설정이 표시됩니다.

디바이스 모빌리티 상호 작용

표 7: 디바이스 모빌리티 상호 작용

기능	상호 작용
발신자 정규화	발신자 정규화는 일부 전화기의 전화걸기 기능을 개선하고 통화가 여러 지리적 위치로 전송될 때 콜백 기능을 향상시킵니다. 따라서 이 기능을 사용하면 착신자는 전화기의 통화 로그 디렉터리에서 디렉터리 번호를 수정하지 않고도 회신할 수 있습니다. 또한 발신자 정규화를 통해 전화 번호를 전역화 및 지역화할 수 있으므로 적절한 발신 번호 표시가 전화기에 표시됩니다.

기능	상호 작용
로밍	<p>디바이스를 동일한 디바이스 이동 그룹에서 로밍하는 경우 Unified Communications Manager은 디바이스 모빌리티 CSS를 사용하여 로컬 게이트웨이에 연결합니다. 사용자가 전화기에 CFA(모든 통화 착신 전환)를 설정하는 경우 CFA CSS가 [없음]으로 설정되고 CFA CSS 활성화 정책이 [디바이스/회선 CSS 활성화]로 설정되어 있으면 디바이스 위치에 따라 다음과 같은 현상이 발생합니다.</p> <ul style="list-style-type: none"> • 디바이스가 홈 위치에 있는 경우 디바이스 CSS 및 회선 CSS가 CFA CSS로 사용됩니다. • 동일한 디바이스 모빌리티 그룹에서 디바이스가 로밍 중인 경우 로밍 디바이스폴의 디바이스 모빌리티 CSS 및 회선 CSS가 CFA CSS로 사용됩니다. • 디바이스가 다른 디바이스 모빌리티 그룹에서 로밍 중인 경우 디바이스 CSS 및 회선 CSS가 CFA CSS로 사용됩니다.

디바이스 모빌리티 제한 사항

표 8: 디바이스 모빌리티 제한 사항

제한 사항	설명
IP 주소	<p>디바이스 모빌리티 기능은 Unified Communications Manager에 등록되는 디바이스의 IPv4 주소 또는 IPv6 주소에 따라 다릅니다.</p> <ul style="list-style-type: none"> • 디바이스 모빌리티를 사용하려면 전화기에 동적 IPv4 주소 또는 IPv6 주소가 있어야 합니다. • NAT(네트워크 주소 변환)/PAT(포트 주소 변환)를 사용하여 디바이스에 IP 주소를 할당한 경우 등록 중에 제공된 IP 주소는 디바이스의 실제 IP 주소와 일치하지 않을 수 있습니다. • Cisco IP 전화기가 IPv4 전용 스택 또는 IPv6 전용 스택을 지원하는 경우, 전화기는 정의된 IP 주소 지정 모드 기본 설정에 따라 IPv4 또는 IPv6 디바이스 모빌리티 정보를 사용하여 다시 연결됩니다. 예를 들어, 전화기가 IPv6 기본 설정으로 정의되었지만 일치하는 디바이스 모빌리티 정보(IPv6 서브넷 및 마스크 크기)가 없는 경우 IPv4에 연결됩니다. 일치하는 IPv6 디바이스 모빌리티 정보를 추가하면 전화기가 IPv6 디바이스 모빌리티 정보와 다시 연결됩니다.



6 장

확장 및 연결

- 확장 및 연결 개요, 65 페이지
- 확장 및 연결 사전 요건, 66 페이지
- 구성 작업 흐름 확장 및 연결, 66 페이지
- CTIRD (CTI 원격 디바이스) 통화 흐름, 71 페이지
- 확장 및 연결 상호 작용, 72 페이지
- 확장 및 연결 제한 사항, 73 페이지

확장 및 연결 개요

확장 및 연결은 관리자가 엔드포인트와 상호 작용하는 Unified Communications Manager UC CTI(Computer Telephony Integration) 애플리케이션을 배포하는 기능입니다. 확장 및 연결을 통해 사용자는 어디서나 모든 디바이스에서 UC 애플리케이션에 액세스할 수 있습니다.

Unified Communications Manager의 확장 및 연결 기능은 다음 UC 기능을 제공합니다.

- 엔터프라이즈 착신 통화 수신
- 전화 걸기
- 연결 끊기
- 보류 및 검색
- 재전송 및 착신 전환
- 모든 통화 착신 전환
- 통화 중 착신 전환
- 응답 없음 착신 전환
- DND(Do Not Disturb)
- DTMF(복합 주파수 부호) 재생(대역 외 및 대역 내)
- 상담 호전환, 전화회의

- 원격 대상 추가, 편집 및 삭제
- 원격 대상을 활성화 또는 비활성으로 설정
- 영구 연결
- 콧속말 알림 재생

확장 및 연결 사전 요건

- Cisco Jabber, 릴리스 9.1(1) 이상
- Cisco Unified Workspace License(CUWL) 표준, CUWL Professional 또는 Cisco User Connect License(UCL) - 고급

구성 작업 흐름 확장 및 연결

이 섹션에서는 Unified Communications Manager 사용자에게 확장 및 연결 기능을 제공하기 위해 수행해야 하는 절차에 대해 설명합니다. 확장 및 연결을 사용하여 Windows 사용자를 위한 Cisco Jabber 프로비저닝에 대한 자세한 내용은 [Windows용 Cisco Jabber 설치 및 설정 가이드](#)를 참조하십시오.

시작하기 전에

프로시저

	명령 또는 동작	목적
단계 1	사용자 계정 구성, 67 페이지	CTI 원격 디바이스를 사용할 수 있도록 사용자에게 이동성을 활성화합니다. CTI 디바이스는 Cisco UC 애플리케이션을 사용하는 오프 클러스터 전화기입니다.
단계 2	사용자 권한 추가, 67 페이지	액세스 컨트롤 그룹 권한을 추가합니다.
단계 3	CTI 원격 디바이스 생성, 68 페이지	사용자가 Cisco UC 애플리케이션에 사용할 수 있는 오프 클러스터 전화기를 구성합니다.
단계 4	디바이스에 디렉터리 번호 추가, 69 페이지	디렉터리 번호를 CTI 원격 디바이스와 연결합니다.
단계 5	원격 대상 추가, 69 페이지	사용자가 소유하고 있는 다른 전화기를 나타내는 숫자 주소 또는 디렉터리 URI를 추가합니다.
단계 6	원격 대상 확인, 70 페이지	원격 대상이 사용자에게 성공적으로 추가되었는지 확인합니다.

	명령 또는 동작	목적
단계 7	사용자를 디바이스에 연결, 71 페이지	최종 사용자 계정을 CTI 원격 디바이스에 연결합니다.

사용자 계정 구성

다음 절차를 사용하여 Unified Communications Manager에서 새 사용자 또는 기존 사용자를 구성하려면 CTI 원격 디바이스를 사용할 수 있도록 사용자 이동성을 활성화해야 합니다. 사용자의 이동성을 활성화하지 않는 경우 이러한 사용자를 CTI 원격 디바이스의 소유자로 할당할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 다음 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 사용자를 구성합니다.
- 사용자 위치 찾기 필드를 사용하여 필터를 적용한 다음, 찾기를 선택하여 사용자 목록을 검색합니다.

참고 LDAP 통합이나 로컬 구성을 통해 새 최종 사용자 계정을 추가할 수 있습니다.

단계 3 이동성 정보 섹션을 찾습니다.

단계 4 이동성 활성화 확인란을 선택합니다.

단계 5 저장을 클릭합니다.

사용자 권한 추가

최종 사용자가 Unified Communications Manager에서 활성화되고 나면 액세스 컨트롤 그룹 권한을 추가합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 사용자 위치 찾기 필드에 적절한 필터를 지정한 다음, 찾기를 선택하여 사용자 목록을 검색합니다.

단계 3 목록에서 사용자를 선택합니다.

단계 4 권한 정보 섹션을 찾습니다.

단계 5 액세스 제어 그룹에 추가를 클릭합니다.

액세스 컨트롤 그룹 찾기 및 나열 창이 나타납니다.

단계 6 찾기를 클릭합니다.

표준 사용자에게 대한 액세스 컨트롤 그룹 목록이 나타납니다.

단계 7 다음 권한 옆에 있는 확인란을 선택합니다.

- 표준 CCM 최종 사용자
- 표준 CTI 활성화

단계 8 선택한 항목 추가를 클릭합니다.

단계 9 저장을 클릭합니다.

CTI 원격 디바이스 생성

다음 절차에 따라 CTI 원격 디바이스를 생성하는 것은 사용자가 Cisco UC 애플리케이션과 함께 사용할 수 있는 클러스터 외부 전화기를 나타내는 디바이스 유형입니다. 디바이스 유형은 하나 이상의 회선(디렉터리 번호)과 하나 이상의 원격 대상으로 구성됩니다.

Unified Communications Manager는 PSTN(Public Switched Telephone Network) 전화기 및 PBX(Private Branch Exchange) 디바이스 같은 디바이스에서 통화를 제어할 수 있는 확장 및 연결 기능을 제공합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 새로 추가를 클릭합니다.

단계 3 전화기 유형 드롭다운 목록에서 **CTI** 원격 디바이스를 선택하고 다음을 클릭합니다.

단계 4 소유자 사용자 ID 드롭다운 목록에서 적절한 사용자 ID를 선택합니다.

참고 이동성을 활성화한 사용자만 소유자 사용자 ID 드롭다운 목록에서 사용할 수 있습니다.

Unified Communications Manager가 디바이스 이름 필드를 사용자 ID와 CTRID 접두사(예: *CTRIDusername*)로 채웁니다.

단계 5 필요하다면 디바이스 이름 필드의 기본값을 편집합니다.

단계 6 설명 필드에 유의미한 설명을 입력합니다.

참고 Cisco Jabber에서 사용자에게 디바이스 설명을 표시합니다. Cisco Jabber 사용자가 동일한 모델의 디바이스 여러 개를 갖고 있는 경우 Unified Communications Manager의 설명은 사용자가 디바이스의 차이점을 구분하는 데 도움이 됩니다.

단계 7 프로토콜별 정보 섹션의 재라우팅 발신 검색 공간 드롭다운 목록에서 적절한 옵션을 선택해야 합니다.

재라우팅 발신 검색 공간 드롭다운 목록은 재전송할 발신 검색 공간을 정의하고 사용자가 CTI 원격 디바이스에서 통화를 송수신할 수 있게 합니다.

단계 8 전화기 구성 창에서 나머지 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 9 저장을 클릭합니다.

디렉터리 번호를 연결하고 원격 대상을 추가하는 필드가 전화기 구성 창에 표시됩니다.

디바이스에 디렉터리 번호 추가

DN(디렉터리 번호)이란 CTI 원격 디바이스에서 회선으로 구성된 숫자 주소를 말합니다. 일반적으로 DN은 사용자의 기본 직장 전화 번호(예: 2000 또는 +1 408 200 2000)를 나타냅니다.



참고

- 디바이스에서 CSS(발신 검색 공간) 및 DN 파티션은 필수입니다.
- CTI 원격 디바이스는 자체 DN을 차단해서는 안 됩니다. CSS는 CTIRD 디바이스에서 자체 DN에 도달하는 데 중요합니다.

다음 단계에 따라 CTI 원격 디바이스에 디렉터리 번호를 추가합니다.

프로시저

단계 1 전화기 구성 창에서 연결 정보 섹션을 찾습니다.

단계 2 새 **DN** 추가를 클릭합니다.

단계 3 디렉터리 번호 필드에 디렉터리 번호를 지정합니다.

단계 4 기타 모든 필수 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

원격 대상 추가

다음 절차를 사용하여 사용자가 소유한 다른 전화기(예: 홈 오피스 회선 또는 다른 PBX 전화기)를 나타내는 숫자 주소 또는 디렉터리 URI인 원격 대상을 추가합니다. 원격 대상은 모든 클러스터 외부 디바이스가 될 수 있습니다. Unified Communications Manager는 CTI 원격 디바이스에 대한 애플리케이션 다이얼 규칙을 모든 원격 대상 번호에 자동으로 적용합니다. 기본적으로, 디바이스당 4개의 원격 대상이 지원됩니다. 사용사 설정 창에서 원격 대상 최대 수를 디바이스당 10개로 설정할 수 있습니다.



참고

Cisco 통합 커뮤니케이션 매니저 관리 인터페이스에서 전화기 설정 창을 열어 Jabber 클라이언트가 활성으로 설정한 원격 대상을 확인할 수 있습니다.



참고 Unified Communications Manager 사용자는 Cisco Jabber 인터페이스를 통해 원격 대상을 추가할 수 있습니다. 자세한 내용은 [Windows용 Cisco Jabber 설치 및 구성 설명서](#)를 참조하십시오.

- Unified Communications Manager는 Cisco Jabber 사용자가 클라이언트 인터페이스를 통해 추가한 원격 대상 통화를 전송할 수 있는지 여부를 자동으로 확인합니다.
- Unified Communications Manager는 Cisco Unified Communications Manager 관리 인터페이스를 통해 추가된 원격 대상 통화를 전송할 수 있는지 여부를 확인하지 않습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 전화기 위치 찾기 필드에 적절한 필터를 지정한 다음 찾기를 클릭하여 전화기 목록을 검색합니다.

단계 3 목록에서 CTI 원격 디바이스를 선택합니다.

단계 4 연결된 원격 대상 섹션을 찾습니다.

단계 5 새 원격 대상 추가를 클릭합니다.

단계 6 대상 번호 필드에 대상 번호를 입력합니다.

Cisco Jabber 클라이언트에서 원격 대상을 사용하려면 *JabberRD*로 대상 이름을 구성해야 합니다.

단계 7 원격 대상 정보 창에서 나머지 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 8 저장을 클릭합니다.

원격 대상 확인

원격 대상이 사용자에게 성공적으로 추가되었는지 확인하려면 다음 단계를 수행합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 전화기 위치 찾기 필드에 적절한 필터를 지정한 다음 찾기를 클릭하여 전화기 목록을 검색합니다.

단계 3 목록에서 CTI 원격 디바이스를 선택합니다.

단계 4 연결된 원격 대상 섹션을 찾아 원격 대상이 사용 가능한 지 확인합니다.

단계 5 구성 적용을 클릭합니다.

참고 전화기 구성 창의 디바이스 정보 섹션은 원격 대상이 활성 상태이거나 Cisco Jabber에 의해 제어되는지 경우를 나타냅니다.

사용자를 디바이스에 연결

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자
- 단계 2 사용자 위치 찾기 필드에 적절한 필터를 지정한 다음, 찾기를 선택하여 사용자 목록을 검색합니다.
- 단계 3 목록에서 사용자를 선택합니다.
- 단계 4 디바이스 정보 섹션을 찾습니다.
- 단계 5 디바이스 연결을 클릭합니다.
- 단계 6 CTI 원격 디바이스를 찾아 선택합니다.
- 단계 7 연결을 완료하려면 선택 항목/변경 사항 저장을 클릭합니다.
- 단계 8 관련 링크 드롭다운 목록에서 사용자로 돌아가기를 선택한 다음 이동을 클릭합니다.
최종 사용자 구성 창이 나타나고 선택한 연결 디바이스가 제어된 이바이스 창에 표시됩니다.

CTIRD (CTI 원격 디바이스) 통화 흐름

Unified Communications Manager 는 사용자가 CTI 원격 디바이스로 추가되는 경우 별도의 발신자 번호 및 청구 번호 기능을 지원합니다. 각 CTI 원격 디바이스에는 사용자 디렉터리 번호(DN)(예: 2000)와 오프-클러스터 디바이스(예: 번호가 +1 408 111 1111인 PBX 전화)를 나타내는 원격 대상이 구성되어 있습니다.

PSTN 네트워크에서 CTIRD 회선으로 통화가 시작되면 Unified Communications Manager는 FROM 및 PAID 헤더 정보를 찾습니다. FROM 헤더에는 외부 표시 이름 및 번호가 포함되어 있으며 PAID에는 사용자의 ID(사용자의 DN 또는 DDI)가 포함되어 있습니다.

FROM 및 PAID 헤더의 번호가 다르고 SIP 프로파일에서 외부 표시 이름 및 번호 활성화 확인란이 선택되고 외부 표시 이름 및 번호 표시 서비스 매개 변수 값이 *True*로 설정된 경우 Unified Communications Manager는 호출된 디바이스에 FROM 헤더 정보를 표시합니다. 동일한 방식으로, 하나의 옵션이 비활성화된 경우에는 Unified Communications Manager는 착신 디바이스에 대한 PAID 헤더 정보를 표시합니다.

마찬가지로 발신 통화 시나리오에서 사용자는 디렉터리 번호 구성 페이지의 외부 표시 이름 및 외부 표시 번호로 구성된 원격 대상(CTIRD 회선)에서 SIP 프로파일에 외부 표시 이름 및 번호가 구성되어 있는 SIP 트렁크를 통해 PSTN 네트워크로 전화를 겁니다. 그런 다음, Unified Communications Manager는 발신 SIP 메시지의 FROM 헤더에 있는 디렉터리 번호 구성 페이지에 구성된 외부 표시 정보를 전송하여 착신 디바이스에 표시합니다.

외부 표시 이름 및 번호 활성화 확인란을 선택하지 않은 경우 Unified Communications Manager는 FROM 및 PAID의 디렉터리 번호 정보를 보내 X-Cisco-Presentation 헤더의 착신 디바이스와 구성된 외부 표시 정보를 표시합니다.

익명 외부 표시 확인란을 선택하면 구성된 외부 표시 이름과 번호가 해당 필드 및 착신 디바이스에 익명으로 표시된 외부 표시에서 제거됩니다.

외부 표시 정보를 구성하는 방법에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 디렉터리 번호 구성 장을 참조하십시오.

확장 및 연결 상호 작용

표 9: 확장 및 연결 상호 작용

기능	상호 작용
디렉터리 URI 다이얼	CTI 원격 디바이스에 대해 디렉터리 URI를 DN, 원격 대상 또는 둘 다로 구성합니다.
Unified Mobility	<p>확장 및 지원은 Cisco Unified IP Phone 및 원격 대상 간 활성화 통화 이동을 지원하지 않습니다.</p> <p>Unified Mobility와 확장 및 연결 기능을 모두 원하는 경우 두 디바이스 유형의 소유자 ID가 같을 때 원격 디바이스 프로파일 및 CTI 원격 디바이스 유형에 동일한 원격 대상을 구성하면 됩니다. 이렇게 구성하면 Cisco Mobility 기능을 확장 및 연결과 동시에 사용할 수 있습니다. 두 디바이스 유형에 동일한 원격 대상을 구성하는 기능은 Cisco Unified Communications Manager 릴리스 10.0(1) 이상을 사용하여 지원됩니다.</p> <p>Cisco 확장 및 연결 기능과 함께 사용하는 원격 대상은 iPhone용 Cisco 듀얼 모드, Android용 Cisco 듀얼 모드 및 통신사업자 통합 모바일 디바이스 유형에서 구성하지 마십시오. 접두사를 사용하여 동일한 원격 대상 주소를 구분하지 마십시오. 예를 들어, 91- 4085555555 및 +1- 4085555555는 동일한 번호로 처리됩니다.</p>
헌트 목록	<p>사용자는 확장 및 연결 기능을 사용하여 다음과 같은 조건의 원격 대상 전화기에서 헌트 전화를 받을 수 있습니다.</p> <ul style="list-style-type: none"> • 사용자에게 Cisco Unified IP Phone이 있습니다. • Cisco Unified IP Phone을 사용하여 헌트 전화를 받을 수 있습니다(로그인됨/HLog). • Cisco Jabber를 확장 및 연결 모드로 실행 중입니다.

기능	상호 작용
CallerID 정보	<ul style="list-style-type: none"> 수신되는 발신자 ID 정보(이름 및 번호)가 Jabber 클라이언트에 표시됩니다. 이 정보는 해당 통신업체 및 트렁크 구성에 따라 디바이스에 표시될 수도 있습니다. 원격 대상에 거는 DVO(Dial-via-Office) 발신 통화는 이름으로 음성 연결, 번호로 트렁크 DID를 표시합니다. Unified CM 트렁크 패턴, 경로 패턴 또는 Cisco 게이트웨이에 트렁크 DID를 구성하십시오. 이 구성은 통신업체가 할당할 수도 있습니다. 트렁크 DID가 구성되지 않은 경우 번호 필드가 빈 것으로 표시될 수 있습니다. 원하는 상대에 거는 발신 통화는 Unified Communications Manager에 구성된 CTI 원격 디바이스 표시 이름 및 DN(디렉터리 번호)을 표시합니다. 원격 대상 번호는 착신자에게 표시되지 않습니다.

확장 및 연결 제한 사항

표 10: 확장 및 연결 제한 사항

제한 사항	설명
최대 원격 대상 수	<p>각 CTI 원격 디바이스에 대해 최대 10개의 원격 대상을 구성할 수 있습니다.</p> <p>참고 기본적으로, 디바이스당 4개의 원격 대상이 지원됩니다. 원격 대상 최대 수를 디바이스당 10개로 설정할 수 있습니다.</p>
오프-클러스터 디바이스	<ul style="list-style-type: none"> 원격 대상 번호는 클러스터 외부(off-cluster) 디바이스를 나타내야 합니다. 원격 대상은 클러스터 외부 URI일 수 있습니다.
디렉터리 번호	디렉터리 번호는 원격 대상 번호로 구성할 수 없습니다.
Cisco Jabber	Cisco Jabber를 사용하여 구성된 원격 대상을 저장하기 전에 구성된 다이얼 플랜으로 원격 대상을 라우팅할 수 있는지 확인하십시오.

제한 사항	설명
애플리케이션 다이얼 규칙	<p>Cisco 통합 커뮤니케이션 매니저 관리 인터페이스와 Cisco Jabber를 통해 CTI 원격 디바이스에서 구성된 모든 원격 대상에 애플리케이션 다이얼 규칙이 적용됩니다.</p> <p>참고 애플리케이션 다이얼 규칙이 지원하도록 구성된 번호 형식(예: nn-nnn-nnnn, E.164, 둘 다)을 최종 사용자에게 알려십시오.</p>
원격 대상 번호	<p>각 원격 대상 번호는 클러스터 내에서 고유해야 합니다.</p> <p>참고 동일한 원격 대상 번호를 두 명 이상의 사용자가 사용할 수 없습니다.</p>
원격 대상 검증	<ul style="list-style-type: none"> 원격 대상 번호는 CTI 원격 디바이스 재전송 발신 검색 공간을 사용하여 검증됩니다. Cisco 통합 커뮤니케이션 매니저 관리 인터페이스와 AXL 인터페이스를 사용하여 구성된 원격 대상은 검증되지 않습니다.
등록되지 않은 착신 전환	확장 및 연결은 등록되지 않은 내부 또는 등록되지 않은 외부 착신 전환을 지원하지 않습니다.
전화 상대 번호별 다음 홉 경로 지정	확장 및 연결은 "발신자 번호로 다음 홉 라우팅" 옵션을 활성화한 경우 변환 패킷을 지원하지 않습니다.



7 장

원격 작업자 비상 통화

- 원격 작업자 비상 통화 개요, 75 페이지
- 원격 작업자 비상 통화 사전 요건, 75 페이지
- 원격 작업자 비상 통화 구성 작업 흐름, 76 페이지

원격 작업자 비상 통화 개요

원격 작업자 비상 통화 기능을 사용하면 고객이 원격 VPN(가상 사설망) 연결을 사용하여 원격 작업자에게 신뢰할 수 있는 비상 통화 지원을 제공할 수 있습니다. 오프-프레미스 사용자의 비상 통화는 PSAP(공공 안전 응답 지점)로 라우팅되고, 사용자가 제공한 위치 정보는 각 통화와 함께 전달됩니다.

이 기능을 사용하려면 원격 작업자는 디바이스 등록이 중단될 때마다 위치를 확인하거나 업데이트해야 합니다. 사용자 정의 가능한 면책사항 알림은 먼저 오프-프레미스(고객 네트워크에 원격으로 연결)용으로 지정된 디바이스에 표시되며, 이 알림은 사용자에게 올바른 위치 정보를 제공하도록 조언합니다. 위치 정보가 제공되면 지정된 디바이스와 현재 연결된 오프-프레미스 위치가 표시됩니다. 사용자는 자신의 현재 위치를 확인하거나 자신의 디바이스 표시에서 이전에 저장한 다른 위치를 선택할 수 있습니다. 위치가 새 위치인 경우 Cisco Emergency Responder 오프-프레미스 사용자 웹 페이지로 전송되어 새 위치가 생성됩니다.

이 프로세스를 완료하기 전에 관리자가 단일 구성된 대상을 호출하도록 디바이스를 제한할 수 있습니다. 이 작업을 수행하면 디바이스 사용자가 정상적인 사용을 위해 디바이스를 활성화하기 전에 면책사항을 인식하고 자신의 현재 위치 정보를 제공할 수 있습니다.

원격 작업자 비상 통화 사전 요건

원격 작업자 비상 통화 기능을 구성 하기 전에 Cisco Emergency Responder에서 Intrado(타사 애플리케이션)를 구성해야 합니다. Cisco Emergency Responder의 Intrado 구성에 대한 자세한 내용은 [Cisco Emergency Responder 관리 지침서](#)의 내용을 참조하십시오.

원격 작업자 비상 통화 구성 작업 흐름

시작하기 전에

프로시저

	명령 또는 동작	목적
단계 1	사용자를 원격 작업자로 구성, 76 페이지	오프-프레미스 디바이스를 디바이스의 소유자와 연결합니다.
단계 2	비상 통화에 대한 대체 라우팅 지정, 77 페이지	이러한 매개 변수는 사용자가 위치를 설정하지 않기로 선택한 등록된 오프-프레미스 디바이스에서 건 통화에 대한 라우팅을 제한하는데 사용되는 발신 검색 공간 및 대상 번호를 지정합니다. 이러한 매개 변수를 구성하지 않은 경우에는 통화가 정상적으로 라우팅됩니다.
단계 3	애플리케이션 서버 구성, 77 페이지	최종 사용자를 디바이스 위치를 입력하는 곳인 애플리케이션 서버로 안내합니다.
단계 4	E911 메시지 구성, 78 페이지	오프-프레미스 최종 사용자 전화기에 표시되는 E911 메시지를 구성합니다.

사용자를 원격 작업자로 구성

시작하기 전에

Cisco Emergency Responder에서 Intrado를 구성했는지 확인합니다. Cisco Emergency Responder의 Intrado 구성에 대한 자세한 내용은 [Cisco Emergency Responder 관리 지침서](#)의 내용을 참조하십시오.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 전화기를 찾을 적절한 검색 조건을 입력하고 찾기를 클릭합니다.
검색 조건과 일치하는 전화기 목록이 표시됩니다.
- 단계 3 원격 작업자 비상 통화를 구성하려는 전화기를 선택합니다.
전화기 구성 창이 표시됩니다.
- 단계 4 디바이스 정보 섹션의 소유자 사용자 ID 드롭다운 목록에서 적절한 사용자 ID를 선택하고 오프-프레미스 위치 필요 확인란을 선택합니다.
- 단계 5 저장을 클릭합니다.
-

비상 통화에 대한 대체 라우팅 지정

발신 검색 공간 및 대상 번호를 구성하려면 다음 단계를 수행합니다. 이러한 매개 변수는 사용자가 위치를 설정하지 않은 등록된 외부 디바이스에서 걸려오는 모든 통화의 라우팅을 제한하는 데 사용됩니다. 이러한 매개 변수를 구성하지 않은 경우에는 통화가 정상적으로 라우팅됩니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
서비스 매개 변수 구성 창이 표시됩니다.
- 단계 4 클러스터 수준 매개 변수(필수 오프 프레미스 위치에 대한 비상 통화) 섹션에서 비상 통화에 대한 대체 대상을 지정합니다.
- 단계 5 비상 통화의 대체 발신 검색 공간을 지정합니다.
- 단계 6 저장을 클릭합니다.

애플리케이션 서버 구성

애플리케이션 서버를 프로비저닝하여 Cisco Emergency Responder과(와) 통신할 수 있도록 E911 프록시를 활성화해야 합니다. E911 프록시는 사용자를 디바이스 위치를 입력하는 곳인 애플리케이션 서버로 안내하는 데 사용됩니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 애플리케이션 서버.
- 단계 2 새로 추가를 클릭합니다.
애플리케이션 서버 창이 나타납니다.
- 단계 3 애플리케이션 서버 유형 드롭다운 목록에서 **CER** 위치 관리를 선택합니다.
- 단계 4 다음을 클릭합니다.
- 단계 5 이름 필드에서 구성하는 애플리케이션 서버를 식별하는 이름을 지정합니다.
- 단계 6 IP 주소 필드에서 구성하는 서버의 IP 주소를 지정합니다.
- 단계 7 사용 가능한 애플리케이션 사용자 목록에서 애플리케이션 사용자를 선택하고 아래쪽 화살표를 클릭합니다.
- 단계 8 최종 사용자 URL 필드에 이 애플리케이션 서버와 연결된 최종 사용자의 URL을 입력합니다.
- 단계 9 저장을 클릭합니다.

E911 메시지 구성

다음 절차에 따라 오프-프레미스 디바이스에 대한 E911 메시지를 선택 및 편집합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > **E911** 메시지.

단계 **2** E911 메시지에 대해 필요한 언어 링크를 선택합니다.

E911 메시지 구성 페이지에 계약, 면책사항 및 오류 메시지가 표시됩니다.

단계 **3** (선택 사항) 오프-프레미스 디바이스에 표시될 E911 메시지를 편집합니다.

단계 **4** 저장을 클릭합니다.



8 장

모바일 및 원격 액세스 구성

- 모바일 및 원격 액세스 개요, 79 페이지
- 모바일 및 원격 액세스 사전 요건, 81 페이지
- 모바일 및 원격 액세스 구성 작업 흐름, 82 페이지
- 경량 Keepalive를 통한 MRA 페일오버, 88 페이지

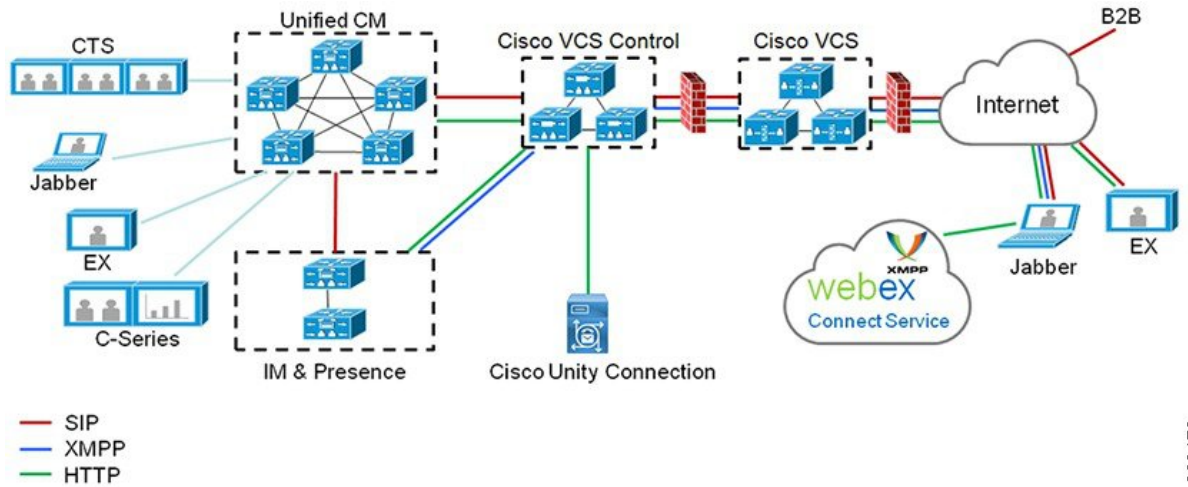
모바일 및 원격 액세스 개요

Unified Communications Manager 모바일 및 원격 액세스는 Cisco Collaboration Edge Architecture의 핵심 부분입니다. Cisco Jabber와 같은 엔드포인트가 엔터프라이즈 네트워크에 없는 경우, 해당 엔드포인트에서 Unified Communications Manager에서 제공하는 등록, 통화 제어, 제공, 메시징 및 프레즌스 서비스를 사용할 수 있습니다. Cisco Expressway는 모바일 엔드포인트를 온프레미스 네트워크에 연결하여 Unified CM 등록을 위한 안전한 방화벽 트래버설 및 회선 측 지원을 제공합니다.

전체 솔루션은 다음과 같은 기능을 제공합니다.

- 오프-프레미스 액세스: Jabber 및 EX/MX/SX 시리즈 클라이언트에 대해 네트워크 외부의 일관된 경험.
- 보안: 비즈니스 간 통신 보호.
- 클라우드 서비스: 풍부한 Webex 통합 및 서비스 공급자 오퍼링을 제공하는 엔터프라이즈급 유연성 및 확장 가능한 솔루션.
- 게이트웨이 및 상호운용성 서비스: 미디어 및 신호 정규화, 비표준 엔드포인트 지원.

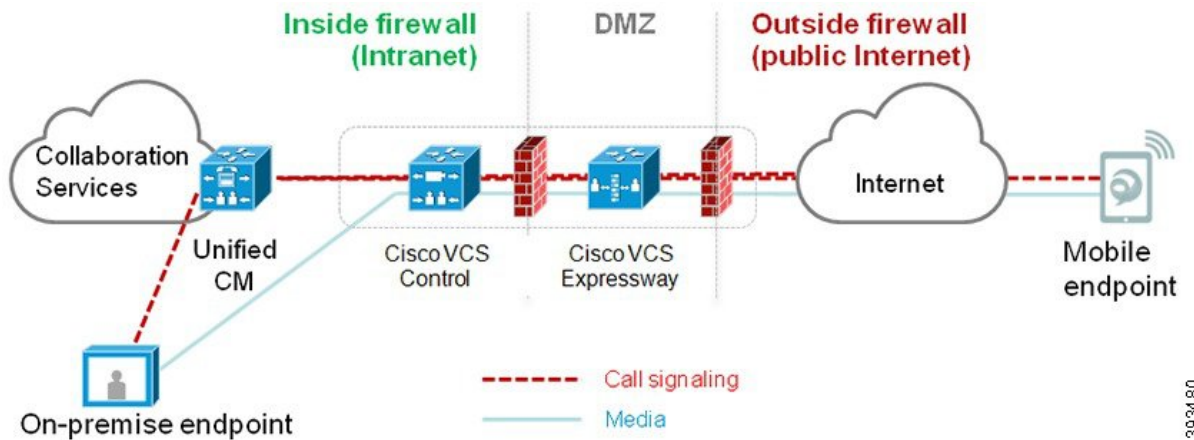
그림 2: Unified Communications: 모바일 및 원격 액세스



393479

타사 SIP 또는 H.323 디바이스는 Expressway-C에 등록할 수 있으며, 필요한 경우 SIP 트렁크를 통해 Unified CM 등록 디바이스와 상호 작용할 수 있습니다.

그림 3: 일반적인 통화 흐름: 신호 처리 및 미디어 경로



393480

- Unified CM은 모바일 및 온-프레미스 엔드포인트 모두에 대해 통화 제어 기능을 제공합니다.
- 신호 처리는 모바일 엔드포인트와 Unified CM 간에 Expressway 솔루션을 트래버스합니다.
- 미디어는 Expressway 솔루션을 트래버스하고 엔드포인트 간에 직접 릴레이됩니다. Expressway-C와 모바일 엔드포인트 간에 모든 미디어가 암호화됩니다.

모바일 및 원격 액세스 구성

모바일 및 원격 액세스 기능을 사용하여 Cisco Jabber 사용자를 활성화하려면 Unified Communications Manager의 사용자 프로파일 구성 창에서 모바일 및 원격 액세스 사용자 정책을 설정합니다. 비 Jabber 엔드포인트에는 모바일 및 원격 액세스 사용자 정책이 필요하지 않습니다.

뿐만 아니라, 모바일 및 원격 액세스를 사용하여 Cisco Expressway를 구성해야 합니다. 자세한 내용은 [Mobile and Remote Access via Cisco Expressway 구축 설명서](#)를 참조하십시오.

모바일 및 원격 액세스 사전 요건

Cisco Unified Communications Manager 요구 사항

다음과 같은 요구 사항이 적용됩니다.

- 여러 Unified Communications Manager 클러스터를 구축하는 경우에는 ILS 네트워크를 설정합니다.
- 모바일 및 원격 액세스를 사용하려면 구축을 위해 NTP 서버를 설정해야 합니다. 네트워크에 NTP 서버가 구축되어 있고 SIP 엔드포인트에 대해 전화기 NTP 참조가 있는지 확인합니다.
- 미디어 경로 최적화를 위해 ICE를 배포하는 경우에는 TURN 및 STUN 서비스를 제공할 수 있는 서버를 구축해야 합니다.

DNS 요구 사항

Cisco Expressway에 대한 내부 연결의 경우 Unified Communications Manager를 가리키는 로컬에서 확인할 수 있는 DNS SRV를 구성합니다.

`_cisco-uds._tcp<도메인>`

모바일 및 원격 액세스에 사용되는 모든 통합 커뮤니케이션 노드에 대한 정방향 및 역방향 조회 모두에 대해 내부 DNS 레코드를 생성해야 합니다. 이렇게 하면 Expressway-C가 FQDN 대신 IP 주소 또는 호스트 이름을 사용하는 경우 노드를 찾을 수 있습니다. 로컬 네트워크 외부에서 SRV 레코드를 확인할 수 없는지 확인합니다.

Cisco Expressway 요구 사항

이 기능을 사용하려면 Unified Communications Manager를 Cisco Expressway와 통합해야 합니다. 모바일 및 원격 액세스에 대한 Cisco Expressway 구성 세부 정보는 [Cisco Expressway 구축 설명서](#)를 통한 [모바일 및 원격 액세스](#)를 참조하십시오.

Cisco Jabber에서 지원하는 모바일 및 원격 액세스 액세스 정책에 대한 최소 Expressway 릴리스는 X8.10입니다.

인증서 사전 요건

Unified Communications Manager, IM and Presence Service 및 Cisco Expressway-C 사이에 인증서를 교환해야 합니다. 각 시스템에 대해 동일한 CA를 사용하는 CA 서명 인증서를 사용하는 것이 좋습니다. 이러한 경우:

- 각 시스템에 CA 루트 인증서 체인을 설치합니다(Unified Communications Manager 및 IM and Presence 서비스서비스의 경우 tomcat 신뢰 저장소에 인증서 체인을 설치).

- Unified Communications Manager의 경우 CA 서명 tomcat(AXL 및 UDS 트래픽의 경우) 및 Cisco CallManager(SIP의 경우) 인증서를 요청하는 CSR을 발행합니다.
- IM and Presence 서비스 서비스의 경우 CA 서명 tomcat 인증서를 요청하는 CSR을 발행합니다.



참고 다른 CA를 사용하는 경우 Unified Communications Manager, IM and Presence 서비스 서비스 및 Expressway-C에 각 CA의 루트 인증서 체인을 설치해야 합니다.



참고 Unified Communications Manager 및 IM and Presence 서비스 서비스 모두에 대해 자체 서명 인증서를 사용할 수도 있습니다. 이 경우에는 Expressway-C에 Unified Communications Manager의 경우 tomcat 및 Cisco CallManager 인증서, IM and Presence 서비스 서비스의 경우 tomcat 인증서를 업로드해야 합니다.

모바일 및 원격 액세스 구성 작업 흐름

모바일 및 원격 액세스 엔드포인트를 배포하려는 경우 Unified Communications Manager에서 이러한 작업을 완료합니다.

프로시저

	명령 또는 동작	목적
단계 1	Cisco AXL 웹 서비스 활성화, 83 페이지	Cisco AXL 웹 서비스가 퍼블리셔 노드에서 활성화되어 있는지 확인합니다.
단계 2	비디오에 대한 최대 세션 비트 레이트 구성, 83 페이지	선택 사항. 모바일 및 원격 액세스 엔드포인트에 대한 지역별 설정을 구성합니다. 예를 들어, 모바일 및 원격 액세스 엔드포인트에서 비디오를 사용할 것으로 예상되는 경우 기본 설정인 384 kbps는 일부 비디오 엔드포인트에 대해 너무 낮을 수 있으므로 영상 통화에 대한 최대 세션 비트 속도 설정을 증가시킬 수 있습니다.
단계 3	모바일 및 원격 액세스를 위한 디바이스폴 구성, 84 페이지	모바일 및 원격 액세스 엔드포인트에서 사용하는 디바이스폴에 날짜/시간 그룹 및 지역 구성을 할당합니다.
단계 4	ICE 구성, 85 페이지	선택 사항. ICE는 STUN 및 TURN 서비스를 사용하여 모바일 및 원격 액세스 통화에서 사용할 수 있는 미디어 경로를 분석하고 최적의 경로를 선택하는 선택적 배포입니다. ICE는 통

	명령 또는 동작	목적
		화 설정 시간에 잠재적으로 추가되지만 모바일 및 원격 액세스 통화의 신뢰성이 향상됩니다.
단계 5	모바일 및 원격 액세스용 전화기 보안 프로파일 구성, 86 페이지	이 절차를 사용하여 모바일 및 원격 액세스 엔드포인트에서 사용할 전화기 보안 프로파일을 설정합니다.
단계 6	Cisco Jabber 사용자에게 대한 모바일 및 원격 액세스 액세스 정책 구성, 86 페이지	Cisco Jabber만 해당. Cisco Jabber 사용자에게 대한 모바일 및 원격 액세스 액세스 정책을 설정합니다. 모바일 및 원격 액세스 기능을 사용하려면 사용자 프로파일 내에서 Cisco Jabber 사용자의 모바일 및 원격 액세스를 활성화해야 합니다.
단계 7	모바일 및 원격 액세스를 위한 사용자 구성, 88 페이지	Cisco Jabber 사용자의 경우 설정하는 사용자 정책이 최종 사용자 구성에 적용되어야 합니다.
단계 8	모바일 및 원격 액세스를 위한 엔드포인트 구성, 88 페이지	모바일 및 원격 액세스 기능을 사용하는 엔드포인트를 구성하고 프로비전합니다.
단계 9	모바일 및 원격 액세스를 위한 Cisco Expressway 구성, 88 페이지	모바일 및 원격 액세스를 위해 Cisco Expressway를 구성합니다.

Cisco AXL 웹 서비스 활성화

Cisco AXL 웹 서비스가 퍼블리셔 노드에서 활성화되어 있는지 확인합니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. 도구 > 서비스 활성화.

단계 2 서버 드롭다운 목록에서 퍼블리셔 노드를 선택하고 이동을 클릭합니다.

단계 3 데이터베이스 및 관리 서비스에서 **Cisco AXL** 웹 서비스가 활성화되었는지 확인합니다.

단계 4 서비스가 활성화되지 않은 경우 해당 확인란을 선택하고 저장을 클릭하여 서비스를 활성화합니다.

비디오에 대한 최대 세션 비트 레이트 구성

모바일 및 원격 액세스 엔드포인트에 대한 지역 설정을 구성합니다. 대부분의 경우 기본 설정으로 충분하지만, 모바일 및 원격 액세스 엔드포인트에서 비디오를 사용하는 것으로 예상되는 경우 지역 구

성 내에서 영상 통화에 대한 최대 세션 비트 레이트를 증가시킬 수 있습니다. 기본 설정인 384kbps가 일부 비디오 엔드포인트(예: DX 시리즈)에 비해 너무 낮을 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 지역 정보 > 지역.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 지역을 선택하여 기존 지역 내의 비트 레이트를 편집합니다.
- 새로 추가를 클릭하여 새 지역을 생성합니다.

단계 3 다른 지역에 대한 관계 수정 영역에서 영상 통화에 대한 최대 세션 비트 레이트에 대한 새 설정을 구성합니다. 예를 들어, 6000kbps가 있습니다.

단계 4 지역 구성 창에서 다른 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오..

단계 5 저장을 클릭합니다.

모바일 및 원격 액세스를 위한 디바이스폴 구성

새 지역을 만들 때 모바일 및 원격 액세스 엔드포인트에서 사용하는 디바이스폴에 지역을 할당합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 디바이스폴.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 편집할 기존 디바이스폴을 선택합니다.
- 새로 추가를 클릭하여 새 디바이스 폴을 만듭니다.

단계 3 디바이스 폴 이름을 입력합니다.

단계 4 중복 Cisco Unified Communications Manager 그룹을 선택합니다.

단계 5 설정하는 날짜/시간 그룹을 할당합니다. 이 그룹에는 모바일 및 원격 액세스 엔드포인트에 대해 설정된 전화기 NTP 참조가 포함되어 있습니다.

단계 6 지역 드롭다운 목록에서 모바일 및 원격 액세스를 위해 구성한 지역을 선택합니다.

단계 7 디바이스 폴 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 8 저장을 클릭합니다.

ICE 구성

이 절차는 사용자가 모바일 및 원격 액세스 통화에 대한 통화 설정을 처리하도록 ICE를 구축하려는 경우에 사용됩니다. ICE는 STUN 및 TURN 서비스를 사용하여 모바일 및 원격 액세스 통화에 사용할 수 있는 미디어 경로를 분석하고 최적의 경로를 선택하는 선택적 배포입니다. ICE는 통화 설정 시간에 잠재적으로 추가되지만 모바일 및 원격 액세스 통화의 신뢰성이 향상됩니다.

시작하기 전에

ICE를 구축하는 방법을 결정합니다. 일반 전화 프로파일 구성, 개별 Cisco Jabber 데스크톱 디바이스 또는 모든 전화기에 적용되는 시스템 수준 기본값을 통해 전화기 그룹에 대한 ICE를 구성할 수 있습니다.

ICE는 대체 메커니즘으로 TURN 서버를 사용하여 미디어를 릴레이할 수 있습니다. TURN 서버를 구축했는지 확인합니다.

프로시저

단계 1 Cisco Unified CM 관리에서:

- 시스템 > 엔터프라이즈 전화기를 선택하여 ICE에 대한 시스템 기본값을 구성합니다.
- 디바이스 > 디바이스 설정 > 일반 전화 프로파일 을 선택하여 엔드포인트 그룹에 대한 ICE를 구성하고 편집할 프로파일을 선택합니다.
- 디바이스 > 전화기를 선택하여 개별 Cisco Jabber 데스크톱 엔드포인트에 대한 ICE를 구성하고 편집할 엔드포인트를 선택합니다.

단계 2 ICE(상호 연결 설정) 섹션까지 아래로 스크롤합니다.

단계 3 ICE 드롭다운 목록을 활성화됨으로 설정합니다.

단계 4 기본 후보 유형을 설정합니다.

- 호스트—호스트 디바이스에서 IP 주소를 선택하여 가져온 후보입니다. 이것이 기본값입니다.
- 서버 재귀—STUN 요청을 전송하여 가져온 IP 주소 및 포트 후보입니다. 대부분의 경우 이것은 NAT의 공용 IP 주소를 나타낼 수 있습니다.
- **Relayed**—TURN 서버에서 가져온 IP 주소 및 포트 후보입니다. IP 주소 및 포트는 해당 미디어가 TURN 서버를 통해 릴레이될 수 있도록 TURN 서버에 상주합니다.

단계 5 서버 재귀 주소 드롭다운 목록에서 이 필드를 활성화됨 또는 비활성화됨으로 설정하여 STUN와 유사한 서비스를 활성화할 지 여부를 선택합니다. 서버 재귀를 기본 후보로 구성한 경우 이 필드를 활성화로 설정해야 합니다.

단계 6 기본 및 보조 TURN 서버에 대한 IP 주소 또는 호스트 이름을 입력합니다.

단계 7 TURN 서버 전송 유형을 자동(기본 설정), UDP, TCP 또는 TLS로 설정합니다.

단계 8 TURN 서버의 사용자 이름 및 암호를 입력합니다.

단계 9 저장을 클릭합니다.

참고 일반 전화 프로파일에 대해 ICE를 구성한 경우 전화기가 프로파일을 사용할 수 있도록 일반 전화 프로파일에 연결해야 합니다. 전화기 구성 창을 사용하여 전화기에 프로파일을 적용할 수 있습니다.

모바일 및 원격 액세스용 전화기 보안 프로파일 구성

이 절차를 사용하여 모바일 및 원격 액세스 엔드포인트에서 사용할 전화기 보안 프로파일을 설정합니다.

프로시저

- 단계 1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 보안 > 전화기 보안 프로파일.
- 단계 2** 새로 추가를 클릭합니다.
- 단계 3** 전화기 보안 프로파일 유형 드롭다운 목록에서 디바이스 유형을 선택합니다. 예를 들어, Jabber 애플리케이션에 대한 **Cisco Unified Client Service Framework**를 선택할 수 있습니다.
- 단계 4** 다음을 클릭합니다.
- 단계 5** 프로파일의 이름을 입력합니다. 모바일 및 원격 액세스의 경우 이름은 FQDN 형식이어야 하며 엔터프라이즈 도메인을 포함해야 합니다.
- 단계 6** 디바이스 보안 모드 드롭다운 목록에서 암호화를 선택합니다.

참고 이 필드는 암호화됨으로 설정해야 합니다. 그렇지 않으면 Expressway가 통신을 거부합니다.
- 단계 7** 전송 유형을 **TLS**로 설정합니다.
- 단계 8** 이 옵션을 활성화한 경우 전화기에 모바일 및 원격 액세스가 작동하지 않으므로 DX 시리즈, IP 전화기 7800 또는 IP 전화기 8811, 8841, 8845, 8861 및 8865 전화기에 대한 **TFTP** 암호화 구성 확인란을 선택하지 않은 상태로 둡니다.
- 단계 9** 전화기 보안 프로파일 구성 창에서 남아 있는 필드를 완료해야 합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 10** 저장을 클릭합니다.

참고 모바일 및 원격 액세스 엔드포인트 각각에 대한 전화기 구성에 이 프로파일을 적용해야 합니다.

Cisco Jabber 사용자에게 대한 모바일 및 원격 액세스 액세스 정책 구성

이 절차를 사용하여 Cisco Jabber 사용자에게 대한 모바일 및 원격 액세스 액세스 정책을 설정합니다. 모바일 및 원격 액세스 기능을 사용하려면 사용자 프로파일 내에서 Cisco Jabber 사용자의 모바일 및 원

격 액세스를 활성화해야 합니다. Cisco Jabber에서 지원되는 모바일 및 원격 액세스 정책에 대한 최소 Expressway 릴리스는 X8.10입니다.



참고 비 Jabber 사용자에게는 모바일 및 원격 액세스 정책이 필요하지 않습니다.

사용자 프로파일에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "사용자 프로파일 개요" 섹션을 참조하십시오.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 사용자 설정 > 사용자 프로파일.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 사용자 프로파일의 이름 및 설명을 입력합니다.
- 단계 4 사용자의 데스크폰, 모바일 및 데스크탑 디바이스 및 원격 대상/디바이스 프로파일에 적용할 유니버설 디바이스 템플릿을 할당합니다.
- 단계 5 이 사용자 프로파일의 사용자에게 대한 전화 회선에 적용할 범용 회선 템플릿을 할당합니다.
- 단계 6 이 사용자 프로파일의 사용자가 자신의 전화기를 프로비저닝하는 데 셀프 프로비저닝 기능을 사용할 있도록하려면 다음을 수행합니다.
 - a) 최종 사용자에게 자신의 전화기 프로비저닝 허용 확인란을 선택합니다.
 - b) 최종 사용자가 이렇게 많은 전화기를 가지고 있으면 프로비저닝 제한 필드에 사용자가 프로비저닝하도록 허용되는 전화기의 최대 수를 입력합니다. 최대값은 20입니다.
 - c) 다른 엔드 유저에게 이미 할당된 전화의 프로비저닝 허용 확인란에 체크 표시하여 이 프로파일에 연결된 사용자에게 이미 다른 사용자가 소유하는 디바이스를 마이그레이션 또는 재할당할 권한이 있는지 여부를 결정합니다. 기본값으로 이 확인란은 선택되어 있지 않습니다.
- 단계 7 이 사용자 프로파일과 연결된 Cisco Jabber 사용자가 모바일 및 원격 액세스 기능을 사용할 수 있도록하려면 모바일 및 원격 액세스 활성화 확인란에 체크 표시합니다.

참고

 - 기본적으로 이 확인란은 선택되어 있습니다. 이 확인란의 체크 표시를 취소하면 클라이언트 정책 섹션이 비활성화되고 기본값으로 서비스 클라이언트 없음 정책 옵션이 선택됩니다.
 - 이 설정은 OAuth 새로 고침 로그인을 사용하는 Cisco Jabber 사용자의 경우에만 필수입니다. 비 Jabber 사용자는 이 설정이 없어도 모바일 및 원격 액세스를 사용할 수 있습니다. 모바일 및 원격 액세스 기능은 Jabber 모바일 및 원격 액세스 사용자에게 대해서만 적용 가능하며, 다른 엔드포인트 또는 클라이언트에게는 적용되지 않습니다.
- 단계 8 이 사용자 프로파일에 대해 Jabber 정책을 할당합니다. 데스크톱 클라이언트 정책 및 모바일 클라이언트 정책 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
 - 서비스 없음 - 이 정책은 모든 Cisco Jabber 서비스에 대한 액세스를 비활성화합니다.
 - IM & 프레즌스만 해당—이 정책은 인스턴트 메시징 및 프레즌스 기능을 활성화합니다.

- IM & 프레즌스, 음성 및 영상 통화—이 정책은 음성 또는 영상 디바이스가 있는 모든 사용자에게 대해 인스턴트 메시징, 프레즌스, 음성 메일 및 전화 회의 기능을 활성화합니다. 이것이 기본 옵션입니다.

참고 Jabber 데스크톱 클라이언트는 Windows용 Cisco Jabber와 Mac용 Cisco Jabber 사용자를 포함합니다. Jabber 모바일 클라이언트는 iPad 및 iPhone용 Cisco Jabber 사용자와 Android용 Cisco Jabber 사용자를 포함합니다.

단계 9 사용자가 Unified Communications 셀프 서비스 포털을 통해 내선 이동 또는 인터클러스터 내선 이동에 대한 최대 로그인 시간을 설정하도록 허용하려면 엔드 유저가 내선 이동을 최대 로그인 시간을 설정하도록 허용 확인란에 체크 표시합니다.

참고 기본적으로 최종 사용자가 **Extension Mobility**를 최대 로그인 시간을 설정하도록 허용 확인란은 선택 해제되어 있습니다.

단계 10 저장을 클릭합니다.

모바일 및 원격 액세스를 위한 사용자 구성

Cisco Jabber 사용자의 경우, 구성하는 모바일 및 원격 액세스 액세스 정책이 LDAP 동기화 중에 Cisco Jabber 사용자에게 연결되어 있어야 합니다. 최종 사용자를 프로비저닝하는 방법에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "최종 사용자 구성" 섹션을 참조하십시오.

모바일 및 원격 액세스를 위한 엔드포인트 구성

모바일 및 원격 액세스용 엔드포인트 프로비저닝 및 구성:

- Cisco Jabber 클라이언트의 경우 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "Cisco Jabber 구성 작업 흐름" 섹션을 참조하십시오.
- 다른 엔드포인트의 경우 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "엔드포인트 디바이스 구성" 섹션을 참조하십시오.

모바일 및 원격 액세스를 위한 Cisco Expressway 구성

모바일 및 원격 액세스를 위해 Cisco Expressway를 구성하는 방법에 대한 자세한 내용은 [Cisco Expressway를 통한 모바일 및 원격 액세스 구축 설명서](#)를 참조하십시오.

경량 Keepalive를 통한 MRA 페일오버

엔드포인트 등록에 대한 MRA 고가용성은 Cisco Webex 및 Cisco Jabber에서 등록 경로의 Cisco Expressway-E, Cisco Expressway-C 및 Cisco 통합 커뮤니케이션 매니저 관리 같은 네트워크 요소의 오

류를 감지하고 다음 사용 가능한 경로를 통해 Unified CM에 다시 등록하는 정정 작업을 수행할 수 있습니다.

엔드포인트는 등록 경로에서 연결을 확인할 수 있도록 경량 STUN keepalive 메시지를 보냅니다. Unified Communications Manager이 경량 STUN keepalive 메시지를 수신하면 Cisco Expressway-C IP의 유효성을 검사하고 메시지에 응답합니다. 다른 IP에서 수신한 경우에는 Unified CM이 STUN keepalive 메시지를 삭제합니다.

등록 경로의 노드가 실패하는 경우 엔드포인트는 경량 STUN keepalive 응답을 통해 오류를 학습하고 향후 메시지에 대해 다른 라우트 경로를 선택합니다. 이 서비스를 사용하면 중단 또는 기타 유지 보수 모드와 관계 없이 사용자가 원활하고 지속적인 수신 및 발신 통화를 할 수 있습니다.

Cisco Webex 또는 Cisco Jabber가 Unified Communications Manager에 MRA 디바이스로 등록하면 시스템은 Unified CM(디바이스 > 전화기 > **IPv4** 주소 열)에 Expressway-C의 IP를 표시합니다.



참고 Cisco IP 전화기는 등록 페일오버를 지원하지 않습니다.

자세한 내용은 [Cisco Expressway를 통한 모바일 및 원격 액세스 구축 설명서](#)를 참조하십시오.



III 부

원격 네트워크 액세스

- 무선랜, 93 페이지
- VPN 클라이언트, 97 페이지



9 장

무선랜

- 무선 LAN 개요, 93 페이지
- 무선 LAN 구성 작업 흐름, 93 페이지

무선 LAN 개요

이 기능은 사용자가 전화기에서 WiFi 매개 변수를 구성하지 않아도 됩니다. WiFi 프로파일을 구성할 수 있습니다. 그러면 디바이스에서 시스템의 WiFi 구성을 자동으로 다운로드하여 적용할 수 있습니다. VPN 연결 및 HTTP 프록시 설정과 관련된 추가 보안 계층이 포함된 네트워크 접속 프로파일을 구성할 수 있습니다.

무선 LAN 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	무선 LAN 프로파일이 있는 디바이스를 식별하는 보고서를 생성합니다.
단계 2	네트워크 액세스 프로파일 구성, 94 페이지	옵션: 무선 LAN 프로파일에 연결할 수 있는 VPN 및 HTTP 프록시 설정을 구성하려면 네트워크 액세스 프로파일을 구성합니다.
단계 3	무선 LAN 프로파일 구성, 94 페이지	엔터프라이즈의 디바이스 또는 디바이스풀에 적용되도록 일반 WiFi 설정을 사용하여 무선 LAN 프로파일을 구성합니다.
단계 4	무선 LAN 프로파일 그룹 구성, 94 페이지	무선 LAN 프로파일을 함께 그룹화합니다.
단계 5	무선 LAN 프로파일 그룹을 디바이스 또는 디바이스풀에 연결, 95 페이지에 대해 다음 하위 작업을 수행합니다.	디바이스 연결을 완료한 이후에는 TFTP가 무선 LAN 프로파일 그룹을 기존 디바이스 구성 파일에 추가하여 디바이스(또는 디바이스풀

	명령 또는 동작	목적
	<ul style="list-style-type: none"> 무선 LAN 프로파일 그룹을 디바이스에 연결, 95 페이지 무선 LAN 프로파일 그룹을 디바이스폴에 연결합니다., 95 페이지 	에 연결된 디바이스)에서 다운로드가 진행됩니다.

네트워크 액세스 프로파일 구성

무선 LAN 프로파일에 연결할 수 있는 VPN 및 HTTP 프록시 설정을 구성하려면 네트워크 액세스 프로파일을 구성합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 네트워크 액세스 프로파일.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 네트워크 액세스 프로파일 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 4 저장을 클릭합니다.

무선 LAN 프로파일 구성

엔터프라이즈의 디바이스 또는 디바이스폴에 적용되도록 일반 WiFi 설정을 사용하여 무선 LAN 프로파일을 구성합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 무선 LAN 프로파일
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 무선 LAN 프로파일 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 4 저장을 클릭합니다.

무선 LAN 프로파일 그룹 구성

무선 LAN 프로파일을 그룹화합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 무선 LAN 프로파일 그룹.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 무선 LAN 프로파일 그룹 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 4 저장을 클릭합니다.

무선 LAN 프로파일 그룹을 디바이스 또는 디바이스풀에 연결

디바이스 연결을 완료한 이후에는 TFTP가 무선 LAN 프로파일 그룹을 기존 디바이스 구성 파일에 추가하여 디바이스(또는 디바이스풀에 연결된 디바이스)에서 다운로드가 진행됩니다.

프로시저

	명령 또는 동작	목적
단계 1	무선 LAN 프로파일 그룹을 디바이스에 연결, 95 페이지	
단계 2	무선 LAN 프로파일 그룹을 디바이스풀에 연결합니다., 95 페이지	

무선 LAN 프로파일 그룹을 디바이스에 연결

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 다음 작업 중 하나를 수행합니다.
- 찾기를 클릭하여 검색 기준을 입력하고 결과 목록에서 기존 디바이스를 선택합니다.
 - 새로 추가를 클릭하고 전화기 유형 드롭다운 목록에서 디바이스 유형을 선택합니다.
- 단계 3 무선 LAN 프로파일 그룹 드롭다운 목록에서 생성한 무선 LAN 프로파일 그룹을 선택합니다.
- 단계 4 저장을 클릭합니다.

무선 LAN 프로파일 그룹을 디바이스풀에 연결합니다.

디바이스 및 디바이스풀 수준에서 무선 LAN 프로파일 그룹을 연결하는 경우 시스템에서 디바이스풀 설정을 사용합니다.

무선 **LAN** 프로파일 그룹을 디바이스폴에 연결합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 디바이스폴.

단계 **2** 다음 작업 중 하나를 수행합니다.

- 찾기를 클릭하여 검색 기준을 입력하고 결과 목록에서 기존 디바이스폴을 선택합니다.
- 새로 추가를 클릭합니다.

단계 **3** 무선 **LAN** 프로파일 그룹 드롭다운 목록에서 생성한 무선 LAN 프로파일 그룹을 선택합니다.

단계 **4** 저장을 클릭합니다.



10 장

VPN 클라이언트

- VPN 클라이언트 개요, 97 페이지
- VPN 클라이언트 사전 요건, 97 페이지
- VPN 클라이언트 구성 작업 흐름, 97 페이지

VPN 클라이언트 개요

Cisco Unified IP Phone의 Cisco VPN 클라이언트는 재택 근무하는 직원에 대한 보안 VPN 연결을 생성합니다. Cisco VPN 클라이언트의 모든 설정은 Cisco 통합 커뮤니케이션 매니저 관리를 통해 구성됩니다. 엔터프라이즈 내에서 전화기를 구성한 후에는 사용자가 인스턴트 연결을 위해 해당 디바이스를 광대역 라우터에 연결할 수 있습니다.



참고 Unified Communications Manager의 미국 수출 무제한 버전에서는 VPN 메뉴 및 관련 옵션을 사용할 수 없습니다.

VPN 클라이언트 사전 요건

전화기를 사전 준비하고 회사 네트워크 내에서 초기 연결을 설정하여 전화기 구성을 검색합니다. 전화기에서 구성이 이미 검색되었으므로 VPN을 사용하여 후속 연결을 설정할 수 있습니다.

VPN 클라이언트 구성 작업 흐름

전화기를 사전 준비하고 회사 네트워크 내에서 초기 연결을 설정하여 전화기 구성을 검색합니다. 전화기에서 구성이 이미 검색되었으므로 VPN을 사용하여 후속 연결을 설정할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	전체 Cisco IOS 사전 요건, 99 페이지	전체 Cisco IOS 사전 요건 Cisco IOS VPN을 구성하려는 경우 이 작업을 수행합니다.
단계 2	IP 전화기를 지원하도록 Cisco IOS SSL VPN 구성, 99 페이지	IP 전화기에서 VPN 클라이언트용 Cisco IOS를 구성합니다. Cisco IOS VPN을 구성하려는 경우 이 작업을 수행합니다.
단계 3	AnyConnect에 대한 전체 ASA 사전 요건, 101 페이지	AnyConnect에 대한 전체 ASA 사전 요건 ASA VPN을 구성하려면 이 작업을 수행합니다.
단계 4	IP 전화기에서 VPN 클라이언트에 대한 ASA 구성, 102 페이지	IP 전화기에서 VPN 클라이언트에 대한 ASA를 구성합니다. ASA VPN을 구성하려면 이 작업을 수행합니다.
단계 5	각 VPN 게이트웨이에 대한 VPN 집중 디바이스를 구성합니다.	사용자가 원격 전화기에서 펌웨어 또는 구성 정보를 업그레이드할 때 오랜 지연이 발생하지 않도록 하려면 네트워크에서 TFTP 또는 Unified Communications Manager 서버에 VPN 집중 디바이스 단기를 설정합니다. 네트워크에서 이 방법이 적합하지 않은 경우에는 VPN 집중 디바이스 옆에 있는 대체 TFTP 또는 로드 서버를 설정할 수 있습니다.
단계 6	VPN 집중 디바이스 인증서 업로드, 104 페이지	VPN 집중 디바이스 인증서를 업로드합니다.
단계 7	VPN 게이트웨이 구성, 105 페이지	VPN 게이트웨이를 구성합니다.
단계 8	VPN 그룹 구성, 106 페이지	VPN 그룹을 만든 후에는 방금 구성한 VPN 게이트웨이 중 하나를 여기 추가할 수 있습니다.
단계 9	다음 중 하나를 수행합니다. • VPN 프로파일 구성, 107 페이지 • VPN 기능 매개 변수 구성, 108 페이지	여러 VPN 그룹이 있는 경우에만 VPN 프로파일을 구성해야 합니다. VPN 프로파일 필드는 VPN 기능 구성 필드보다 우선합니다.
단계 10	일반 전화 프로파일에 VPN 세부 정보 추가, 110 페이지	VPN 그룹 및 VPN 프로파일을 일반 전화 프로파일에 추가합니다.
단계 11	VPN을 지원하는 버전으로 Cisco Unified IP Phone의 펌웨어를 업그레이드합니다.	Cisco VPN 클라이언트를 실행하려면 지원되는 Cisco Unified IP Phone에서 펌웨어 릴리스 9.0(2) 이상을 실행하고 있어야 합니다. 펌웨어 업그레이드에 대한 자세한 내용은 해당 Cisco Unified IP Phone 모델에 대한 Unified Communications Manager의 <i>Cisco Unified IP Phone</i> 관리 지침서를 참조하십시오.

	명령 또는 동작	목적
단계 12	지원되는 Cisco Unified IP Phone을 사용하여 VPN 연결을 설정합니다.	Cisco Unified IP Phone을(를) VPN에 연결합니다.

전체 Cisco IOS 사전 요건

이 절차를 사용하여 Cisco IOS 사전 요건을 완료합니다.

프로시저

단계 1 Cisco IOS 소프트웨어 버전 15.1(2)T 이상을 설치합니다.

기능 집합/라이선스: IOS ISR-G2 및 ISR-G3에 대한 유니버설(데이터와 보안 및 UC)

기능 집합/라이선스: IOS ISR에 대한 고급 보안

단계 2 SSL VPN 라이선스를 활성화합니다.

IP 전화기를 지원하도록 Cisco IOS SSL VPN 구성

이 절차를 사용하여 IP 전화기를 지원하기 위해 Cisco IOS SSL VPN을 완료할 수 있습니다.

프로시저

단계 1 Cisco IOS를 로컬로 구성합니다.

a) 네트워크 인터페이스를 구성합니다.

예:

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b) 다음 명령을 사용하여 정적 및 기본 라우트를 구성합니다.

```
router(config)# ip route <dest_ip> <mask> <gateway_ip>
```

예:

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

단계 2 CAPF 인증서를 생성 및 등록하여 LSC를 사용하여 IP 전화기를 인증합니다.

단계 3 Unified Communications Manager에서 CAPF 인증서를 가져옵니다.

- a) Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

참고 이 위치는 Unified Communications Manager 버전을 기반으로 변경됩니다.

- b) Cisco_Manufacturing_CA 및 CAPF 인증서를 찾습니다. .pem 파일을 다운로드하고 .txt 파일로 저장합니다.
- c) Cisco IOS 소프트웨어에서 트러스트 포인트를 생성합니다.

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

Base64 인코딩 CA 인증서를 묻는 메시지가 나타나면 다운로드한 .pem 파일에 BEGIN 및 END 라인과 함께 텍스트를 복사하여 붙여넣습니다. 다른 인증서에 대해 절차를 반복합니다.

- d) 다음 Cisco IOS 자체 서명 인증서를 생성하고 Unified Communications Manager로 등록하거나 CA에서 가져오는 인증서로 대체합니다.

- SSC(자가서명 인증서)를 생성합니다.

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 2048 2048
Router(ca-trustpoint)# authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Unified Communications Manager의 VPN 프로파일에서 호스트 ID 확인을 활성화한 상태에서 SSC(자가서명 인증서)를 생성합니다.

예:

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain name>
Router(config-ca-trustpoint)# subject-name CN=<full domain name>, CN=<IP>
Router(ca-trustpoint)# authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- 생성된 인증서를 Unified Communications Manager에 등록합니다.

예:

```
Router(config)# crypto pki export <name> pem terminal
```

터미널에서 텍스트를 복사하여 .pem 파일로 저장하고 Cisco Unified OS 관리를 사용하여 Unified Communications Manager에 업로드합니다.

단계 4 Cisco IOS에 AnyConnect를 설치합니다.

cisco.com에서 Anyconnect 패키지를 다운로드하고 플래시에 설치합니다.

예:

```
router(config)#webvpn install svc
flash:/webvpn/anyconnect-win-2.3.2016-k9.pkg
```

단계 5 VPN 기능을 구성합니다.

참고 인증서 및 암호 인증과 함께 전화기를 사용하려면 전화기 MAC 주소를 사용하여 사용자를 만듭니다. 사용자 이름 일치는 대/소문자를 구분합니다. 예:

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxycO4ti9 encrypted
```

AnyConnect에 대한 전체 ASA 사전 요건

이 절차를 사용하여 AnyConnect에 대한 ASA 사전 요건을 완료합니다.

프로시저

단계 1 ASA 소프트웨어(버전 8.0.4 이상)와 호환되는 ASDM을 설치합니다.

단계 2 호환되는 AnyConnect 패키지를 설치합니다.

단계 3 라이선스를 활성화합니다.

a) 다음 명령을 사용하여 현재 라이선스의 기능을 확인합니다.

```
show activation-key detail
```

b) 필요한 경우 추가 SSL VPN 세션을 사용하여 새 라이선스를 받고 Linksys 전화기를 활성화합니다.

단계 4 다음과 같이 기본이 아닌 URL을 사용하여 터널 그룹을 구성해야 합니다.

```
tunnel-group phonevpn type remote-access
tunnel-group phonevpn general-attribute
address-pool vpnpool
tunnel-group phonevpn webvpn-attributes
group-url https://172.18.254.172/phonevpn enable
```

기본값이 아닌 URL을 구성하는 경우 다음 사항을 고려하십시오.

- 서버의 IP 주소에 공용 DNS 항목이 있는 경우 FQDN(정규화된 도메인 이름)으로 바꿀 수 있습니다.
- Unified Communications Manager의 VPN 게이트웨이에서는 단일 URL(FQDN 또는 IP 주소)만 사용할 수 있습니다.
- 인증서 CN 또는 주체 대체 이름이 group-url의 FQDN 또는 IP 주소와 일치하는 것이 좋습니다.
- ASA 인증서 CN 또는 SAN이 FQDN 또는 IP 주소와 일치하지 않으면 Unified Communications Manager에서 호스트 ID 확인란의 선택을 취소합니다.

IP 전화기에서 VPN 클라이언트에 대한 ASA 구성

이 절차를 사용하여 IP 전화기의 VPN 클라이언트에 대해 ASA를 구성합니다.



참고 ASA 인증서를 대체하면 Unified Communications Manager를 사용할 수 없게 됩니다.

프로시저

단계 1 로컬 구성

- a) 네트워크 인터페이스를 구성합니다.

예:

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

- b) 정적 경로 및 기본 경로를 구성합니다.

```
ciscoasa(config)# route <interface_name> <ip_address> <netmask> <gateway_ip>
```

예:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

- c) DNS를 구성합니다.

예:

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

단계 2 Unified Communications Manager 및 ASA에 필요한 인증서를 생성하고 등록합니다.

Unified Communications Manager에서 다음 인증서를 가져옵니다.

- CallManager - TLS 핸드셰이크 중 Cisco UCM을 인증합니다(혼합 모드 클러스터에만 필요).
- Cisco_Manufacturing_CA - 제조업체에서 설치한 인증서(MIC)를 사용하여 IP 전화기를 인증합니다.
- CAPF - LSC를 사용하여 IP 전화기를 인증합니다.

Unified Communications Manager 인증서를 가져오려면 다음을 수행합니다.

- Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
- 인증서 Cisco_Manufacturing_CA 및 CAPF를 찾습니다. .pem 파일을 다운로드하고, asa.txt 파일로 저장합니다.

- c) ASA에 트러스트 포인트를 만듭니다.

예:

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

Base 64 인코딩 CA 인증서를 입력하라는 메시지가 표시되면 다운로드한 .pem 파일의 텍스트를 BEGIN 및 END 줄과 함께 복사합니다. 다른 인증서에 대해 절차를 반복합니다.

- d) 다음의 ASA 자체 서명 인증서를 생성하고 이를 사용하여 Unified Communications Manager에 등록하거나 CA에서 가져오는 인증서로 대체합니다.

- SSC(자가서명 인증서)를 생성합니다.

예:

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# keypair <name>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Unified Communications Manager의 VPN 프로파일에서 호스트 ID 확인을 활성화한 상태에서 SSC(자가서명 인증서)를 생성합니다.

예:

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# fqdn <full domain name>
ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- 생성된 인증서를 Unified Communications Manager에 등록합니다.

예:

```
ciscoasa(config)# crypto ca export <name> identity-certificate
```

터미널에서 텍스트를 복사하여 .pem 파일로 저장하고 Unified Communications Manager에 업로드합니다.

단계 3 VPN 기능을 구성합니다. 아래 샘플 ASA 구성 요약을 사용하여 구성을 안내할 수 있습니다.

참고 인증서 및 암호 인증과 함께 전화기를 사용하려면 전화기 MAC 주소를 사용하여 사용자를 만듭니다. 사용자 이름 일치하는 대/소문자를 구분합니다. 예:

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9
encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)#service-type remote-access
```

ASA 인증서 구성

ASA 인증서 구성에 대한 자세한 내용은 [ASA에서 인증서 인증을 사용하여 Anyconnect VPN 전화기 구성](#)을 참조하십시오.

VPN 집중 디바이스 인증서 업로드

VPN 기능을 지원하도록 설정하는 경우에는 인증서가 ASA에서 생성됩니다. 생성된 인증서를 PC 또는 워크스테이션에 다운로드한 다음 Unified Communications Manager가 이 섹션의 절차를 사용하여 업로드합니다. Unified Communications Manager는 전화기-VPN-신뢰 목록에 인증서를 저장합니다.

ASA는 이 인증서를 SSL 핸드셰이크 중에 전송되며, Cisco Unified IP Phone은 이 인증서를 전화기-VPN-신뢰 목록에 저장된 값과 비교합니다.

LSC (로컬 중요 인증서)가 Cisco Unified IP Phone에 설치된 경우 LSC가 기본적으로 전송됩니다.

디바이스 수준 인증서 인증을 사용하려면 Cisco Unified IP Phone를 신뢰할 수 있도록 ASA에 루트 MIC 또는 CAPF 인증서를 설치합니다.

Unified Communications Manager에 인증서를 업로드하려면 Cisco 통합 OS 관리를 사용하십시오.

프로시저

단계 1 Cisco Unified OS 관리에서 다음을 선택합니다보안 > 인증서 관리.

단계 2 인증서 업로드를 클릭합니다.

단계 3 인증서 용도 드롭다운 목록에서 전화기-VPN-신뢰를 선택합니다.

단계 4 찾아보기를 클릭하여 업로드할 파일을 선택합니다.

단계 5 파일 업로드를 클릭합니다.

단계 6 업로드할 다른 파일을 선택하거나 단기를 클릭합니다.

자세한 내용은 인증서 관리 장을 참조하십시오.

VPN 게이트웨이 구성

각 VPN 게이트웨이에 대해 VPN 집중 디바이스를 구성했는지 확인합니다. VPN 집중 디바이스를 구성한 후 VPN 집중 디바이스 인증서를 업로드합니다. 자세한 내용은 [VPN 집중 디바이스 인증서 업로드, 104 페이지](#)의 내용을 참조하십시오.

이 절차를 사용하여 VPN 프로파일을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > **VPN** > **VPN 게이트웨이**

단계 2 다음 작업 중 하나를 수행합니다.

- a) 새로 추가를 클릭하여 새 프로파일을 구성합니다.
- b) 복사하려는 VPN 게이트웨이 옆에 있는 복사를 클릭합니다.
- c) 적절한 VPN 게이트웨이를 찾고 설정을 수정하여 기존 프로파일을 업데이트합니다.

단계 3 **VPN** 게이트웨이 구성 창에서 필드를 구성합니다. 자세한 내용은 [VPN 클라이언트용 VPN 게이트웨이 필드, 105 페이지](#)의 내용을 참조하십시오.

단계 4 저장을 클릭합니다.

VPN 클라이언트용 VPN 게이트웨이 필드

이 표는 VPN 클라이언트에 대한 VPN 게이트웨이 필드를 설명합니다.

표 11: VPN 클라이언트용 VPN 게이트웨이 필드

필드	설명
VPN 게이트웨이 이름	VPN 게이트웨이의 이름을 입력합니다.
VPN 게이트웨이 설명	VPN 게이트웨이에 대한 설명을 입력합니다.
VPN 게이트웨이 URL	<p>게이트웨이의 기본 VPN 집중기에 대한 URL을 입력합니다.</p> <p>참고 그룹 URL을 사용하여 VPN 집중기를 구성하고 이 URL을 게이트웨이 URL로 사용해야 합니다.</p> <p>구성 정보는 다음과 같은 VPN 집중기에 대한 설명서를 참조하십시오.</p> <ul style="list-style-type: none"> • ASDM을 사용하여 ASA에 SVC(SSL VPN 클라이언트) 구성 예제

필드	설명
이 게이트웨이의 VPN 인증서	위쪽 및 아래쪽 화살표 키를 사용하여 게이트웨이에 인증서를 할당합니다. 게이트웨이에 대한 인증서를 할당하지 않으면 VPN 클라이언트가 해당 집중기에 연결하는 데 실패합니다. 참고 VPN 게이트웨이에 최대 10개의 인증서를 할당할 수 있으며 각 게이트웨이에 하나 이상의 인증서를 할당해야 합니다. 전화기-VPN-신뢰 역할과 연결된 인증서만 사용 가능한 VPN 인증서 목록에 표시됩니다.

VPN 그룹 구성

이 절차를 사용하여 VPN 그룹을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > VPN > VPN 그룹

단계 2 다음 작업 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 프로파일을 구성합니다.
- 기존 VPN 그룹을 복사할 VPN 그룹 옆에 있는 복사를 클릭합니다.
- 적절한 VPN 그룹을 찾고 설정을 수정하여 기존 프로파일을 업데이트합니다.

단계 3 VPN 그룹 구성 창에서 필드를 구성합니다. 자세한 내용은 [VPN 클라이언트용 VPN 게이트웨이 필드, 105 페이지](#)의 필드 설명 세부 정보를 참조하십시오.

단계 4 저장을 클릭합니다.

VPN 클라이언트용 VPN 그룹 필드

이 표는 VPN 클라이언트에 대한 VPN 그룹 필드를 설명합니다.

표 12: VPN 클라이언트용 VPN 그룹 필드

필드	정의
VPN 그룹 이름	VPN 그룹의 이름을 입력합니다.
VPN 그룹 설명	VPN 그룹에 대한 설명을 입력합니다.
사용 가능한 모든 VPN 게이트웨이	스크롤하여 사용 가능한 모든 VPN 게이트웨이를 확인합니다.

필드	정의
이 VPN 그룹에서 선택한 VPN 게이트웨이	위쪽 및 아래쪽 화살표 버튼을 사용하여 사용 가능한 VPN 게이트웨이를 이 VPN 그룹의 내부 및 외부로 이동합니다. VPN 클라이언트에 심각한 오류가 발생하고 특정 VPN 게이트웨이에 연결할 수 없는 경우 목록에 있는 다음 VPN 게이트웨이로 이동하려고 시도합니다. 참고 최대 3개의 VPN 게이트웨이를 VPN 그룹에 추가할 수 있습니다. 또한 VPN 그룹의 총 인증서 수는 10개를 초과할 수 없습니다.

VPN 프로파일 구성

이 절차를 사용하여 VPN 프로파일을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > VPN > VPN 프로파일

단계 2 다음 작업 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 프로파일을 구성합니다.
- 기존 프로파일을 복사하려는 VPN 프로파일 옆에 있는 복사를 클릭합니다.
- 기존 프로파일을 업데이트하려면 VPN 프로파일 위치 찾기에서 해당 필터를 지정하고 찾기를 클릭한 다음 설정을 수정합니다.

단계 3 VPN 프로파일 구성 창에서 필드를 구성합니다. 자세한 내용은 [VPN 클라이언트용 VPN 프로파일 필드, 107 페이지](#)의 필드 설명 세부 정보를 참조하십시오.

단계 4 저장을 클릭합니다.

VPN 클라이언트용 VPN 프로파일 필드

이 표는 VPN 프로파일 필드 세부 정보를 설명합니다.

표 13: VPN 프로파일 필드 세부 정보

필드	정의
이름	VPN 프로파일의 이름을 입력합니다.
설명	VPN 프로파일에 대한 설명을 입력합니다.

필드	정의
자동 네트워크 감지 활성화	이 확인란을 선택하는 경우 VPN 클라이언트가 회사 네트워크 외부에 있다는 것을 감지하는 경우에만 실행될 수 있습니다. 기본값: 비활성화됨
MTU	MTU(최대 전송 단위) 크기(바이트)를 입력합니다. 기본값: 1290바이트
연결 실패	이 필드는 시스템이 VPN 터널을 생성하는 동안 로그인 또는 연결 작업이 완료될 때까지 기다리는 시간을 지정합니다. 기본값: 30초
호스트 ID 확인 활성화	이 확인란을 선택하는 경우 게이트웨이 인증서 subjectAltName 또는 CN이 VPN 클라이언트가 연결된 URL과 일치해야 합니다. 기본값: 활성화됨
클라이언트 인증 방법	드롭다운 목록에서 클라이언트 인증 방법을 선택합니다. <ul style="list-style-type: none"> • 사용자 및 암호 • 암호 전용 • 인증서(LSC 또는 MIC)
암호 지속성 활성화	이 확인란을 선택하면 실패한 로그인 시도가 발생하거나, 사용자가 수동으로 암호를 지우거나, 전화기가 재설정되거나, 전화기 전원이 유실될 때까지 사용자 암호가 전화기에 저장됩니다.

VPN 기능 매개 변수 구성

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > **VPN** > **VPN 기능 구성**.

단계 2 **VPN 그룹 구성** 창에서 필드를 구성합니다. 자세한 내용은 [VPN 기능 파라미터, 109 페이지](#)의 내용을 참조하십시오.

단계 3 저장을 클릭합니다.

다음 작업을 수행하십시오.

- Cisco Unified IP Phone에 대한 펌웨어를 VPN을 지원하는 버전으로 업그레이드합니다. 펌웨어 업그레이드에 대한 자세한 내용은 해당 Cisco Unified IP Phone 모델에 대한 *Cisco Unified IP Phone* 관리 지침서를 참조하십시오.

- 지원되는 Cisco Unified IP Phone을 사용하여 VPN 연결을 설정합니다.

VPN 기능 파라미터

이 표는 VPN 기능 파라미터를 설명합니다.

표 14: VPN 기능 파라미터

필드	기본값
자동 네트워크 감지 활성화	참이면 VPN 클라이언트가 회사 네트워크 외부에 있다는 것을 감지하는 경우에만 실행될 수 있습니다. 기본값: 거짓
MTU	이 필드는 최대 전송 단위를 지정합니다. 기본값: 1290바이트 최소값: 256바이트 최대값: 1406바이트
연결 유지	이 필드는 시스템이 연결 유지 메시지를 전송하는 레이트를 지정합니다. 참고 0이 아니고 Unified Communications Manager에 지정된 값보다 작은 경우 VPN 집중기의 연결 유지 설정이 이 설정을 덮어씁니다. 기본값: 60초 최소값: 0 최대값: 120초
연결 실패	이 필드는 시스템이 VPN 터널을 생성하는 동안 로그인 또는 연결 작업이 완료될 때까지 기다리는 시간을 지정합니다. 기본값: 30초 최소값: 0 최대값: 600초

필드	기본값
클라이언트 인증 방법	드롭다운 목록에서 클라이언트 인증 방법을 선택합니다. <ul style="list-style-type: none"> • 사용자 및 암호 • 암호 전용 • 인증서(LSC 또는 MIC) 기본값: 사용자 및 암호
암호 지속성 활성화	참(True)일 때 사용자 암호는 전화기에 저장됩니다(재설정 버튼 또는 “***#”가 재설정에 사용되는 경우). 전화기의 전원이 끊기거나 공장 재설정을 초기화할 경우 암호가 저장되지 않고 전화기에서 자격 증명을 요청합니다. 기본값: 거짓
호스트 ID 확인 활성화	참인 경우 게이트웨이 인증서 subjectAltName 또는 CN이 VPN 클라이언트가 연결된 URL과 일치해야 합니다. 기본값: 참

일반 전화 프로파일에 VPN 세부 정보 추가

이 절차를 사용하여 VPN 세부 정보를 일반 전화 프로파일에 추가합니다.

프로시저

-
- 단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 전화 프로파일
- 단계 **2** 찾기를 클릭하고 VPN 세부 정보를 추가할 일반 전화 프로파일을 선택합니다.
- 단계 **3** VPN 정보 섹션에서 적절한 VPN 그룹 및 VPN 프로파일을 선택합니다.
- 단계 **4** 저장 및 구성 적용을 클릭합니다.
- 단계 **5** 구성 적용 창에서 확인을 클릭합니다.
-



IV 부

라이선싱

• [라이선싱, 113 페이지](#)



11 장

라이선싱

- 라이선싱, 113 페이지
- Unified Communications Manager 라이선싱, 114 페이지
- 라이선스 준수, 115 페이지
- 사용자 전용 라이선스, 116 페이지
- 디바이스 전용, 116 페이지
- 사용자 및 디바이스, 116 페이지
- 사용자당 최대 디바이스 수, 124 페이지
- TelePresence Room 라이선스, 124 페이지
- 라이선스 대체, 125 페이지
- 라이선스 시나리오, 125 페이지
- 사용자 추가, 125 페이지
- 연결 안 된 디바이스 추가, 125 페이지
- 연결된 디바이스와 사용자 추가, 126 페이지
- 사용자당 디바이스 수, 127 페이지
- 라이선스 사용 보고서, 127 페이지
- Cisco Unified Reporting, 128 페이지

라이선싱

Cisco Unified Communications Manager 라이선스는 Cisco Unified Communications 라이선스의 전체 상용 제공의 일부입니다.

		사용자 연결 라이선스 (Essential)	사용자 연결 라이선스(Basic)	사용자 연결 라이선스 (Enhanced/ Enhanced Plus)	Unified Workspace Licensing
Cisco Unified CM 기능	휴대폰 연결 (SNR)	해당 없음	포함	포함	포함

		사용자 연결 라이선스 (Essential)	사용자 연결 라이선스(Basic)	사용자 연결 라이선스 (Enhanced/ Enhanced Plus)	Unified Workspace Licensing
디바이스 지원	디바이스 수	1	1	1/2	10
	디바이스 유형 지원	아날로그/음성 (자세한 내용은 사용자 및 디바이스 테이블 참조)	음성(자세한 내용은 사용자 및 디바이스 테이블 참조)	음성(자세한 내용은 사용자 및 디바이스 테이블 참조)	음성(자세한 내용은 사용자 및 디바이스 테이블 참조)
	사용자 프로파일 수	1	1	1	1
클라이언트	Jabber Mobile	해당 없음	해당 없음	포함	포함
	Jabber 데스크 톱	해당 없음	해당 없음	포함	포함
	Jabber IM/Presence	포함	포함	포함	포함
애플리케이션	Webex Meetings	추가 기능	추가 기능	추가 기능	포함
	Webex Social	추가 기능	추가 기능	추가 기능	포함
	Unity Connection	추가 기능	추가 기능	추가 기능	포함
	Cisco Unified CM	포함	포함	포함	포함

Cisco Unified Communications Manager의 라이선싱은 구성된 총 사용자 수, 사용자 기능, 디바이스에 따라 결정됩니다. Cisco Unified Communications Manager는 시스템에 구성된 총 사용자 수(사용자 기능 및 연결 디바이스 포함) 및 디바이스를 기준으로 라이선스 사용을 계산합니다. Cisco Unified Communications Manager는 총 라이선스 사용량(게시자당)을 Cisco Smart Software Manager에 보고하고 라이선스 규정 준수 또는 규정 비준수 상태를 반환합니다.

Unified Communications Manager 라이선싱

Cisco Unified Workspace Licensing(UWL)을 사용하면 기업에서는 간소화된 저렴한 패키지로 제공되는 광범위한 Cisco Collaboration 애플리케이션 및 서비스를 이용할 수 있습니다. 여기에는 사용자 별로 소프트웨어 클라이언트, 애플리케이션 서버 소프트웨어 및 라이선스를 포함합니다.

Cisco User Connect Licensing(UCL)은 개별 Cisco Unified Communications 제품에 대한 사용자 기반 라이선스입니다. 여기에는 소프트웨어 클라이언트, 애플리케이션 서버 소프트웨어 라이선스 및 기본 통합 커뮤니케이션 애플리케이션을 포함됩니다. 요구사항 및 선택 디바이스에 따라 UCL은 Essential, Basic, Enhanced 또는 Enhanced Plus로 사용할 수 있습니다.

다음은 Unified Communications Manager의 라이선스 유형입니다.

UC Manager 필수(Essential)	Essential 사용자 연결 라이선스 - 기본 음성 또는 아날로그 디바이스(전화기 또는 팩스)를 제공하는 하나의 디바이스를 지원합니다. (예: 아날로그 전화기, ATA 186, ATA 187, Cisco 3905, Cisco 6901)
UC Manager 기본(Basic)	Basic 사용자 연결 라이선스- 기본(음성 및 영상) 통화 제어 기능을 비롯하여 모든 Essential 디바이스를 포함한 하나의 디바이스를 지원합니다. (예: Cisco 6911, Cisco 6921)
UC Manager 인핸스드(Enhanced)	Enhanced 사용자 연결 라이선스- 모든 Basic 디바이스와 데스크톱, 모바일 클라이언트를 비롯한 고급(음성 및 영상) 통화 제어 기능을 포함한 하나의 디바이스를 지원합니다. (예: Cisco 3911, Cisco 3951, Cisco 6941, Cisco 6945, Cisco 6961, Cisco 79xx, Cisco 89xx, Cisco 99xx, Cisco E20, Cisco TelePresence EX60, Cisco TelePresence EX90, 타사 SIP)
UC Manager 인핸스드 플러스(Enhanced Plus)	Enhanced Plus 사용자 연결 라이선스- 모든 Enhanced 디바이스를 포함하여 디바이스를 2개까지 지원합니다.
UC Manager CUWL	사용자당 최대 10개의 디바이스를 갖춘 데스크톱 및 모바일, 전문가 협업 작업 영역 애플리케이션 기능을 포함하여 고급(음성 및 영상) 통화 제어 기능을 지원합니다.
UC Manager TelePresence Room	TelePresence Room 라이선스 - 회의실 기반 물입형 및 다목적 Cisco TelePresence 시스템 엔드포인트 및 Spark 회의실을 지원합니다. (예: Cisco TelePresence System 시리즈 3200, 3000, 1300; Cisco TelePresence MX 시리즈. Cisco TelePresence TX 시리즈; Cisco TelePresence System Profile 시리즈)

라이선스 준수

처음 설치될 때 Unified Communications Manager는 Cisco Smart Software Manager에 성공적으로 등록될 때까지 평가 기간 90일간 데모 모드에서 완벽하게 작동합니다. 등록 후에는 Unified Communications

Manager가 Cisco Smart Software Manager와 정기적으로 통신합니다. Unified Communications Manager는 Cisco Smart Software Manager에 대한 라이선스 유형별 총 라이선스 요구 사항을 보고한 다음 라이선스 상태를 다시 가져옵니다.

Unified Communications Manager에 대한 비 준수 상태의 라이선스는 90일 초과 기간 후에 적용됩니다. 유예 기간이 끝나면 Unified Communications Manager는 다음과 같은 서비스 성능 저하 시 비 호환성을 적용합니다.

디바이스 및 사용자를 프로비저닝할 수 없습니다. 라이선스에 영향을 미치는 사용자의 구성 변경(예: IM and Presence 상태 활성화/비활성화 및 이동성 활성화/비활성화 확인란)은 허용되지 않습니다.

스마트 라이선스 작동에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 내용을 참조하십시오.

사용자 전용 라이선스

사용자가 시스템에 구성되어 있지만 디바이스에 연결되지 않은 경우 사용자는 어떤 디바이스도 소유하고 있지 않는 것으로, 이를 "사용자 전용"이라고 합니다. 사용자의 사용자 ID가 디바이스의 "OwnerUserID" 필드에 입력된 경우 사용자가 디바이스에 연결되어 있거나 디바이스를 "소유"하고 있는 것입니다. 어떤 디바이스에도 연결되지 않은 사용자에 대한 "사용자 전용" 라이선스는 사용자 및 디바이스 지원 표에 나와 있습니다.

간단히 말해, 사용자가 디바이스를 소유하고 있지 않거나 사용이 허가된 사용자 기능을 사용하지 않는 경우 사용자를 시스템에 추가하더라도 라이선스를 사용할 수 없습니다. 그러나 사용자가 사용이 허가된 사용자 기능으로 구성되어 있거나 디바이스를 소유하고 있는 경우에는 라이선스를 사용할 수 있습니다. 현재 사용이 허가된 유일한 기능은 모바일 연결(이동성 또는 단일 번호 연락 또는 SNR이라고도 함)입니다.

사용자에 대한 Mobile Connect(또는 이동성 또는 단일 번호 연락)는 최종 사용자가 디바이스 소유자(사용자 ID 필드)로 설정된 RDP(원격 대상 프로파일)가 생성될 때 구성됩니다.

디바이스 전용

디바이스가 Cisco Unified Communications Manager에 추가되고 디바이스 구성 페이지의 OwnerUserID 필드에 입력된 항목이 없는 경우 디바이스가 할당되지 않았거나 사용자와 연결되지 않고 "디바이스만"이라고 합니다. "디바이스만" 디바이스의 라이선스는 Cisco Unified Communications Manager 라이선스 - 사용자 및 디바이스 지원 표에 나열되어 있습니다. 디바이스가 Cisco Unified Communications Manager에 추가되고 OwnerUserID 항목이 없을 경우 라이선스 - 사용자 및 디바이스 지원 표와 같이 디바이스별 최소 라이선스 유형만 필요합니다.

사용자 및 디바이스

디바이스의 OwnerUserID 필드에 사용자 ID를 입력하여 디바이스가 할당되거나 사용자에게 연결된 경우, 해당 사용자와 디바이스에 대한 라이선스 요구 사항은 사용자에게 할당된 디바이스 유형 및 디바

이 수에 따라 결정됩니다. 하나의 디바이스를 소유하는 사용자의 경우 해당 사용자의 사용자 ID가 OwnerUserID로 하나의 필수(Essential) 디바이스(예: 3905, 6901 또는 아날로그 디바이스)에 추가되어 있으면 이 사용자 및 디바이스에 필요한 최소 라이선스는 필수(Essential) 라이선스 1개입니다. 즉, 하나의 필수(Essential) 라이선스는 사용자와 디바이스를 모두 지원합니다. 대신, 해당 사용자의 사용자 ID가 OwnerUserID로 하나의 기본(Basic) 디바이스(예: 6911 또는 6921)에 추가된 경우 이 사용자 및 디바이스에 필요한 최소 라이선스는 기본(Basic) 라이선스 1개입니다. 사용자의 사용자 ID가 OwnerUserID로 하나의 인핸스드(Enhanced) 디바이스에 추가된 경우 이 사용자 및 디바이스에 필요한 최소 라이선스는 인핸스드(Enhanced) 라이선스 1개입니다.

2개 이상의 디바이스를 소유하는 사용자의 경우 최소 라이선스는 사용자가 소유하고 있는 디바이스의 수에 따라 결정됩니다. Cisco Unified Communications Manager 라이선스 표에는 사용자 라이선스 당 지원되는 최대 디바이스 수가 나와 있습니다. 2개의 디바이스를 소유하는 사용자는 최소 하나의 인핸스드 플러스(Enhanced Plus) 라이선스가 필요합니다. 3개 이상의 디바이스를 소유하는 사용자는 최소 하나의 CUWL 라이선스가 필요합니다.

Cisco Unified Communications Manager 라이선스 - 사용자 및 디바이스 지원 표에 사용자 전용, 디바이스 전용, 그리고 사용자 및 디바이스에 대한 Cisco Unified Communications Manager 라이선스 요약 정보가 나와 있습니다.

표 15: Cisco Unified Communications Manager 라이선스 - 사용자 및 디바이스 지원

라이선스 유형	디바이스 전용	사용자 및 디바이스	사용자 전용
UC Manager 필수(Essential)	<ul style="list-style-type: none"> • Cisco 유니파이드 SIP 전화기 3905 • Cisco Unified IP Phone 6901 • 아날로그 디바이스 	필수(Essential) 디바이스 1개를 소유한 사용자.	해당 없음
UC Manager 기본(Basic)	Cisco Unified IP Phone 6911 및 6921 모델 또는 UC Manager 필수(Essential) 라이선스 유형의 디바이스.	기본(Basic) 디바이스 1개를 소유한 사용자. 또는 UC Manager 필수(Essential) 라이선스 유형의 사용자 및 연결된 디바이스.	단일 번호 도달(Mobile Connect)을 소유한 사용자. 또는 UC Manager 필수(Essential) 라이선스 유형을 소유한 사용자.

라이선스 유형	디바이스 전용	사용자 및 디바이스	사용자 전용
UC Manager 인핸스드 (Enhanced)		<p>인핸스드(Enhanced) 디바이스 1개를 소유한 사용자.</p> <p>또는</p> <p>UC Manager 필수(Essential) or UC Manager 기본(Basic) 라이선스 유형을 소유한 사용자 및 연결된 디바이스.</p>	해당 없음

라이선스 유형	디바이스 전용	사용자 및 디바이스	사용자 전용
	<ul style="list-style-type: none"> • Cisco Unified IP Phone 3911, 3941, 3951 • Cisco Unified IP Phone 6941, 6945 및 6961 모델 • Cisco Unified IP Phone 7900 Series(7900G, 7911G, 7912G, 7931G, 794xG, 796xG 및 7975G 모델) • Cisco Unified IP Phone 8900 Series(8941, 8945 및 8961 모델) • Cisco Unified IP Phone 9900 Series(9951 및 9971 모델), 카메라 포함 또는 제외 • Cisco Unified 무선 IP 전화기 Series(792xG 및 7925G-EX 모델) • Cisco Unified IP 전화회의 스테이션 (7936G 및 7937G 스테이션) • Cisco Unified 소프트폰(Cisco Unified Personal Communicator, Cisco UC Integration for Lync, Cisco UC Integration for Connect, and Cisco IP Communicator) • Jabber 클라이언트 (Jabber for Mac, 		

라이선스 유형	디바이스 전용	사용자 및 디바이스	사용자 전용
	<p>Jabber for Windows, Jabber for iPhone, Jabber for Android, Jabber for iPad 및 Jabber SDK)</p> <ul style="list-style-type: none"> • Cisco Virtual Experience Client(VXC), 음성 및 비디오 펌웨어 포함 • Cisco IP Video Phone E20 • Cisco TelePresence System EX Series(EX60 및 EX90) • 타사 SIP 디바이스 • Cisco Desktop Collaboration Experience DX600 시리즈 • Transnova S3 • Cisco Spark 룸 디바이스 • IMS <p>또는</p> <p>UC Manager 필수(Essential) 또는 UC Manager 기본(Basic) 라이선스 유형의 모든 디바이스.</p>		

라이선스 유형	디바이스 전용	사용자 및 디바이스	사용자 전용
UC Manager 인핸스드 플러스(Enhanced Plus)	해당 없음	<p>디바이스 2개를 소유한 사용자.</p> <p>또는</p> <p>UC Manager 필수(Essential), UC Manager 기본(Basic), UC Manager 인핸스드(Enhanced) 또는 UC Manager 인핸스드 플러스(Enhanced Plus) 라이선스 유형을 소유한 사용자 및 연결된 디바이스.</p>	해당 없음

라이선스 유형	디바이스 전용	사용자 및 디바이스	사용자 전용
UC Manager TelePresence 회의실 라 이선스		1개의 UC Manager TelePresence 회의실 디 바이스가 연결된 사용 자.	해당 없음

라이선스 유형	디바이스 전용	사용자 및 디바이스	사용자 전용
	<ul style="list-style-type: none"> • Cisco TelePresence System 500 Series • Cisco TelePresence System 1100 • Cisco TelePresence System 1300 Series • Cisco TelePresence System 3000 Series • Cisco TelePresence System 3200 Series • Cisco TelePresence TX9000 Series(TX9000, TX9200) • Cisco TelePresence TX1300 Series • Cisco TelePresence System Profile Series(42인치 6000 MXP, 52인치 MXP, 52인치 Dual MXP, 65인치 및 65인치 Dual) • Cisco TelePresence System Codecs C90/C60/C40 • Cisco TelePresence System Quick Set C20 • Cisco TelePresence MX Series(MX300 및 MX200) • Cisco TelePresence 1000 • Cisco TelePresence SX Series • Cisco Webex Devices 		

라이선스 유형	디바이스 전용	사용자 및 디바이스	사용자 전용
	<ul style="list-style-type: none"> 일반 데스크톱 비디오 종점 일반 다중 화면 룸 시스템 일반 단일 화면 룸 시스템 		

디바이스 전용이란 OwnerUserID 필드가 비어 있어 사용자가 연결되어 있지 않은 Cisco Unified Communications Manager에 구성된 디바이스를 의미합니다.

사용자 및 디바이스란 OwnerUserID 필드에 등록된 사용자 ID가 있어 사용자가 연결되어 있는 Cisco Unified Communications Manager에 구성된 디바이스를 의미합니다.

사용자 전용이란 사용자와 연결된 디바이스가 없는 Cisco Unified Communications Manager에 구성된 사용자를 의미하는데, 이 경우 Cisco Unified Communications Manager 디바이스에 대한 OwnerUserID로 사용자 ID가 발견되지 않습니다.

위 표에서 굵게 표시된 텍스트는 나열된 라이선스 유형 중 하위 수준 라이선스 요구 사항을 충족하기 위해 사용 가능한 라이선스를 사용할 수 있는 라이선스 대체를 통해 디바이스가 지원됨을 의미합니다. 이 작업은 Cisco Smart Software Manager에서 수행됩니다.



참고 MGCP FXS 포트는 아날로그 전화기로 간주되지 않으므로 라이선스가 필요하지 않습니다.

사용자당 최대 디바이스 수

필수, 기본 및 인핸스드 라이선스는 사용자 ID가 1개 디바이스의 OwnerUserId 필드에 입력되는 1개 연결 디바이스를 사용하는 사용자를 지원합니다. 인핸스드 플러스 라이선스는 2개 연결 디바이스를 사용하는 사용자를 지원합니다. UWL은 최대 10개 연결 디바이스를 사용하는 사용자를 지원합니다.

TelePresence Room 라이선스

다용도 및 몰입형 TelePresence 디바이스는 TelePresence Room 라이선스라는 별도의 디바이스 라이선스 유형으로 사용이 허가됩니다. TelePresence Room 라이선스는 TelePresence 디바이스와 Cisco Unified Communications Manager에 등록된 전화기를 모두 포괄합니다. 단, TelePresence 디바이스 및 전화기에 대한 OwnerUserID 필드로 동일한 사용자 ID를 입력한 경우에만 해당 라이선스가 유효합니다.

TelePresence 디바이스와 전화기 모두에 대한 OwnerUserID로 동일한 사용자 ID를 입력하지 않으면 디바이스가 연결되지 않아 2개의 라이선스가 필요합니다. 즉, 디바이스를 위한 TelePresence Room 라이선스 하나와 전화기를 위한 인핸스드(Enhanced) 하나가 필요합니다. TelePresence 터치 디바이스는

Cisco Unified Communications Manager에 등록되지 않으므로 별도의 라이선스 또는 OwnerUserID 연결이 필요하지 않습니다.

라이선스 대체

Cisco Smart Software Manager(CSSM)를 사용하면 사용 가능한 라이선스의 계층형 라이선스 대체를 통해 준수를 보장할 수 있습니다. 하위 수준 라이선스 요구 사항을 충족하도록 사용 가능한 상위 수준 라이선스가 대체되거나 대여됩니다. 예를 들어 고객에게 100개의 UC Manager CUWL 라이선스가 설치되어 있지만 Cisco Unified Communications Manager에서 10개의 CUWL 라이선스와 50개의 UC Manager Enhanced Plus 라이선스에 대한 역방향 라이선스 요구 사항을 보고하는 경우 CSSM은 100-10 또는 90개의 UC Manager CUWL 라이선스를 상위 계층으로 대여할 수 있음을 계산합니다. 사용 가능한 90개 UC Manager CUWL 라이선스 중 50개 CUWL은 50개의 Enhanced Plus 라이선스에 대한 요구 사항을 충족하기 위해 사용됩니다. CSSM은 40개의 UC Manager CUWL 라이선스를 사용 가능한 것으로 표시합니다.

라이선스 시나리오

다음 라이선스 시나리오에서는 Cisco Unified Communications Manager 관리에서 구성을 변경하는 과정을 안내합니다. 이 경우 라이선스가 요구됩니다.

사용자 추가

새 사용자(사용자 A)가 최종 사용자 구성 또는 벌크 관리 도구를 통해 Cisco Unified Communications Manager 관리에 처음 추가될 때 사용자에게 이동성 활성화 아래에 원격 디바이스 프로파일이 없는 경우 새 사용자에게 라이선스가 필요하지 않습니다.

새 사용자(사용자 B)가 이동성 활성화 아래에 원격 대상 프로파일이 구성된 상태로 Cisco Unified Communications Manager에 처음 추가되는 경우 새 사용자인 사용자 B에게 기본 라이선스가 필요합니다.

UserID	사용이 허가된 사용자 기능	필요한 라이선스	참고
사용자 A	없음	없음	할당된 디바이스 없음
사용자 B	이동성	기본(Basic)	할당된 디바이스 없음

연결 안 된 디바이스 추가

Cisco Unified Communications Manager에 새 디바이스가 등록되어 있지만 디바이스의 [OwnerUserID] 필드에 입력된 사용자 ID가 없으므로 디바이스가 사용자와 연결되지 않았으며, 연결 안 된 디바이스에 대해서는 Cisco Unified Communications Manager 9.x 라이선스 - 사용자 및 디바이스 지원 표에 표

시된 대로 디바이스 유형별 라이선스가 필요합니다. 예를 들어, Device6901을 추가하면 필수 라이선스가 있어야 합니다. Device6921을 추가하면 기본 라이선스가 필요합니다. DeviceEX60을 추가하면 향상된 라이선스가 필요합니다.

현재는 인헨스드 플러스(Enhanced Plus), CUWL 표준(Standard) 또는 CUWL 전문가(Professional) 라이선스가 필요한 디바이스가 없습니다. 따라서 인헨스드 플러스 또는 위의 라이선스가 필요한 연결 안 된 디바이스의 경우 Cisco Unified Communications Manager에 요구 사항이 표시되지 않습니다.

표 16: 디바이스 전용 라이선스 요구 사항의 예

장치	필요한 라이선스	참고
Device6901	UC Manager 필수(Essential)	OwnerUserID 없음
Device6921	UC Manager 기본(Basic)	OwnerUserID 없음
DeviceEX60	UC Manager 인헨스드(Enhanced)	OwnerUserID 없음

연결된 디바이스와 사용자 추가

디바이스가 사용자와 연결된 경우, 디바이스를 추가하면 사용자와 디바이스가 하나의 라이선스를 공유합니다. 사용자당 디바이스가 하나인 경우, 필요한 라이선스는 필요한 사용자 라이선스 또는 디바이스 라이선스 중 더 큰 값이 됩니다. 다음 시나리오에서는 사용자당 디바이스가 하나인 경우의 다양한 디바이스 및 사용자 연결 조합에 대해 살펴봅니다.

사용자와 연결된 필수 디바이스

Device6901(필수 디바이스)이 UserA에게 할당된 경우 OwnerUserID = UserA를 입력하면 디바이스와 사용자 모두 Essential 라이선스로 지원됩니다.

하지만 Device6901(필수 디바이스)이 UserB(기본 사용자)에 할당된 경우에는 OwnerUserID = UserB를 입력하면 디바이스와 사용자 모두 하나의 Basic 라이선스로 지원됩니다.

사용자에 연결된 기본 디바이스

Device6921(기본 디바이스)이 UserA에게 할당된 경우 OwnerUserID = UserA를 입력하면 디바이스와 사용자 모두 Basic 라이선스로 지원됩니다. 마찬가지로 OwnerUserID = UserB를 입력하여 Device6921(기본 디바이스)을 UserB(기본 사용자)에 할당한 경우 디바이스와 사용자 모두 Basic 라이선스 하나로 지원됩니다.

사용자와 연결된 인헨스드 디바이스

대부분의 물리적 전화 및 소프트웨어 클라이언트와 데스크톱 비디오 디바이스(예: EX60 및 EX90)가 인헨스드 디바이스 수준에 포함됩니다. OwnerUserID = UserA를 입력하여 DeviceEX60(인헨스드 디바이스)을 UserA에게 할당한 경우 디바이스와 사용자 모두 Enhanced 라이선스 하나로 지원됩니다. 마찬가지로 OwnerUserID = UserB를 입력하여 DeviceEX60(인헨스드 디바이스)을 UserB(기본 사용자)에 할당한 경우 디바이스와 사용자 모두 Enhanced 라이선스 하나로 지원됩니다.

표 17: 사용자 및 디바이스 라이선스 요구 사항 예

장치	OwnerUserID	사용이 허가된 사용자 기능	필요한 라이선스
Device6901	사용자 A	없음	UC Manager 필수 (Essential)
	사용자 B	이동성	UC Manager 기본(Basic)
Device6921	사용자 A	없음	UC Manager 기본(Basic)
	사용자 B	이동성	UC Manager 기본(Basic)
DeviceEX60	사용자 A	없음	UC Manager 인핸스드 (Enhanced)
	사용자 B	이동성	UC Manager 인핸스드 (Enhanced)

사용자당 디바이스 수

사용자와 디바이스에 대한 위의 예는 사용자가 1개 디바이스에 연결된 경우에만 적용됩니다. 이 경우 사용자 ID는 단일 디바이스 구성 OwnerUserID 필드에만 있습니다. 사용자가 2개 이상 디바이스에 연결되면 디바이스 유형과 관계없이 더 높은 수준의 라이선스가 필요합니다.

사용자 A가 1개 디바이스에 대한 OwnerUserID에 할당되면 위의 시나리오가 적용됩니다. 그러나 사용자 A에 2개 디바이스에 대한 OwnerUserID가 할당되면 사용자 및 2개 연결 디바이스에 대해 1개 인핸스드 플러스 라이선스가 필요합니다. 사용자 A에게 2개 이상 디바이스에 대한 OwnerUserID가 할당되면 1개 UWL 표준 라이선스가 필요합니다. 사용자 A에는 1개 UWL 표준 라이선스로 최대 10개 디바이스가 할당될 수 있습니다. 한 사용자에게 10개 이상 디바이스가 할당되면 사용자에게 1개 UWL 표준 라이선스가 필요하고 추가 디바이스에 대해서는 추가 라이선스가 필요합니다.

라이선스 사용 보고서

사용 세부 정보는 라이선스 유형, 사용자, 할당되지 않은 디바이스에 따라 제공됩니다. 사용 정보는 6시간마다 한 번씩 업데이트되며 사용 세부 정보 업데이트를 클릭하여 수동으로 업데이트할 수도 있습니다. [사용 세부 정보 업데이트]를 클릭하는 작업은 리소스가 많이 사용되는 프로세스로, 시스템 크기에 따라 몇 분이 걸릴 수 있습니다. 모든 라이선스 유형 설명 및 디바이스 분류 보기에는 Unified Communications 라이선스 정보를 검토할 수 있는 링크가 있습니다.

알람 또는 라이선스 경고(라이선스 비준수)가 있는 경우 상태 메시지가 표시됩니다. 상태 메시지에 대한 자세한 내용은 [알람] 경고 및 라이선스 상태 알림을 참조하십시오. 라이선스 준수 및 비준수에 대한 자세한 내용은 [라이선스 준수]를 참조하십시오.

유형별 라이선스 요구 사항 표에는 현재 시스템의 라이선스 요구 사항이 표시되어 있습니다. 라이선스 유형별 현재 라이선스 사용(필요한 라이선스 수)이 표시되고, 라이선스 유형별로 라이선스가 필요한 사용자 및 할당되지 않은 디바이스의 수가 요약되어 있습니다. 라이선스 유형별 [보고서]는 사용자(수) 또는 할당되지 않은 디바이스(수)에 따라 제공되며 드릴다운 링크를 사용할 수 있습니다. 사용자 보고서의 경우 사용자 ID 링크는 사용자 ID별 사용자 구성에 대한 세부 정보를 제공합니다. 세부 정보 보기 링크는 사용자 ID 별 라이선스 요구 사항을 제공합니다. 할당되지 않은 장치 보고서의 경우, 할당되지 않은 각 장치에 대해 필요한 장치 유형 및 라이선스 유형이 표시됩니다.

사용자 및 할당되지 않은 디바이스별로 라이선스 사용 보고서를 요약할 수도 있습니다. [사용자] 행에는 시스템에 구성된 총 사용자 수가 나열됩니다. 사용자에 대한 [사용 보고서 보기]에서는 시스템에 구성된 모든 사용자에 대한 보고서 및 해당 라이선스 요구 사항을 제공합니다. 할당되지 않은 디바이스에 대한 [사용 보고서 보기]에서는 총 할당되지 않은 디바이스(연결된 사용자가 없는 디바이스) 수가 표시됩니다.



참고 Cisco Unified Communications 관리를 사용하여 디바이스에 사용자 ID를 할당하면 디바이스가 라이선스 사용 보고서의 "할당되지 않은 디바이스"에서 "사용자"로 이동합니다. 그러나 디바이스를 최종 사용자의 제어된 디바이스 목록에 추가해도 디바이스의 라이선스 사용 보고서 결과는 수정되지 않습니다.

Cisco Unified Reporting

Cisco Unified Communications 솔루션의 Cisco Unified Reporting 콘솔에서 다음 보고서를 사용할 수 있습니다.

1. Cisco Unified Communications Manager 관리 로그인 페이지 탐색 표시줄에서 Cisco Unified Reporting을 클릭합니다.
2. 시스템 보고서를 선택합니다.
3. Unified CM 디바이스 수 요약을 선택합니다.

클러스터당 모델별 디바이스 수가 요약된 보고서가 생성됩니다.

1. Cisco Unified Communications Manager 관리 로그인 페이지 탐색 표시줄에서 Cisco Unified Reporting을 클릭합니다.
2. 시스템 보고서를 선택합니다.
3. Unified CM 사용자 디바이스 수를 선택합니다.

클러스터당 전화기-사용자 관계, 사용자 없는 전화기 수, 전화기가 1대인 사용자 수, 전화기가 2대 이상인 사용자 수가 요약된 보고서가 생성됩니다.

1. Cisco Unified Communications Manager 관리 로그인 페이지 탐색 표시줄에서 Cisco Unified Reporting을 클릭합니다.
2. 시스템 보고서를 선택합니다.

3. Unified CM 사용자 디바이스 수를 선택합니다.

클러스터당 전화기-사용자 관계, 사용자 없는 전화기 수, 전화기가 1대인 사용자 수, 전화기가 2대 이상인 사용자 수가 요약된 보고서가 생성됩니다.



V 부

모니터링 및 녹음

- 사일런트 모니터링 , 133 페이지
- 녹음 , 143 페이지



12 장

사일런트 모니터링

- 사일런트 모니터링 개요, 133 페이지
- 자동 모니터링 사전 요건, 134 페이지
- 사일런트 모니터링 작업 흐름 구성, 134 페이지
- 사일런트 모니터링 상호 작용, 140 페이지
- 사일런트 모니터링 제한 사항, 140 페이지

사일런트 모니터링 개요

무성 통화 모니터링을 통해 관리자는 전화 통화를 엿들을 수 있습니다. 가장 일반적인 시나리오는 콜 센터에서 통화 상담사가 고객과 말하는 내용에 있습니다. 콜 센터에서는 콜 센터 상담사가 제공하는 고객 서비스의 품질을 보증할 수 있어야 합니다. 무성 통화 모니터링을 사용하면 감독자가 두 통화 참가자를 모두 들을 수 있지만 통화 참가자 중 어느 누구도 감독자가 하는 말을 들을 수 없습니다.

무성 모니터링은 JTAPI 또는 TAPI 인터페이스를 통해 CTI 애플리케이션에서만 호출할 수 있습니다. Cisco Unified Contact Center Enterprise 및 Cisco Unified Contact Center Express와 같은 여러 Cisco 애플리케이션에서는 무성 모니터링을 사용할 수 있습니다. 통화를 모니터링하는 CTI 애플리케이션은 해당 모니터링 권한이 애플리케이션 사용자 또는 최종 사용자 계정에 활성화되어 있어야 합니다.

무성 모니터링은 통화를 기반으로 합니다. 감독자가 무성 모니터링 세션을 호출하면 다음과 같은 상황이 발생합니다.

- 감독자가 모니터링할 특정 통화를 선택합니다.
- 애플리케이션의 모니터링 시작 요청은 감독자 전화가 연결 해제되도록 트리거하고 상담사에 대한 모니터링 호출을 자동으로 트리거합니다.
- 에이전트 전화기는 모니터링 전화를 자동으로 받습니다. 모니터링 통화는 상담사에게 표시되지 않습니다.

보안 사일런트 모니터링

보안 사일런트 모니터링을 구성할 수도 있습니다. 보안 무성 모니터링을 사용하면 암호화된 미디어 (sRTP) 통화를 모니터링할 수 있습니다. 모니터링 통화는 항상 관찰 대상 통화의 보안 상태와 상관없이 에이전트 전화기의 기능에 따라 결정되는 최고 보안 수준을 사용하여 설정됩니다. 최고 보안 수준

은 고객, 에이전트, 감독자 사이의 모든 통화에서 보안 미디어 키를 교환함으로써 유지됩니다. 보안 미디어를 사용한 모니터링 통화는 표준 보안 미디어(sRTP) 통화와 마찬가지로 약 4000 bps의 추가 대역폭 오버헤드를 수반합니다.

상담사 전화기에 활성화된 암호화가 있는 경우 보안 사일런트 모니터링을 허용하려면 관리자 전화기의 암호화도 활성화해야 합니다. 상담사 전화기에 활성화된 암호화가 있지만 감독자 전화기에 없는 경우 모니터링 요청이 실패합니다.

콧속말 코칭

Unified Communications Manager는 또한 고객의 요청 없이 모니터링 세션이 진행되는 동안 관리자가 상담사와 통화할 수 있도록 자동 모니터링에 대한 CTI 개선인 위스퍼 코칭도 지원합니다. 위스퍼 코칭은 CTI 애플리케이션에서만 시작할 수 있습니다. 사일런트 모니터링이 이미 구성된 경우에는 위스퍼 코칭에 Unified Communications Manager의 추가 구성이 필요하지 않습니다.

자동 모니터링 사전 요건

사일런트 모니터링은 외부 CTI 애플리케이션의 경우에만 호출할 수 있습니다. Cisco Unified Contact Center Enterprise 또는 Cisco Unified Contact Center Express와 같은 Cisco 애플리케이션은 사일런트 모니터링 세션을 시작할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- Cisco Unified Contact Center Enterprise — Cisco Unified Contact Center Enterprise에서 사일런트 모니터링을 설정하는 방법에 대한 자세한 내용은 [Cisco Remote Silent Monitoring 설치 및 관리 지침서](#)를 참조하십시오.
- Cisco Unified Contact Center Express - 이 장에는 Cisco Finesse를 통한 Contact Center Express에 대한 사일런트 모니터링을 설정하는 샘플 구성이 포함되어 있습니다. Cisco Unified Contact Center Express 구축과 관련된 추가 설명서를 보려면 <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html>(으)로 이동하십시오.

사일런트 모니터링 작업 흐름 구성

이 작업 흐름에서는 CTI 애플리케이션에서 모니터링 기능을 사용할 수 있도록 하기 위해 Unified Communications Manager에서 수행해야 하는 작업에 대해 설명합니다.

시작하기 전에

- 전화기 기능 목록 보고서를 실행하여 자동 모니터링을 지원하는 전화기를 결정합니다. 자세한 내용은 [전화기 기능 목록 생성, 7 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	다음 절차 중 하나를 수행합니다. <ul style="list-style-type: none"> • 전화기 클러스터 수준에 빌트-인 브리지(BIB) 활성화, 135 페이지 • 전화기의 빌트-인 브리지(BIB) 활성화, 136 페이지 	상담사 전화기에서 빌트-인 브리지(BIB)를 설정합니다. 서비스 매개 변수를 사용하여 클러스터 수준 기본 설정을 구성하거나 개별 전화기에 빌트-인 브리지(BIB)를 활성화할 수 있습니다. 참고 개별 전화기의 빌트-인 브리지(BIB) 설정은 클러스터 수준 기본 설정을 무시합니다.
단계 2	감독자에 대한 모니터링 권한 활성화, 136 페이지	자동 모니터링을 허용하는 그룹에 감독자를 추가합니다.
단계 3	발신 검색 공간 모니터링 할당, 137 페이지	감독자 전화기에 대한 발신 검색 공간 모니터링을 설정합니다.
단계 4	사일런트 모니터링 알림 신호음 구성, 137 페이지	통화 참가자에게 알림 신호음을 재생할지 여부를 구성합니다.
단계 5	보안 사일런트 모니터링 구성, 138 페이지	선택 사항. 통화가 암호화된 경우에는 보안 자동 모니터링을 구성합니다.
단계 6	Unified Contact Center Express에 대한 사일런트 모니터링 구성, 139 페이지	Unified Contact Center Express 구축의 경우 Cisco Finesse를 통해 자동 모니터링을 구성합니다.

전화기 클러스터 수준에 빌트-인 브리지(BIB) 활성화

빌트-인 브리지(BIB) 클러스터 수준 서비스 매개 변수를 활성화로 설정하면 클러스터의 모든 전화기에 대해 빌트-인 브리지(BIB) 기본 설정이 활성화로 변경됩니다. 그러나 개별 전화기에 대한 전화기 구성 창에서 빌트-인 브리지(BIB) 설정은 클러스터 수준 서비스 매개 변수를 무시합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 CallManager 서비스가 실행 중인 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- 단계 4 빌트-인 브리지(BIB) 활성화 서비스 매개 변수를 켜기로 설정합니다.
- 단계 5 저장을 클릭합니다.

전화기의 빌트-인 브리지(BIB) 활성화

이 절차를 사용하여 개별 전화기에서 빌트-인 브리지(BIB)를 활성화합니다. 개별 전화기의 빌트-인 브리지(BIB) 설정은 클러스터 수준 서비스 매개 변수를 무시합니다.

시작하기 전에

서비스 매개 변수를 사용하여 클러스터의 모든 전화기에 대해 기본 제공 브리지 기본값을 설정합니다. 자세한 내용은 [전화기 클러스터 수준에 빌트-인 브리지\(BIB\) 활성화, 135 페이지](#)를 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하여 상담사 전화기를 선택합니다.

단계 3 빌트-인 브리지(BIB) 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 켜기 - 빌트-인 브리지(BIB)가 활성화됩니다.
- 끄기 - 빌트-인 브리지(BIB)가 비활성화됩니다.
- 기본값 - 클러스터 수준 빌트-인 브리지(BIB) 활성화 서비스 매개 변수 설정이 사용됩니다.

단계 4 저장을 클릭합니다.

감독자에 대한 모니터링 권한 활성화

감독자가 상담사 대화를 모니터링할 수 있으려면 감독자가 모니터링을 허용하는 그룹의 일부여야 합니다.

시작하기 전에

다음 절차 중 하나를 수행하여 상담사 전화기에서 빌트-인 브리지(BIB)를 활성화합니다.

- [전화기 클러스터 수준에 빌트-인 브리지\(BIB\) 활성화, 135 페이지](#)
- [전화기의 빌트-인 브리지\(BIB\) 활성화, 136 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 사용자 목록에서 감독자를 선택합니다.

단계 3 권한 정보 섹션에서 액세스 컨트롤 그룹에 추가를 클릭합니다.

단계 4 표준 CTI 통화 모니터링 허용 및 표준 CTI 지원 활성화됨 사용자 그룹에 추가합니다.

단계 5 저장을 클릭합니다.

발신 검색 공간 모니터링 할당

모니터링이 작동하려면 관리자 전화 회선에 모니터링 발신 검색 공간을 할당해야 합니다. 모니터링 발신 검색 공간에는 감독자 전화 회선과 상담사 전화 회선이 모두 포함되어야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하고 감독자 전화기를 선택합니다.

왼쪽 탐색 창에는 감독자의 전화기에 사용할 수 있는 전화 회선이 표시됩니다.

단계 3 모니터링에 사용되는 각 감독자의 전화 회선에 대해 다음 단계를 수행합니다.

- a) 전화 회선을 클릭합니다. 디렉터리 번호 구성 창에 해당 전화 회선에 대한 구성 정보가 표시됩니다.
- b) 발신 검색 공간 모니터링 드롭다운 목록에서 관리자 전화 회선과 상담사 전화 회선이 모두 포함된 발신 검색 공간을 선택합니다.
- c) 저장을 클릭합니다.

사일런트 모니터링 알림 신호음 구성

특정 관할 지역에서는 통화가 모니터링되고 있음을 나타내는 알림 신호음을 상담사나 고객 또는 둘 다에게 재생해야 합니다. 기본적으로 Unified Communications Manager는 알림 신호음을 재생하지 않습니다. 알림 신호음을 허용하도록 서비스 매개 변수를 구성해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 CallManager 서비스가 실행 중인 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 Cisco CallManager를 선택합니다.

단계 4 다음 서비스 매개 변수에 대한 값을 구성합니다.

- 상담사에게 알림 신호음을 재생하려면 관찰 대상에게 모니터링 알림 신호음 재생 서비스 매개 변수를 **True**로 변경합니다.
- 고객에게 알림음을 재생하려면 연결된 관찰 상대에게 모니터링 알림 신호음 재생의 값을 **True**로 변경합니다.

단계 5 저장을 클릭합니다.

단계 6 서비스 매개 변수 구성을 변경한 경우 상담사 전화기를 재설정합니다.

보안 사일런트 모니터링 구성

SRTP를 사용하여 보안된 사일런트 모니터링을 구성하려면 암호화를 포함하는 전화기 보안 프로파일을 구성하고 모니터링 중인 상담사 전화기 및 감독자 전화기에 적용해야 합니다.

프로시저

	명령 또는 동작	목적
단계 1	암호화된 전화기 보안 프로파일 구성, 138 페이지	상담사 전화기 및 감독자 전화기에 대한 암호화를 포함하는 전화기 보안 프로파일을 구성합니다.
단계 2	전화기에 보안 프로파일 할당, 138 페이지	암호화된 전화기 보안 프로파일을 상담사 전화기 및 감독자 전화기에 적용합니다.

암호화된 전화기 보안 프로파일 구성

보안 자동 모니터링을 구성하려면 관리자 전화기 및 상담사 전화기의 전화기 보안 프로파일을 구성하여 디바이스 보안 모드로 암호화됨을 지정해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 보안 > 전화기 보안 프로파일.

단계 2 다음 단계 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 전화기 보안 프로파일을 만듭니다.
- 찾기를 클릭하고 기존 전화기 보안 프로파일을 선택합니다.

단계 3 새 전화기 보안 프로파일을 만든 경우 전화기 보안 프로파일 유형 드롭다운 목록에서 전화기 모델을 선택합니다.

단계 4 전화기 보안 프로파일의 이름을 입력합니다.

단계 5 디바이스 보안 모드 드롭다운 목록에서 암호화됨을 선택합니다.

단계 6 저장을 클릭합니다.

단계 7 위의 단계를 반복하여 감독자 전화기 및 상담사 전화기에 대한 전화기 보안 프로파일을 구성합니다.

전화기에 보안 프로파일 할당

전화기 보안 프로파일을 전화기에 할당하려면 다음 단계를 수행합니다. 보안 사일런트 모니터링이 작동하려면 전화기 보안 프로파일을 상담사 전화기와 감독자 전화기 모두에 할당해야 합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기.
- 단계 2 찾기를 클릭하고 전화기 보안 프로파일을 구성하려는 상담사 전화기를 선택합니다.
- 단계 3 디바이스 보안 프로파일 드롭다운 목록에서 설정된 전화기 보안 프로파일을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 감독자 전화기에 대해 이전 단계를 반복합니다.

Unified Contact Center Express에 대한 사일런트 모니터링 구성

다음 단계에는 Cisco Finesse를 통한 Cisco Unified Contact Center Express 구성에 대한 샘플 자동 모니터링이 포함되어 있습니다.

시작하기 전에

상담사 및 감독자 전화기가 Cisco Finesse에 대해 호환되어야 합니다. <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html>에서 Unified CCX 소프트웨어 호환성 매트릭스를 참조하십시오.

프로시저

- 단계 1 테스트 상담사 및 감독자를 통합 Unified Contact Center Express에 구성합니다.
 - 참고 상담사 및 감독자에 대한 IPCC(IP Contact Center) 내선 번호는 고유해야 합니다. 이는 Cisco Unified Communications Manager의 통화 라우팅 > 라우트 플랜 보고서 아래에서 확인할 수 있습니다.
- 단계 2 상담사 전화기에 빌트-인 브리지(BIB)가 있는지 확인합니다. 전화기 또는 클러스터 수준에서 이 작업을 수행할 수 있습니다(기본 서비스 매개 변수를 커짐으로 설정).
- 단계 3 Finesse에 상담사로 로그인합니다.
- 단계 4 Finesse에 감독자로 로그인하고 감독자가 준비 안 됨 상태인지 확인합니다.
- 단계 5 RMCM(Resource Manager Contact Manager) 사용자에게 통화 모니터링 및 통화 녹음 - CTI(표준 컴퓨터 텔레포니 통합) 통화 모니터링 및 녹음 허용에 필요한 역할이 있는지 확인합니다.
 - 참고 이 작업은 RMCM 사용자의 초기 설정에서 Unified Contact Center Express에 의해 자동으로 수행됩니다. Cisco Unified Communications Manager의 애플리케이션 사용자 창에 역할이 존재하는지 확인합니다.
- 단계 6 상담사 회선의 파티션을 포함하도록 감독자 전화기에서 모니터링 CSS(발신 검색 공간)를 할당합니다.

단계 7 통화가 로그인된 상담사에게 전송되도록 Unified Contact Center Express에 전화를 겁니다. 상담사가 통화 중 상태에 있는 경우 감독자로부터 사일런트 모니터링을 시작합니다. 그러면 감독자는 상담사 및 발신자 간의 대화를 들을 수 있습니다.

사일런트 모니터링 상호 작용

기능	상호 작용
통화 유지	모니터링 중인 에이전트 통화가 통화 유지로 전환되면 Unified Communications Manager에서 모니터링 통화를 유지 모드로 전환합니다.
보안 모니터링 전화 호 전환	Unified Communications Manager는 대상 감독자 디바이스가 모니터링 중인 상담사의 보안 기능을 초과하는 경우 보안 모니터링 세션의 전송을 지원합니다.
녹음 톤	녹음 톤은 녹음되고 모니터링되는 통화의 모니터링 신호음보다 우선합니다. 통화를 녹음하고 모니터링하는 경우 녹음 톤이 재생됩니다.
보안 신호음	보안 신호음을 구성하고 통화에 보안을 설정하면 모니터링 신호음이 구성되었는지 여부에 관계 없이 통화를 시작할 때 보안 신호음이 두 통화 참가자 모두에게 재생됩니다. 보안 신호음과 모니터링 신호음을 둘 다 구성된 경우 보안 신호음이 한 번 재생된 후 모니터링 신호음이 재생됩니다. 보안 신호음, 모니터링 신호음 및 녹음 톤이 모두 구성되고 통화가 녹음되고 모니터링되는 경우 보안 신호음이 한 번 재생된 후 녹음 톤이 재생됩니다. 모니터링 신호음은 재생되지 않습니다.

사일런트 모니터링 제한 사항

기능	제한 사항
참여	Unified Communications Manager에서는 자동 모니터링을 사용한 참여를 지원하지 않습니다. 상담사 통화가 모니터링되고 있는 경우 공유 회선을 통한 통화 참여가 실패합니다. 상담사 통화가 이미 참여한 경우 모니터링 통화는 실패합니다.
인터클러스터 트렁크를 통한 보안 사일런트 모니터링 전환	Unified Communications Manager는 인터클러스터 트렁크를 통한 보안 사일런트 모니터링 통화의 전환을 지원하지 않습니다.

기능	제한 사항
사일런트 모니터링 제한 사항	관리자가 비보안 모드를 통해 로그인하고 상담사가 MRA 모드에 로그인하면 모니터링이 실패합니다. 자세한 내용은 보안 사일런트 모니터링 섹션을 참조하십시오.



13 장

녹음

- 녹음 개요, 143 페이지
- 녹음 사전 요건, 147 페이지
- 녹음 구성 작업 흐름, 147 페이지
- 녹음 통화 흐름 예, 157 페이지
- 녹음 상호 작용 및 제한 사항, 157 페이지

녹음 개요

통화 녹음은 녹음 서버가 상담사 대화를 보관할 수 있도록 하는 Unified Communications Manager 기능입니다. 통화 녹음은 콜 센터, 금융 기관 및 기타 기업에서 중요한 기능 중 하나입니다. 통화 녹음 기능은 상담사 및 최종 사용자 미디어 스트림 복사본을 SIP 트렁크를 통해 레코딩 서버로 보냅니다. 각 미디어 스트림은 다양한 음성 분석 애플리케이션을 최적으로 지원할 수 있도록 개별적으로 전송됩니다.

Unified Communications Manager는 IP 전화기 기반 또는 네트워크 기반 녹음을 제공합니다.

- IP 전화기 기반 녹음은 전화기에서 녹음 미디어를 공급합니다. 전화기는 2개의 미디어 스트림을 레코딩 서버로 포킹합니다.
- 네트워크 기반 녹음은 전화기 또는 게이트웨이에서 녹음 미디어를 공급할 수 있습니다. 네트워크 기반 녹음을 구현할 때는 네트워크의 게이트웨이를 SIP 트렁크를 통해 Unified Communications Manager에 연결해야 합니다.

Unified Communications Manager에서는 단일 클러스터 및 멀티 클러스터 환경에서 모두 통화 녹음을 지원하며 다음과 같은 세 가지 녹음 모드를 제공합니다.

- 자동 녹음 — 자동 녹음은 회선 표시의 모든 통화를 자동으로 녹음합니다. Unified Communications Manager는 활성 녹음 세션이 설정된 전화기에서 시각적으로 표시되지 않는 상태에서 녹음 세션을 자동으로 호출합니다.
- 선택적 자동 녹음 - 감독자는 CTI 지원 기능이 있는 데스크톱을 통해 녹음 세션을 시작하거나 중지할 수 있습니다. 또는 녹음 서버는 미리 정의된 비즈니스 규칙 및 이벤트에 따라 세션을 호출할 수 있습니다. 활성 녹음 세션이 설정된 전화기에는 시각적 표시가 없습니다.

- 선택적 사용자 통화 녹음 — 상담사는 녹음할 통화를 선택할 수 있습니다. 상담사는 CTI 지원 데스크톱을 통해 또는 소프트키나 프로그램 가능한 라인 키를 사용하여 녹음 세션을 호출합니다. 선택적 사용자 통화 녹음이 사용되면 Cisco IP 전화기에는 녹음 세션 상태 메시지가 표시됩니다.

Unified Communications Manager는 단일 레코딩 서버에 대한 녹음을 지원하며, 두 개 이상의 레코딩 서버에 녹화할 수 있도록 CUBE와 함께 구축할 수 있습니다.

- 멀티 포크 녹음의 경우 Unified Communications Manager는 SIP 트렁크를 통해 CUBE 미디어 프록시 서버에 연결됩니다. CUBE 미디어 프록시 서버는 전화기나 게이트웨이에서 두 개의 미디어 스트림을 수신하고 미디어 스트림을 하나 이상의 레코딩 서버에 동시에 포크합니다.
- 단일 레코딩 서버에 대한 녹음의 경우 Unified Communications Manager는 SIP 트렁크를 통해 레코딩 서버에 직접 연결됩니다. 전화기 또는 게이트웨이는 2개의 미디어 스트림을 레코딩 서버로 포킹합니다.

멀티 포크 녹음

Unified Communications Manager는 Cisco Unified Border Element(CUBE)를 사용하여 미디어 프록시로 동시에 다중 스트림 녹음을 지원합니다. 멀티 포크 녹음의 경우 녹음 스트림은 CUBE 미디어 프록시 서버로 전송되어 미디어 스트림을 최대 5개의 녹음 서버로 동시에 릴레이합니다. 이는 전화기 기반 및 네트워크 기반 녹음, 자동 및 선택적 녹음 모두에 대해 지원됩니다.

멀티 포크 기능은 다음과 같은 이점을 제공합니다.

- 리턴던시 및 페일오버를 녹음 구축에 추가합니다.
- 음성 분석과 모니터링을 위한 추가 미디어 스트림을 제공합니다.
- 금융 산업과 같은 조직이 여러 녹음 서버에 대해 고객 통화 녹음을 의무화하는 MiFID 요구 사항을 준수할 수 있도록 지원합니다.

멀티 포크 녹음을 구현하는 경우 SIP 트렁크를 통해 Unified Communications Manager에 연결되는 네트워크에서 CUBE 미디어 프록시 서버를 구성해야 합니다.

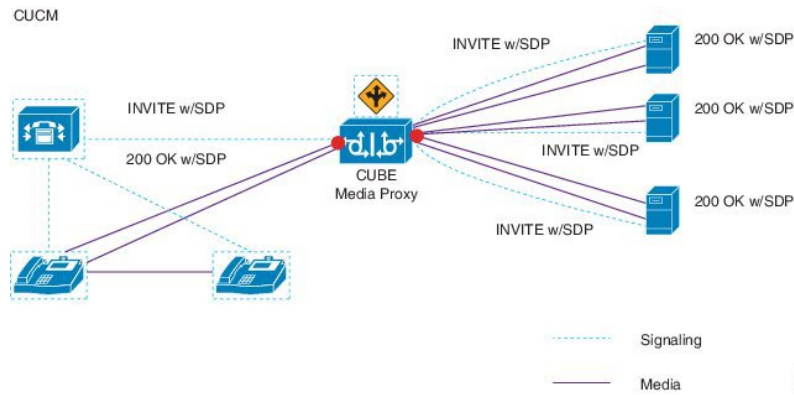
CUBE 큐브 미디어 프록시에 대한 자세한 내용은 [Cisco Unified Border Element 구성 설명서](#)를 참조하십시오.



참고 SIP 트렁크를 통해 CUBE 미디어 프록시 서버에 대한 Unified Communications Manager 연결은 얼리 오퍼로 구성해야 합니다.

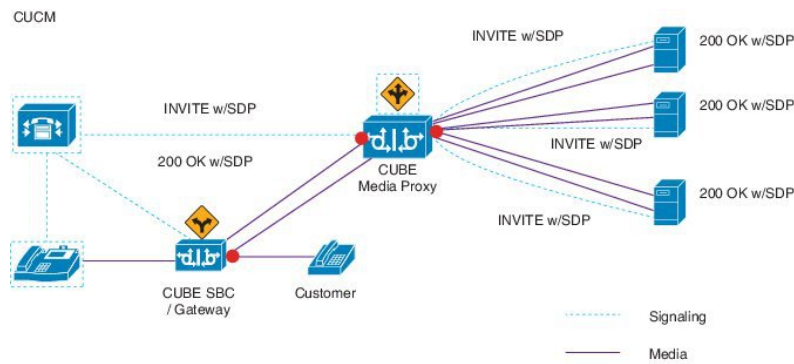
다음 예는 CUBE 미디어 프록시를 통해 멀티 포크 녹음의 전화기 기반 녹음을 보여줍니다.

그림 4: 전화기 기반 녹음



다음 예는 CUBE 미디어 프록시를 통해 멀티 포크 녹음의 네트워크 기반 녹음을 보여줍니다.

그림 5: 네트워크 기반 녹음



방법 요약에 대한 자세한 내용은 [Cisco Unified Communications Manager 릴리스 12.5\(1\) Cisco Unified JTAPI 개발자 설명서](#)의 "Cisco 디바이스별 내선 번호" 섹션을 참조하십시오.

지원되는 플랫폼

CUBE 미디어 프록시 서버를 통한 멀티 포크 녹음은 Cisco IOS XE Gibraltar 릴리스 16.10.1에서 실행되는 다음 Cisco 라우터 플랫폼에서 지원됩니다.

- Cisco 4000 Series-Integrated Services Routers(ISR G3 - ISR4331, ISR4351, ISR4431, ISR4451).
- Cisco Aggregated Services Routers(ASR - ASR1001-X, ASR1002-X, ASR1004(RP2 포함), ASR1006(RP2 포함)).
- Cisco Cloud Services Routers(CSR1000V 시리즈).

CUBE 미디어 프록시를 통한 멀티 포크 녹음에 대한 제한 사항

CUBE 미디어 프록시 서버를 통한 멀티 포크 녹음은 다음 기능을 지원하지 않습니다.

- 비디오 녹화.

- 비보안 통화의 보안 미디어(SRTP) 포크.
- SRTP 폴백.
- 통화 중 차단.

녹음 미디어 원본 선택

네트워크 기반 녹음을 구성할 때 전화기 또는 게이트웨이를 상담사 전화 회선에 대한 녹음 미디어의 기본 소스로 구성해야 합니다. 그러나 구축에 따라 Unified Communications Manager에서는 선호하는 선택 항목을 녹음 미디어 소스로 선택하지 않을 수도 있습니다. 다음 표에는 녹음 미디어 소스를 선택하는 데 사용하는 논리 Unified Communications Manager가 표시되어 있습니다.

표 18: 녹음 미디어 원본 선택

기본 미디어 원본	미디어 유형	통화 경로의 게이트웨이?	선택한 미디어 원본
게이트웨이	비보안(RTP)	예	게이트웨이
		아니요	전화기
	보안(sRTP)	예	전화기
		아니요	전화기
전화기	비보안(RTP)	예	전화기
		아니요	전화기
	보안(sRTP)	예	전화기
		아니요	전화기

대체 녹음 미디어 소스(첫 번째 선택 항목을 사용할 수 없는 경우)

Unified Communications Manager에서 선택한 녹음 미디어 소스를 사용할 수 없는 경우 Unified Communications Manager는 대체 소스를 사용합니다. 다음 표에서는 Unified Communications Manager에서 미디어 녹음을 위한 대체 소스를 선택하는 데 사용되는 논리를 보여줍니다.

표 19: 첫 번째 선택 항목을 사용할 수 없는 경우 대체 녹음 미디어 소스

선택한 미디어 원본	게이트웨이 선호됨	전화기 선호됨
첫 번째 시도	통화 경로의 첫 번째 게이트웨이	전화기
두 번째 시도	통화 경로의 마지막 게이트웨이	통화 경로의 첫 번째 게이트웨이
세 번째 시도	전화기	통화 경로의 마지막 게이트웨이

녹음 사전 요건

- Cisco Unified IP Phone 지원 - 녹음을 지원하는 Cisco Unified IP Phone의 목록을 보고, Cisco 통합 보고에 로그인하고, Unified CM 전화 기능 목록 보고서를 실행하여 녹음을 기능으로 선택합니다. 자세한 절차는 [전화기 기능 목록 생성, 7 페이지](#)의 내용을 참조하십시오.
- 게이트웨이 지원 — 게이트웨이가 녹음을 지원하는 데 대한 자세한 내용은 <https://developer.cisco.com/web/sip/wiki/-/wiki/Main/Unified+CM+Recording+Gateway+Requirements>의 내용을 참조하십시오.
- 다중 스트림 녹음을 구성하는 경우에는 CUBE 미디어 프록시를 구축하고 구성합니다. 자세한 내용은 [Cisco Unified Border Element 구성 설명서](#)의 **CUBE 미디어 프록시** 섹션을 참조하십시오.

녹음 구성 작업 흐름

시작하기 전에

프로시저

	명령 또는 동작	목적
단계 1	녹음 프로파일 만들기, 148 페이지	녹음 프로파일을 만듭니다.
단계 2	녹음에 대한 SIP 프로파일 구성, 148 페이지	선택 사항. 전화회의 브리지 식별자를 레코더에 전달하려면 SIP 프로파일을 구성합니다.
단계 3	녹음에 대한 SIP 트렁크 구성, 149 페이지	레코더 서버 또는 CUBE 미디어 프록시를 SIP 트렁크 디바이스로 구성합니다.
단계 4	녹음을 위한 경로 패턴 구성, 149 페이지	레코더 서버 또는 CUBE 미디어 프록시로 라우팅하는 라우트 패턴을 만듭니다.
단계 5	녹음을 위한 상담사 전화 회선 구성, 150 페이지	녹음을 위해 상담사 전화 회선을 구성합니다.
단계 6	<p>상담사 전화기에 대한 빌트-인 브리지(BIB)를 활성화합니다. 다음 작업 중 하나를 수행하여 녹음을 위해 빌트-인 브리지(BIB)를 활성화합니다.</p> <ul style="list-style-type: none"> • 클러스터에 대해 빌트-인 브리지(BIB) 활성화, 151 페이지 • 전화기의 빌트-인 브리지(BIB) 활성화, 151 페이지 	<p>상담사 전화기를 녹음 미디어 소스로 사용하려면 녹음을 위해 전화기의 빌트-인 브리지(BIB)를 활성화해야 합니다. 서비스 매개 변수를 사용하여 클러스터 전체에서 빌트-인 브리지(BIB) 기본값을 설정하거나 개별 전화기에서 빌트-인 브리지(BIB)를 활성화할 수 있습니다.</p> <p>참고 개별 전화기의 빌트-인 브리지(BIB) 설정은 클러스터 수준 기본값을 무시합니다.</p>

	명령 또는 동작	목적
단계 7	녹음을 위한 게이트웨이 활성화, 152 페이지	게이트웨이에서 Unified Communications 서비스를 구성합니다.
단계 8	녹음 알림 신호음 구성, 152 페이지	통화가 녹음될 때 알림 신호음을 재생할지 여부를 구성합니다.
단계 9	전화기가 기능 버튼 또는 소프트키를 사용하는지 여부에 따라 다음 절차 중 하나를 수행합니다. <ul style="list-style-type: none"> • 녹음 기능 버튼 구성, 153 페이지 • 녹음 소프트키 구성, 154 페이지 	전화기에 대한 녹음 기능 버튼 또는 소프트키를 구성합니다.

녹음 프로파일 만들기

이 절차를 사용하여 프로파일을 만듭니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 녹음 프로파일.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 이름 필드에 녹음 프로파일의 이름을 입력합니다.
- 단계 4 녹음 발신 검색 공간 필드에서 녹음 서버에 대해 구성된 라우트 패턴을 사용하여 파티션을 포함하는 발신 검색 공간을 선택합니다.
- 단계 5 녹음 대상 주소 필드에 녹음 서버의 디렉터리 번호나 URL 또는 CUBE 미디어 프록시 서버의 URL을 입력합니다.
- 단계 6 저장을 클릭합니다.

녹음에 대한 SIP 프로파일 구성

이 절차를 사용하여 전화회의 브리지 식별자를 레코더에 전달하고 SIP 프로파일을 구성합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > SIP 프로파일.
- 단계 2 네트워크에 사용할 SIP 프로파일을 선택합니다.
- 단계 3 음성 및 영상 통화애 **Early Offer** 지원 필드에 대한 값을 설정합니다. Early Offer 지원을 받으려면 Unified Communications Manager에서 CUBE 미디어 프록시 서버까지의 SIP 트렁크를 사용하도록 설정해야 하며 구성 옵션은 **Best Effort**(MTP 삽입 없음) 및 필수(필요한 경우 **MTP** 삽입)입니다.

참고 필수로 SIP 트렁크를 활성화하는 것이 좋습니다(필요한 경우 MTP 삽입).

단계 4 전화회의 브리지 식별자 전달 확인란을 선택합니다.

단계 5 저장을 클릭합니다.

녹음에 대한 SIP 트렁크 구성

이 절차를 사용하여 SIP 트렁크 구성 창에서 녹음 서버 정보를 할당합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 트렁크.

단계 2 새로 추가를 클릭합니다.

단계 3 트렁크 유형 드롭다운 목록에서 SIP 트렁크를 선택합니다.

디바이스 프로토콜은 SIP에 자동으로 채워집니다. 이 옵션은 유일하게 사용할 수 있습니다.

단계 4 트렁크 서비스 유형 드롭다운 목록에서 네트워크에서 사용할 서비스 유형을 선택합니다. 기본값은 없음입니다.

단계 5 다음을 클릭합니다.

단계 6 SIP 정보 창의 대상 주소 필드에 녹음 서버 또는 CUBE 미디어 프록시의 IP 주소, 정규화된 도메인 이름 또는 DNS SRV를 입력합니다.

단계 7 SIP 정보 창의 SIP 프로파일 드롭다운 목록에서 네트워크에서 사용할 SIP 프로파일을 선택합니다.

단계 8 녹음 정보 창에서 다음 옵션 중 하나를 선택합니다.

- 없음 - 이 트렁크는 녹음에 사용되지 않습니다.
- 이 트렁크는 녹음 사용 기능이 있는 게이트웨이에 연결됩니다.
- 이 트렁크는 녹음 사용 기능이 있는 게이트웨이를 포함한 다른 클러스터에 연결됩니다.

단계 9 저장을 클릭합니다.

참고 이 트렁크에 사용되는 SIP 프로파일에서 초기 제공 지원을 위해 Unified Communications Manager에서 미디어 프록시로의 SIP 트렁크를 활성화해야 합니다. 구성 옵션은 필수(필요한 경우 MTP 삽입) 및 최선의 노력(MTP 삽입 없음)입니다.

녹음을 위한 경로 패턴 구성

이 절차를 사용하여 레코더와 관련된 라우트 패턴 구성을 설명합니다. 녹음 서버 또는 CUBE 미디어 프록시 서버로 라우팅하는 라우트 패턴을 구성해야 합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 라우트/헌트 > 라우트 패턴.
- 단계 2 새로 추가를 클릭하여 새 라우트 패턴을 생성합니다.
- 단계 3 라우트 패턴 구성 창에서 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 4 통화 녹음의 경우 다음 필드를 완료합니다.
- 패턴—녹음 프로파일의 녹음 대상 주소와 일치하는 패턴을 입력합니다.
 - 게이트웨이/라우트 목록 - 녹음 서버를 가리키는 SIP 트렁크 또는 라우트 목록을 선택합니다.
- 단계 5 저장을 클릭합니다.
-

녹음을 위한 상담사 전화 회선 구성

이 절차를 사용하여 녹음을 위한 상담사 전화 회선을 구성합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭합니다.
- 단계 3 상담사의 전화기를 선택합니다.
- 단계 4 왼쪽 연결 창에서 상담사가 설정을 볼 수 있는 전화 회선을 클릭합니다.
- 단계 5 녹음 옵션 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
- 통화 녹음 비활성화 - 이 전화 회선의 통화가 녹음되지 않습니다.
 - 자동 통화 녹음 활성화 - 이 전화 회선의 통화가 녹음됩니다.
 - 선택적 통화 녹음 활성화 - 이 전화 회선에서 선택한 통화만 녹음됩니다.
- 단계 6 녹음 프로파일 드롭다운 목록에서 상담사에 대해 구성된 녹음 프로파일을 선택합니다.
- 단계 7 녹음 미디어 소스 드롭다운 목록에서 게이트웨이 또는 전화기를 녹음 미디어의 기본 소스로 사용할지 여부를 선택합니다.
- 단계 8 사용자가 다중 수준 우선 순위 및 선점(MLPP)을 구성한 경우 사용 중 트리거 필드를 최소 3으로 설정합니다.
- 단계 9 저장을 클릭합니다.
-

클러스터에 대해 빌트-인 브리지(BIB) 활성화

이 절차를 사용하여 녹음을 위해 전화기의 빌트-인 브리지(BIB)에서 상담사 전화기를 녹음 미디어 소스로 사용 하도록 설정할 수 있습니다.

빌트-인 브리지(BIB) 클러스터 수준 서비스 매개 변수를 활성화로 설정하면 클러스터의 모든 전화기에 대해 빌트-인 브리지(BIB) 기본 설정이 활성화로 변경됩니다. 그러나 해당 전화기에 대해 기본 옵션이 선택되지 않은 경우 개별 전화기에 대한 전화기 구성 창의 빌트-인 브리지(BIB) 설정은 클러스터 수준 서비스 매개 변수 설정을 무시합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 CallManager 서비스가 실행 중인 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 Cisco CallManager를 선택합니다.
- 단계 4 빌트-인 브리지(BIB) 활성화 서비스 매개 변수를 켜기로 설정합니다.
- 단계 5 저장을 클릭합니다.

전화기의 빌트-인 브리지(BIB) 활성화

이 절차를 사용하여 개별 전화기에서 빌트-인 브리지(BIB)를 활성화합니다. 기본 옵션을 선택하지 않으면 전화기 구성 창에서 빌트-인 브리지(BIB) 설정이 클러스터 수준 서비스 매개 변수를 무시합니다.

선택적으로 서비스 매개 변수를 사용하여 클러스터에서 빌트-인 브리지(BIB) 기본값을 설정합니다. 자세한 내용은 [클러스터에 대해 빌트-인 브리지\(BIB\) 활성화, 151 페이지](#)의 내용을 참조하십시오.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기.
- 단계 2 찾기를 클릭하여 상담사 전화기를 선택합니다.
- 단계 3 빌트-인 브리지(BIB) 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 켜기 - 빌트-인 브리지(BIB)가 활성화됩니다.
- 끄기 - 빌트-인 브리지(BIB)가 비활성화됩니다.
- 기본값 - 클러스터 수준 빌트-인 브리지(BIB) 활성화 서비스 매개 변수 설정이 사용됩니다.

참고 빌트-인 브리지(BIB)가 설정되어 있고 미디어 터미네이션 포인트 필요 확인란을 선택하는 경우에는 녹음에 실패할 수 있습니다.

- 단계 4 저장을 클릭합니다.

녹음을 위한 게이트웨이 활성화

이 절차를 사용하여 녹음을 위한 게이트웨이를 구성합니다. 통합 커뮤니케이션 게이트웨이 서비스를 활성화해야 합니다. 다음 작업 흐름에는 통합 커뮤니케이션 게이트웨이 서비스를 활성화하는 상위 수준 프로세스가 포함되어 있습니다.

프로시저

단계 1 디바이스에서 Unified Communications Manager IOS 서비스를 구성합니다.

단계 2 XMF 공급자를 구성합니다.

단계 3 통합 커뮤니케이션 게이트웨이 서비스를 확인합니다.

예를 포함하여 자세한 구성 단계를 보려면 다음 문서 중 하나에 대한 Cisco Unified Communications 게이트웨이 서비스 장을 참조하십시오.

- 자세한 내용은 ISR 라우터 [Cisco Unified Border Element\(엔터프라이즈\) 프로토콜 독립적 기능 및 설정 구성 설명서](#), Cisco IOS XE 릴리스 35를 참조하십시오.
- 자세한 내용은 ASR 라우터 [Cisco Unified Border Element \(엔터프라이즈\) 프로토콜 독립적 기능 및 설정 구성 설명서](#), Cisco IOS 릴리스 15M&T를 참조하십시오.

녹음 알림 신호음 구성

이 절차를 사용하여 통화가 녹음될 때 재생되도록 알림 신호음을 구성합니다. 법적 준수를 위해 녹음 세션이 진행 중임을 나타내는 주기적 신호음 형태의 명시적 알림이 에이전트, 통화자 또는 두 상대방에게 들립니다. 이 신호음을 비활성화할 수도 있습니다.



참고 같은 통화에 대해 녹음 및 모니터링 신호음이 둘 다 활성화되면 녹음 신호음 설정이 모니터링 신호음 설정을 무시합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 Cisco CallManager 서비스가 실행 중인 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 상담사에게 알림음을 재생하려면 관찰 대상에게 녹음 알림 신호음 재생(상담사) 서비스 매개 변수를 **True**로 설정합니다.

단계 5 고객에게 알림음을 재생하려면 연결된 관찰 상대방에게 녹음 알림 신호음 재생(고객) 서비스 매개 변수의 값을 **True**로 설정합니다.

단계 6 저장을 클릭합니다.

녹음 기능 버튼 구성

전화기에서 기능 버튼을 사용하는 경우 이 절차를 사용하여 녹음 기능 버튼을 전화기에 할당합니다.

프로시저

	명령 또는 동작	목적
단계 1	녹음을 위한 전화기 버튼 템플릿 구성, 153 페이지	녹음 버튼을 포함하는 전화기 버튼 템플릿을 구성합니다.
단계 2	전화기 버튼 템플릿을 전화기와 연결, 154 페이지	녹음을 위해 설정하는 전화기 버튼 템플릿을 전화기에 연결합니다.

녹음을 위한 전화기 버튼 템플릿 구성

이 절차를 사용하여 녹음 기능 버튼을 포함하는 전화기 버튼 템플릿을 생성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.

단계 2 [찾기]를 클릭하여 지원 되는 전화기 템플릿 목록을 표시합니다.

단계 3 새 전화기 버튼 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.

- 전화기의 모델에 대한 기본 템플릿을 선택하고 복사를 클릭합니다.
- 전화기 버튼 템플릿 정보 필드에 템플릿의 새 이름을 입력합니다.
- 저장을 클릭합니다.

단계 4 기존 템플릿에 전화기 버튼을 추가하려는 경우 다음 단계를 수행합니다.

- 찾기를 클릭하고 검색 기준을 입력합니다.
- 기존 템플릿을 선택합니다.

단계 5 회선 드롭다운 목록에서 템플릿에 추가하려는 기능을 선택합니다.

단계 6 저장을 클릭합니다.

단계 7 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다.

전화기 버튼 템플릿을 전화기와 연결

이 절차를 사용하여 전화기의 녹음 버튼에 대해 생성한 전화기 버튼 템플릿을 연결합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.
- 단계 3 전화기 버튼 템플릿을 추가할 전화기를 선택합니다.
- 단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.
- 단계 5 저장을 클릭합니다.
전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

녹음 소프트웨어 구성

전화기에서 소프트웨어를 사용하는 경우 이 절차를 사용하여 전화기에 녹화 소프트웨어를 추가합니다. 이 녹화 소프트웨어는 기능 하드웨어 템플릿을 사용하는 Cisco Chaperone Phone에 대해 연결된 통화 상태에서만 사용할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	녹음을 위한 소프트웨어 템플릿 구성, 154 페이지	녹화 소프트웨어를 포함하는 소프트웨어 템플릿을 구성합니다.
단계 2	다음 절차 중 하나를 수행합니다. <ul style="list-style-type: none"> 소프트웨어 템플릿을 전화기에 연결, 155 페이지 소프트웨어 템플릿을 일반 디바이스 구성에 연결, 156 페이지 	소프트웨어 템플릿을 전화기에 직접 연결하거나 일반 디바이스 구성에 연결합니다. 그런 다음 일반 디바이스 구성을 전화기 그룹에 연결할 수 있습니다.

녹음을 위한 소프트웨어 템플릿 구성

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트웨어 템플릿.
- 단계 2 새 소프트웨어 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
 - a) 새로 추가를 클릭합니다.

- b) 기본 템플릿을 선택하고 복사를 클릭합니다.
- c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
- d) 저장을 클릭합니다.

단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.

- a) 찾기를 클릭하고 검색 기준을 입력합니다.
- b) 필요한 기존 템플릿을 선택합니다.

단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.

참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.

단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.

단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.

단계 7 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.

단계 8 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.

단계 9 저장을 클릭합니다.

단계 10 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

소프트키 템플릿을 전화기에 연결

이 절차를 사용하여 레코드 소프트키를 포함하는 소프트키 템플릿을 전화기에 직접 연결하여 전화기에 녹화 소프트키를 할당합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하고 전화기를 선택하여 소프트키 템플릿을 추가합니다.

단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 재설정을 눌러 전화기 설정을 업데이트합니다.

소프트키 템플릿을 일반 디바이스 구성에 연결

이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하여 전화기에 녹음 소프트키를 추가합니다.

프로시저

	명령 또는 동작	목적
단계 1	소프트키 템플릿을 일반 디바이스 구성에 추가, 156 페이지	
단계 2	전화기에 일반 디바이스 구성 추가, 157 페이지	

소프트키 템플릿을 일반 디바이스 구성에 추가

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성

단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.

- 새로 추가를 클릭합니다.
- 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
- 저장을 클릭합니다.

단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.

- 찾기를 클릭하고 검색 기준을 입력합니다.
- 기존 일반 디바이스 구성을 클릭합니다.

단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

단계 6 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

전화기에 일반 디바이스 구성 추가

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정 을 클릭하여 전화기 설정을 업데이트합니다.

녹음 통화 흐름 예

네트워크 기반 통화 녹음 및 IP 전화 기반 통화 녹음 사용 사례 모두에 대한 통화 흐름 예는 다음 URL에서 네트워크 기반 및 전화 기반 녹음에 대한 통화 녹음 예를 참조하십시오.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/configExamples/cucm_b_recording-use-cases.html

녹음 상호 작용 및 제한 사항

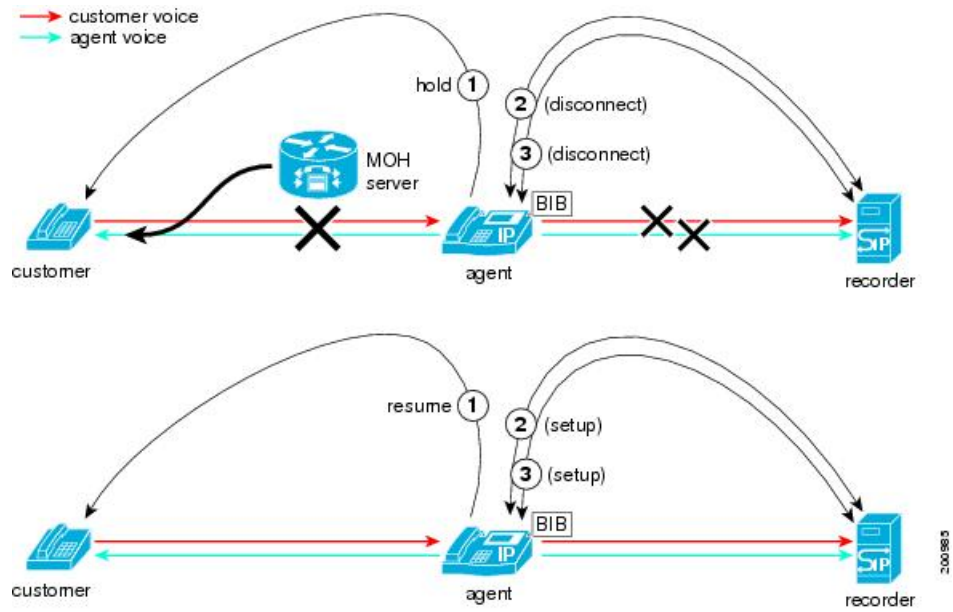
기능	상호 작용 및 제한 사항
모니터링 신호음	녹음 톤은 녹음되고 모니터링되는 통화의 모니터링 신호음보다 우선합니다. 둘 다 구성되고 통화가 녹음되고 모니터링되는 경우 녹음 톤이 재생됩니다.
MLPP(Multilevel Precedence and Preemption)	MLPP(다중 수준 우선 순위 및 선점)도 구성된 경우 녹음 중인 상담사 전화선의 통화 중 트리거 설정을 최소 3으로 설정해야 합니다.
보안 신호음	보안 신호음이 구성된 경우, 녹음 톤의 구성 여부와 관계 없이 보안 통화가 시작될 때 보안 신호음이 두 통화 참가자 모두에게 재생됩니다. 보안 신호음 및 녹음 톤이 모두 구성되고 통화가 안전한 경우 통화를 시작할 때 보안 신호음이 한 번 재생된 후 녹음 톤이 재생됩니다. 보안 신호음, 녹음 톤 및 모니터링 신호음을 모두 구성하고 통화를 보안, 녹음 및 모니터링한 경우 보안 신호음이 한 번 재생된 후 녹음 톤이 재생됩니다. 모니터링 신호음은 재생되지 않습니다.
Customer Voice Portal	고객 음성 포털을 통해 라우팅되는 상담사 고객 통화는 상담사 전화기를 녹음 소스로 사용하여 녹음할 수 있습니다.

기능	상호 작용 및 제한 사항
SIP 프록시 서버	게이트웨이를 녹음 소스로 사용하는 경우에는 Unified Communications Manager와 게이트웨이 사이에 SIP 프록시 서버를 배치할 수 없습니다.
최번시 통화 완료 비율	각 녹음 세션은 BHCC(최번시 통화 완료 수)에 두 개의 통화를 추가하여 CTI 리소스에 최소한의 영향을 미칩니다.
Media Sense를 사용한 선택적 녹음	<p>선택적 녹음이 구성되면 Media Sense 서버는 호 전환 중에 상담 통화를 녹음하지 않습니다. 예를 들어 상담사와 고객 간의 통화가 녹음되고 상담사가 두 번째 상담사에게 호 전환을 시작하는 경우 통화를 호 전환하기 전에 두 상담사 사이에서 발생하는 상담 통화는 녹음되지 않습니다.</p> <p>상담 통화가 녹음되도록 하려면 상담 통화가 시작될 때 상담사가 '녹음' 소프트웨어를 눌러야 합니다.</p>
인증된 전화기에서 녹음	인증된 전화기에 대한 통화를 녹음하려면 Cisco Unified CM 서비스 매개 변수 페이지에서 인증된 전화기 녹음 필드를 녹음 허용으로 설정합니다. 기본값은 녹음 허용 안 함입니다. Unified Communications Manager에서는 비보안 레코더를 사용하는 동안 인증된 전화기에 대한 통화 녹음을 허용합니다. 보안 레코더의 경우, 레코더에서 보안 SRTP(실시간 전송 프로토콜) 폴백을 지원하는 경우에만 녹음을 사용할 수 있습니다.
전화회의의 선택 및 참가의 자동 녹음 통화에 대한 코덱 잠금	SCCP(Skinny Client Control Protocol) 전화기는 녹음이 활성화되어 있고 Unified Communications Manager에서 전화회의의 선택 및 참가를 수행하는 경우 하나의 단일 코덱을 광고합니다.

통화 녹음은 상담사 보류 상태를 유지하지 않음

통화 녹음은 상담사가 통화를 보류하면 해제되고, 상담사가 통화를 재개하면 다시 설정됩니다.

그림 6: 통화 녹음은 상담사 보류 상태를 유지하지 않음





VI 부

콜 센터 기능

- 상담사 인사말 , 163 페이지
- Auto-Attendant , 167 페이지
- Manager Assistant , 177 페이지



14 장

상담사 인사말

- 상담사 인사말 개요, 163 페이지
- 상담사 인사말 사전 요건, 163 페이지
- 상담사 인사말 구성 작업 흐름, 164 페이지
- 상담사 인사말 문제 해결, 165 페이지

상담사 인사말 개요

상담사 인사말을 사용하면 Unified Communications Manager에서 상담사 디바이스에 대한 미디어 연결 성공 후에 미리 녹음된 알림을 자동으로 재생할 수 있습니다. 상담사 인사말은 상담사 및 고객이 들을 수 있습니다.

인사말을 녹음하는 과정은 음성 메일로 메시지를 녹음하는 것과 유사합니다. 컨택 센터가 설정된 방식에 따라 다른 유형의 발신자에 대해 재생되는 다른 인사말(예: 영어 사용자의 경우 영어 인사말 또는 이탈리아어 사용자의 경우 이탈리아어 인사말)을 녹음할 수 있습니다.

상담사 인사말은 상담사 데스크톱에 로그인할 때 기본적으로 활성화되어 있지만 필요에 따라 켜다 가 켤 수 있습니다.

상담사 인사말 사전 요건

- Cisco Unified Contact Center Enterprise를 설치합니다. [Cisco Unified Contact Center Express 설치 및 업그레이드 설명서](#)를 참조하십시오.
- Cisco Unified Customer Voice Portal을 설치합니다. [Cisco Unified Customer Voice Portal용 설치 및 업그레이드 가이드](#)를 참조하십시오.
- 빌트-인 브리지(BIB)가 활성화되었는지 확인합니다. 세부 정보를 보려면 [빌트-인 브리지\(BIB\) 구성, 165 페이지](#)의 내용을 참조하십시오.

상담사 인사말 구성 작업 흐름

상담사 인사말 구성 작업은 Cisco Unified Contact Center Enterprise(Unified CCE) 및 Cisco Unified Customer Voice Portal(Unified CVP)에서 완료됩니다. 다음 작업에 대한 세부 단계를 보려면 [Cisco Unified Contact Center Enterprise 기능 설명서](#)의 상담사 인사말 섹션을 참조하십시오.

시작하기 전에

- [상담사 인사말 사전 요건](#), 163 페이지 검토

프로시저

	명령 또는 동작	목적
단계 1	<p>상담사 인사말을 위한 미디어 서버를 구성합니다.</p> <ul style="list-style-type: none"> • 미디어 서버로 작동하도록 서버를 구성합니다. • Unified CVP에서 미디어 서버를 추가합니다. • 파일을 쓰도록 미디어 서버를 구성합니다. 	<p>상담사 인사말은 Unified CVP 미디어 서버를 사용하여 프롬프트 및 인사말 파일을 저장하고 제공합니다.</p>
단계 2	<p>.tcl 스크립트를 VXML Voice Extensible Markup Language) 게이트웨이로 다시 게시합니다.</p>	<p>Unified CVP 릴리스 9.0(1)과 함께 제공되는 .tcl 스크립트 파일은 상담사 인사말을 지원하는 업데이트를 포함합니다. 이러한 업데이트된 파일을 VXML 게이트웨이에 다시 게시해야 합니다.</p> <p>VXML 게이트웨이에 대한 스크립트를 다시 게시하는 것은 Unified CVP 업그레이드의 표준 작업입니다. Unified CVP를 업그레이드하고 스크립트를 다시 게시하지 않은 경우 상담사 인사말을 사용하려면 먼저 스크립트를 다시 게시해야 합니다.</p>
단계 3	<p>VXML 게이트웨이에 캐시 크기를 설정합니다.</p>	<p>적절한 성능을 보장하려면 VXML 게이트웨이의 캐시 크기를 허용되는 최대값으로 설정합니다. 최대 크기는 100메가바이트입니다. 기본값은 15kb입니다. VXML 게이트웨이 캐시를 최대로 설정하지 못하면 성능이 저하되어 미디어 서버에 대한 트래픽이 증가할 수 있습니다.</p>

	명령 또는 동작	목적
단계 4	음성 프롬프트를 작성하여 인사말을 녹음합니다.	상담사가 인사말을 녹음할 때 들리는 각 음성 프롬프트에 대한 오디오 파일을 생성합니다.
단계 5	통화 유형을 구성합니다.	상담사 인사말 녹음 및 재생을 완료합니다.
단계 6	전화 건 번호를 구성합니다.	상담사 인사말 녹음 및 재생을 완료합니다.
단계 7	스크립트를 예약합니다.	
단계 8	네트워크 VRU 스크립트를 정의합니다.	Unified CVP와 상호 작용하기 위한 상담사 인사말 녹음 및 재생 스크립트의 경우 네트워크 VRU 스크립트가 필요합니다.
단계 9	(선택 사항) 샘플 상담사 인사말 스크립트를 가져옵니다.	
단계 10	Unified CCE 통화 라우팅 스크립트를 수정합니다.	상담사 인사말 재생 스크립트를 사용하도록 Unified CCE 통화 라우팅 스크립트를 수정합니다.

빌트-인 브리지(BIB) 구성

개별 전화기에 대한 전화기 구성 창에서 빌트-인 브리지(BIB) 설정은 빌트-인 브리지(BIB) 활성화 클러스터 수준 서비스 매개 변수 설정을 무시합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하여 상담사 전화기를 선택합니다.

단계 3 빌트-인 브리지(BIB) 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 켜기 - 빌트-인 브리지(BIB)가 활성화됩니다.
- 끄기 - 빌트-인 브리지(BIB)가 비활성화됩니다.
- 기본값 - 클러스터 수준 빌트-인 브리지(BIB) 활성화 서비스 매개 변수 설정이 사용됩니다.

단계 4 저장을 클릭합니다.

상담사 인사말 문제 해결

상담사 인사말 문제를 해결하는 방법에 대한 자세한 내용은 [Cisco Unified Contact Center Enterprise의 상담사 인사말 및 위스퍼 알림 기능 설명서](#)의 “상담사 인사말 문제 해결”을 참조하십시오.



15 장

Auto-Attendant

- [오토 어텐던트 개요, 167 페이지](#)
- [Cisco Unity Connection 구성, 168 페이지](#)
- [Cisco Unified CCX 구성, 173 페이지](#)
- [Cisco Unity Express 구성, 175 페이지](#)

오토 어텐던트 개요

오토 어텐던트를 사용하면 발신자는 접수원을 통하지 않고도 조직에서 사람을 찾을 수 있습니다. 발신자에게 재생되는 프롬프트를 사용자 정의할 수 있습니다.

Unified Communications Manager에서 오토 어텐던트는 특정 전화기 내선 번호에서 통화를 수신하는데 사용됩니다. 소프트웨어는 발신자와 상호 작용하여 발신자가 연결하려고 하는 (조직 내) 당사자의 내선 번호를 검색하고 선택할 수 있도록 합니다.

오토 어텐던트는 다음 기능을 제공합니다.

- 전화에 응답
- 사용자 구성 가능 환영 프롬프트 재생
- 발신자가 세 가지 작업 중 하나를 수행하도록 요청하는 주 메뉴 프롬프트 재생
 - 오퍼레이터와 통화하려면 0을 누르세요.
 - 내선 번호를 입력하려면 1을 누르세요.
 - 이름 철자를 입력하려면 2를 누르세요.

발신자가 2를 눌러 이름 철자 입력을 선택할 경우 시스템에서 입력된 문자와 사용 가능한 내선이 구성된 이름을 비교합니다. 다음 결과 중 하나가 발생할 수 있습니다.

- 일치하는 내선 번호가 있을 경우 시스템에서 일치되는 사용자로 호전환을 수행한다는 알림을 내보내고 발신자가 아무 DTMF(복합 주파수 부호) 키를 눌러 호전환을 중지할 수 있도록 최대 2초간 대기합니다. 발신자가 호전환을 중지하지 않을 경우 시스템이 명시적 확인을 수행합니다. 즉, 사용자에게 이름 확인을 요청하고 해당 사용자의 기본 내선 번호로 호전환을 실시합니다.

- 일치하는 내선 번호가 두 개 이상인 경우 시스템은 발신자에게 올바른 내선 번호를 선택할 것을 요청합니다.
- 일치하는 내선 번호가 너무 많을 경우 시스템은 발신자에게 추가 문자를 입력하도록 요청합니다.
- 일치하는 항목이 없는 경우, 즉 사용자가 잘못된 옵션을 누르면 시스템에서 잘못된 옵션을 눌렀다는 메시지를 표시하고 사용자에게 올바른 옵션을 누르라는 메시지를 표시합니다.
- 발신자가 대상을 지정하면 호전환이 실시됩니다.
- 회선이 통화 중이거나 사용 중인 회선이 아닐 경우 시스템은 발신자에게 그러한 내용을 알리고 주 메뉴 프롬프트를 재생합니다.

오토 어텐던트 솔루션은 대화식 음성응답(IVR) 기능을 제공할 수 있는 다양한 Cisco 제품을 사용하여 다음과 같은 세 가지 방법으로 배포할 수 있습니다.

- Cisco Unity Connection(CUC)을 사용하는 오토 어텐던트, 고객이 가장 많이 사용하는 오토 어텐던트 솔루션 구성
- Cisco Unified Contact Center Express(Unified CCX)를 사용하는 오토 어텐던트
- Cisco Unity Express(CUE)를 사용하는 오토 어텐던트

Cisco Unity Connection 구성

Cisco Unity Connection 서버는 외부 및 내부 발신자 모두에 대해 무인 자동 교환 시스템 기능을 제공합니다. 오토 어텐던트를 사용하면 운영자 또는 접수 담당자 개입 없이 발신자를 자동으로 내선 번호로 전송할 수 있습니다.

오토 어텐던트는 메뉴 시스템을 제공합니다. 또한 발신자가 번호(일반적으로 “0”)로 전화를 걸어 라 이브 운영자에게 전화를 걸 수 있습니다. 개별 사이트 위치를 지원하기 위해 여러 개의 오토 어텐던 트가 구현될 수 있습니다. Cisco Unity Connection 내에서 오토 어텐던트는 여러 통화 처리기를 함께 만들고 연결하여 작성되는 사용자 정의된 애플리케이션 트리 구조입니다. 오토 어텐던트는 시작 및 종료 포인트에 의해 정의되며, 발신자 DTMF 입력 선택 사항에 따라 중간 라우팅 결정을 할 수 있습니다.

오토 어텐던트 기본 동작 및 예에 대한 자세한 내용은 [Cisco Unity Connection 시스템 관리 지침서](#)를 참조하십시오.

Cisco Unity Connection 구성 작업 흐름

이 작업 흐름을 사용하여 Cisco Unity Connection을 사용하는 오토 어텐던트를 구성할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	CTI 라우트 포인트 구성, 170 페이지	Cisco Unified CM 관리에서 이 작업을 수행합니다. 회사의 DID(Direct-Inward Dial) 번호 (보드 번호)로 매핑되는 CTI 경라우트 포인트를 만듭니다.
단계 2	오토 어텐던트 시스템 통화 처리기 구성, 170 페이지	<p>통화 처리기는 통화에 응답하고, 발신자에게 녹음된 프롬프트로 인사하고, 발신자에게 정보와 옵션을 제공하고, 통화를 라우팅하고 메시지를 받습니다.</p> <p>참고 편집 > 인사말을 선택하여 오토 어텐던트 통화 처리기의 인사말을 사용자 정의할 수 있습니다. 인사말 사용자 정의에 대한 자세한 내용은 Cisco Unity Connection 시스템 관리 지침서를 참조하십시오.</p>
단계 3	발신자 입력 옵션 구성, 171 페이지	발신자 입력 옵션을 사용하면 단일 숫자를 지정하여 사용자 내선 번호, 대체 연결 번호, 통화 처리기, 인터뷰 처리기 또는 디렉터리 처리기를 나타낼 수 있습니다. 발신자는 전체 내선 번호를 입력하는 대신에 통화 처리기 인사말 중에 단일 키를 누르고 Cisco Unity Connection은 그에 따라 응답합니다. 발신자 입력 옵션으로 구성된 여러 다른 키가 발신자에게 통화 처리기 인사말의 선택 메뉴를 제공합니다.
단계 4	운영자 통화 처리기에 대한 내선 번호 구성, 171 페이지	발신자가 통화 처리기 인사말 중에 운영자에게 말할 수 있도록 운영자에 대한 내선 번호를 구성합니다.
단계 5	운영자에 대한 표준 호 전환 규칙 수정, 172 페이지	발신자가 0을 눌러 운영자에게 말할 때 통화가 운영자에게 전달될 수 있도록 표준 통화 전환 규칙을 수정합니다.
단계 6	기본 시스템 전송 제한 테이블 업데이트, 172 페이지	기본 시스템 전송 제한 테이블을 업데이트합니다. 기본 시스템 전송 제한 테이블은 발신자 시스템 전환에 사용할 수 있는 번호를 제한하며, 식별되지 않은 발신자가 지정된 번호로 전환할 수 있습니다.

CTI 라우트 포인트 구성

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > **CTI** 라우트 포인트.
 - 단계 2 새로 추가를 클릭합니다.
 - 단계 3 디바이스 이름 필드에 라우트 포인트에 대한 디바이스 이름을 입력합니다.
 - 단계 4 디바이스폴 드롭다운 목록에서 기본값을 선택합니다.
 - 단계 5 저장을 클릭합니다.
추가 성공 메시지가 표시됩니다.
 - 단계 6 연결 영역에서 회선 [1] - 새 **DN** 추가를 클릭합니다.
디렉터리 번호 구성 창이 표시됩니다.
 - 단계 7 디렉터리 번호 필드에 회사의 DID와 일치하는 디렉터리 번호를 입력합니다.
 - 단계 8 라우트 파티션 드롭다운 목록에서 필요한 라우트 파티션을 선택합니다.
 - 단계 9 착신 전환 및 당겨 받기 설정 영역에서 모두 착신 전환을 위해 적절한 발신 검색 공간을 선택하고 음성 메일 확인 확인란을 선택합니다.
 - 단계 10 저장을 클릭합니다.
-

오토 어텐던트 시스템 통화 처리기 구성

프로시저

-
- 단계 1 Cisco Unity Connection 관리에서 왼쪽의 Cisco Unity Connection 트리에서 통화 관리로 이동하여 시스템 통화 처리기를 선택합니다.
 - 단계 2 새로 추가를 클릭합니다.
새 통화 처리기 창이 표시됩니다.
 - 단계 3 표시 이름 필드에 **AutoAttendant**를 입력합니다.
 - 단계 4 내선 번호 필드에 CTI 라우트 포인트에 대해 제공한 것과 동일한 내선 번호를 입력합니다.
 - 단계 5 저장을 클릭합니다.
통화 처리기 기본 사항 편집(**AutoAttendant**) 창이 표시됩니다.
 - 단계 6 필수 필드를 편집하고 저장을 클릭합니다.
-

발신자 입력 옵션 구성

프로시저

-
- 단계 1 Cisco Unity Connection 관리에서 왼쪽의 Cisco Unity Connection 트리에서 통화 관리로 이동하여 시스템 통화 처리기를 선택합니다.
 - 단계 2 **AutoAttendant**를 클릭합니다.
통화 처리기 기본 사항 편집(**AutoAttendant**) 창이 표시됩니다.
 - 단계 3 편집 > 발신자 입력을 선택합니다.
발신자 입력 창이 표시됩니다.
 - 단계 4 키 열에서 **0**을 클릭합니다.
발신자 입력 (**0**) 편집 창이 표시됩니다.
 - 단계 5 통화 처리기 라디오 버튼을 클릭하고 드롭다운 목록에서 운영자를 선택한 다음 호 전환 시도 라디오 버튼을 클릭합니다.
 - 단계 6 저장을 클릭합니다.
업데이트된 발신자 입력 상태 메시지가 표시됩니다.
 - 단계 7 편집 > 발신자 입력을 선택합니다.
발신자 입력 창이 표시됩니다.
 - 단계 8 키 열에서 **1**을 클릭합니다.
발신자 입력 (**0**) 편집 창이 표시됩니다.
 - 단계 9 대화 라디오 버튼의 드롭다운 목록에서 발신자 시스템 호 전환을 선택합니다.
 - 단계 10 저장을 클릭합니다.
업데이트된 발신자 입력 상태 메시지가 표시됩니다.
-

운영자 통화 처리기에 대한 내선 번호 구성

프로시저

-
- 단계 1 Cisco Unity Connection 관리에서 왼쪽의 Cisco Unity Connection 트리에서 통화 관리로 이동하여 시스템 통화 처리기를 선택합니다.
 - 단계 2 운영자를 클릭합니다.
통화 처리기 기본 사항 편집(운영자) 창이 표시됩니다.
 - 단계 3 내선 번호 필드에 운영자 내선 번호를 입력하고 저장을 클릭합니다.
업데이트된 발신자 입력 상태 메시지가 표시됩니다.
-

운영자에 대한 표준 호 전환 규칙 수정

프로시저

- 단계 1 Cisco Unity Connection 관리에서 왼쪽의 Cisco Unity Connection 트리에서 통화 관리로 이동하여 시스템 통화 처리기를 선택합니다.
- 단계 2 운영자를 클릭합니다.
통화 처리기 기본 사항 편집(운영자) 창이 표시됩니다.
- 단계 3 편집 메뉴에서 호전환 규칙을 선택합니다.
호전환 규칙 창이 표시됩니다.
- 단계 4 표준 을 클릭합니다.
호전환 규칙 편집(표준) 창이 표시됩니다.
- 단계 5 호전환 대상 옵션에서 내선 번호 라디오 버튼을 클릭하고 구성된 운영자 내선 번호를 입력합니다.
- 단계 6 저장을 클릭합니다.

기본 시스템 전송 제한 테이블 업데이트

프로시저

- 단계 1 Cisco Unity Connection 관리에서 왼쪽의 Cisco Unity Connection 트리에서 시스템 설정으로 이동하고 제한 테이블을 선택합니다.
- 단계 2 기본 시스템 호 전환을 클릭합니다.
제한 테이블 기본 사항 편집(기본 시스템 호전환) 창이 표시됩니다.
- 단계 3 순서 열에서 6에 대한 차단됨 열의 확인란을 선택 취소합니다.
- 단계 4 저장을 클릭합니다.

Cisco Unity Connection 오토 어텐던트 문제 해결

Cisco Unity Connection을 사용하여 오토 어텐던트 문제를 해결하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- <http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/107517-calltrf.html>
- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/troubleshooting/guide/8xcuctsgx/8xcuctsg110.html
- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/troubleshooting/guide/8xcuctsgx/8xcuctsg040.html

- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/troubleshooting/guide/8xcuctsgx/8xcuctsg180.html

Cisco Unified CCX 구성

오토 어텐던트는 Cisco Unified Contact Center Express(Unified CCX)의 5 사용자 번들을 표준으로 제공합니다.



참고 Unified Communications Manager에 지원되는 Cisco Unified CCX 버전에 대한 자세한 내용은 [IP 전화 통신에 대한 Cisco Collaboration 시스템 릴리스 요약 매트릭스](#)를 참조하십시오.

스크립트를 시작하는 방법에 대한 자세한 내용은 스크립트로 [Cisco Unified Contact Center Express 시작하기](#)를 참조하십시오.

Cisco Unified CCX 사전 요건

- 오토 어텐던트를 사용하려면 먼저 Cisco Unified CCX를 설치하고 구성합니다. Cisco Unified CCX는 소프트웨어 및 전화 통신 시스템에 대한 연결을 제어합니다.
- Unified Communications Manager에서 사용자를 구성합니다.

Cisco Unified CCX 오토 어텐던트 작업 흐름

오토 어텐던트 구성 작업은 Cisco Unified Contact Center Express(Unified CCX)에서 완료됩니다. 다음 작업에 대한 세부 단계를 보려면 [Cisco Unified CCX 관리 지침서](#) 및 [Cisco Unified Contact Center Express 스크립트로 시작하기](#)를 참조하십시오.

시작하기 전에

- [오토 어텐던트 개요, 167 페이지](#)의 내용을 검토하여 오토 어텐던트 기능에 대해 알아보십시오.
- [Cisco Unified CCX 구성, 173 페이지](#)의 내용을 검토하여 오토 어텐던트 기능을 사용하는 Cisco UCCX에 대해 알아보십시오.
- [Cisco Unified CCX 사전 요건, 173 페이지](#)를 검토합니다.

프로시저

	명령 또는 동작	목적
단계 1	Unified CM 전화 통신 통화 제어 그룹을 구성합니다.	Unified CCX 시스템은 Unified CM 전화 통신 통화 제어 그룹을 사용하여 연속된 CTI 포트를 함께 폴링 하며, 이를 사용하여 시스템이

	명령 또는 동작	목적
		Unified CCX 서버에 도착하거나 서버에서 출발할 때 통화를 처리하는 데 사용합니다.
단계 2	CMT(Cisco Media Termination) 대화 상자 제어 그룹을 추가합니다.	<p>Cisco Media 하위 시스템은 Unified CCX 엔진의 하위 시스템입니다. Cisco Media 하위 시스템은 CMT 미디어 리소스를 관리합니다. Unified CCX가 미디어를 재생하거나 녹음할 수 있으려면 CMT 채널이 필요합니다.</p> <p>Cisco Media 하위 시스템은 대화 상자 그룹을 사용하여 애플리케이션 간에 리소스를 구성하고 공유합니다. 대화 상자 그룹은 각 채널이 발신자와의 대화 상자 상호 작용을 수행하는 데 사용되는 대화 상자 채널의 풀이며, 이 경우 발신자는 터치톤 전화기에서 버튼을 눌러 자동 프롬프트에 응답합니다.</p> <p>주의 모든 미디어 터미네이션 문자열은 “auto”로 시작하고 CMT 대화 상자 그룹이 아닌 통화 제어 그룹과 동일한 ID를 포함합니다. 기본 미디어 터미네이션이 구성되어 있고 ID가 다른 경우 이 절차를 수행합니다.</p>
단계 3	Cisco 스크립트 애플리케이션을 구성합니다.	Unified CCX 스크립트 애플리케이션에는 Unified CCX 편집기에서 만든 스크립트를 기반으로 하는 애플리케이션이 있습니다. 이러한 애플리케이션에는 모든 Unified CCX 시스템과 함께 제공되고 Unified CCX 편집기에서 생성된 스크립트가 실행됩니다.
단계 4	Unified CM 전화 통신 트리거를 프로비전합니다.	Unified CM 전화 통신 트리거는 전화 통신 및 미디어 리소스를 선택하여 통화를 서비스하고 통화를 처리하기 위해 애플리케이션 스크립트를 호출하여 특정 라우트 포인트에 도착하는 통화에 응답합니다.
단계 5	<p>오토 어텐던트를 사용자 정의합니다.</p> <ul style="list-style-type: none"> • 기존 오토 어텐던트 인스턴스 수정 • 오토 어텐던트 프롬프트 구성 	<p>Cisco Unified CCX 관리 페이지에서는 필요에 따라 기존 오토 어텐던트 인스턴스를 수정할 수 있습니다.</p> <p>Cisco Unified CCX를 사용하면 Cisco Unified CCX 관리 미디어 구성 창에서 오토 어텐던트 메시지를 사용자 정의할 수 있습니다. 이 기능을 사용하여 시작 프롬프트를 녹음하고, 환영</p>

	명령 또는 동작	목적
		프롬프트를 구성하고, 음성 이름을 업로드할 수 있습니다.

Cisco Unified CCX 오토 어텐던트 문제 해결

Cisco Unified CCX를 사용하여 오토 어텐던트 문제를 해결하는 방법에 대한 자세한 내용은 http://docwiki.cisco.com/wiki/List_of_Troubleshooting_Tips_for_Unified_CCX_7.0#Cisco_Unified_Communications_Manager_Automated_Attendant(Windows 버전에만 해당)의 내용을 참조하십시오.

Cisco Unity Express 구성

Cisco Unity Express를 사용하는 오토 어텐던트 구성에 대한 자세한 내용은 [Cisco Unity Express 음성 메일 구성 및 3.0 및 이후 버전에 대한 오토 어텐던트 CLI 관리자 설명서](#)의 “오토 어텐던트 구성”을 참조하십시오.

샘플 오토 어텐던트 스크립트 구축에 대한 자세한 내용은 [Cisco Unified IP IVR 시작하기](#)에서 “샘플 스크립트 aa.aef 구축” 장을 참조하십시오.

오토 어텐던트 예에 대한 자세한 내용은 [7.0 이상 버전에 대한 스크립트 작성 및 편집용 Cisco Unity Express 설명서](#)의 “오토 어텐던트 스크립트 예” 장을 참조하십시오.

오토 어텐던트 설계 고려 사항에 대한 자세한 내용은 [Cisco Unity Express 설계 설명서](#)에서 “오토 어텐던트 설계 고려 사항” 장을 참조하십시오.

Cisco Unity Express 오토 어텐던트 문제 해결

Cisco Unity Connection 사용 시 오토 어텐던트 문제 해결에 대한 자세한 내용은 [Cisco IP Communications Express: CallManager Express with Cisco Unity Express의 발췌](#)에서 “Cisco Unity Express 오토 어텐던트 문제 해결”을 참조하십시오.



16 장

Manager Assistant

- Cisco Unified Communications Manager Assistant 개요, 177 페이지
- Manager Assistant 사전 요건, 179 페이지
- 프록시 회선에 대한 Manager Assistant 작업 흐름, 180 페이지
- 공유 회선에 대한 Manager Assistant 작업 흐름, 188 페이지
- Manager Assistant 상호 작용, 208 페이지
- Manager Assistant 제한, 211 페이지
- Cisco Unified Communications Manager Assistant 문제 해결, 212 페이지

Cisco Unified Communications Manager Assistant 개요

Unified Communications Manager Assistant 기능은 보조자가 관리자 대신 통화를 처리하고 관리자 통화를 차단하고 적절히 라우팅하는 데 사용할 수 있는 플러그인입니다.

Manager Assistant에서는 최대 3500명의 관리자와 3500명의 보조자를 지원합니다. 이 만큼의 사용자를 수용하려면 관리자는 하나의 Unified Communications Manager 클러스터에 최대 3개의 Manager Assistant 애플리케이션을 구성하고 애플리케이션의 각 인스턴스에 관리자와 보조자를 할당할 수 있습니다.

Manager Assistant는 공유 회선 및 프록시 회선을 지원합니다.

Manager Assistant 아키텍처

Manager Assistant 아키텍처는 다음과 같이 구성됩니다.

- **Cisco IP 매니저 어시스턴트 (Cisco IPMA)** 서비스—Unified Communications Manager를 설치한 후 Cisco 유니파이드 Serviceability 인터페이스에서 이 서비스를 활성화합니다.
- **Assistant Console** 인터페이스—보조자가 관리자를 위해 통화를 처리하는 컴퓨터에서 Manager Assistant 기능에 액세스할 수 있습니다. Manager Assistant는 한 명의 보조자와 최대 33명의 관리자에 대한 통화를 처리합니다.
- **Cisco Unified IP Phone** 인터페이스: 관리자와 보조자는 소프트키와 Cisco Unified IP Phone 서비스 버튼을 사용하여 Manager Assistant 기능에 액세스합니다.

자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서](#)의 Manager Assistant 장을 참조하십시오.

Manager Assistant 데이터베이스 액세스 아키텍처

데이터베이스는 모든 Manager Assistant 구성 정보를 저장합니다. 관리자나 보조자가 로그인하면 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스는 데이터베이스에서 관리자나 보조자와 관련된 데이터를 모두 검색하여 메모리에 저장합니다. 데이터베이스에는 두 가지 인터페이스가 있습니다.

- 관리자 인터페이스—관리자 전화기에서는 관리자 구성을 제외한 관리자 기능을 사용할 수 있습니다. Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스가 시작되면 Manager Assistant가 관리자를 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스로 로그인합니다.



참고 또한 방해사절, 지정전환 등의 Unified Communications Manager 기능에 액세스할 수 있습니다.

- 보조자 인터페이스—보조자는 Assistant Console 애플리케이션 및 Cisco Unified IP Phone을 사용하여 Manager Assistant 기능에 액세스합니다. Assistant Console 애플리케이션은 전화받기, 전환, 호전환 및 보류 같은 통화 제어 기능을 제공합니다. 보조자는 Assistant Console을 사용하여 로그인 및 로그오프하고, 보조자 환경 설정을 설정하고, 관리자 환경 설정을 구성하는 데 사용되는 관리자 구성 창을 표시합니다.

자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서](#)의 Manager Assistant 장을 참조하십시오.

소프트키

Manager Assistant는 다음 소프트키를 지원합니다.

- 재전송
- 음성메일로 호전환
- DND(Do Not Disturb)

Manager Assistant는 다음 소프트키 템플릿을 지원합니다.

- 표준 관리자—관리자에게 프록시 모드 지원
- 표준 공유 모드 관리자—관리자에게 공유 모드 지원
- 표준 보조자—프록시 또는 공유 모드에서 보조자 지원
- 표준 사용자—시스템에서 표준 사용자 템플릿에서 사용할 수 있는 통화 처리(예: 보류 및 다이얼) 소프트키를 만듭니다.

Manager Assistant 공유 회선 개요

공유 회선 모드에서 Manager Assistant를 구성할 경우 관리자와 보조자는 디렉터리 번호(예: 8001)를 공유합니다. 보조자는 관리자를 위해 공유된 디렉터리 번호에서 통화를 처리합니다. 관리자가 8001에서 전화를 받으면 관리자 전화기와 보조자 전화기가 모두 울립니다.

공유 회선 모드에서 적용할 수 없는 Manager Assistant 기능에는 기본 도우미 선택, 도우미 감시, 통화 필터링, 모든 통화 전환이 있습니다. 보조자는 Assistant Console 애플리케이션에서 이러한 기능을 보거나 액세스할 수 없습니다.

Manager Assistant 프록시 회선 개요

프록시 회선 모드에서 Manager Assistant를 구성하는 경우 보조자는 프록시 번호를 사용하는 관리자에 대한 통화를 처리합니다. 프록시 번호는 관리자의 디렉터리 번호가 아니라 시스템에서 선택하고 보조자가 관리자 통화를 처리하기 위해 사용하는 대체 번호입니다. 프록시-회선 모드에서 관리자와 보조자는 기본 보조자 선택, 보조자 감시, 통화 필터링, 모두 전환 등을 비롯해 Manager Assistant에서 사용할 가능한 모든 기능에 액세스할 수 있습니다.

Manager Assistant 사전 요건

- 사용자가 Manager Assistant 클라이언트를 릴리스 11.5(1)SU9, 12.0(1)SU4 및 14에 대한 최신 버전으로 업그레이드 하기 전에 사용자가 32 또는 64 비트 Windows 플랫폼에 JRE를 설치해야 합니다.



중요 업그레이드를 수행하기 전에 현재 시스템에 설치되어 있는 Cisco Unified Communications Manager Assistant 클라이언트를 제거해야 합니다. 이는 릴리스 12.0 (1) SU4와 14에서 적용할 수 있습니다.

- Manager Assistant는 다음과 같은 브라우저 및 플랫폼을 지원합니다.
 - Unified Communications Manager Assistant 관리 및 Assistant Console은 Internet Explorer 11(Windows 10(64비트) 이상), Firefox(Windows 10(64비트) 이상) 및 Safari(MacOS (10.x) 이상)에서 지원됩니다.
 - 고객은 Windows 10 또는 Apple MAC OS X가 실행되는 컴퓨터에서 위에 지정된 브라우저 중 하나를 열 수 있습니다.
- 다른 언어로 Manager Assistant 기능을 표시하려면 Manager Assistant를 구성하기 전에 로캘 설치 관리자를 설치합니다.
- Assistant Console 애플리케이션은 Windows 10 이상을 실행하는 컴퓨터에서 지원됩니다.
- 전화기 및 사용자를 구성하고 디바이스를 사용자에게 연결해야 합니다. 뿐만 아니라, 관리자와 보조자 간에 공유 회선을 표시할 경우 관리자 기본 회선 및 보조자 보조 회선에 동일한 디렉터리 번호를 구성해야 합니다.

- 관리자 및 보조자를 벌크로 추가하려면 Cisco Unified Communications Manager 벌크 관리 도구를 설치합니다. 자세한 내용은 벌크 관리 지침서를 참조하십시오.

프록시 회선에 대한 **Manager Assistant** 작업 흐름

시작하기 전에

- [Manager Assistant 사전 요건](#), 179 페이지를 검토합니다.

프로시저

	명령 또는 동작	목적
단계 1	Cisco Unified CM Assistant 구성 마법사 실행 , 180 페이지	
단계 2	프록시 회선에 대한 관리자 구성 및 보조자 할당 , 186 페이지	
단계 3	프록시 회선에 대한 보조자 회선 표시 구성 , 187 페이지	
단계 4	Assistant Console 플러그인 설치 , 207 페이지	보조자는 Assistant Console 애플리케이션 및 Cisco Unified IP Phone을 사용하여 Unified Communications Manager Assistant 기능에 액세스합니다. Assistant Console은 전화받기, 전환, 호전환 및 보류 같은 통화 제어 기능을 제공합니다.
단계 5	관리자 및 보조자 콘솔 애플리케이션을 구성합니다.	Cisco Unified Communications Manager용 Cisco Unified Communications Manager Assistant 사용 설명서 를 참조하십시오.

Cisco Unified CM Assistant 구성 마법사 실행

Cisco Unified CM Assistant 구성 마법사를 실행하여 파티션, 발신 검색 공간 및 라우트 포인트를 자동으로 만들 수 있습니다. 마법사는 관리자 전화기, 보조자 전화기 및 다른 모든 사용자 전화기에 대한 BAT(벌크 관리 도구) 템플릿도 생성합니다. BAT 템플릿을 사용하여 관리자, 보조자 및 다른 모든 사용자를 구성할 수 있습니다. BAT에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서](#)의 내용을 참조하십시오.

시작하기 전에

구성 마법사가 벌크 관리 도구와 동일한 서버(Unified Communications Manager 서버)에서 실행되는지 확인하십시오.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 애플리케이션 > **Cisco Unified CM Assistant** 구성 마법사.
- 단계 2 다음을 클릭하여 Cisco Unified CM Assistant 구성 마법사 프로세스를 시작합니다.
- 단계 3 관리자용 파티션 창에 이름을 입력하고 설명을 제공한 후 다음을 클릭합니다. 또는 기본 파티션 이름 및 설명을 수락할 수 있습니다.
- 단계 4 **CTI** 라우트 포인트용 파티션 창에 이름을 입력하고 설명을 제공한 후 다음을 클릭합니다. 또는 기본 CTI 라우트 포인트 이름을 수락할 수 있습니다.
- 단계 5 모든 사용자용 파티션 창에 이름을 입력하고 설명을 제공한 후 다음을 클릭합니다. 또는 모든 사용자에 대해 기본 파티션 이름 및 설명을 수락할 수 있습니다.
- 단계 6 인터컴 파티션 창에 이름을 입력하고 설명을 제공한 후 다음을 클릭합니다. 또는 기본 인터컴 파티션 이름을 수락할 수 있습니다.
- 단계 7 보조자 발신 검색 공간 창에 이름을 입력하고 설명을 제공합니다. 또는 기본 발신 검색 공간 이름 및 설명을 사용할 수 있습니다.
[이 발신 검색 공간의 경로 파티션] 아래의 [사용 가능한 파티션] 및 [선택한 파티션] 상자에는 보조자 발신 검색 공간용 파티션이 자동으로 나열됩니다. 기본값을 수락하거나 [사용 가능한 파티션] 상자에서 적절한 파티션을 선택할 수 있습니다. 위쪽 및 아래쪽 화살표를 사용하여 상자 간에 파티션을 이동합니다.
- 단계 8 다음을 클릭합니다.
- 단계 9 모든 사용자 발신 검색 공간 창에 이름을 입력하고 설명을 제공합니다. 또는 모든 사용자의 기본 발신 검색 공간 이름 및 설명을 수락할 수 있습니다.
[이 발신 검색 공간의 경로 파티션] 아래의 [사용 가능한 파티션] 및 [선택한 파티션] 상자에는 보조자 발신 검색 공간용 파티션이 자동으로 나열됩니다. 기본값을 수락하거나 [사용 가능한 파티션] 상자에서 적절한 파티션을 선택할 수 있습니다. 위쪽 및 아래쪽 화살표를 사용하여 상자 간에 파티션을 이동합니다.
- 단계 10 다음을 클릭합니다.
시스템에 기존 발신 검색 공간이 구성되어 있는 경우 기존 발신 검색 공간 창이 표시됩니다. 그렇지 않으면, 다음 단계로 진행합니다.
- Manager Assistant에서 기존 발신 검색 공간에는 접두사 **Generated_Route** 포인트 및 **Generated_Everyone** 파티션을 추가해야 합니다. [사용 가능한 발신 검색 공간] 및 [선택한 발신 검색 공간] 상자에 자동으로 이러한 파티션이 나열됩니다. 위쪽 및 아래쪽 화살표를 사용하여 상자 간에 파티션을 이동합니다.
- 참고 관리자가 파티션 이름을 변경한 경우 기존 발신 검색 공간에 추가된 접두사가 변경될 수 있습니다.
- 단계 11 다음을 클릭합니다.
- 단계 12 **CTI** 라우트 포인트 창에서 CTI 라우트 포인트 이름 필드에 이름을 입력합니다. 그렇지 않으면 기본 CTI 라우트 포인트 이름을 사용합니다.
- 단계 13 드롭다운 목록에서 적절한 디바이스폴을 선택합니다.
- 단계 14 라우트 포인트 디렉터리 번호를 입력합니다. 그렇지 않으면 기본 라우트 포인트 디렉터리 번호를 사용합니다.

- 단계 15 드롭다운 목록에서 적절한 번호 지정 플랜을 선택하고 다음을 클릭합니다.
- 단계 16 전화 서비스 창에서 기본 전화 서비스 이름을 입력합니다. 그렇지 않으면 기본 전화 서비스 이름을 사용합니다.
- 단계 17 드롭다운 목록에서 기본 Cisco Unified Communications Manager Assistant 서버를 선택하거나, 서버 이름 또는 IP 주소를 입력합니다.
- 단계 18 보조 전화 서비스 이름을 입력합니다. 그렇지 않으면 기본 전화 서비스 이름을 사용합니다.
- 단계 19 드롭다운 목록에서 보조 Cisco Unified Communications Manager 서버를 선택하거나, 서버 이름 또는 IP 주소를 입력한 후에 다음을 클릭합니다.
확인 창이 표시됩니다. 선택한 모든 정보를 제공합니다. 정보가 올바르지 않으면 구성 프로세스를 취소하거나 이전 구성 창으로 돌아갈 수 있습니다.
- 단계 20 마침을 클릭합니다.
완료되면 최종 상태 창이 표시됩니다.

구성 마법사에서 생성된 오류는 추적 파일로 보내집니다. 다음 CLI 명령을 사용하여 이 파일에 액세스합니다. **file get activelog tomcat/logs/ccmadmin/log4j**

다음에 수행할 작업

Cisco Unified CM Assistant 구성 마법사는 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수만 생성합니다. 나머지 서비스 매개 변수는 수동으로 입력해야 합니다. 서비스 매개 변수 정보는 [프록시 회선의 Manager Assistant 서비스 매개 변수, 182 페이지](#)의 내용을 참조하십시오.

프록시 회선의 **Manager Assistant** 서비스 매개 변수

Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수. Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스가 활성화된 서버를 선택하고 자세한 설명을 보려면 ?를 클릭합니다.

설정	설명
Cisco IP 매니저 어시스턴트 (Cisco IPMA)(활성) 매개 변수	
CTIManager(기본) IP 주소	이 매개 변수는 이 Cisco IPMA 서버가 통화를 처리하는 데 사용하는 기본 CTIManager 지정합니다. 기본값은 없습니다.
CTIManager(백업) IP 주소	이 매개 변수는 기본 CTIManager가 종료되었을 때 이 Cisco IPMA 서버가 통화를 처리하는 백업 CTIManager의 IP 주소를 지정합니다. 기본값은 없습니다.
프록시 모드용 라우트 포인트 디바이스 이름	이 매개 변수는 이 Cisco IPMA 서버가 지능형 통화 라우팅을 위해 관리자의 기본 호 통화를 차단하는 CTI 라우트 포인트의 디바이스 이름을 지정합니다. IPMA 서비스를 실행하는 모든 서버에 대해 동일한 CTI 라우트 포인트 디바이스를 종속합니다. 관리자 또는 보조자가 프록시 모드를 사용하도록 구성할 경우 CTI 라우터 이름 이름을 구성해야 합니다.

설정	설명
CTIManager에 보안 연결을 위한 CAPF 프로파일 인스턴스 ID	이 서비스 매개 변수는 이 Manager Assistant가 CTIManager에 대한 보안 연결을 플리케이션 사용자 IPMASecureSysUser 에 대한 애플리케이션 CAPF 프로파일 지정합니다. CTIManager 연결 보안 플래그를 활성화한 경우 이 매개 변수를 구성합니다.
클러스터 수준 매개 변수(모든 서버에 적용되는 매개 변수) 중요 고급을 클릭하여 숨겨진 매개 변수를 봅니다.	
Cisco IPMA 서버(기본) IP 주소	이 매개 변수는 기본 Cisco IPMA 서버의 IP 주소를 지정합니다. 기본값은 없습니다.
Cisco IPMA 서버(백업) IP 주소	이 매개 변수는 백업 Cisco IPMA 서버의 IP 주소를 지정합니다. 백업 서버는 기 패하는 경우 IPMA 서비스를 제공합니다. 기본값은 없습니다.
Cisco IPMA 서버 포트	이 매개 변수는 IPMA Assistant Console에서 소켓 연결을 여는 Cisco IPMA 서버의 정합니다. 포트 충돌이 있는 경우 매개 변수를 변경할 수 있습니다. 기본값: 2912
Cisco IPMA Assistant Console 하트비트 간격	이 매개 변수는 Cisco IPMA 서버가 IPMA Assistant Console에 킵 얼라이브 메시 비트라고도 함)를 보내는 간격(초)을 지정합니다. IPMA Assistant Console은 이 시간이 만료되기 전에 서버에서 하트비트를 수신하지 못할 때 장애 조치를 시작 기본값: 30초
Cisco IPMA Assistant Console 요청 시간 초과	이 매개 변수는 IPMA Assistant Console이 Cisco IPMA 서버로부터 응답 수신 을 지정합니다. 기본값: 30초
Cisco IPMA RNA 통화 착신 전환	이 매개 변수는 Cisco IPMA 벨 울림에 응답 없음(RNA) 착신 전환을 활성화할지 다. 유효한 값은 True (Cisco IPMA가 응답하지 않은 통화를 다음 사용 가능한 보 는 False (Cisco IPMA가 착신 전환하지 않음)입니다. 이 매개 변수는 Cisco IPMA RNA 시간 초과 매개 변수와 함께 작동합니다. Cisc 초과 매개 변수에 지정된 시간이 지난 후 통화가 착신 전환됩니다. 회선에 대해 이 지정된 경우 응답하지 않은 통화를 보조자에게 착신 전환할 수 없으면 이 타 음성 메일로 전송됩니다. 기본값: 거짓
영숫자 사용자 ID	이 매개 변수는 Cisco IPMA Assistant 전화기가 영숫자 사용자 ID 또는 숫자 사용 여부를 결정합니다. 기본값: True

설정	설명
Cisco IPMA RNA 시간 초과	이 매개 변수는 다음 사용 가능한 보조자에게 응답하지 않은 통화를 착신 전환하기 전에 서버가 대기하는 시간(초)을 지정합니다. 이 매개 변수는 Cisco IPMA RNA 통화 착수와 함께 작동합니다. Cisco IPMA RNA 통화 착신 전환 매개 변수가 True 로 설정되면 착신 전환이 발생합니다. 기본값: 10초
CTIManager 연결 보안 플러그	이 매개 변수는 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 CTIManager 연결 활성화할지 여부를 결정합니다. 활성화되면 Cisco IPMA는 애플리케이션 IPMASE 인스턴스 ID(CTIManager 연결 보안 플러그 및 CAPF 프로파일 인스턴스 ID 서비스 지정)에 대해 구성된 CAPF 프로파일을 사용하여 CTIManager에 대한 보안 연결을 생성합니다. 기본값: 비보안 보안을 활성화하려면 CTIManager 연결 보안 플러그 및 CAPF 프로파일 인스턴스 ID 매개 변수에서 인스턴스 ID를 선택해야 합니다.
보조자에게 연결 실패 시 관리자에게 통화 재전송	이 매개 변수는 통화가 선택한 프록시 보조자에게 연결되지 않을 경우 Cisco Unified Assistant 애플리케이션이 원하는 관리자에게 통화를 다시 재전송할지 여부를 결정합니다. 기본값: 거짓
고급 클러스터 수준 매개 변수	
중요 Cisco IPMA 서버 IP 주소에 풀이 두 개 이상 나타나지 않도록 각 풀에 고유의 IP 주소를 구성합니다.	
여러 활성 모드 활성화	이 매개 변수는 확장성을 위해 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스의 여러 활성 모드를 실행해야 하는지 여부를 결정합니다. 활성화된 경우 풀 2 및 풀 3 매개 변수에 구성된 노드에서 Cisco IPMA를 실행할 수 있습니다. 여러 활성 모드를 활성화하려면 Cisco IPMA의 추가 인스턴스를 실행하려는 노드의 IP 주소를 지정해야 합니다. 이러한 노드에서 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수를 구성합니다. 기본값: 거짓
풀 2: Cisco IPMA 서버(기본) IP 주소	다중 활성 모드가 활성화된 경우 이 매개 변수는 Cisco IPMA의 두 번째 인스턴스의 기본 서버 IP 주소를 지정합니다. 이 노드에서 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수를 구성합니다.
풀 2: Cisco IPMA 서버(백업) IP 주소	다중 활성 모드가 활성화된 경우 이 매개 변수는 Cisco IPMA의 두 번째 인스턴스의 백업 서버 IP 주소를 지정합니다. 백업 서버는 기본 IPMA 서버가 실패하는 경우 IPMA 서비스를 실행합니다. 이 노드에서 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수를 구성합니다.
풀 3: Cisco IPMA 서버(기본) IP 주소	다중 활성 모드가 활성화된 경우 이 매개 변수는 Cisco IPMA의 세 번째 인스턴스의 기본 서버 IP 주소를 지정합니다. 이 노드에서 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수를 구성합니다.

설정	설명
폴 3: Cisco IPMA 서버(백업) IP 주소	다중 활성화 모드가 활성화된 경우 이 매개 변수는 Cisco IPMA의 세 번째 인스턴스의 서버 IP 주소를 지정합니다. 백업 서버는 기본 IPMA 서버가 실패하는 경우 IPMA입니다. 이 노트에서 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수를 구성
클러스터 수준 매개변수(소프트키 템플릿)	
중요 관리자와 보조자를 위해 Manager Assistant 구성을 사용하려면 이러한 매개 변수를 구성합니다.	
보조자 소프트키 템플릿	이 매개 변수는 자동 구성하는 동안 보조자 디바이스에 할당되는 보조자 소프트키 템플릿을 지정합니다. 이 매개 변수에 지정된 값은 Cisco IPMA Assistant 구성 페이지에서 자동 선택될 때 사용됩니다.
프록시 모드용 관리자 소프트키 템플릿	이 매개 변수는 자동 구성하는 동안 관리자 디바이스에 할당되는 프록시 모드용 소프트키 템플릿을 지정합니다. 이 매개 변수는 프록시 모드를 사용하는 관리자에만 적용됩니다.
클러스터 수준 매개 변수(프록시 모드용 IPMA 디바이스 구성 기본값)	
관리자 파티션	이 매개 변수는 자동 구성하는 동안 IPMA가 관리자 디바이스에서 처리하는 관리 파티션을 정의합니다. 사용하려는 파티션이 Cisco Unified CM 관리에 이미 추가되어 있습니다. Cisco IPMA 구성 마법사가 실행되는 경우 이 값을 채웁니다. 이 매개 변수는 프록시 모드를 사용하는 관리자에만 적용됩니다.
모든 사용자 파티션	이 매개 변수는 자동 구성하는 동안 관리자 디바이스의 인터콤 회선 뿐만 아니라 모든 프록시 회선 및 인터콤 회선에 구성되는 파티션을 지정합니다. 사용하려는 파티션이 Cisco Unified CM 관리에 이미 추가되었는지 확인합니다. Cisco IPMA 구성 마법사가 실행되는 경우 이 값을 채웁니다. 이 매개 변수는 프록시 모드를 사용하는 관리자 또는 보조자에만 적용됩니다.
IPMA 발신 검색 공간	이 매개 변수는 자동 구성하는 동안 IPMA가 처리하는 관리자 디바이스의 관리 파티션 및 보조자 디바이스의 보조자 인터콤 회선에 대해 구성되는 발신 검색 공간을 지정합니다. 이 발신 검색 공간이 Cisco Unified CM 관리에 이미 추가되었는지 확인합니다. 구성 마법사가 실행되는 경우 이 값을 채웁니다. 이 매개 변수는 프록시 모드를 사용하는 보조자에만 적용됩니다.
관리자 발신 검색 공간	이 매개 변수는 자동 구성하는 동안 보조자 디바이스의 프록시 회선에 구성되는 발신 검색 공간을 정의합니다. 이 발신 검색 공간은 시스템에 이미 있는 발신 검색 공간입니다. IPMA 구성 마법사가 실행되는 경우 이 값을 채웁니다. 이 매개 변수는 프록시 모드를 사용하는 보조자에만 적용됩니다.
Cisco IPMA 기본 전화 서비스	이 매개 변수는 자동 구성하는 동안 관리자/보조자 디바이스가 가입할 IP 전화 서비스를 지정합니다. Cisco IPMA 구성 마법사가 실행되는 경우 이 값을 채웁니다. 이 매개 변수는 프록시 모드를 사용하는 관리자 또는 보조자에만 적용됩니다.
Cisco IPMA 기본 전화 서비스	이 매개 변수는 자동 구성하는 동안 관리자 또는 보조자 디바이스가 가입할 보조자 전화 서비스를 지정합니다. Cisco IPMA 구성 마법사가 실행되는 경우 이 값을 채웁니다. 이 매개 변수는 프록시 모드를 사용하는 관리자 또는 보조자에만 적용됩니다.

설정	설명
클러스터 수준 매개 변수(프록시 모드용 프록시 디렉터리 번호 범위)	
시작 디렉터리 번호	이 매개 변수는 IPMA 보조자를 구성하는 동안 프록시 디렉터리 번호를 자동 생성하는 데 사용되는 시작 디렉터리 번호를 지정합니다. 자동 생성된 프록시 회선 번호가 번호 범위 후 다음 번호가 다음 보조자를 위해 생성됩니다. 이 매개 변수는 프록시 모드를 사용하는 보조자에만 적용됩니다.
끝 디렉터리 번호	이 매개 변수는 IPMA 보조자를 구성하는 동안 프록시 디렉터리 번호를 자동 생성하는 데 사용되는 끝 디렉터리 번호를 지정합니다. 이 번호에서 구성이 중단됩니다. 이 매개 변수는 프록시 모드를 사용하는 보조자에만 적용됩니다.
클러스터 수준 매개 변수(프록시 모드용 프록시 디렉터리 번호 범위)	
관리자 DN에서 제거할 문자 수	이 매개 변수는 프록시 DN을 생성하는 동안 관리자 디렉터리 번호(DN)에서 제거할 문자 수를 지정합니다. 프록시 DN을 생성하면 일부 자릿수가 제거되고 접두사가 추가될 수 있습니다. 왼쪽부터 제거됩니다. 이 매개 변수는 프록시 모드를 사용하는 보조자에만 적용됩니다.
관리자 DN용 접두사	이 매개 변수는 프록시 DN을 생성하는 동안 관리자 DN에 추가할 접두사를 지정합니다. 프록시 DN을 생성하면 일부 자릿수가 제거되고 접두사가 추가될 수 있습니다. 이 매개 변수는 프록시 모드를 사용하는 보조자에만 적용됩니다.

프록시 회선에 대한 관리자 구성 및 보조자 할당

새 사용자를 구성하고 디바이스를 사용자에게 연결하는 방법에 대한 정보를 [Cisco 통합 커뮤니케이션 매니저 관리 지침서](#)를 참조하십시오.



참고 보조자에 대한 보조자 정보를 구성하기 전에 관리자 정보를 구성해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.사용자 관리 > 최종 사용자

단계 2 찾기를 클릭합니다.

검색 결과에는 Unified Communications Manager에서 구성한 최종 사용자가 모두 표시됩니다.

단계 3 관련 링크 드롭다운 목록에서 관리자 구성을 선택하고 이동을 클릭합니다.

팁 기존 보조자 구성 정보를 보려면 [연결된 보조자] 목록에서 보조자 이름을 클릭하고 세부 정보 보기를 클릭합니다. **Cisco Unified CM Assistant** - 보조자 구성 창이 표시됩니다. 관리자 구성 정보로 돌아가려면 [연결된 보조자] 목록에서 관리자 이름을 클릭하고 세부 정보 보기를 클릭합니다.

Cisco Unified CM Assistant - 관리자 구성 창이 표시됩니다.

단계 4 디바이스 이름/프로파일 드롭다운 목록에서 디바이스 이름 또는 디바이스 프로파일을 관리자 와 연결할 디바이스 이름 또는 디바이스 프로파일을 선택합니다. Manager assistant 기능이 있는 Extension Mobility에 대한 자세한 내용은 [Manager Assistant 상호 작용, 208 페이지](#)를 참조하십시오.

참고 관리자가 재택 근무하는 경우 모바일 관리자 확인란을 클릭하고 선택적으로 디바이스 이름/프로파일 드롭다운 목록에서 디바이스 프로파일을 선택합니다. 디바이스 프로파일을 선택한 후에 관리자는 Extension Mobility를 사용하여 전화기로 로그인해야만 Manager Assistant에 액세스할 수 있습니다.

단계 5 인터콤 회선 드롭다운 목록 상자에서 관리자의 인터콤 회선 표시를 선택합니다(해당되는 경우).

참고 선택한 인터콤 회선을 Manager Assistant 및 Unified Communications Manager 인터콤 기능에 적용합니다.

단계 6 보조자 폴 드롭다운 목록에서 적절한 폴 번호(1 ~ 3)를 선택합니다.

단계 7 사용 가능한 회선 선택 상자에서 Manager Assistant에서 제어할 회선을 선택하고 아래쪽 화살표를 클릭하여 [선택한 회선] 선택 상자에서 회선 표시를 만듭니다. 최대 5개의 Manager Assistant—제어되는 회선을 구성합니다.

팁 [선택한 회선] 선택 상자 및 Manager Assistant 제어에서 회선을 제거하려면 위쪽 화살표를 클릭합니다.

단계 8 자동 구성 확인란을 선택하여 소프트키 템플릿 구성, Manager Assistant 전화 서비스 가입, Manager Assistant에서 제어하는 선택한 회선 및 인터콤 회선을 위한 발신 검색 공간 및 파티션, Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수를 기반으로 관리자 전화기용 인터콤 회선에 대해 스피커폰으로 자동 응답 등을 자동으로 구성합니다.

참고 인터콤에 대한 자동 구성은 Cisco Unified IP Phone 7940 및 7960에 Manager Assistant 인터콤 기능을 사용하는 경우에만 적용됩니다.

단계 9 저장을 클릭합니다.

자동 구성 확인란을 선택했지만 서비스 매개 변수가 잘못된 경우 메시지가 표시됩니다. 서비스 매개 변수가 올바른지 확인하십시오. 자동 구성이 완료되면 관리자 디바이스가 재설정됩니다. 디바이스 프로파일을 구성한 경우, 관리자가 디바이스에서 로그아웃했다가 다시 로그인해야 설정이 적용됩니다.

프록시 회선에 대한 보조자 회선 표시 구성

프록시 회선은 보조자 Cisco Unified IP Phone에 표시되는 전화 회선을 지정합니다. Manager Assistant는 프록시 회선을 사용하여 관리자를 위한 통화를 관리합니다. 관리자는 보조자 전화기에서 프록시 회선으로 사용할 회선을 수동으로 구성할 수도 있고 자동 구성 확인란을 사용하여 DN을 생성하고 회선을 보조자 전화기에 추가할 수도 있습니다.



- 참고
1. 관리자 정보를 구성하고 보조자에 대한 보조자 정보를 구성하기 전에 관리자에게 보조자를 할당해야 합니다.
 2. 보조자 전화기에서 프록시 회선을 자동으로 구성하려면 프록시 디렉터리 번호 범위 및 프록시 디렉터리 번호 접두사 섹션에서 서비스 매개 변수를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 찾기를 클릭합니다.

단계 3 한 사용자 이름을 클릭하여 선택한 보조자에 대한 사용자 정보를 표시합니다.
최종 사용자 구성 창이 표시됩니다.

단계 4 관련 링크 드롭다운 목록에서 보조자 구성을 선택하고 이동을 클릭합니다.

참고 자동 구성 확인란을 선택한 경우 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수 설정을 기준으로 소프트키 템플릿 및 인터콤 회선이 자동으로 설정됩니다. 또한 인터콤 회선에 스피커폰으로 자동 응답이 설정됩니다.

보조자 구성 창이 표시됩니다.

단계 5 디바이스 이름 드롭다운 목록에서 보조자와 연결할 디바이스 이름을 선택합니다.

단계 6 인터콤 회선 드롭다운 목록에서 보조자의 착신 인터콤 회선 표시를 선택합니다.

단계 7 기본 회선 드롭다운 목록에서 보조자의 기본 회선을 선택합니다.

단계 8 관리자 회선을 보조자 회선에 연결하려면 [보조자 회선에 대한 관리자 연결] 선택 상자에서 다음 단계를 수행합니다.

- a) 사용 가능한 회선 드롭다운 목록에서 관리자 회선과 연결할 보조자 회선을 선택합니다.
- b) 관리자 이름 드롭다운 목록에서 이 프록시 회선을 적용할 미리 구성된 관리자 이름을 선택합니다.
- c) 관리자 회선 드롭다운 목록에서 이 프록시 회선을 적용할 관리자 회선을 선택합니다.

단계 9 저장을 클릭합니다.

업데이트는 즉시 적용됩니다. 자동 구성을 선택하는 경우 보조자 디바이스가 자동으로 재설정됩니다.

공유 회선에 대한 **Manager Assistant** 작업 흐름

시작하기 전에

- [Manager Assistant 사전 요건](#), 179 페이지를(를) 검토합니다.

프로시저

	명령 또는 동작	목적
단계 1	Manager Assistant 공유 회선 지원을 위한 파티션 구성, 190 페이지	Manager Assistant 에서 사용되는 회선의 파티션을 구성합니다.
단계 2	Manager Assistant 공유 회선 지원에 대한 발신 검색 공간 구성, 191 페이지	관리자 및 보조자 회선에 대한 발신 검색 공간을 구성합니다.
단계 3	Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수 구성, 192 페이지	관리자 및 보조자에 대해 자동 구성을 사용하려면 이 매개 변수를 구성합니다.
단계 4	인터콤 설정 구성 <ul style="list-style-type: none"> • 인터콤 파티션 구성, 193 페이지 • 인터콤 발신 검색 공간 구성, 343 페이지 • 인터콤 디렉터리 번호 구성, 344 페이지 • 인터콤 변환 패턴 구성, 344 페이지 	
단계 5	여러 Manager Assistant 풀 구성, 195 페이지	많은 수의 관리자와 보조자를 지원하는 데 필요한 경우 여러 개의 풀을 구성합니다. 관리자와 보조자의 쌍을 최대 2,500개까지 관리하는 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서버를 최대 3개까지 구성할 수 있습니다.
단계 6	Manager Assistant 용 CTI에 보안 TLS 연결 구성 <ul style="list-style-type: none"> • IPMASecureSysUser 애플리케이션 사용자 구성, 196 페이지 • CAPF 프로파일 구성, 197 페이지 • Cisco WebDialer 웹 서비스 구성, 199 페이지 	시스템을 혼합된 모드에서 실행하는 경우 이 절차를 수행합니다.
단계 7	CTI 라우트 포인트 구성, 200 페이지	Cisco 통합 커뮤니케이션 매니저 Assistant 에서는 관리자로부터의 통화를 차단하고 라우팅하기 위해 CTI 라우트 포인트 를 만들어야 합니다.
단계 8	관리자 및 보조자에 대한 IP 전화 서비스 구성, 200 페이지	
단계 9	관리자, 보조자 및 모든 사용자용 전화 버튼 템플릿 구성, 204 페이지	
단계 10	관리자 구성 및 공유 회선 모드에 사용할 보조자 할당, 205 페이지	

	명령 또는 동작	목적
단계 11	공유 회선에 대한 보조자 회선 표시 구성, 206 페이지	
단계 12	Assistant Console 플러그인 설치, 207 페이지	보조자는 Assistant Console 애플리케이션 및 Cisco Unified IP Phone를 사용하여 Cisco 통합 커뮤니케이션 매니저 Assistant 기능에 액세스합니다. Assistant Console은 전화받기, 전환, 호전환 및 보류 같은 통화 제어 기능을 제공합니다.
단계 13	관리자 및 보조자 콘솔 애플리케이션을 구성합니다.	Cisco Unified Communications Manager용 Cisco Unified Communications Manager Assistant 사용 설명서를 참조하십시오.

Manager Assistant 공유 회선 지원을 위한 파티션 구성

파티션 3개(Generated_Everyone, Generated_Managers 및 Generated_Route_Point)를 만들어야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 파티션.

단계 2 새로 추가를 클릭하여 새 파티션을 생성합니다.

단계 3 파티션 이름, 설명 필드에 경로 플랜에 고유한 파티션 이름을 입력합니다.

파티션 이름에는 영숫자 문자는 물론 공백, 하이픈(-) 및 밑줄(_)을 사용할 수 있습니다. 파티션 이름에 대한 지침은 온라인 도움말을 참조하십시오.

단계 4 파티션 이름 뒤에 쉼표(.)를 입력하고 동일한 줄에 파티션 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\), 꺾쇠괄호(<>) 또는 대괄호([])는 사용할 수 없습니다.

설명을 입력하지 않으면 Cisco Unified Communications Manager에서 자동으로 이 필드에 파티션 이름을 입력합니다.

단계 5 여러 파티션을 생성하려면 각 파티션 항목마다 한 행을 사용합니다.

단계 6 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.

시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성 상태로 유지됩니다.

단계 7 구성할 다음 라디오 버튼 중 하나를 선택하고 시간대를 구성합니다.

- 시작 디바이스—이 라디오 버튼을 선택하면 시스템은 발신 디바이스의 표준 시간대를 시간 일정과 비교하여 파티션을 수신 통화를 받는 데 사용할 수 있는지 여부를 확인합니다.
- 특정 표준 시간대—이 라디오 버튼을 선택한 후에 드롭다운 목록에서 표준 시간대를 선택합니다. 시스템은 선택한 표준 시간대를 시간 일정과 비교하여 수신 통화를 받는 데 파티션을 사용할 수 있는지 여부를 확인합니다.

단계 8 저장을 클릭합니다.

Manager Assistant 공유 회선 지원을 위한 파티션 이름 지침

발신 검색 공간의 파티션 목록에서 최대 문자 수는 1024자로 제한됩니다. 즉, CSS의 최대 파티션 수는 파티션 이름의 길이에 따라 달라집니다. 다음 표를 사용하여 파티션 이름이 고정 길이인 경우 발신 검색 공간에 추가할 수 있는 최대 파티션 수를 결정합니다.

표 20: 파티션 이름 지침

파티션 이름 길이	최대 파티션 수
2자	340
3자	256
4자	204
5자	172
...	...
10자	92
15자	64

Manager Assistant 공유 회선 지원에 대한 발신 검색 공간 구성

발신 검색 공간은 일반적으로 디바이스에 할당되어 있는 정렬된 경로 파티션 목록입니다. 발신 검색 공간은 통화를 완료하려고 시도할 때 발신 디바이스에서 검색할 수 있는 파티션을 결정합니다.

두 발신 검색 공간(Generated_CSS_I_E 및 Generated_CSS_M_E)을 만들어야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 제어 클래스> 발신 검색 공간.

단계 2 새로 추가를 클릭합니다.

단계 3 이름 필드에 이름을 입력합니다.

각 발신 검색 공간 이름은 시스템에 고유해야 합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.

단계 4 설명 필드에 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.

단계 5 사용 가능한 파티션 드롭다운 목록에서 다음 단계 중 하나를 수행합니다.

- 단일 파티션의 경우 해당 파티션을 선택합니다.
- 여러 파티션의 경우 컨트롤(CTRL) 키를 누른 상태에서 해당 파티션을 선택합니다.

단계 6 상자 사이에서 아래쪽 화살표를 선택하여 선택한 파티션 필드로 파티션을 이동합니다.

단계 7 (선택 사항) 선택한 파티션 상자 오른쪽의 화살표 키를 사용하여 선택한 파티션의 우선 순위를 변경합니다.

단계 8 저장을 클릭합니다.

Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수 구성

관리자와 보조자를 위해 Manager Assistant 구성을 사용하려면 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수를 구성합니다. 모든 Cisco IP 매니저 어시스턴트 (Cisco IPMA)에 대해 클러스터 수준 매개 변수를 한 번, 그리고 설치된 각 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스에 대해 일반 매개 변수를 지정해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스가 활성화된 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco IP 매니저 어시스턴트 (Cisco IPMA)** 서비스를 선택합니다. 매개 변수를 나열하는 서비스 매개 변수 구성 창이 표시됩니다.

단계 4 **Cisco IP 매니저 어시스턴트 (Cisco IPMA)** 매개 변수, 클러스터 수준 매개 변수(모든 서버에 적용되는 매개 변수) 및 클러스터 수준 매개 변수(소프트키 템플릿)를 구성합니다.

자세한 설명을 보려면 ?를 클릭하십시오.

단계 5 저장을 클릭합니다.

인터콤 설정 구성

프로시저

	명령 또는 동작	목적
단계 1	인터콤 파티션 구성, 193 페이지	
단계 2	인터콤 발신 검색 공간 구성, 193 페이지	
단계 3	인터콤 디렉터리 번호 구성, 194 페이지	

	명령 또는 동작	목적
단계 4	인터콤 변환 패턴 구성, 194 페이지	

인터콤 파티션 구성

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 인터콤 > 인터콤 경로 파티션.
인터콤 파티션 패턴 찾기 및 나열 창이 나타납니다.
- 단계 2 새로 추가를 클릭합니다.
새 인터콤 파티션 추가 창이 나타납니다.
- 단계 3 인터콤 파티션 정보 섹션의 이름 상자에, 추가할 인터콤 파티션의 이름 및 설명을 입력합니다.
참고 여러 파티션을 입력하려면 각 파티션 항목마다 하나의 회선을 사용합니다. 최대 75개의 파티션을 입력할 수 있습니다. 이름과 설명으로 최대 총 1,475자를 사용할 수 있습니다. 파티션 이름은 50자를 초과할 수 없습니다. 각 줄에서 쉼표(,)를 사용하여 파티션 이름과 설명을 구분하십시오. 설명을 입력하지 않으면 Unified Communications Manager에서 파티션 이름을 설명으로 사용합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 구성할 파티션을 찾습니다.
인터콤 파티션 구성 창이 표시됩니다.
- 단계 6 [인터콤 파티션 구성] 필드 영역에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 7 저장을 클릭합니다.
인터콤 파티션 구성 창이 나타납니다.
- 단계 8 설정을 적절히 입력합니다. 인터콤 파티션 구성 매개 변수에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 9 저장을 클릭합니다.
- 단계 10 구성 적용을 클릭합니다.

인터콤 발신 검색 공간 구성

프로시저

- 단계 1 메뉴 모음에서 통화 라우팅 > 인터콤 > 인터콤 발신 검색 공간을 선택합니다.
- 단계 2 새로 추가를 클릭합니다.

단계 3 [인터콧 발신 검색 공간] 필드 영역에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

인터콧 디렉터리 번호 구성

프로시저

단계 1 통화 라우팅 > 인터콧 > 인터콧 디렉터리 번호를 선택합니다.

인터콧 디렉터리 번호 찾기 및 나열 창이 표시됩니다.

단계 2 특정 인터콧 디렉터리 번호를 찾으려면 검색 조건을 입력하고 찾기를 클릭합니다.
검색 조건과 일치하는 인터콧 디렉터리 번호 목록이 표시됩니다.

단계 3 다음 작업 중 하나를 수행합니다.

- a) 인터콧 디렉터리 번호를 추가하려면 새로 추가 버튼을 클릭합니다.
- b) 인터콧 디렉터리 번호를 업데이트하려면 업데이트할 인터콧 디렉터리 번호를 클릭합니다.

인터콧 디렉터리 번호 구성 창이 표시됩니다.

단계 4 [인터콧 디렉터리 번호 구성] 필드 영역에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

단계 6 구성 적용을 클릭합니다.

단계 7 전화 재설정을 클릭합니다.

단계 8 디바이스를 재시작합니다.

다시 시작하는 동안 게이트웨이의 전화가 끊어질 수 있습니다.

인터콧 변환 패턴 구성

프로시저

단계 1 통화 라우팅 > 인터콧 > 인터콧 변환 패턴을 선택합니다.

인터콧 변환 패턴 찾기 및 나열 창이 나타납니다.

단계 2 다음 작업 중 하나를 수행합니다.

- a) 기존 인터콧 변환 패턴을 복사하려면 구성할 파티션을 찾아 복사할 인터콧 변환 패턴 옆에 있는 복사 버튼을 클릭합니다.
- b) 새 인터콧 변환 패턴을 추가하려면 새로 추가를 클릭합니다.

단계 3 [인터콤 변환 패턴 구성] 필드 영역에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

선택한 파티션, 경로 패턴 및 번호 지정 플랜 조합을 사용하는 인터콤 변환 패턴이 고유한지 확인합니다. 중복 항목을 나타내는 오류 메시지가 표시되는 경우 경로 패턴이나 헛트 파일럿, 변환 패턴, 디렉터리 번호, 통화 지정 보류 번호, 통화 당겨 받기 번호 또는 Meet-Me 구성 창을 확인합니다.

인터콤 변환 패턴 구성 창에는 새로 구성된 인터콤 변환 패턴이 표시됩니다.

다음에 수행할 작업

공유 회선에 대한 Manager Assistant 작업 흐름, 188 페이지를 참조하여 완료할 다음 작업을 결정합니다.

여러 Manager Assistant 풀 구성

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스가 활성화된 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스를 선택합니다. 매개 변수를 나열하는 서비스 매개 변수 구성 창이 표시됩니다.

단계 4 고급을 클릭합니다.

클러스터 수준 매개 변수(모든 서버에 적용되는 매개 변수)용 고급 매개 변수가 표시됩니다.

단계 5 클러스터 수준 매개 변수(모든 서버에 적용되는 매개 변수)에 여러 관리자 보조자를 추가하려면 다음 매개 변수를 구성합니다.

- 여러 활성 모드 활성화—기본값은 False입니다. 이 매개 변수를 [참]으로 설정하면 관리자가 다중 풀을 사용하여 최대 7,000명의 관리자와 보조자를 구성할 수 있습니다.
- 풀 2: Cisco IPMA 서버(기본) IP 주소—기본값 없음. 관리자가 이 IP 주소를 수동으로 입력해야 합니다. 관리자는 최대 2500개 관리자 및 보조자에 이 주소를 할당할 수 있습니다.
- 풀 2: Cisco IPMA 서버(백업) IP 주소—기본값 없음. 관리자가 이 IP 주소를 수동으로 입력해야 합니다.
- 풀 3: Cisco IPMA 서버(기본) IP 주소—기본값 없음. 관리자가 이 IP 주소를 수동으로 입력해야 하고 이 주소에 최대 2500개 관리자 및 보조자를 지정할 수 있습니다.
- 풀 3: Cisco IPMA 서버(백업) IP 주소—기본값 없음. 관리자가 이 IP 주소를 수동으로 입력해야 합니다.

자세한 설명을 보려면 ?를 클릭하십시오.

단계 6 저장을 클릭합니다.

다음에 수행할 작업

공유 회선에 대한 Manager Assistant 작업 흐름, 188 페이지를 참조하여 완료할 다음 작업을 결정합니다.

Manager Assistant용 CTI에 보안 TLS 연결 구성

Manager Assistant는 WDSecureSysUser 애플리케이션 사용자 인증서를 사용하여 CTI에 보안 TLS 연결을 설정한 후 전화를 겁니다.

WDSecureSysUser 애플리케이션 사용자를 구성하여 보안 TLS 연결을 설정하려면 다음 작업을 수행합니다.

시작하기 전에

- Cisco CTL 클라이언트를 설치하고 구성합니다.

CTL 클라이언트에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 보안 설명서](#)의 내용을 참조하십시오.

- 엔터프라이즈 매개 변수 구성 창의 클러스터 보안 모드가 **1**(혼합 모드)인지 확인합니다. 시스템을 혼합 모드에서 작동하면 시스템의 다른 보안 기능에 영향을 미칩니다. 시스템이 현재 혼합 모드에서 실행되지 않으면, 이러한 상호 작용을 이해할 때까지 혼합 모드로 전환하지 마십시오. 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 보안 설명서](#)의 내용을 참조하십시오.
- 엔터프라이즈 매개 변수 구성 창의 클러스터 **SIPOAuth** 모드가 활성화됨인지 확인합니다.
- 첫 번째 노드에서 Cisco Certificate Authority Proxy Function(CAPF) 서비스를 활성화합니다.

프로시저

	명령 또는 동작	목적
단계 1	IPMASecureSysUser 애플리케이션 사용자 구성, 196 페이지	IPMASecureSysUser 애플리케이션 사용자를 구성합니다.
단계 2	CAPF 프로파일 구성, 197 페이지	IPMASecureSysUser 애플리케이션 사용자에 대한 CAPF(Certificate Authority Proxy Function) 프로파일을 구성합니다.
단계 3	Cisco WebDialer 웹 서비스 구성, 199 페이지	Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스에 대한 서비스 매개 변수를 구성합니다.

IPMASecureSysUser 애플리케이션 사용자 구성

IPMASecureSysUser 애플리케이션 사용자를 구성하려면 이 절차를 사용합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 애플리케이션 사용자.
- 단계 2 찾기를 클릭합니다.
- 단계 3 애플리케이션 사용자 찾기 및 나열 창에서 **WDSecureSysUser**를 선택합니다.
- 단계 4 애플리케이션 사용자 구성 창의 필드를 구성하고 저장을 클릭합니다.

CAPF 프로파일 구성

CAPF(Certificate Authority Proxy Function)는 보안 인증서를 발급하고 인증하는 작업을 수행하는 구성 요소입니다. 애플리케이션 사용자 CAPF 프로파일을 만들 때 프로파일은 구성 세부 정보를 사용하여 애플리케이션에 대한 보안 연결을 엽니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 애플리케이션 사용자 **CAPF** 프로파일.
- 단계 2 다음 작업 중 하나를 수행합니다.
- 새 CAPF 프로파일을 추가하려면 찾기 창에서 새로 추가를 클릭합니다.
 - 기존 프로파일을 복사하려면 적절한 프로파일 찾아 복사 열에 있는 해당 레코드에 대한 복사 아이콘을 클릭합니다.
- 기존 항목을 업데이트하려면 해당 프로파일을 찾아 표시합니다.
- 단계 3 관련 CAPF 프로파일 필드를 구성하거나 업데이트합니다. 필드 및 해당 구성 옵션에 대한 정보는 관련 항목 섹션을 참조하십시오.
- 단계 4 저장을 클릭합니다.
- 단계 5 보안을 사용하려는 각 애플리케이션 및 최종 사용자에 대해 절차를 반복합니다.

CAPF 프로파일 설정

설정	설명
애플리케이션 사용자	드롭다운 목록에서 CAPF 작업의 애플리케이션 사용자를 선택합니다. 이 설정은 구성된 애플리케이션 사용자를 표시합니다. 이 설정은 최종 사용자 CAPF 프로파일 창에 나타나지 않습니다.
최종 사용자 ID	드롭다운 목록에서 CAPF 작업의 최종 사용자를 선택합니다. 이 설정은 구성된 최종 사용자를 표시합니다. 이 설정은 애플리케이션 CAPF 프로파일 창에 나타나지 않습니다.

설정	설명
인스턴스 ID	<p>1 ~ 128자의 영숫자(a-z, A-Z, 0-9)를 입력합니다. 인스턴스 ID는 인증서 작업의 사용자를 식별합니다.</p> <p>다중 애플리케이션 연결(인스턴스)을 구성할 수 있습니다. 애플리케이션과 CTIManager 간 연결을 보호하려면 애플리케이션 PC(최종 사용자의 경우) 또는 서버(애플리케이션 사용자의 경우)에서 실행되는 각 인스턴스에 고유 인증서가 있어야 합니다.</p> <p>이 필드는 웹 서비스 및 애플리케이션을 지원하는 CTIManager에 보안 연결(Secure Connection to CTIManager) 서비스 파라미터에 대한 CAPF 프로파일 인스턴스 ID와 관련되어 있습니다.</p>
인증서 작업	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 보류 중인 작업 없음 - 이 메시지는 인증서 작업이 발생하지 않을 때 표시됩니다. (기본 설정) • 설치/업그레이드 - 이 옵션은 새 인증서를 설치하거나 애플리케이션의 기존 LSC를 업그레이드합니다.
인증 모드	<p>설치/업그레이드 인증서 작업에 대한 인증 모드는 [인증 문자열별]이며, 이는 사용자 또는 관리자가 JTAPl/TSP 기본 설정 창에서 CAPF 인증 문자열을 입력하는 경우에만 CAPF에서 LSC 설치/업그레이드 또는 문제 해결을 수행함을 나타냅니다.</p>
인증 문자열	<p>자체 인증 문자열을 생성하려면 고유 문자열을 입력합니다.</p> <p>각 문자열은 4~10자를 포함해야 합니다.</p> <p>LSC 인증서를 설치 또는 업그레이드하려면 관리자가 애플리케이션 PC의 JTAPl/TSP 기본 설정 GUI에 인증 문자열을 입력해야 합니다. 이 문자열은 일회용으로, 인스턴스에 대한 문자열을 사용한 후에는 다시 사용할 수 없습니다.</p>
문자열 생성	<p>인증 문자열을 자동으로 생성하려면 이 버튼을 클릭합니다. 4~10자리 인증 문자열은 인증 문자열 필드에 나타납니다.</p>
키 크기(비트)	<p>드롭다운 목록에서 인증서의 키 크기를 선택합니다. 기본 설정은 1024입니다. 기타 키 크기 옵션은 512입니다.</p> <p>키 생성은 우선 순위가 낮게 설정되어 있어, 작업이 수행되는 동안 애플리케이션이 작동됩니다. 키 생성에는 최대 30분 이상이 소요될 수 있습니다.</p>

설정	설명
작업 완료 시간	<p>이 필드는 모든 인증서 작업을 지원하며, 해당 작업을 완료해야 하는 날짜 및 시간을 지정합니다.</p> <p>표시되는 값이 첫 번째 노드에 적용됩니다.</p> <p>이 설정은 인증서 작업을 완료해야 하는 기본 일수를 지정하는 CAPF 작업 유효 기간(CAPF Operation Expires in)(일) 엔터프라이즈 매개 변수와 함께 사용됩니다. 이 매개 변수를 언제든지 업데이트할 수 있습니다.</p>
인증서 작업 상태	<p>이 필드에는 인증서 작업의 진행 상태(예: 보류 중, 실패 또는 성공)가 표시됩니다.</p> <p>이 필드에 표시되는 정보를 변경할 수 없습니다.</p>

Cisco WebDialer 웹 서비스 구성

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 Cisco WebDialer 웹 서비스가 활성화된 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco WebDialer** 웹 서비스를 선택합니다.
매개 변수 목록이 나타납니다.
- 단계 4 CTIManager 연결 보안 플러그 및 CAPF 프로파일 인스턴스 ID로 이동하고 보안 연결을 위해 CTIManager 매개 변수로 업데이트합니다.

매개 변수 설명을 보려면 매개 변수 이름 링크를 클릭합니다.
참고 CTIManager는 IPv4 및 IPv6 주소를 지원합니다.
- 단계 5 저장을 클릭합니다.
- 단계 6 서비스가 활성화된 각 서버에서 이 절차를 반복합니다.

다음에 수행할 작업

[공유 회선에 대한 Manager Assistant 작업 흐름, 188 페이지](#)를 참조하여 완료할 다음 작업을 결정합니다.

CTI 라우트 포인트 구성

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > **CTI 라우트 포인트**.
- 단계 2 새로 추가를 클릭합니다.
CTI 라우트 포인트 구성 창이 표시됩니다.
- 단계 3 디바이스 이름 필드에 디바이스 이름을 입력합니다.
- 단계 4 디바이스폴 드롭다운 목록에서 기본값을 선택합니다.
- 단계 5 발신 검색 공간드롭다운 목록에서 **Generated_CSS_M_E**를 선택합니다.
- 단계 6 디바이스폴 발신자 변환 **CSS** 사용 확인란을 선택합니다.
- 단계 7 저장을 클릭합니다.
추가 성공 상태 메시지가 표시됩니다.
- 단계 8 [연결] 영역에서 회선 [1] - 새 **DN** 추가를 클릭합니다.
디렉터리 번호 구성 창이 표시됩니다.
- 단계 9 디렉터리 번호 필드에 디렉터리 번호를 입력합니다.
- 단계 10 경로 파티션 드롭다운 목록에서 **Generated_Route_Point**를 선택합니다.
- 단계 11 저장을 클릭합니다.

관리자 및 보조자에 대한 IP 전화 서비스 구성

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화 서비스.
- 단계 2 새로 추가를 클릭합니다.
IP Phone 서비스 구성 창이 표시됩니다.
- 단계 3 관리자 및 보조자의 지원되는 각 전화기에 대해 필수 필드를 입력하고 저장을 클릭합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [Cisco IP Phone 서비스, 구성 필드, 200 페이지](#)를 참조하십시오.
업데이트 성공 메시지가 표시됩니다.

Cisco IP Phone 서비스, 구성 필드

필드	설명
서비스 정보	

필드	설명
서비스 이름	<p>서비스의 이름을 입력합니다. 서비스가 엔터프라이즈 가입으로 표시되지 않을 경우 서비스에 가입(예: Cisco Unified Communications 셀프 서비스 포털 아래)시킬 수 있는 영역에 서비스 이름이 표시됩니다.</p> <p>최대 128자의 서비스 이름을 입력합니다.</p> <p>Java MIDlet 서비스의 서비스 이름은 JAD(Java Application Descriptor) 파일에 정의된 이름과 정확히 일치해야 합니다.</p> <p>참고 Unified Communications Manager 동일한 이름으로 IP 전화 서비스를 두 개 이상 생성할 수 있습니다. 전화기 사용자 전체 또는 대부분이 고급 사용자이거나 관리자가 항상 IP 전화 서비스를 구성하는 경우를 제외하고는 이처럼 동일한 이름을 사용하는 것은 권장하지 않습니다. AXL 또는 타사 도구에서 구성을 위해 IP 전화 서비스 목록에 액세스하는 경우 IP 전화 서비스에 고유한 이름을 사용해야 합니다.</p> <p>참고 서비스 URL이 사용자 정의된 외부 URL을 가리키는 경우 전화기의 디바이스 로컬에 따라 서비스 이름을 지역화할 수 없습니다. 서비스 이름은 영문자로만 표시됩니다.</p>
ASCII 서비스 이름	전화기에서 유니코드를 표시할 수 없는 경우에 표시될 서비스의 이름을 입력합니다.
서비스 설명	서비스에서 제공하는 내용에 대한 설명을 입력합니다. 설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표(") 또는 작은 따옴표(')는 사용할 수 없습니다.

필드	설명
서비스 URL	<p>IP 전화 서비스 애플리케이션이 있는 서버의 URL을 입력합니다. 이 서버는 Unified Communications Manager 클러스터의 서버와 상관없이 유지되어야 합니다. Unified Communications Manager 서버 또는 Unified Communications Manager와 연결된 서버(예: TFTP 서버 또는 디렉토리 데이터베이스 게시자 서버)는 지정하지 마십시오.</p> <p>서비스를 사용할 수 있으려면 Unified Communications Manager 클러스터의 전화기가 서버에 대한 네트워크 연결을 유지해야 합니다.</p> <p>Cisco에서 서명한 Java MIDlet의 경우 JAD 파일을 다운로드할 수 있는 위치(예: Java MIDlet이 통신하는 웹 서버 또는 백엔드 애플리케이션 서버)를 입력합니다.</p> <p>Cisco에서 제공하는 기본 서비스의 경우 기본 서비스 URL은 <code>Application:Cisco/<name of service></code>으로 표시됩니다. 예를 들어, <code>Application:Cisco/CorporateDirectory</code>입니다. Cisco에서 제공하는 기본 서비스의 서비스 URL을 수정하는 경우 서비스 프로비저닝 설정으로 [모두]를 구성했는지 확인합니다. 이 설정은 전화기, 엔터프라이즈 매개 변수 및 일반 전화 프로파일 구성 창에 표시됩니다. 예를 들어, 사용자 정의 기업 디렉토리를 사용하므로 <code>Application:Cisco/CorporateDirectory</code>를 사용자 정의 디렉토리의 외부 서비스 URL로 변경합니다. 이 경우 서비스 프로비저닝 값을 둘 다로 설정합니다.</p>
보안-서비스 URL	<p>Cisco Unified IP Phone 서비스 애플리케이션이 있는 서버의 URL을 입력합니다. 이 서버는 Unified Communications Manager 클러스터의 서버와 상관없이 유지되어야 합니다. Unified Communications Manager 서버 또는 Unified Communications Manager와 연결된 서버(예: TFTP 서버 또는 퍼블리셔 데이터베이스 서버)는 지정하지 마십시오.</p> <p>서비스를 사용할 수 있으려면 Unified Communications Manager 클러스터의 전화기가 서버에 대한 네트워크 연결을 유지해야 합니다.</p> <p>참고 보안 서비스 URL을 제공하지 않는 경우 디바이스는 비보안 URL을 사용합니다. 보안 URL과 비보안 URL을 모두 제공하는 경우 디바이스에서 해당 기능에 따라 적절한 URL을 선택합니다.</p>
서비스 카테고리	<p>서비스 애플리케이션 유형(XML 또는 Java MIDlet)을 선택합니다.</p> <p>Java MIDlet을 선택하면 전화기에서 업데이트된 구성 파일을 수신할 때 전화기는 지정된 서비스 URL로부터 Cisco에서 서명한 MIDlet 애플리케이션(JAD 및 JAR)을 가져와서 애플리케이션을 설치합니다.</p>

필드	설명
서비스 유형	전화기의 [서비스], [디렉터리] 또는 [메시지] 버튼 또는 옵션 중 어떤 항목으로 서비스를 설정할지 선택합니다(단, 전화기에 이러한 버튼 또는 옵션이 있는 경우) 이러한 버튼 또는 옵션 중 전화기에서 지원할 항목을 결정하려면 현재 전화기 모델을 지원하는 <i>Cisco Unified IP Phone</i> 관리 지침서를 참조하십시오.
서비스 공급업체	<p>서비스 공급업체 또는 제조업체를 지정할 수 있습니다. 이 필드는 XML 애플리케이션의 경우 선택 항목이지만, Cisco에서 서명한 Java MIDlet의 경우에는 필수 항목입니다.</p> <p>Cisco에서 서명한 Java MIDlet의 경우 이 필드에 입력하는 값은 MIDlet JAD 파일에 정의된 공급업체와 정확히 일치해야 합니다.</p> <p>Cisco에서 제공하는 기본 서비스에 대해 이 필드는 빈 것으로 표시됩니다.</p> <p>최대 64자를 입력할 수 있습니다.</p>
서비스 버전	<p>애플리케이션에 대한 버전 번호를 입력합니다.</p> <p>XML 애플리케이션의 경우 이 필드는 선택 항목이며 정보 제공을 위해 사용됩니다. Cisco에서 서명한 Java MIDlet의 경우 다음 정보를 고려하십시오.</p> <ul style="list-style-type: none"> 버전을 입력하는 경우 서비스 버전은 JAD 파일에 정의된 버전과 정확히 일치해야 합니다. 버전을 입력하는 경우 버전이 전화기에 설치된 버전과 다르면 전화기는 MIDlet을 업그레이드하거나 다운그레이드합니다. 이 필드를 비워 두면 서비스 URL에서 버전이 검색됩니다. 이 필드를 비워 두면 전화기가 Unified Communications Manager에 등록되는 경우에 항상, 그리고 Cisco에서 서명한 Java MIDlet이 시작될 때마다 전화기에서 JAD 파일을 다운로드하려고 합니다. 이를 통해 전화기에서는 항상 Cisco에서 서명한 최신 버전의 Java MIDlet이 실행될 수 있으므로 서비스 버전 필드를 수동으로 업데이트할 필요가 없습니다. <p>Cisco에서 제공하는 기본 서비스에 대해 이 필드는 빈 것으로 표시됩니다.</p> <p>이 필드에는 숫자 및 마침표를 입력할 수 있습니다(최대 16자 ASCII).</p>
활성화	<p>Cisco Unified CM 관리에서 구성을 제거하지 않고(데이터베이스에서 서비스를 제거하지 않고)도 서비스를 활성화하거나 비활성화할 수 있습니다.</p> <p>확인란의 선택을 취소하면 전화기 구성 파일 및 전화기에서 서비스가 제거됩니다.</p>

필드	설명
서비스 매개 변수 정보	
파라미터	<p>이 IP 전화 서비스에 적용되는 서비스 매개 변수가 나열됩니다. 다음 버튼을 사용하여 이 창에 대한 서비스 매개 변수를 구성합니다.</p> <ul style="list-style-type: none"> • 새 매개 변수—이 IP 전화 서비스에 대해 새 서비스 매개 변수를 구성할 수 있는 Cisco Unified IP 전화 서비스 매개 변수 구성 창을 표시하려면 이 버튼을 클릭합니다. • 매개 변수 편집—매개 변수 창에 표시되는 서비스 매개 변수를 강조 표시한 다음 이 버튼을 클릭하여 현재 IP 전화 서비스에 대해 선택한 서비스 매개 변수를 편집할 수 있는 Cisco Unified IP 전화 서비스 매개 변수 구성 창을 표시합니다. • 매개 변수 삭제—매개 변수 창에 표시되는 서비스 매개 변수를 강조 표시한 다음 이 버튼을 클릭하여 이 IP 전화 서비스에 대한 서비스 매개 변수를 삭제합니다. 팝업 창에 삭제를 확인하는 메시지가 표시됩니다.

관리자, 보조자 및 모든 사용자용 전화 버튼 템플릿 구성

이 섹션의 절차에서는 관리자 및 보조자를 위해 전화기 버튼을 구성하는 방법을 설명합니다.

프로시저

	명령 또는 동작	목적
단계 1	Manager Assistant에 대한 전화기 버튼 템플릿 구성, 204 페이지	회선 또는 단축 다이얼 키에 관리자 및 보조자 버튼 기능을 할당하려면 이 단계를 수행합니다.
단계 2	Manager Assistant 버튼 템플릿을 전화기와 연결, 205 페이지	전화기에 대해 관리자 및 보조자 버튼을 구성하려면 이 단계를 수행합니다.

Manager Assistant에 대한 전화기 버튼 템플릿 구성

Manager Assistant 기능에 대한 전화기 버튼 템플릿을 구성하려면 이 절차를 사용합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.
 단계 2 [찾기]를 클릭하여 지원되는 전화기 템플릿 목록을 표시합니다.

단계 3 새 전화기 버튼 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.

- a) 전화기의 모델에 대한 기본 템플릿을 선택하고 복사를 클릭합니다.
- b) 전화기 버튼 템플릿 정보 필드에 템플릿의 새 이름을 입력합니다.
- c) 저장을 클릭합니다.

단계 4 기존 템플릿에 전화기 버튼을 추가하려는 경우 다음 단계를 수행합니다.

- a) 찾기를 클릭하고 검색 기준을 입력합니다.
- b) 기존 템플릿을 선택합니다.

단계 5 회선 드롭다운 목록에서 템플릿에 추가하려는 기능을 선택합니다.

단계 6 저장을 클릭합니다.

단계 7 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다.

Manager Assistant 버튼 템플릿을 전화기와 연결

시작하기 전에

[Manager Assistant에 대한 전화기 버튼 템플릿 구성, 204 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.

단계 3 전화기 버튼 템플릿을 추가할 전화기를 선택합니다.

단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

관리자 구성 및 공유 회선 모드에 사용할 보조자 할당

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

- 단계 2** 찾기를 클릭합니다.
검색 결과에는 Unified Communications Manager에서 구성한 최종 사용자가 모두 표시됩니다.
- 단계 3** 관련 링크 드롭다운 목록에서 관리자 구성을 선택하고 이동을 클릭합니다.
- 단계 4** 소프트키 템플릿을 자동으로 구성하고 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수를 기반으로 관리자 전화기의 인터콤 회선에 스피커폰으로 자동 응답하려면 자동 구성 확인란을 선택합니다.
- 참고 인터콤에 대한 자동 구성은 Cisco Unified IP Phones 7940 및 7960에 Unified Communications Manager Assistant 인터콤 기능을 사용하는 경우에만 적용됩니다.
- 단계 5** 공유 회선 사용 확인란을 선택합니다.
- 단계 6** 디바이스 이름/프로파일 드롭다운 목록에서 디바이스 이름 또는 디바이스 프로파일을 관리자과 연결할 디바이스 이름 또는 디바이스 프로파일을 선택합니다.
- 참고 관리자가 재택 근무하는 경우 모바일 관리자 확인란을 선택하고 선택적으로 디바이스 이름/프로파일 드롭다운 목록에서 디바이스 프로파일을 선택합니다. 디바이스 프로파일을 선택하는 경우 관리자는 Cisco Extension Mobility를 사용하여 전화기로 로그인해야만 Manager Assistant에 액세스할 수 있습니다.
- Manager assistant 기능이 있는 Extension Mobility에 대한 자세한 내용은 관련 항목을 참조하십시오.
- 단계 7** 인터콤 회선 드롭다운 목록 상자에서 관리자의 인터콤 회선 표시를 선택합니다(해당되는 경우). 선택한 인터콤 회선을 Manager Assistant 및 Unified Communications Manager 인터콤 기능에 적용합니다.
- 단계 8** 보조자 풀 드롭다운 목록에서 적절한 풀 번호(1~3)를 선택합니다.
- 단계 9** 사용 가능한 보조자 선택 상자에서 보조자 이름을 선택하고 아래쪽 화살표를 클릭하여 연결된 보조자 선택 상자로 이동하여 관리자에게 보조자를 할당합니다.
- 보조자 이름을 선택하고 세부 정보 보기 링크를 클릭하여 보조자 구성 창으로 이동할 수 있습니다.
- 단계 10** 사용 가능한 회선 목록 상자에서 적절한 회선을 선택하고 아래쪽 화살표를 클릭하여 선택한 회선 목록 상자로 이동하고 Manager Assistant 제어 회선을 구성합니다.
- 제어 회선은 항상 공유 회선 DN이어야 합니다.
- 단계 11** 저장을 클릭합니다.
- 자동 구성 확인란을 선택했지만 서비스 매개 변수가 잘못된 경우 메시지가 표시됩니다. 서비스 매개 변수가 올바른지 확인하십시오. 자동 구성이 완료되면 관리자 디바이스가 재설정됩니다. 디바이스 프로파일을 구성한 경우, 관리자가 디바이스에서 로그아웃했다가 다시 로그인해야 변경 내용이 적용됩니다.

공유 회선에 대한 보조자 회선 표시 구성

관리자는 하나 이상의 회선을 공유 회선 표시로 설정할 수 있습니다. Unified Communications Manager 시스템에서는 디렉터리 번호가 동일한 파티션의 디바이스 둘 이상에 표시되는 경우 공유 회선으로 간주합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자
- 단계 2 찾기를 클릭합니다.
검색 결과에는 Unified Communications Manager에서 구성한 최종 사용자가 모두 표시됩니다.
- 단계 3 한 사용자 이름을 클릭하여 선택한 보조자에 대한 사용자 정보를 표시합니다.
최종 사용자 구성 창이 표시됩니다.
- 단계 4 관련 링크 드롭다운 목록에서 보조자 구성을 선택하고 이동을 클릭합니다.
보조자 구성 창이 표시됩니다. 자동 구성 확인란을 선택한 경우 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스 매개 변수 설정을 기준으로 소프트키 템플릿 및 인터콤 회선이 자동으로 설정됩니다.
또한 인터콤 회선에 스피커폰으로 자동 응답이 설정됩니다.
- 단계 5 디바이스 이름 드롭다운 목록에서 보조자와 연결할 디바이스 이름을 선택합니다.
- 단계 6 인터콤 회선 드롭다운 목록에서 보조자의 착신 인터콤 회선 표시를 선택합니다.
- 단계 7 기본 회선 드롭다운 목록에서 보조자의 기본 회선을 선택합니다.
- 기존 관리자 구성 정보를 보려면, 연결된 관리자 목록에서 해당 관리자 이름을 강조 표시한 다음 세부 정보 보기 링크를 클릭합니다.
관리자 구성 창이 표시됩니다.
 - 보조자 구성 창으로 돌아가려면 관리자 구성 창에서 보조자 이름을 강조 표시하고 세부 정보 보기 링크를 클릭합니다.
연결된 관리자 선택 목록 상자에 기존에 구성한 관리자의 이름이 표시됩니다.
- 단계 8 관리자 회선을 보조자 회선에 연결하려면 [보조자 회선에 대한 관리자 연결] 선택 상자에서 다음 단계를 수행합니다.
- 사용 가능한 회선 드롭다운 목록에서 관리자 회선과 연결할 보조자 회선을 선택합니다.
 - 관리자 이름 드롭다운 목록에서 이 프록시 회선을 적용할 미리 구성된 관리자 이름을 선택합니다.
 - 관리자 회선 드롭다운 목록에서 이 프록시 회선을 적용할 관리자 회선을 선택합니다.
- 단계 9 저장을 클릭합니다.
업데이트는 즉시 적용됩니다. 자동 구성을 선택하는 경우 보조자 디바이스가 자동으로 재설정됩니다.

Assistant Console 플러그인 설치

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 애플리케이션 > 플러그인.
플러그인 찾기 및 나열 창이 표시됩니다.
- 단계 2 찾기를 클릭합니다.
설치 가능한 플러그인 목록이 표시됩니다.

- 단계 3 Cisco Unified CM Assistant Console의 다운로드 링크를 클릭하고 실행 파일을 위치에 저장합니다.
- 단계 4 실행 파일을 실행합니다.
- 참고 Windows Vista PC에서 애플리케이션을 설치하는 경우 보안 창이 표시됩니다. 설치가 계속되게 합니다.
- Cisco Unified CallManager Assistant Console** 설치 마법사가 표시됩니다.
- 단계 5 소개 창에서 다음을 클릭합니다.
- 단계 6 사용권 계약 창에서 다음을 클릭합니다.
- 단계 7 애플리케이션을 설치할 위치를 선택하고 다음을 클릭합니다.
- 참고 기본적으로 애플리케이션은 C:\Program Files\Cisco\ Unified CallManager Assistant Console에 설치됩니다.
- 단계 8 설치 전 요약 창에서 요약을 검토하고 설치를 클릭합니다.
설치가 시작됩니다.
- 단계 9 설치가 완료되면 마침을 클릭합니다.
- 단계 10 콘솔에 로그인 하는 데 필요한 사용자 이름 및 암호를 보조자에게 제공합니다.
- 단계 11 Assistant Console을 시작하려면 바탕 화면 아이콘을 클릭하거나 시작...프로그램 메뉴에서 **Cisco Unified Communications Manager Assistant > Assistant Console**을 선택합니다.
- 단계 12 **Cisco Unified Communications Manager Assistant** 설정 창의 고급 탭에서는 Assistant Console에 대한 추적을 활성화할 수 있습니다.
- 단계 13 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스가 활성화된 Unified Communications Manager 서버의 포트 번호 및 IP 주소 또는 호스트 이름을 보조자에게 제공합니다. 보조자는 콘솔에 처음 로그인할 때 **Cisco Unified Communications Manager Assistant** 서버 포트와 Cisco Unified **Cisco Unified Communications Manager Assistant** 서버 호스트 이름 또는 IP 주소 필드에 정보를 입력해야 합니다.

Manager Assistant 상호 작용

기능	상호 작용
벌크 관리 도구	<p>사용자를 개별적으로 추가하지 않고 벌크 관리 도구를 사용하여 여러 사용자(관리자 및 보조자)를 한 번에 추가할 수 있습니다.</p> <p>Cisco Unified CM Assistant 구성 마법사에서 Cisco Unified IP Phone 용으로 생성되는 벌크 관리 도구 템플릿은 Unified Communications Manager 인터콤 회선만 지원합니다.</p> <p>자세한 내용은 Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서를 참조하십시오.</p>

기능	상호 작용
발신자 정규화	발신자 정규화 기능을 구성할 경우 Manager Assistant는 지역화 및 전역화된 통화를 자동으로 지원합니다. Manager Assistant의 사용자 인터페이스에는 지역화된 발신자 번호가 표시될 수 있습니다. 또한 관리자에 대한 수신 통화의 경우 Manager Assistant에서는 필터 패턴 일치 발생 시 지역화된 발신자 번호와 전역화된 발신자 번호를 표시할 수 있습니다.
Extension Mobility	<p>Cisco Extension Mobility 기능과 동시에 Manager Assistant를 사용할 수 있습니다. Extension Mobility를 사용하여 Cisco Unified IP Phone에 로그인하면 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스에 해당 전화기에서 자동으로 활성화됩니다. 그런 다음 Manager Assistant 기능에 액세스할 수 있습니다.</p> <p>Cisco Extension Mobility에 대한 자세한 내용은 Extension Mobility 개요, 439 페이지를 참조하십시오.</p>
IPv6(Internet Protocol Version 6)	Manager Assistant는 IPv6을 지원하지 않으므로, Manager Assistant에서는 IP 주소 지정 모드가 IPv6 전용인 전화기를 사용할 수 없습니다. 전화기에서 Manager Assistant를 사용하려면 IP 주소 지정 모드로 [IPv4 전용] 또는 [IPv4 및 IPv6]을 사용하도록 전화기를 구성하십시오.
보고 도구	<p>Manager Assistant는 CAR(CDR Analysis and Reporting) 도구에서 통계 정보를 제공하고 변경 로그에서 구성 변경 사항에 대한 요약を提供합니다.</p> <p>관리자는 Unified CM AssistantChangeLog*.txt에서 관리자 또는 보조자 구성을 변경한 사항에 대한 요약을 볼 수 있습니다. 관리자(manager)는 URL을 통해 [관리자 구성]에 액세스하여 기본값을 변경할 수 있습니다. 보조자는 Assistant Console에서 관리자 기본값을 변경할 수 있습니다. URL 및 관리자 구성에 대한 내용은 <i>Cisco Unified Communications Manager Assistant</i> 사용 설명서를 참조하십시오.</p> <p>관리자 또는 보조자가 변경을 하면 변경 사항이 ipma_changeLogxxx.log라는 로그 파일로 전송됩니다. 로그 파일은 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스를 실행하는 서버에 있습니다. 다음 명령을 사용하여 로그 파일을 가져옵니다. file get activelog tomcat/logs/ipma/log4j/</p> <p>로그 파일 다운로드에 대한 자세한 내용은 <i>Cisco Unified Real - Time Monitoring Tool</i> 관리 지침서를 참조하십시오.</p>

기능	상호 작용
CDR Analysis and Reporting	<p>Manager Assistant는 관리자 및 보조자를 위한 통화-완료 통계와 재고 보고를 지원합니다. CAR 도구는 통화-완료 통계를 지원합니다. Cisco 유니파이드 Serviceability에서는 재고 목록 보고를 지원합니다.</p> <p>자세한 내용은 다음 설명서를 참조하십시오.</p> <ul style="list-style-type: none"> • <i>Cisco Unified Serviceability</i> 관리 지침서 • Cisco 통합 커뮤니케이션 매니저 통화 보고 및 청구 관리 지침서
MLPP(Multilevel Precedence and Preemption)	<p>다음 내용에서는 공유 회선 지원을 포함하는 Manager Assistant와 MLPP 사이의 상호 작용에 대해 설명합니다.</p> <ul style="list-style-type: none"> • 시스템은 Manager Assistant에서 통화를 처리할 때 통화 우선 순위를 유지합니다. 예를 들어 보조자가 통화를 전환할 때 통화의 우선 순위가 유지됩니다. • 우선 순위 통화에 대한 필터링은 다른 모든 통화와 동일한 방식으로 수행됩니다. 통화의 우선 순위는 통화가 필터링되는지 여부에 영향을 주지 않습니다. • Manager Assistant에는 통화의 우선 순위에 대한 정보가 없으므로 Assistant Console에 통화 우선 순위를 추가로 표시하지 않습니다.
인터콤	<p>Manager Assistant는 다음 두 가지 유형의 인터콤을 지원합니다.</p> <ul style="list-style-type: none"> • Manager Assistant 인터콤(Cisco Unified IP Phone 7940 및 7960에 사용됨). 이 인터콤 기능은 DN 구성 및 최종 사용자(관리자 및 보조자) 구성 창을 사용하여 구성할 수 있습니다. • Unified Communications Manager 인터콤(Cisco Unified IP Phones 7940 및 7960에 사용됨). 이 인터콤 기능은 인터콤 파티션, 인터콤 발신 검색 공간, 인터콤 디렉터리 번호, 인터콤 변환 패턴, DN 및 최종 사용자(관리자 및 보조자) 구성 창을 사용하여 구성할 수 있습니다.
메시지 대기 중 표시기	<p>메시지 대기 표시기 기능은 프록시 회선 지원에서만 상호 작용합니다.</p> <p>MWI(메시지 대기 표시기) 켜기 및 끄기 번호의 발신 검색 공간에는 관리자 회선의 파티션이 있어야 합니다. 파티션은 각 발신 검색 공간 내에서 임의의 우선 순위로 있을 수 있습니다.</p>

기능	상호 작용
시간 기준 라우팅	<p>시간 기준 기능은 프록시 회선 지원에서만 상호 작용합니다.</p> <p>시간 기준 라우팅에서는 전화가 걸린 시간을 기반으로 여러 위치로 통화를 전송합니다. 예를 들어 업무 시간 중에는 통화가 관리자 사무실로 전송되고 업무 시간 이후의 통화는 음성 메일 서비스로 직접 전달됩니다.</p> <p>시간 라우팅에 대한 자세한 내용을 참조하십시오 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서.</p>

Manager Assistant 제한

기능	제한 사항
Assistant Console 애플리케이션	Microsoft Internet Explorer 7(이상)이 설치된 컴퓨터에 Assistant Console 애플리케이션을 설치하려면, Assistant Console을 설치하기 전에 Microsoft Java Virtual Machine(JVM)을 설치합니다.
통화 관리 기능	Assistant Console은 헛트 그룹이나 대기열, 녹음과 모니터링, 원터치 통화 당겨 받기 및 온 훅 호전환(호전환을 완료하기 위해 [호전환] 소프트웨어 키를 누르고 온 훅하여 통화를 전환할 수 있는 기능)을 지원하지 않습니다.
Cisco IP 전화기	<p>Manager Assistant에서 Cisco Unified IP Phone 7940 및 7960을 제외하고 Cisco Unified IP Phones 7900 시리즈에서 SIP을 지원합니다.</p> <p>Manager Assistant는 여러 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서버(폴)를 구성하여 최대 3500명의 관리자와 3500명의 보조자를 지원합니다. 여러 폴이 사용되는 경우, 관리자와 해당 관리자에 대해 구성된 모든 보조자가 동일한 폴에 속해야 합니다.</p> <p>Cisco Unified IP Phone 7960 및 7940은 Unified Communications Manager 보조자 인터콤 회선 기능만 지원합니다. Cisco Unified IP Phone 7900(7940 및 7960 제외)은 Unified Communications Manager 인터콤 기능만 지원합니다.</p> <p>한 명의 관리자에게 최대 10명의 보조자를 할당할 수 있고 한 명의 보조자는 최대 33명의 관리자를 지원할 수 있습니다(각 관리자에게 하나의 Unified Communications Manager 제어 회선이 있는 경우).</p> <p>한 번에 한 보조자만 관리자를 지원할 수 있습니다.</p> <p>Manager Assistant에서는 Unified Communications Manager 클러스터당 최대 3500명의 관리자와 3500명의 보조자를 지원합니다.</p>

기능	제한 사항
인터콤	업그레이드 후 수신 인터콤 회선을 사용하는 Manager Assistant 사용자는 자동으로 Unified Communications Manager 인터콤 기능으로 업그레이드되지 않습니다. 이 시스템은 Unified Communications Manager 인터콤 기능과 일반 회선 간의 통화를 지원하지 않습니다(이는 Manager Assistant 인터콤 회선으로 구성할 수 있습니다).
SSO(Single Sign-On)	Manager Assistant는 Single Sign-On 환경에서 지원되지 않습니다.
바로 호출	Cisco Unified IP Phone 7940, 7942, 7945는 2개의 회선 또는 [단축 다이얼] 버튼만 지원합니다.

Cisco Unified Communications Manager Assistant 문제 해결

이 섹션에서는 Manager Assistant를 위한 문제 해결 도구 및 Manager Assistant를 위한 클라이언트 데스크톱 및 문제 해결 정보를 설명합니다.

도구 설명	위치
Cisco Unified CM Assistant 서버 추적 파일	추적 파일은 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스를 실행하는 서버에 있습니다. 다음 방법 중 하나를 사용하여 서버에서 이러한 파일을 다운로드할 수 있습니다. <ul style="list-style-type: none">CLI 명령 file get activelog tomcat/logs/ipma/log4j를 사용합니다.Cisco Unified Real-Time Monitoring Tool(RTMT)의 추적 수집 기능을 사용합니다. 자세한 내용은 <i>Cisco Unified Real Time Monitoring Tool</i> 관리 설명서를 참조하십시오. Cisco Unified Serviceability > 추적 > 구성을 선택하여 디버그 추적을 활성화할 수 있습니다.
Cisco IPMA 클라이언트 추적 파일	Unified CM Assistant 보조자 콘솔이 있는 곳과 동일한 위치인 클라이언트 데스크탑의 \$INSTALL_DIR\logs\ACLog*.txt . 디버그 추적을 활성화하려면 Assistant Console의 설정 대화 상자로 이동합니다. 고급 패널에서 추적 활성화 확인란을 선택합니다. 참고 이 확인란은 디버그 추적만 활성화합니다. 오류 추적은 항상 켜져 있습니다.
Cisco IPMA 클라이언트 설치 추적 파일	Assistant Console이 있는 곳과 동일한 위치인 클라이언트 데스크탑의 \$INSTALL_DIR\InstallLog.txt .

도구 설명	위치
Cisco IPMA 클라이언트 AutoUpdater 추적 파일	Unified CM Assistant Console이 있는 곳과 동일한 위치인 클라이언트 데스크탑의 \$INSTALL_DIR\UpdatedLog.txt .
설치 디렉터리	기본적으로—C:\Program Files\Cisco\Unified Communications Manager Assistant Console\

전화하는 사용자에게 다시 걸기 신호음 가져오기

문제

발신자에게 다시 걸기 신호음이나 메시지가 들립니다.

이 통화는 전화를 걸 때 완료할 수 없습니다.

가능한 원인

발신 회선의 발신 검색 공간이 올바르게 구성되지 않았을 수 있습니다.

해결 방법

회선의 발신 검색 공간을 확인합니다. 구성에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 내용을 참조하십시오.

Cisco 다이얼 번호 분석기 서비스를 사용하여 발신 검색 공간에서 결함을 확인할 수도 있습니다. 자세한 내용은 *Cisco Unified Communications Manager Dialed Number Analyzer Guide*를 참조하십시오.

필터링이 설정 또는 해제되어 있으면 통화가 라우팅되지 않음

문제

통화가 제대로 라우팅되지 않음

가능한 원인 1

Cisco CTI 관리자 서비스가 중지되었을 수 있습니다.

해결 방법 1

Cisco 통합 서비스 가용성 > 도구 > 제어 센터—기능 서비스에서 Cisco CTI 매니저 및 Cisco IP 매니저 어시스턴트 서비스를 다시 시작합니다.

가능한 원인 2

Unified Communications Manager 보조자 라우트 포인트가 올바르게 구성되지 않았습니다.

해결 방법 2

Unified Communications Manager 보조자 CTI 라우트 포인트의 디렉터리 번호 및 Unified Communications Manager 보조자에 대해 구성된 모든 관리자의 기본 디렉터리 번호를 일치시키려면 와일드카드를 사용합니다.

가능한 원인 3

관리자 전화기의 상태 창에 메시지 필터링 꺼짐이 표시됩니다. 이 메시지는 Unified Communications Manager 보조자 CTI 라우트 포인트를 삭제했거나 서비스 중이 아닐 수 있음을 나타낼 수 있습니다.

해결 방법 3

다음 절차를 사용하여 CTI 라우트 포인트를 구성하고 Cisco IP 매니저 어시스턴트(Cisco IPMA) 서비스를 다시 시작합니다.

1. Cisco Unified CM 관리에서 디바이스 > **CTI** 라우트 포인트를 선택합니다.
2. 라우트 포인트를 찾거나 새 라우트 포인트를 추가합니다. 구성에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 내용을 참조하십시오.
3. **Cisco** 통합 서비스 가용성 > 도구 > 제어 센터—기능 서비스에서 Cisco CTI 매니저 및 Cisco IP 매니저 어시스턴트 서비스를 다시 시작합니다.

Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스에 연결할 수 없음

문제

Assistant Console을 열면 다음 메시지가 표시됩니다.

Cisco IPMA 서비스에 연결할 수 없음

가능한 원인 1

Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스가 중지되었을 수 있습니다.

해결 방법 1

Cisco 통합 서비스 가용성 > 도구 > 제어 센터—기능 서비스에서 Unified Communications Manager Assistant를 다시 시작합니다.

가능한 원인 2

기본 및 보조 Unified Communications Manager Assistant 서버의 서버 주소는 DNS 이름으로 구성될 수 있지만 DNS 이름은 DNS 서버에 구성되지 않습니다.

해결 방법 2

다음 절차를 사용하여 DNS 이름을 대체합니다.

1. Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서버.
2. 서버의 DNS 이름을 해당 IP 주소로 대체합니다.
3. Cisco 통합 서비스 가용성 > 도구 > 제어 센터—기능 서비스에서 Unified Communications Manager Assistant를 다시 시작합니다.

가능한 원인 3

Cisco CTI 매니저 서비스가 중지되었을 수 있습니다.

해결 방법 3

Cisco 통합 서비스 가용성 > 도구 > 제어 센터—기능 서비스에서 Unified Communications Manager Assistant를 다시 시작합니다.

가능한 원인 4

보안 모드에서 CTI 연결을 열도록 Unified Communications Manager Assistant 서비스를 구성할 수 있지만 보안 구성이 완료되지 않을 수 있습니다.

이 시나리오가 발생하는 경우 알람 뷰어나 Unified Communications Manager Assistant 서비스 로그에 다음 메시지가 표시됩니다.

IPMA 서비스를 초기화할 수 없음 - 공급자를 가져올 수 없음

해결 방법 4

Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스의 서비스 매개 변수에서 보안 구성을 확인합니다.

Cisco 통합 서비스 가용성 > 도구 > 제어 센터—기능 서비스에서 Unified Communications Manager Assistant를 다시 시작합니다.

Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스를 초기화할 수 없음

문제

Cisco IP 매니저 어시스턴트(Cisco IPMA) 서비스에서 CTI 관리자에 대한 연결을 열 수 없으며 다음 메시지가 표시됩니다.

IPMA 서비스를 초기화할 수 없음 - 공급자를 가져올 수 없음

가능한 원인

Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스에서 CTIManager에 대한 연결을 열 수 없습니다. 알람 뷰어 또는 Unified CM Assistant 서비스 로그에서 메시지를 볼 수 있습니다.

해결 방법

Cisco 통합 서비스 가용성 > 도구 > 제어 센터—기능 서비스에서 Cisco CTI 매니저 및 Cisco IP 매니저 어시스턴트 서비스를 다시 시작합니다.

웹에서 Assistant Console 설치 실패

문제

웹에서 Assistant Console 설치에 실패합니다. 다음과 같은 메시지가 표시됩니다.

예외: java.lang.ClassNotFoundException: InstallerApplet.class

가능한 원인

표준 Unified Communications Manager Assistant Console을 사용하여 Microsoft JVM 대신 Sun Java 플러그인 가상 머신을 사용하면 오류가 발생합니다.

해결 방법

관리자는 Sun Java 플러그인을 지원하는 JSP 페이지인 다음 URL로 사용자를 안내합니다.

`https://<servername>:8443/ma/Install/IPMAConsoleInstallJar.jsp`

HTTP 상태 503 —이 애플리케이션은 현재 사용할 수 없습니다.

문제

`http://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp`는 다음과 같은 오류 메시지를 표시합니다.

HTTP 상태 503 —이 애플리케이션은 현재 사용할 수 없습니다.

가능한 원인

Cisco IP 매니저 어시스턴트(Cisco IPMA) 서비스가 활성화되지 않았거나 실행되고 있지 않습니다.

해결 방법

Cisco 통합 서비스 가용성 > 도구 > 서비스 활성화에서 서비스의 활성화 상태를 확인하여 Cisco IP 매니저 어시스턴트(Cisco IPMA) 서비스가 활성화되었는지 확인합니다.

Cisco IP 매니저 어시스턴트(Cisco IPMA) 서비스가 이미 활성화된 경우 **Cisco** 통합 서비스 가용성 > 도구 > 제어 센터 - 기능 서비스에서 Unified Communications Manager 보조자를 다시 시작합니다.

서비스가 계속 실행되는 동안 관리자가 로그아웃됨

문제

관리자가 Unified Communications Manager Assistant에서 로그아웃되더라도 서비스는 계속 실행됩니다. 관리자 IP 전화기에 표시되는 표시가 사라집니다. 필터링이 켜져 있어도 통화는 라우팅되지 않습니다. 관리자가 로그아웃되었는지 확인하려면 Cisco Unified 실시간 모니터링 도구를 사용하여 애플리케이션 로그를 봅니다. Cisco IP 매니저 어시스턴트(Cisco IPMA) 서비스에서 로그아웃했음을 나타내는 Cisco Java 애플리케이션에서 경고를 확인합니다.

가능한 원인

관리자가 초당 4번 이상 소프트키를 눌렀습니다(최대 허용 한도).

해결 방법

Unified Communications Manager 관리자가 관리자 구성을 업데이트해야 합니다. 문제를 해결하려면 다음 절차를 수행합니다.

1. Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자 사용자 찾기 및 나열 창이 표시됩니다.
2. 검색 필드에 관리자 이름을 입력하고 찾기를 클릭합니다.
3. 검색 결과 목록에서 업데이트할 관리자를 선택합니다.
최종 사용자 구성 창이 표시됩니다.
4. 관련 링크 드롭다운 목록에서 **Cisco IPMA Manager**를 선택하고 이동을 클릭합니다.
5. 필요에 따라 관리자 구성을 변경하고 업데이트를 클릭합니다.

관리자가 보조 프록시 회선에서 벨이 울리는 통화를 가로챌 수 없음

문제

관리자가 보조 프록시 회선에서 벨이 울리는 통화를 가로챌 수 없습니다.

가능한 원인

프록시 회선의 발신 검색 공간이 올바르게 구성되지 않았습니다.

해결 방법

보조 전화기에 대한 프록시 회선의 발신 검색 공간을 확인합니다. 문제를 해결하려면 다음 절차를 수행합니다.

1. Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
전화기 찾기 및 나열 검색 창이 표시됩니다.

2. 보조 전화기를 클릭합니다.

전화기 구성 창이 표시됩니다.

3. 전화기에 대한 발신 검색 공간 구성 및 디렉터리 번호(회선)를 확인하고 적절하게 업데이트합니다.

페이지를 찾을 수 없음 오류

문제

`http://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp`는 다음과 같은 오류 메시지를 표시합니다.

페이지를 찾을 수 없음 오류

가능한 원인 1

네트워크 문제.

해결 방법 1

클라이언트가 서버에 연결되어 있는지 확인합니다. URL에 지정된 서버 이름에 대해 Ping을 수행하여 연결할 수 있는지 확인합니다.

가능한 원인 2

잘못된 URL.

해결 방법 2

URL은 대/소문자를 구분하므로 URL이 지침의 URL과 정확하게 일치하는지 확인합니다.

시스템 오류 - 시스템 관리자에게 문의하십시오.

문제

Assistant Console을 열면 다음 메시지가 표시됩니다.

시스템 오류 - 시스템 관리자에게 문의하십시오.

가능한 원인 1

Unified Communications Manager를 업그레이드했을 수 있습니다. Unified Communications Manager을(를) 업그레이드하면 시스템에서 Assistant Console이 자동으로 업그레이드되지 않습니다.

해결 방법 1

시작 > 프로그램 > Cisco Unified Communications Manager Assistant > Assistant Console 제거를 선택하여 콘솔을 제거하고

https://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp에서 콘솔을 다시 설치합니다.

가능한 원인 2

사용자가 데이터베이스에 올바르게 구성되지 않았습니다.

해결 방법 2

사용자 ID 및 암호가 Cisco Unified CM 관리를 통해 Unified Communications Manager 사용자로 실행되는지 확인합니다.

가능한 원인 3

보조자에서 관리자를 삭제한 경우 Cisco Unified CM 관리에 보조자에 대한 행이 비어 있습니다.

해결 방법 3

보조자 구성 창에서 프록시 회선을 재할당합니다.

Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스가 다운되면 관리자를 호출할 수 없습니다

문제

Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스가 다운되면 통화가 관리자에게 제대로 라우팅되지 않습니다.

가능한 원인

Unified Communications Manager 어시스턴트 CTI 라우트 포인트에는 응답 없음 착신 전환 기능이 활성화되어 있지 않습니다.

해결 방법

다음 절차를 수행하여 Unified Communications Manager 어시스턴트 라우트 포인트를 적절히 구성합니다.

1. Cisco Unified CM 관리에서 디바이스 > **CTI** 라우트 포인트를 선택합니다.

CTI 라우트 포인트 찾기 및 나열 검색 창이 표시됩니다.

2. 찾기를 클릭합니다.

구성된 CTI 라우트 포인트 목록이 표시됩니다.

3. 업데이트할 Unified Communications Manager 어시스턴트 CTI 라우트 포인트를 선택합니다.

4. **CTI** 라우트 포인트 구성 창의 연결 영역에서 업데이트할 회선을 클릭합니다.
5. 통화 착신 전환 및 당겨받기 설정 섹션에서 응답 없음 착신 전환 및 응답 없음 외부 착신 전환 확인란을 선택하고 통화권/대상 필드에 **CTI** 라우트 포인트 DN을 입력합니다(예: 라우트 포인트 DN 1xxx).
6. 발신 검색 공간 드롭다운 목록에서 **CSS-M-E**(또는 적절한 발신 검색 공간)를 선택합니다.
7. 업데이트를 클릭합니다.

사용자 인증 실패

문제

Assistant Console에서 로그인 창을 사용하여 로그인하면 사용자 인증이 실패합니다.

가능한 원인

다음과 같은 원인일 수 있습니다.

- 데이터베이스에서 사용자를 잘못 관리
- 사용자를 보조자 또는 관리자로 잘못 관리

해결 방법

사용자 ID 및 암호가 Cisco Unified CM 관리를 통해 Unified Communications Manager 사용자로 실행되는지 확인합니다.

사용자 관리 > 최종 사용자에서 Cisco Unified CM 관리를 통해 액세스하는 Unified Communications Manager 보조자 사용자 정보를 연결하여 보조자 또는 관리자로 사용자를 실행해야 합니다.



VII 부

음성 메시지 기능

- 음성 메시지 대기 중 표시기 , 223 페이지
- 지정전환 , 227 페이지



17 장

음성 메시지 대기 중 표시기

- 음성 메시지 대기 표시 개요, 223 페이지
- 음성 메시지 대기 표시 사전 요건, 223 페이지
- 음성 메시지 대기 표시 작업 흐름, 223 페이지
- 음성 메시지 대기 표시 문제 해결, 226 페이지

음성 메시지 대기 표시 개요

사용자에게 새 음성 메시지를 알리기 위해 Cisco Unified IP Phone에서 AMWI(음성 메시지 대기 중 표시기)를 구성하여 Stutter 신호음을 재생할 수 있습니다. 음성 메시지가 남겨진 회선에서 전화기가 오프 훅 될 때마다 Stutter 신호음이 들립니다.

클러스터의 모든 전화기 또는 특정 디렉터리 번호에 대해서만 AMWI를 구성할 수 있습니다. 디렉터리 번호 수준 구성이 클러스터 수준 구성보다 우선 적용됩니다.

음성 메시지 대기 표시 사전 요건

전화기 펌웨어 릴리스 8.3(1) 이상을 실행 중인 경우에만 Cisco Unified IP Phone에 AMWI를 구성할 수 있습니다.

음성 메시지 대기 표시 작업 흐름

시작하기 전에

- 음성 메시지 대기 표시 사전 요건, 223 페이지을(를) 검토합니다.

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	음성 메시지 대기 중 표시기 기능을 지원하는 디바이스를 식별하는 보고서를 생성합니다.
단계 2	음성 메시지 대기 표시 서비스 매개 변수 구성, 224 페이지	클러스터의 모든 전화기에 대해 AMWI 기본 설정을 구성합니다.
단계 3	디렉터리 번호에 대한 음성 메시지 대기 표시 구성, 224 페이지	디바이스에 연결된 디렉터리 번호에 대한 AMWI를 구성합니다.
단계 4	SIP 프로파일에 대한 음성 메시지 대기 표시기 구성, 225 페이지	SIP 프로파일에 대한 AMWI를 구성합니다. 이 절차를 수행하여 SIP 전화기에 대한 AMWI를 구성합니다.

음성 메시지 대기 표시 서비스 매개 변수 구성

이 절차에서는 클러스터의 모든 전화기에 대해 AMWI 기본 설정을 구성하는 방법에 대해 설명합니다.

시작하기 전에

전화기 기능 목록 생성, 7 페이지

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- 단계 4 클러스터 수준 매개 변수(기능 - 일반) 섹션에서 음성 메시지 대기 중 표시 정책 서비스 매개 변수를 선택합니다. 이 매개 변수는 클러스터의 모든 디바이스에 대해 음성 메시지 대기 표시기가 켜졌는지 여부를 결정합니다.
- 단계 5 저장을 클릭합니다.
-

디렉터리 번호에 대한 음성 메시지 대기 표시 구성

다음 단계에 따라 디바이스에 연결된 디렉터리 번호에 대해 AMWI를 구성합니다.



참고 개별 디렉터리 번호의 AMWI 설정은 클러스터 수준 설정을 무시합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 연결 섹션에서 새 **DN** 추가를 클릭합니다.
디렉터리 번호 구성 창이 나타납니다.
- 단계 3 음성 메시지 대기 중 표시기 정책을 선택합니다. 다음 옵션 중 하나를 선택합니다.
- 끄기
 - 켜기 - 이 옵션을 선택하면 핸드셋이 오프 훅일 때 셔터음이 발생합니다.
 - 기본값 - 이 옵션을 선택하면 전화기에서 시스템 수준에서 설정된 기본값을 사용합니다.
- 단계 4 디렉터리 번호 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 5 저장을 클릭합니다.

SIP 프로파일에 대한 음성 메시지 대기 표시기 구성

다음 단계에 따라 SIP 프로파일에 대한 AMWI(음성 메시지 대기 중 표시기)를 구성합니다.



참고 개별 SIP 프로파일의 AMWI 설정은 클러스터 수준 설정을 무시합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > **SIP** 프로파일.
SIP 프로파일 찾기 및 나열 창이 표시됩니다.
- 단계 2 사용할 검색 조건을 입력하고 찾기를 클릭합니다.
창에 검색 조건과 일치하는 **SIP** 프로파일 목록이 표시됩니다.
- 단계 3 업데이트할 **SIP** 프로파일을 클릭합니다.
SIP 프로파일 구성 창이 나타납니다.
- 단계 4 전화기가 오프 훅 상태이고 메시지가 대기 중일 때 **Stutter** 발신음을 활성화하려면 **Stutter** 메시지 대기 중 확인란을 선택합니다.
- 단계 5 저장을 클릭합니다.
- 단계 6 구성 적용을 클릭합니다.

음성 메시지 대기 표시 문제 해결

음성 메시지 대기 표시가 전화기에서 들리지 않음

문제 전화기에서 새 음성 메시지를 사용자에게 알리기 위해 스테터 신호음을 재생하지 않습니다.

사용자가 SCCP 전화기를 사용하는 경우 다음을 확인하십시오.

- 전화기 펌웨어 릴리스가 8.3(1) 이상인지 확인하십시오.
- 사용자가 오프 hook 상태에 있는 전화기 및 회선에 대한 AMWI 설정을 확인합니다.
- Cisco CallManager 서비스가 서버에서 실행 중인지 확인합니다.
- 전화기와 Unified Communications Manager의 스니퍼 추적을 확인합니다. 전화기에서 신호음 유형이 42인 StartTone 메시지를 수신하는지 확인합니다.

사용자가 SIP 전화기를 사용하는 경우 다음을 확인합니다.

- 전화기 펌웨어 릴리스가 8.3(1) 이상인지 확인하십시오.
- 회선(디렉터리 번호) 구성을 확인합니다. 전화기에 line1_msgWaitingAMWI : 1, line2_msgWaitingAMWI : 0 같은 설정이 표시되어야 합니다.
- Cisco Unified CM 관리의 **SIP** 프로파일 구성 창에서 **Stutter** 메시지 대기 확인란을 선택해야 합니다.

지역화된 **AMWI** 신호음이 특정 로캘에서 재생되지 않음

문제 영어가 아닌 로캘에서 구성된 전화기는 지역화된 신호음을 재생하지 않습니다.

해결 방법 다음 사항을 확인하십시오.

- Cisco Unified CM 관리에서 디바이스 프로파일 구성 창(디바이스 > 디바이스 설정 > 디바이스 프로파일)의 사용자 로케일을 확인합니다.
- 로캘을 변경한 후 사용자가 전화기를 재설정했는지 확인합니다.
- user/local/cm/tftp /<locale name> directory를 확인하고 AMWI 신호음이 지역화된 g3-tones.xml 파일에 정의되었는지 확인합니다.



18 장

지정 전환

- 즉시 전환 개요, 227 페이지
- 즉시 전환 사전 요건, 228 페이지
- 즉시 전환 구성 작업 흐름, 228 페이지
- 즉시 전환 상호 작용, 233 페이지
- 즉시 전환 제한 사항, 235 페이지
- 즉시 전환 문제 해결, 236 페이지

즉시 전환 개요

즉시 전환 기능은 통화를 음성 메일 시스템으로 즉시 전환할 수 있는 Unified Communications Manager 보조 서비스입니다. 즉시 전환으로 통화가 전환되면 해당 회선에서 새 통화를 걸거나 받을 수 있습니다. IP 전화기의 즉시 전환 또는 전환 소프트웨어를 사용하여 즉시 전환 기능에 액세스합니다.

즉시 전환은 다음 기능을 제공합니다.

- 다음과 같은 방법으로 음성 메일 시스템으로 통화를 전환합니다.
 - 레거시 즉시 전환은 즉시 전환 기능을 호출하는 당사자의 음성 사서함으로 통화를 전환합니다.
 - 고급 즉시 전환은 전환 기능을 호출하는 상대방의 음성 메일박스 또는 원래 착신자의 음성 메일박스로 통화를 전환합니다.
- 통화 제공, 통화 보류 또는 통화 활성 상태에 있는 인바운드 통화를 전환합니다.
- 통화 활성 또는 통화 보류 상태에 있는 아웃바운드 통화를 전환합니다.



참고 즉시 전환 기능은 CTI 애플리케이션에서 사용할 수 없지만 즉시 전환과 동일한 기능을 수행하는 CTI 재전송 작업이 있습니다. 따라서 애플리케이션 개발자는 CTI 재전송 작업을 사용하여 즉시 전환을 수행할 수 있습니다.

즉시 전환 사전 요건

- 음성 메일 프로필 및 헌트 파일럿을 구성해야 합니다.

음성 메일 프로필 및 헌트 파일럿을 구성하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

[Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)

- 다음 디바이스는 즉시 전환을 지원합니다.

- SCCP (Skinny Client Control Protocol)를 사용하는 Cisco Unity Connection 등의 음성 메시징 시스템
- 레거시 음성전환사용(Use Legacy Immediate Divert) 및 전환 중 QSIG 허용(Allow QSIG During iDivert) 클러스터 수준 서비스 매개 변수의 설정에 따라, QSIG 디바이스(QSIG 사용 H-323 디바이스, MGCP PRI QSIG T1 게이트웨이, MGCP PRI QSIG E1 게이트웨이).
- 다음 표에는 전환(Divert 또는 iDivert) 소프트웨어를 사용하는 전화기가 표시되어 있습니다.

표 21: 즉시 전환 소프트웨어를 사용하는 **Cisco Unified IP Phone**

Cisco Unified IP Phone 모델	전환(Divert) 소프트웨어	전환(iDivert) 소프트웨어	소프트웨어 템플릿에서 구성하는 항목
Cisco Unified IP Phone 6900 Series(6901 및 6911 제외)	X		전환
Cisco Unified IP Phone 7900 시리즈		X	전환
Cisco Unified IP Phone 8900 시리즈	X		기본값으로 구성됨
Cisco Unified IP Phone 9900 시리즈	X		기본값으로 구성됨



참고 Cisco Unified IP Phone 8900 및 9900 시리즈에서는 [전환] 소프트웨어가 기본적으로 할당되어 있습니다.

즉시 전환 구성 작업 흐름

시작하기 전에

- [즉시 전환 사전 요건](#), 228 페이지를(를) 검토합니다.

프로시저

	명령 또는 동작	목적
단계 1	즉시 전환 서비스 매개 변수 구성, 229 페이지	다양한 디바이스 및 애플리케이션에 대해 전환을 활성화하도록 서비스 매개 변수를 구성합니다.
단계 2	즉시 전환에 대한 소프트키 템플릿 구성, 230 페이지	소프트키 템플릿을 만들고 구성하고 즉시 전환 소프트키를 해당 템플릿에 추가합니다.
단계 3	<p>소프트키 템플릿을 일반 디바이스 구성에 연결, 231 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> • 소프트키 템플릿을 일반 디바이스 구성에 추가, 232 페이지 • 일반 디바이스 구성을 전화기에 연결, 233 페이지 	<p>선택 사항. 전화기에서 소프트키 템플릿을 사용할 수 있게 하려면 이 단계 또는 다음 단계를 완료해야 합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용 하는 경우 이 단계를 수행합니다.</p> <p>이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.</p>
단계 4	소프트키 템플릿을 전화기에 연결, 233 페이지	선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하거나 일반 디바이스 구성과 함께 연결하는 대신 사용할 수 있습니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우 일반 디바이스 구성과 함께 이 절차를 사용합니다.

즉시 전환 서비스 매개 변수 구성

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- 단계 4 관련 서비스 매개 변수를 구성하고 저장을 클릭합니다.

표 22: 즉시 전환을 위한 서비스 매개 변수 필드

필드	설명
통화 대기 표시 타이머	IP 전화기의 즉시 전환 텍스트 표시에 대한 타이머를 제어하려면 0~100(포함) 사이의 숫자를 입력합니다. Cisco CallManager 서비스 및 즉시 전환이 구성된 서버 또는 클러스터 내 각 서버에 이 타이머를 설정합니다. 이 서비스 매개 변수의 기본값은 10초입니다.

필드	설명
레거시 즉시 전환 사용	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • True—즉시 전환 기능을 호출하는 사용자가 수신 통화를 자신의 음성 사서함으로만 전환할 수 있습니다. 이 값이 기본 설정입니다. • False—즉시 전환 기능을 호출하는 사용자의 음성 사서함 또는 원래 호출된 당사자의 음성 사서함으로 수신 통화를 전환할 수 있습니다.
즉시 전환 중 QSIG 허용	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • True — 즉시 전환은 QSIG, SIP 및 QSIG 지원 H.323 디바이스를 통해 연결할 수 있는 음성 메일 시스템으로 통화를 전환합니다. • False—즉시 전환은 QSIG 또는 SIP 트렁크를 통한 음성 메일 시스템에 대한 액세스를 지원하지 않습니다. 이 값이 기본 설정입니다.
즉시 전환 사용자 응답 타이머	<p>5~30(포함) 사이의 숫자를 입력하여 즉시 전환 소프트키 사용자가 통화를 전환하는 상대방을 선택하는 데 걸리는 시간을 결정합니다. 사용자가 상대방을 선택하지 않으면 통화가 연결된 상태로 유지됩니다. 이 서비스 매개 변수의 기본값은 5초입니다.</p>

즉시 전환에 대한 소프트키 템플릿 구성

수신 통화 또는 발신 통화를 전환하려면 소프트키 템플릿을 구성하고 즉시 전환 소프트키를 해당 템플릿에 할당합니다. 다음과 같은 통화 상태에서 [전환] 소프트키를 구성할 수 있습니다.

- 연결됨
- 보류 중
- 링인

즉시 전환은 다음 통화 상태를 지원합니다.

- 수신 통화의 경우:
 - 통화 제공(소프트키 템플릿에서 벨소리로 표시됨)
 - 통화 보류
 - 통화 활성화
- 발신 통화의 경우:
 - 통화 보류
 - 통화 활성화

프로시저

- 단계 1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2** 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- a) 새로 추가를 클릭합니다.
 - b) 기본 템플릿을 선택하고 복사를 클릭합니다.
 - c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - d) 저장을 클릭합니다.
- 단계 3** 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
- a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 필요한 기존 템플릿을 선택합니다.
- 단계 4** 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.
- 참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.
- 단계 5** 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
- 단계 6** 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.
- 단계 7** 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.
- 단계 8** 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.
- 단계 9** 저장을 클릭합니다.
- 단계 10** 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

소프트키 템플릿을 일반 디바이스 구성에 연결

(선택 사항) 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 다음 내용을 참조하십시오. [소프트키 템플릿을 전화기에 연결, 233 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	소프트키 템플릿을 일반 디바이스 구성에 추가, 232 페이지	
단계 2	일반 디바이스 구성을 전화기에 연결, 233 페이지	

소프트키 템플릿을 일반 디바이스 구성에 추가

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성

단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성 하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.

- a) 새로 추가를 클릭합니다.
- b) 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
- c) 저장을 클릭합니다.

단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.

- a) 찾기를 클릭하고 검색 기준을 입력합니다.
- b) 기존 일반 디바이스 구성을 클릭합니다.

단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

단계 6 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

일반 디바이스 구성을 전화기에 연결

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정을 클릭하여 전화기 설정을 업데이트합니다.

소프트키 템플릿을 전화기에 연결

선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성과 연결할 수 있습니다. 이 절차는 일반 디바이스 구성과 함께 작동합니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우에 사용할 수 있습니다.

시작하기 전에

[즉시 전환에 대한 소프트키 템플릿 구성, 230 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.
- 단계 4 저장을 클릭합니다.

즉시 전환 상호 작용

기능	상호 작용
MLPP(Multilevel Precedence and Preemption)	즉시 전환에서는 통화 유형(예: 우선 순위 통화)에 관계 없이 통화를 음성 메시징 사서함으로 전환합니다. 대체 상대 전환(통화 우선 순위)이 활성화된 경우 CFNA(응답 없음 착신 전환)가 비활성화됩니다.

기능	상호 작용
통화 착신 전환	<p>디렉터리 번호 구성 창에 응답 없음 착신 전환 설정이 구성되지 않은 경우 착신 전환은 클러스터 전체의 CFNA 타이머 서비스 매개 변수인 응답 없음 착신 전환 타이머를 사용합니다.</p> <p>통화가 착신 전환됨과 동시에 사용자가 [전환] 소프트키를 누르면 (타이머가 너무 짧았기 때문에) 통화가 음성 사서함으로 전환되지 않고 할당된 착신 전환 디렉터리 번호로 전환됩니다. 이 상황을 해결하려면 CFNA 타이머 서비스 매개 변수에 충분한 시간을 설정하십시오(예: 60초).</p>
CDR(통화 세부 정보 레코드)	즉시 전환에서는 CDR에 있는 Onbehalf 필드(예: joinOnbehalfOf 및 lastRedirectRediectOnBehalfOf)의 즉시 전환 코드 번호를 사용합니다.
통화 지정보류 및 통화 전환 보류	사용자 A가 사용자 B에게 전화를 걸고 사용자 B가 통화를 보류하면 즉시 전환 또는 전환 소프트키를 눌러 통화를 음성 메시징 사서함으로 보낼지 결정합니다. 사용자 A가 사용자 B의 음성 메시징 사서함 인사말을 받습니다.
전화회의	전화회의 참가자가 [전환] 소프트키를 누르면 남은 전화회의 참가자가 음성전환을 시작한 사용자의 음성 메시징 사서함 인사말을 수신합니다. 전화회의 유형은 임시, Meet-Me, 참여, 회의끼기, 통화참가가 있습니다.
헌트 목록	<p>헌트 목록 파일럿을 통해(헌팅 알고리즘의 일부로서) 전화기로 직접 착신되는 통화의 경우, 클러스터 수준 서비스 매개 변수인 레거시 즉시 전환 사용이 True로 설정된 경우 즉시 전환 소프트키가 흐리게 표시됩니다. 그렇지 않으면 흐리게 표시되지 않습니다.</p> <p>헌트 목록 파일럿을 통해(헌팅 알고리즘의 일부로서) 전화기로 직접 착신되지 않는 통화의 경우, 클러스터 수준 서비스 매개 변수인 레거시 즉시 전환 사용이 True 또는 False로 설정된 경우 즉시 전환 소프트키가 흐리게 표시되지 않습니다.</p> <p>참고 사무실 전화기 모드의 Jabber의 경우, 즉시 전환 기능 리디렉션은 '레거시 즉시 전환 사용' 매개 변수를 적용하지 않으며 HP 번호가 음성 메일 서버에 전환 정보로 전송됩니다.</p>
자동 통화 당겨받기	레거시 즉시 전환 사용 클러스터 수준 서비스 매개 변수가 False로 설정되고, 자동 통화 당겨받기 활성화 클러스터 수준 서비스 매개 변수가 True로 설정된 상태에서 통화 당겨받기 그룹의 사용자가 통화 당겨받기를 사용하여 전화를 받으면 사용자가 즉시 전환 소프트키를 눌러도 IP 전화기에 어떠한 옵션도 제공되지 않습니다.

즉시 전환 제한 사항

제한 사항	설명
음성 메일 프로필	음성 메시징 시스템과 QSIG 통합을 사용하는 경우, 음성 메일 파일럿 또는 음성 메일 마스크 또는 둘 다 포함한 음성 메일 프로필에 대해서는 이 프로파일을 시스템의 기본 음성 메일 프로필로 설정 확인란을 선택 해제한 상태로 두어야 합니다. 기본 음성 메일 프로필 설정이 항상 [음성 메일 없음]으로 설정되어 있는지 확인하십시오.
모두 착신 전환(CFA) 및 통화 시 착신 전환(CFB)	CFA(모든 통화 착신 전환)와 CFB(통화 중 착신 전환)가 활성화된 경우, 시스템은 음성전환을 지원하지 않습니다(CFA와 CFB가 음성전환보다 우선).
음성 메일 시스템	<p>즉시 전환은 로컬 또는 SCCP 연결을 통해 즉시 전환이 음성 메일 시스템에 도달하는 경우 음성 메일 포트에서 통화 중 상태를 감지합니다.</p> <p>참고 즉시 전환은 통화 중인 음성 메일 포트에 통화를 전환할 수 없습니다. 음성 메일 포트는 경로 또는 헌트 목록의 구성원으로 존재할 수 있습니다.</p> <p>이 통화는 통화 중 음성 메일 시스템으로 전환될 수 없지만, 원래 통화는 유지됩니다. 통화가 전환되지 않았음을 나타내기 위해 즉시 전환을 호출한 전화기에 “통화 중” 메시지가 표시됩니다.</p> <p>QSIG 또는 SIP 트렁크를 통해 음성 메일 시스템에 도달할 경우, 전환이 감지될 수 있지만 통화는 유지되지 않습니다. 전환 중 QSIG 허용 클러스터 수준 서비스 매개 변수가 True로 설정되었거나 레거시 음성전환 사용 클러스터 수준 서비스 매개 변수가 False로 설정되었으면, 음성전환이 QSIG 또는 SIP 트렁크를 통해 도달할 수 있는 음성 메일 시스템에 대한 액세스를 지원합니다. 즉시 전환 중 QSIG 허용 클러스터 수준 서비스 매개 변수가 False로 설정되었고 레거시 즉시 전환 사용 클러스터 수준 서비스 매개 변수가 True로 설정되었으면, 즉시 전환이 QSIG 또는 SIP 트렁크를 통한 음성 메일 시스템에 대한 액세스를 지원하지 않습니다.</p>
악성 전화 통화자 ID	시스템은 악성 전화 ID 및 음성전환 기능을 함께 사용하는 것을 지원하지 않습니다.
부재중 착신 전환 시간 초과	즉시 전환 소프트웨어를 누를 때 부재중 착신 전환 시간 초과와 관련된 일반적이지 않은 조건이 존재합니다. 예를 들어, 관리자가 응답 없음 착신 전환 시간 초과 후 즉시 [전환] 소프트웨어를 누를 경우, 통화 착신 전환이 해당 통화를 사전 구성된 디렉터리 번호로 착신 전환합니다. 그러나, 관리자가 응답 없음 착신 전환 시간 초과 전에 [전환] 소프트웨어를 누를 경우, 음성전환이 해당 통화를 관리자의 음성 메시징 사서함으로 전환합니다.

제한 사항	설명
발신자 및 착신자	발신자와 착신자가 동시에 즉시 전환 소프트웨어를 누를 경우, 쌍방의 음성 사서함으로 통화를 전환할 수 있습니다.
전화회의 유형	전화회의에서 한 참가자가 [전환] 소프트웨어를 누르면, 모든 나머지 참가자들이 전환을 누른 참가자의 발신 인사말을 받게 됩니다. 전화회의 유형에는 회의개설, 임시, 회의끼기, 통화참가가 있습니다.
분할 또는 참가 작업	통화에서의 마지막 작업이 자동 당겨받기, 호전환, 통화 지정보류, 통화 지정보류 복귀, 전화회의, 회의개설 전화회의, 또는 분할 또는 참가 작업을 수행하는 애플리케이션일 경우, 고급 전환이 착신자에게 음성 사서함을 선택할 수 있는 화면을 제공하지 않습니다. 대신에, 고급 전환은 착신자와 연결된 음성 사서함으로 해당 통화를 즉시 전환합니다.

즉시 전환 문제 해결

키가 활성화 상태가 아님

사용자가 음성 전환을 누르면 전화기에 이 메시지가 표시됩니다.

키가 활성화 상태가 아님

전환을 누른 사용자의 음성 메시징 프로파일에 음성 메시징 파일럿이 없습니다.

사용자 음성 메시징 프로파일에 음성 메시징 파일럿을 구성합니다.

일시적 실패

사용자가 음성 전환을 누르면 전화기에 이 메시지가 표시됩니다.

일시적 실패

음성 메시징 시스템이 작동하지 않거나 네트워크 문제가 있습니다.

음성 메시징 시스템 문제를 해결합니다. 문제 해결 또는 음성 메시징 설명서를 참조하십시오.

통화 중

사용자가 음성 전환을 누르면 전화기에 이 메시지가 표시됩니다.

통화 중

이 메시지는 음성 메시징 시스템이 통화 중임을 의미합니다.

음성 메시징 포트를 더 구성하거나 다시 시도하십시오.

통화 중



VIII 부

전화회의 기능

- 애드-혹 컨퍼런스 , 241 페이지
- 회의개설 컨퍼런싱 , 255 페이지
- Conference Now , 263 페이지



19 장

애드-혹 컨퍼런스

- 애드-혹 컨퍼런스 개요, 241 페이지
- 애드-혹 컨퍼런스 작업 흐름, 241 페이지
- 전화회의 상호 작용, 250 페이지
- 전화회의 제한 사항, 250 페이지

애드-혹 컨퍼런스 개요

애드-혹 컨퍼런스를 사용하면 전화회의의 컨트롤러 (또는 일부 경우에는 다른 참가자)가 전화회의에 참가자를 추가할 수 있습니다.

애드-혹 컨퍼런스는 기본 및 고급의 두 가지 유형으로 구성됩니다. 기본 애드-혹 컨퍼런스에서 전화회의의 주관자는 전화회의의 컨트롤러 역할을 하고 다른 참가자를 추가하거나 제거할 수 있는 유일한 참가자입니다. 고급 전화회의에서는 참가자가 다른 참가자를 추가하거나 제거할 수 있습니다. 고급 애드-혹 컨퍼런스를 사용하면 여러 개의 애드-혹 컨퍼런스를 함께 연결할 수 있습니다.

고급 애드-혹 컨퍼런스를 사용하면 개별 참가자인 것처럼 한 애드-혹 컨퍼런스를 다른 애드-혹 컨퍼런스에 추가하여 여러 애드-혹 컨퍼런스를 함께 연결할 수 있습니다. 고급 애드-혹 컨퍼런스 활성화 서비스 매개 변수가 False로 설정된 경우 여러 전화회의를 함께 연결하려고 하면 IP 전화기에 메시지가 표시됩니다. 개별 참가자를 애드-혹 컨퍼런스에 추가하여 애드-혹 컨퍼런스에 또 다른 전화회의를 추가하는 방법을 사용할 수도 있습니다.

애드-혹 컨퍼런스 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	전화회의용 소프트키 템플릿 구성, 242 페이지	전화회의의 목록, 참가 및 마지막 전화회의의 대상 제거 소프트키를 소프트키 템플릿에 추가합니다.

	명령 또는 동작	목적
단계 2	<p>소프트키 템플릿 일반 디바이스 연결, 244 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> • 소프트키 템플릿을 일반 디바이스 구성에 추가, 244 페이지 • 일반 디바이스 구성을 전화기에 연결, 245 페이지 	선택 사항. 전화기에서 소프트키 템플릿을 사용할 수 있게 하려면 이 단계 또는 다음 단계를 완료해야 합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 이 단계를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.
단계 3	소프트키 템플릿을 전화기에 연결, 245 페이지	선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하거나 일반 디바이스 구성과 함께 연결하는 대신 사용할 수 있습니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우 일반 디바이스 구성과 함께 이 절차를 사용합니다.
단계 4	애드-혹 컨퍼런스 구성, 245 페이지	고급 전화회의를 활성화하고 참가자의 최대 수를 지정하고 전화회의의 연결을 삭제할 시기를 지정합니다.
단계 5	회선 간 조인 구성, 249 페이지	회선 간 통화 참가를 활성화하여 전화회의를 만듭니다.

전화회의용 소프트키 템플릿 구성

이 절차를 사용하여 다음과 같은 전화 회의 소프트키를 사용할 수 있습니다.

소프트키	설명	통화 상태
전화회의 목록(ConfList)	애드-혹 컨퍼런스에 있는 참가자 디렉터리 번호 목록을 봅니다. Cisco Unified Communications Manager 관리에 구성되어 있는 경우 참가자의 이름이 표시됩니다.	온 혹은 연결됨
참가	전화 회의를 만들려면 최대 15개의 설정된 통화(총 16개)에 참가합니다.	보류
마지막 전화회의의 참가자 제거(제거)	전화 회의 컨트롤러는 전화 회의 목록을 호출할 수 있으며, 제거 소프트키를 사용하여 전화 회의에서 참가자를 제거할 수 있습니다.	온 혹은 연결됨

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- a) 새로 추가를 클릭합니다.
 - b) 기본 템플릿을 선택하고 복사를 클릭합니다.
 - c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - d) 저장을 클릭합니다.
- 단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
- a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 필요한 기존 템플릿을 선택합니다.
- 단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.
- 참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.
- 단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
- 단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.
- 단계 7 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.
- 단계 8 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.
- 단계 9 저장을 클릭합니다.
- 단계 10 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

다음에 수행할 작업

다음 절차 중 하나를 완료합니다.

- [소프트키 템플릿 일반 디바이스 연결, 244 페이지](#)
- [소프트키 템플릿을 전화기에 연결, 245 페이지](#)

소프트키 템플릿 일반 디바이스 연결

선택 사항. 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 [소프트키 템플릿을 전화기에 연결, 245 페이지](#)(으)로 이동하십시오.

시작하기 전에

[전화회의용 소프트키 템플릿 구성, 242 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	소프트키 템플릿을 일반 디바이스 구성에 추가, 244 페이지	이 단계를 수행하여 전화회의 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.
단계 2	일반 디바이스 구성을 전화기에 연결, 245 페이지	이 단계를 수행하여 전화회의 소프트키 일반 디바이스 구성을 전화기에 연결합니다.

소프트키 템플릿을 일반 디바이스 구성에 추가

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성

단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성 하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.

- 새로 추가를 클릭합니다.
- 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
- 저장을 클릭합니다.

단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.

- 찾기를 클릭하고 검색 기준을 입력합니다.
- 기존 일반 디바이스 구성을 클릭합니다.

단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

단계 6 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

일반 디바이스 구성을 전화기에 연결

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.

단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 재설정 을 클릭하여 전화기 설정을 업데이트합니다.

소프트키 템플릿을 전화기에 연결

선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성과 연결할 수 있습니다. 이 절차는 일반 디바이스 구성과 함께 작동합니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우에 사용할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하고 전화기를 선택하여 소프트키 템플릿을 추가합니다.

단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 재설정을 눌러 전화기 설정을 업데이트합니다.

애드-hoc 컨퍼런스 구성

비 컨트롤러 참가자가 다른 참가자를 추가 및 제거하는 기능과 모든 참가자가 애드-hoc 컨퍼런스를 함께 연결할 수 있는 고급 애드-hoc 컨퍼런스를 구성합니다.

프로시저

-
- 단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 **2** 서버 드롭다운 목록에서 서버를 선택합니다.
- 단계 **3** 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- 단계 **4** 클러스터 수준 매개 변수(기능 - 전화회의) 영역에서 필드를 구성합니다. 매개 변수 설명은 [애드-혹 컨퍼런스 서비스 매개 변수, 246 페이지](#)의 내용을 참조하십시오.
- 단계 **5** 저장을 클릭합니다.
-

다음에 수행할 작업

[회선 간 조인 구성, 249 페이지](#)

애드-혹 컨퍼런스 서비스 매개 변수

다음 표에는 애드-혹 컨퍼런스에 대한 기본 서비스 매개 변수가 나열되어 있습니다. 추가 전화회의 서비스 매개 변수에 대한 자세한 내용은 서비스 매개 변수 구성 창의 고급 옵션을 참조하십시오. 전화회의의 서비스 매개 변수는 클러스터 수준 매개 변수(기능 - 전화 회의) 아래에 표시됩니다.

표 23: 애드-hoc 컨퍼런스 서비스 매개 변수

서비스 매개 변수	설명
애드-hoc 컨퍼런스 끊기	<p>애드-hoc 컨퍼런스를 끊으면 요금 사기(외부 발신자가 연결된 상태로 유지되는 동안 내부 전화 회의 컨트롤러가 전화 회의에서 연결을 끊는 경우)를 방지할 수 있습니다. 서비스 매개 변수 설정은 애드-hoc 컨퍼런스가 끊어질 때의 조건을 지정합니다.</p> <ul style="list-style-type: none"> • 없음 - 회의가 끊어지지 않습니다. (실수로 전화회의가 종료되지 않도록 하려면 기본 옵션을 사용하는 것이 좋습니다.) • 온 넷 상대방이 전화회의에 남아 있는 경우 - 시스템에서 전화회의에 참가한 마지막 네트워크 상대방이 전화를 끊거나 전화회의를 끊을 때 활성 전화 회의를 끊습니다. Unified Communications Manager는 전화 회의에 할당된 모든 리소스를 해제합니다. <p>참고 학습한 라우트 패턴이 온 넷으로 분류되므로 온넷 상대방이 회의에 남아있지 않는 경우로 설정되면 ILS 구축에서 애드-hoc 컨퍼런스 기능이 상대방과의 연결을 끊지 않습니다.</p> <ul style="list-style-type: none"> • 전화 회의 컨트롤러가 떠날 때 - 기본 컨트롤러(컨퍼런스 생성자)가 전화를 끊으면 활성 전화회의가 종료됩니다. Unified Communications Manager가 전화 회의에 할당된 모든 리소스를 해제합니다. <p>참고 이 서비스 매개 변수를 없음으로 설정하는 것이 좋습니다. 다른 설정은 실수로 전화회의가 종료되는 결과를 초래할 수 있습니다.</p> <p>애드-hoc 컨퍼런스 끊기 매개 변수는 SIP를 실행하는 Cisco Unified IP Phone 7940 또는 7960 또는 SIP를 실행하는 타사 전화기에서 시작된 전화회의 통화에 대해 다르게 작동합니다.</p>
Maximum Ad Hoc Conference	<p>이 매개 변수는 단일 애드-hoc 컨퍼런스에서 허용되는 최대 참가자 수를 지정합니다.</p> <p>기본값: 4</p>
고급 애드-hoc 컨퍼런스 활성화됨	<p>이 매개 변수는 고급 애드-hoc 컨퍼런스 기능이 활성화되는지 여부를 결정합니다. 여기에는 비 컨트롤러 참가자가 다른 참가자를 추가 및 제거하는 기능과 모든 참가자가 애드-hoc 컨퍼런스를 함께 연결할 수 있는 기능을 포함합니다.</p>
비선형 애드-hoc 컨퍼런스 연결 활성화됨	<p>이 매개 변수는 두 개 이상의 애드-hoc 컨퍼런스를 비선형 방식(세 개 이상의 전화 회의가 한 전화회의에 연결됨)으로 애드-hoc 컨퍼런스에 직접 연결할 수 있는지 여부를 결정합니다.</p>

서비스 매개 변수	설명
화상 회의 대신 암호화된 음성 회의 선택	이 매개 변수는 Unified Communications Manager가 전화회의 컨트롤러의 디바이스 보안 모드가 인증됨 또는 암호화됨으로 설정되어 있고 두 명 이상의 전화회의 참가자가 비디오를 사용할 수 있는 경우 애드-혹 컨퍼런스 브리지에 대한 암호화된 음성 회의 브리지 또는 암호화되지 않은 화상 회의 브리지를 선택할지 여부를 결정합니다. 암호화된 화상 회의 브리지는 이 릴리스에서 지원되지 않으므로 Unified Communications Manager는 암호화된 음성 회의 브리지와 암호화되지 않은 화상 회의 브리지 중 하나를 선택해야 합니다. 기본값은 True 입니다.
음성 회의를 할당하는데 사용할 수 있는 최소 비디오 지원 참가자	이 매개 변수는 애드-혹 컨퍼런스에서 화상 회의 브리지를 할당하기 위해 제공해야 하는 비디오 지원 전화회의 참가자 수를 지정합니다. 비디오 지원 참가자 수가 이 매개 변수에 지정된 숫자보다 작으면 Unified Communications Manager는 음성 회의 브리지를 할당합니다. 비디오 지원 참가자 수가 이 매개 변수에 지정된 숫자보다 크거나 같으면 Unified Communications Manager구성된 MRGL(미디어 리소스 그룹 목록)에서 화상 회의 브리지를 할당합니다. 값 0을 지정하면 전화회의에 참가한 참가자가 비디오를 사용할 수 없는 경우에도 음성 회의 브리지가 항상 할당됩니다. 음성 브리지를 사용하여 전화회의를 설정한 후 추가 비디오 지원 참가자가 전화회의에 참가하면 전화회의가 음성 브리지에 유지되고 비디오로 변환되지 않습니다. 기본값은 2 입니다.
화상 회의 브리지의 우선 순위가 더 높은 경우 음성 전용 회의에 화상 회의 브리지 할당	이 매개 변수는 화상 회의 브리지가 MRGL(미디어 리소스 그룹 목록)의 음성 회의 브리지보다 높은 우선 순위를 가지는 경우 임시 음성 전용 회의를 위해 사용 가능한 경우 Unified Communications Manager가 화상 회의 브리지를 선택할지 여부를 결정합니다. 음성 회의 브리지가 MRGL의 화상 회의 브리지보다 우선 순위가 높은 경우에는 Unified Communications Manager가 이 매개 변수를 무시합니다. 이 매개 변수는 로컬 전화회의 브리지가 비디오 브리지이고 우선 순위가 가장 높은 MRGL에 구성되고 오디오 전화회의 브리지는 원격 위치에서만 사용할 수 있는 상황에서 유용합니다. 이 경우 이 매개 변수를 활성화하면 Unified Communications Manager가 음성 전용 전화회의 통화에 대해서도 로컬 화상 회의 브리지를 먼저 사용하려고 시도하는 것을 의미합니다. 기본값은 false 입니다.
타사 애플리케이션에 대한 클릭하여 전화 회의 활성화	이 매개 변수는 Unified Communications Manager에서 SIP 트렁크를 통한 클릭하여 전화 회의 기능을 활성화할지 여부를 결정합니다. 클릭하여 전화회의 기능을 사용하면 타사 애플리케이션에서 대화 상자 REFER 방법을 사용하여 전화 회의를 설정하고 SIP SUBSCRIBE/NOTIFY를 통해 전화회의 이벤트 패키지에 대한 SIP 트렁크를 구독할 수 있습니다. 경고! 이 매개 변수를 활성화하면 이 기능을 지원하도록 코딩되지 않은 CTI 애플리케이션에 부정적인 영향을 줄 수 있습니다. 기본값: 거짓

서비스 매개 변수	설명
클러스터 전화회의 접두사 식별자	이 매개 변수는 최대 8자리(예: 0001)의 숫자를 정의하며, 이는 Cisco Telepresence MCU 또는 Cisco Telepresence Conductor와 같은 SIP 컨퍼런스 브리지에서 호스트되는 임시 및 미팅 시작 전화회의에 대해 생성된 전화회의 식별자에 붙는 접두사입니다. Unified Communications Manager에서 관리하는 SIP 컨퍼런스 브리지를 공유하는 네트워크에 여러 클러스터가 있는 경우 관리자가 이 필드를 채워야 합니다. 모든 클러스터는 특별한 접두사를 사용하여 구성해야 임시 및 미팅 시작 전화회의를 위한 전화회의 ID가 고유합니다. 클러스터 간에 전화회의 리소스가 공유되고 있지 않은 경우 이 필드가 채워지지 않을 수 있습니다.

회선 간 조인 구성

사용자는 회선 간 통화 참가 기능을 사용하여 다중 전화 회선(다른 디렉터리 번호 또는 동일한 디렉터리 번호이지만 다른 파티션)의 통화에 참가하여 전화회의를 만들 수 있습니다.

시작하기 전에

- 전화기 모델이 회선 간 통화 참가를 지원하는지 확인 [전화기 기능 목록 생성, 7 페이지](#)
- [애드-혹 컨퍼런스 구성, 245 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 기본 디바이스 프로파일.
- 기본 디바이스 프로파일 구성 창이 표시됩니다.
- 단계 2 디바이스 프로파일 유형 드롭다운 목록에서 전화기 모델을 선택합니다.
- 단계 3 디바이스 프로토콜 드롭다운 목록에서 관련 SCCP 또는 SIP 프로토콜을 선택합니다.
- 단계 4 회선 간 통화 참가를 켜기로 설정합니다.
- 단계 5 저장을 클릭합니다.
-

전화회의 상호 작용

기능	상호 작용
회의 끼기를 사용하여 전화회의	<p>회의끼기 소프트웨어를 눌러 전화회의를 시작하거나 단일 버튼 회의끼기 기능이 활성화된 경우 활성화 통화의 공유 회선 버튼을 눌러 전화회의를 시작합니다. 회의끼기를 시작하면 공유 컨퍼런스 브리지(사용 가능한 경우)를 사용하여 참여 통화가 설정됩니다. 원래 통화가 분리된 후 컨퍼런스 브리지에 참가합니다. 모든 상대방의 통화 정보가 전화회의로 변경됩니다.</p> <p>참여 통화가 참여 대상 디바이스를 전화회의의 컨트롤러로 사용하는 전화회의의 통화가 됩니다. 컨트롤러는 전화회의에 상대방을 더 추가하거나 제거할 수 있습니다.</p> <p>통화에서 모든 상대방이 떠나고 전화회의에 두 상대방만 남는 경우에는 남아 있는 두 상대방에게 잠깐 동안의 중단이 발생한 후 포인트 간 통화로 재연결되고, 공유 전화회의의 리소스가 해제됩니다.</p>
통화 지정 보류, 통화 호 전환 및 재전송과의 상호 작용	<p>전화회의의 컨트롤러가 전화회의를 다른 상대방에게 호 전환, 지정 보류 또는 재전송하는 경우 통화를 검색하는 상대방이 전화회의에 대한 가상 컨트롤러로 작동합니다. 가상 컨트롤러는 새 상대방을 전화회의에 추가하거나 전화회의에 추가된 상대방을 제거할 수 없지만, 가상 컨트롤러는 전화회의를 다른 상대방에게 호 전환, 지정 보류 또는 재전송하여 전화회의의 가상 컨트롤러가 될 수 있습니다. 이 가상 컨트롤러가 통화를 끊으면 전화회의가 종료됩니다.</p>
SIP 전화기에 소프트웨어 표시	<p>구성 목록과 소프트웨어 제거 기능은 SCCP 전화기에서만 사용할 수 있습니다. SIP 전화기에는 유사한 기능이 있는 세부 정보 표시 버튼이 있습니다.</p>

전화회의 제한 사항

애드-혹 컨퍼런스에는 다음과 같은 제한 사항이 적용됩니다.

기능	제한 사항
Ad Hoc 전화회의	<p>Unified Communications Manager에서는 각 Unified Communications Manager 서버에 대한 최대 100개의 동시 애드-혹 컨퍼런스를 지원합니다.</p> <p>Cisco Unified Communications Manager는 애드-혹 컨퍼런스 당 최대 64명의 참가자(적절한 전화회의 리소스를 제공하는 경우)를 지원합니다. 연결된 애드-혹 컨퍼런스 경우 시스템은 각 전화회의를 한 참가자로 간주합니다.</p>

기능	제한 사항
<p>SIP 전화기에서 애드-혹 컨퍼런스:</p> <ul style="list-style-type: none"> • Cisco Unified IP Phone 7911 • Cisco Unified IP Phone 7941 • Cisco Unified IP Phone 7961 	<p>Unified Communications Manager에서는 새 상대방이 추가 될 때와 새 상대방이 애드-혹 컨퍼런스에서 각각 삭제될 때 “경고음” 및 “beepbeep” 신호음을 사용합니다. 상대방이 애드-혹 컨퍼런스에 추가되면 SIP를 실행하는 전화기의 사용자가 경고음을 들을 수 없습니다. 참가자가 애드-혹 컨퍼런스에서 삭제되면 SIP를 실행하는 전화기의 사용자가 “beepbeep” 소리를 듣지 못할 수 있습니다. 전화회의 프로세스 중에 Unified Communications Manager에서 연결을 설정하고 종료하는 데 걸리는 시간 때문에 사용자가 경고음을 들을 수 없습니다.</p> <p>전화회의 및 호 전환 기능을 사용하여 SIP를 실행하는 전화기에 대해 애드-혹 컨퍼런스 링크를 호출할 수 있습니다. 시스템에서 직접 호 전환 및 참가를 지원하지 않습니다. SIP를 실행하는 지원되는 전화기는 Cisco Unified IP Phone 7911, 7941, 7961로 구성됩니다.</p>

기능	제한 사항
<p>SIP 전화기에서 애드-혹 컨퍼런스:</p> <ul style="list-style-type: none"> • Cisco Unified IP Phone 7940 • Cisco Unified IP Phone 7960 • 타사 전화기 	<ul style="list-style-type: none"> • 전화기는 개별 통화를 전화회의 통화로 표시합니다. Cisco Unified IP Phone 7940 및 7960은 로컬 전화회의 통화를 만들 수 있지만 애드-혹 컨퍼런스 통화는 만들 수 없습니다. • 컨퍼런스 목록(참가 목록)은 사용할 수 없습니다. • 마지막 컨퍼런스 참가자 제거(거부)는 사용할 수 없습니다. • 애드-혹 컨퍼런스 삭제는 지원되지 않습니다. • SIP 프로파일 매개 변수 전화회의 조인은 전화회의 컨트롤러가 로컬로 호스팅된 전화회의를 종료할 때 SIP를 실행하는 전화기의 동작을 제어합니다. 전화회의 참가 활성화됨 확인란을 선택 취소한 경우 전화회의 컨트롤러가 애드-혹 컨퍼런스를 종료할 때 모든 레그의 연결이 끊깁니다. 전화회의 참가 활성화됨 확인란을 선택하면 나머지 두 명의 상대방이 연결된 상태를 유지합니다. • SCCP를 실행하는 전화기에서 시작하는 전화회의 통화에 대해 애드-혹 컨퍼런스 매개 변수 설정이 제공하는 것과 동일한 제어 수준을 얻으려면 SIP를 실행하는 전화기(Cisco Unified IP Phone 7940 또는 60)에서 시작된 전화 회의에 대해 관리자가 전화회의 참가 활성화됨 SIP 프로파일 매개 변수와 오프 넷간 전환 차단 서비스 매개 변수의 조합을 사용할 수 있습니다. (SIP를 실행하는 전화기가 전화회의 통화에서 삭제되면 호 전환을 수행하므로 오프 넷간 전환 차단은 두 개의 오프 넷 전화기가 통화에 유지되지 않도록 하여 요금 사기를 방지할 수 있습니다.) • Unified Communications Manager에서는 새 상대방이 추가 될 때와 새 상대방이 애드-혹 컨퍼런스에서 각각 삭제될 때 “경고음” 및 “beepbeep” 신호음을 사용합니다. 상대방이 애드-혹 컨퍼런스에 추가되면 SIP를 실행하는 전화기의 사용자가 경고음을 들을 수 없습니다. 참가자가 애드-혹 컨퍼런스에서 삭제되면 SIP를 실행하는 전화기의 사용자가 “beepbeep” 소리를 듣지 못할 수 있습니다. 전화회의 프로세스 중에 Unified Communications Manager에서 연결을 설정하고 종료하는 데 걸리는 시간 때문에 사용자가 경고음을 들을 수 없습니다.

기능	제한 사항
두 상대방이 연결된 경우에도 "전화회의로"를 표시하는 전화기	<p>게시자(CmA11) 및 가입자(CmA2)를 사용하여 Call Manager 클러스터를 구성합니다.</p> <p>전화기 A, B, C가 CmA1에 등록됩니다. 전화기 D가 CmA2에 등록됩니다.</p> <ul style="list-style-type: none"> • A(1000), B(4000), C(5000), D(6000) 사이에 상담 또는 블라인드 애드-혹 컨퍼런스를 컨트롤러로 설정합니다. • CmA2를 종료합니다. • 전화기 D가 보호 모드로 이동하면 통화 종료 소프트웨어를 누릅니다. • 전화기 A, B 및 C가 전화회의 중입니다. • 전화기 A, B 및 C가 전화회의 중입니다. • 전화기 A의 연결을 끊으면 전화기 B와 C가 직접 통화 중이어야 합니다. 문제: 전화기 B와 C가 아직 전화회의 중입니다. • 전화기 A의 연결을 끊으면 전화기 B와 C가 직접 통화 중이어야 합니다. 문제: 전화기 B와 C가 아직 전화회의 중입니다. • 전화기 B의 연결을 끊으면 전화기 C에 통화가 없어야 합니다. 전화기 B와 C가 아직 전화회의 중입니다. 문제: 전화기 C가 아직 전화회의 중입니다.



20 장

회의개설 컨퍼런싱

- 회의개설 컨퍼런싱, 255 페이지
- 회의개설 컨퍼런싱 작업 흐름, 255 페이지
- 회의개설 전화회의 제한 사항, 261 페이지

회의개설 컨퍼런싱

사용자는 회의개설 전화회의를 사용하여 전화회의를 설정하거나 참가할 수 있습니다. 전화회의를 설정하는 사용자를 전화회의 컨트롤러라고 합니다. 전화회의에 참가하는 사용자를 참가자라고 합니다.

회의개설 컨퍼런싱 작업 흐름

시작하기 전에

- 라우터와 함께 제공된 구성 설명서를 참조하고 지금 미팅 전화 회의 작업 흐름을 진행하기 전에 구성 해야 할 수 있는 설정이 있는지 확인하십시오.

프로시저

	명령 또는 동작	목적
단계 1	회의개설 컨퍼런싱용 소프트키 템플릿 구성, 256 페이지	지금 미팅 소프트키를 소프트키 템플릿에 추가합니다.
단계 2	<p>소프트키 템플릿을 일반 디바이스 구성에 연결, 257 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> • 소프트키 템플릿을 일반 디바이스 구성에 추가, 258 페이지 	선택 사항. 전화기에서 소프트키 템플릿을 사용할 수 있게 하려면 이 단계 또는 다음 단계를 완료해야 합니다.

	명령 또는 동작	목적
	<ul style="list-style-type: none"> 일반 디바이스 구성을 전화기에 연결, 258 페이지 	
단계 3	일반 디바이스 구성소프트키 템플릿을 전화기에 연결, 259 페이지	선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하거나 일반 디바이스 구성과 함께 연결하는 대신 사용할 수 있습니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우 일반 디바이스 구성과 함께 이 절차를 사용합니다.
단계 4	회의개설 전화회의 번호 구성, 259 페이지	고급 전화회의를 활성화하고 참가자의 최대 수를 지정하고 전화회의의 연결을 삭제할 시기를 지정합니다.

회의개설 컨퍼런싱용 소프트키 템플릿 구성

이 절차를 사용하여 오프 호 통화 상태에서 지금 미팅 소프트키를 사용할 수 있도록 합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- 새로 추가를 클릭합니다.
 - 기본 템플릿을 선택하고 복사를 클릭합니다.
 - 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - 저장을 클릭합니다.
- 단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
- 찾기를 클릭하고 검색 기준을 입력합니다.
 - 필요한 기존 템플릿을 선택합니다.
- 단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.
- 참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.
- 단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
- 단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.

- 단계 7** 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.
- 단계 8** 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.
- 단계 9** 저장을 클릭합니다.
- 단계 10** 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

소프트키 템플릿을 일반 디바이스 구성에 연결

선택 사항. 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 [소프트키 템플릿을 전화기에 연결, 259 페이지](#)의 내용을 참조하십시오.

시작하기 전에

[회의개설 컨퍼런싱용 소프트키 템플릿 구성, 256 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	소프트키 템플릿을 일반 디바이스 구성에 추가, 258 페이지	
단계 2	일반 디바이스 구성을 전화기에 연결, 258 페이지	

소프트키 템플릿을 일반 디바이스 구성에 추가

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성
- 단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.
- 새로 추가를 클릭합니다.
 - 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
 - 저장을 클릭합니다.
- 단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.
- 찾기를 클릭하고 검색 기준을 입력합니다.
 - 기존 일반 디바이스 구성을 클릭합니다.
- 단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.
- 단계 5 저장을 클릭합니다.
- 단계 6 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.
-

일반 디바이스 구성을 전화기에 연결

시작하기 전에

[소프트키 템플릿을 일반 디바이스 구성에 추가, 258 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정을 클릭하여 전화기 설정을 업데이트합니다.
-

소프트키 템플릿을 전화기에 연결

선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성과 연결할 수 있습니다. 이 절차는 일반 디바이스 구성과 함께 작동합니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우에 사용할 수 있습니다.

시작하기 전에

[회의개설 컨퍼런싱용 소프트키 템플릿 구성, 256 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정을 눌러 전화기 설정을 업데이트합니다.
-

회의개설 전화회의 번호 구성

Cisco Unified Communications Manager 관리자는 사용자에게 회의개설 전화회의 디렉터리 번호 범위를 제공하여 사용자가 해당 기능에 액세스할 수 있도록합니다. 사용자는 회의개설 번호 또는 패턴에 대해 지정된 범위에서 디렉터리 번호를 선택하여 회의개설 전화회의를 설정하고 전화회의의 컨트롤러가 됩니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 회의개설 번호/패턴. 회의개설 번호 찾기 및 나열 창이 표시됩니다.
- 단계 2 적절한 검색 조건을 입력하고 찾기를 클릭합니다. 일치하는 레코드가 모두 표시됩니다.
- 단계 3 레코드 목록에서 보려는 레코드의 링크를 클릭합니다.
- 단계 4 다음 작업 중 하나를 수행합니다.
- 회의개설 번호 또는 패턴을 복사하려면 복사하려는 회의개설 번호 또는 패턴을 클릭합니다. 회의개설 번호/패턴 구성 창이 나타납니다. 복사를 클릭합니다.
 - 회의개설 번호 또는 패턴을 추가하려면 새로 추가 버튼을 클릭합니다.
 - 기존 회의개설 번호 또는 패턴을 업데이트하려면 업데이트하려는 회의개설 번호 또는 패턴을 클릭합니다.
- 단계 5 설정을 적절히 입력합니다.

필드 및 해당 구성 옵션에 대한 자세한 내용은 관련 항목 섹션을 참조하십시오.

단계 6 저장을 클릭합니다.

회의개설 번호 및 패턴 설정

필드	설명
디렉토리 번호 또는 패턴	회의개설 번호 또는 번호 범위를 입력합니다. 범위를 구성하려면 대시(-)가 괄호 안에 있고 뒤에 숫자가 있어야 합니다 (예: 1000~1050을 구성하려면 10[0-5]0을 입력).
설명	설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&) 또는 꺾쇠괄호(<>)는 사용할 수 없습니다.
파티션	<p>파티션을 사용하여 회의개설 번호 또는 패턴에 대한 액세스를 제한하려면 드롭다운 목록표에서 원하는 파티션을 선택합니다.</p> <p>회의개설 번호 또는 패턴에 대한 액세스를 제한하지 않으려면 파티션에 대해 <None>을 선택합니다.</p> <p>최대 목록 상자 항목 수(Max List Box Items) 엔터프라이즈 파라미터를 사용하여 이 드롭다운 목록표에 표시되는 파티션 수를 구성할 수 있습니다. 최대 목록 상자 항목 수(Max List Box Items) 엔터프라이즈 파라미터에 지정된 것보다 더 많은 파티션이 존재하는 경우 드롭다운 목록표 옆에 찾기 버튼이 표시됩니다. 찾기 버튼을 클릭하면 파티션 찾기 및 나열 창이 표시됩니다.</p> <p>참고 최대 목록 상자 항목 수를 설정하려면 시스템 > 엔터프라이즈 파라미터를 선택하고 CCMAAdmin 파라미터에 있는 [최대 목록 상자 항목 수] 필드를 업데이트합니다.</p> <p>참고 회의개설 번호 또는 패턴과 파티션의 조합은 Unified Communications Manager 클러스터 내에서 고유해야 합니다.</p>

필드	설명
최소 보안 수준	<p>드롭다운 목록표에서 이 회의개설 번호 또는 패턴에 대해 최소 회의방 개설 전화회의 보안 수준을 선택합니다.</p> <ul style="list-style-type: none"> 비보안 전화기를 사용하는 참가자의 전화회의 참가를 차단하려면 인증됨을 선택합니다. 인증된 또는 비보안 전화기를 사용하는 참가자의 전화회의 참가를 차단하려면 암호화됨을 선택합니다. 모든 참가자가 전화회의에 참가할 수 있도록하려면 비보안을 선택합니다. <p>참고 이 기능을 사용하려면 보안 컨퍼런스 브리지가 구성되어 있고 사용할 수 있어야합니다.</p>

회의개설 전화회의 제한 사항

Unified Communications Manager에서는 각 Unified Communications Manager 서버에 대한 최대 100개의 동시 회의개설 전화회의를 지원합니다.

해당 전화 회의에 대해 지정된 최대 참가자 수를 초과하면 다른 발신자가 전화회의에 참가할 수 없습니다.



21 장

Conference Now

- [Conference Now 개요, 263 페이지](#)
- [Conference Now 사전 요건, 264 페이지](#)
- [Cisco IP Voice Media Streaming 활성화, 264 페이지](#)
- [Conference Now 설정 구성, 264 페이지](#)
- [사용자용 Conference Now 활성화, 265 페이지](#)
- [LDAP를 통해 Conference Now 활성화, 266 페이지](#)
- [Conference Now 상호 작용, 267 페이지](#)
- [Conference Now 제한 사항, 267 페이지](#)

Conference Now 개요

이제 전화회의는 내부 및 외부 발신자가 중앙 집중식 IVR을 통해 전화회의에 참가할 수 있는 소규모 비즈니스 고객을 위한 기본 오디오 회의 솔루션을 제공합니다.

미팅을 호스팅하려면 구성된 사용자가 회의를 시작할 때 미팅 번호와 함께 입력해야 하는 미팅 PIN을 구성해야 합니다. 호스트는 시간 슬롯, 미팅 번호(일반적으로 호스트의 기본 내선 번호) 및 보안 전화회의에 대한 선택적 액세스 코드를 포함하여 관련 미팅 정보를 다른 미팅 참가자에게 제공합니다. 지정된 시간에 다른 참가자는 IVR에 전화를 걸고 미팅 정보를 프롬프트에 입력하여 통화에 참가할 수 있습니다.

관리자는 최종 사용자를 Conference Now 전화회의를 호스팅하는 기능으로 구성해야 합니다. 기능이 구성된 후에는 미팅 호스트가 셀프 서비스 포털 내에서 미팅 액세스 코드를 편집할 수 있습니다.



참고 Conference Now를 위해 IPVMS 소프트웨어 기반 전화회의 브리지를 사용하는 것이 좋습니다. 다른 전화회의 브리지를 사용하는 경우 전화회의의 시작 및 종료 신호음이 참가자에게 재생되지 않을 수 있습니다.

Conference Now 사전 요건

Conference Now를 사용하려면 다음 미디어 리소스가 구성되어 있고 전화회의를 시작할 디바이스에서 사용할 수 있는지 확인해야 합니다.

- 전화회의 브리지 - 최적의 사용자 환경을 위해 소프트웨어 기반 Cisco IPVMS 전화회의 브리지를 사용하는 것이 좋습니다. 다른 전화회의 브리지를 사용하면 전화회의 상대가 들어올 때와 나갈 때 발신음이 제공되지 않을 수 있습니다.
- IVR(Interactive Voice Response)

이러한 리소스를 구성한 후에는 이러한 리소스를 포함하는 미디어 리소스 그룹 목록을 구성하고 디바이스 또는 개별 디바이스에서 사용될 디바이스폴에 해당 미디어 리소스 그룹 목록을 연결하여 디바이스에서 사용할 수 있게 할 수 있습니다. 전화 회의 브리지, 대화형 음성 응답 및 미디어 리소스 그룹을 구성하는 방법에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "미디어 리소스 구성" 섹션을 참조하십시오.

Cisco IP Voice Media Streaming 활성화

IVR 서비스와 Conference Now를 사용하려면 Cisco IP Voice Media Streaming 서비스가 실행되고 있어야 합니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. 도구 > 서비스 활성화.

단계 2 서버 드롭다운 목록에서 Cisco Unified Communications Manager 퍼블리셔 노드를 선택합니다.

단계 3 **Cisco IP Voice Media Streaming** 애플리케이션이 비활성화된 경우 해당 확인란을 선택하고 저장을 클릭합니다.

Conference Now 설정 구성

이 절차를 사용하여 Unified Communications Manager에서 Conference Now 시스템 설정을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > **Conference Now**.

단계 2 **Conference Now IVR** 디렉터리 번호 필드에 외부 발신자에 대한 액세스를 제공하기 위해 Unified Communications Manager 클러스터에 대한 DID(직접 내부 다이얼) 번호를 입력합니다.

단계 3 라우트 파티션 드롭다운 목록에서 파티션을 선택합니다.

참고 조합된 번호와 파티션은 클러스터 내에서 고유해야 합니다.

단계 4 **Conference Now** 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

다음에 수행할 작업

최종 사용자에게 기능을 활성화합니다.

- 아직 LDAP 디렉토리를 동기화하지 않은 경우, Conference Now를 LDAP 동기화에 추가하여 새로 동기화된 사용자가 Conference Now 미팅을 호스트할 수 있게 합니다. [LDAP를 통해 Conference Now 활성화, 266 페이지](#) 참조
- 기존 최종 사용자에게 기능을 활성화 하려면 [사용자용 Conference Now 활성화, 265 페이지](#)의 내용을 참조하십시오.

사용자용 Conference Now 활성화

이 절차를 사용하여 기존 최종 사용자에게 Conference Now 미팅을 호스트할 수 있는 권한을 구성합니다.



참고 별크 관리의 사용자 업데이트 기능을 사용하여 csv 파일을 통해 다수의 사용자에게 대해 Conference Now를 활성화할 수도 있습니다. 아래 작업에서와 동일한 설정이 구성되어 있는지 확인해야 합니다. 업데이트 사용자를 사용하는 방법에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 별크 관리 지침서](#)의 내용을 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 찾기를 클릭하고 Conference Now를 추가하려는 사용자를 선택합니다.

단계 3 **Conference Now**에서 **Conference Now**를 호스팅하도록 최종 사용자 활성화 확인란을 선택합니다.

단계 4 (선택 사항) 보안 전화회의의 경우 참가자 액세스 코드를 입력합니다. 최종 사용자는 셀프 서비스 포털 내에서 액세스 코드 설정을 수정할 수 있습니다.

참고 사용자에게 셀프 서비스 사용자 ID가 할당된 경우 Conference Now 미팅 번호가 사용자의 기본 확장으로 기본 설정인 셀프 서비스 사용자 ID 값으로 미리 채워집니다.

단계 5 최종 사용자 구성 창의 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

LDAP를 통해 Conference Now 활성화

아직 LDAP 디렉터리를 동기화하지 않은 경우 기능 그룹 템플릿에 옵션을 추가하고 해당 기능 그룹 템플릿을 초기 LDAP 동기화에 추가하여 동기화된 사용자에게 대해 Conference Now를 활성화할 수 있습니다. LDAP 동기화를 통해 프로비저닝된 새 사용자는 Conference Now를 활성화할 수 있습니다.



참고 초기 동기화가 이미 발생한 경우에는 기능 그룹 템플릿 편집 내용을 LDAP 디렉터리 동기화에 적용할 수 없습니다. 이러한 편집 내용을 LDAP 동기화에 적용하려면 초기 동기화가 아직 발생하지 않아야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 사용자 전화기/추가 > 기능 그룹 템플릿.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 선택하고 기존 템플릿을 선택합니다.
- 새로 추가를 클릭하여 새 템플릿을 만듭니다.

단계 3 드롭다운 목록에서 서비스 프로파일을 선택합니다.

단계 4 드롭다운 목록에서 사용자 프로파일을 선택합니다.

단계 5 **Conference Now**를 호스팅하도록 최종 사용자 활성화 확인란을 선택합니다.

단계 6 저장을 클릭합니다.

다음에 수행할 작업

동기화된 사용자가 Conference Now에 대해 구성되도록 LDAP 디렉터리 동기화에 템플릿을 할당합니다. LDAP 동기화 구성에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "최종 사용자 구성" 섹션을 참조하십시오.

또는 빠른 사용자/전화기 추가 메뉴를 통해 Conference Now 기능을 사용하여 새 사용자를 추가할 수 있습니다. 기본 내선 번호를 할당하는 것 외에 이 기능 그룹 템플릿을 사용하는 새 사용자를 추가해야 합니다.

Conference Now 상호 작용

기능	상호 작용
이동성 EFA(엔터프라이즈 기능 액세스)	이동성 사용자가 원격 대상에서 엔터프라이즈 기능 액세스 번호에 전화를 겁니다. 통화가 연결되면 원격 대상 전화기가 PSTN 게이트웨이를 통해 Unified Communications Manager에 DTMF 숫자를 전송하는 데 사용됩니다. 다음에 # 키가 있는 사용자 PIN이 Unified Communications Manager에 먼저 인증됩니다. 사용자 PIN 인증에 성공한 후 1번과 # 키를 눌러 2단계로 다이얼된 통화를 표시한 다음 원하는 전화 번호를 표시합니다. 다이얼한 전화 번호가 Conference Now IVR 디렉터리 번호이고 사용자가 미팅 호스트인 경우 사용자는 PIN을 다시 입력해야 합니다.
이동성 MVA(모바일 음성 액세스)	통화는 엔터프라이즈 PSTN H.323 또는 SIP 게이트웨이를 통해 Unified Communications Manager에 전송됩니다. IVR은 사용자에게 사용자 ID, #키, PIN, #키, 번호 1(모바일 음성 액세스 전화를 걸려면)을 입력한 다음 원하는 전화 번호를 입력하라는 메시지를 표시합니다. 전화 번호가 Conference Now IVR 디렉터리 번호이고 사용자가 미팅 호스트인 경우 사용자는 PIN을 다시 입력해야 합니다. 참고 원격 대상에서 직접 전화를 거는 경우 PIN을 입력하라는 메시지가 표시되지 않습니다. 그러나 다른 전화기에서 모바일 음성 액세스 디렉터리 번호로 전화를 거는 경우 전화를 걸려면 먼저 PIN을 입력하라는 메시지가 표시됩니다. 사용자가 Conference Now IVR 디렉터리 번호로 전화를 거는 경우 PIN을 다시 입력하라는 메시지가 표시됩니다.

Conference Now 제한 사항

지금 전화 회의 기능에는 다음과 같은 제한 사항이 있습니다.

- 호스트는 참가자를 음소거할 수 없습니다.
- 참가자는 DTMF 숫자를 입력하여 오디오를 음소거할 수 없습니다.
- Conference Now 참가자 목록은 지원되지 않습니다.
- 전화회의의 최대 참가자 수는 기존 CallManager 서비스 매개 변수 "최대 회의개설 전화회의 유니캐스트"에 의해 제어됩니다. 내부 및 외부 발신자 모두에 적용됩니다.
- 현재 동시 Conference Now의 최대 수와 회의개설 전화회의의 인스턴스를 함께 결합하는 것은 Unified Communications ManagerCallManager 노드당 100입니다.
- 대기 중 비디오는 지원되지 않습니다.

- IPVMS 소프트웨어 컨퍼런스 브리지는 코덱 G.711(ALaw 및 ULaw) 및 광대역 256k만 지원합니다. 발신 디바이스와 소프트웨어 컨퍼런스 브리지 간에 코덱이 일치하지 않는 경우 트랜스코더가 할당됩니다.
- 다음 조건 중 하나 이상이 충족되어야 전화회의 참가자 입장 및 퇴장 신호음이 재생됩니다.
 - 최소 한 명 이상의 전화회의 참가자가 Cisco IP 전화기를 사용하고 있습니다.
 - IPVMS는 할당된 소프트웨어 컨퍼런스 브리지입니다.
- 컨퍼런스 브리지를 설정할 때 호스트 참석 여부에 관계없이 남은 참석자와 회의가 계속됩니다. 호스트가 회의에 다시 참가하려고 할 때 호스트가 참석자 액세스 코드를 구성한 경우에는 이 코드를 입력하라는 알림이 재생됩니다. 호스트가 참석자를 예약하거나 음소거할 수 없으므로 호스트 상태가 더 이상 유효하지 않습니다.
- 호스트가 가장 먼저 회의에 참석할 경우 오디오 알림이 재생되지 않습니다. 하지만 호스트가 내부 IP 전화기에서 Conference Now로 전화를 걸면 IP 전화기에 “회의로”라는 디스플레이가 표시됩니다.



참고 호스트가 외부 전화기에서 Conference Now에 참여할 경우 전화기에 화면이 표시되지 않습니다.



IX 부

전화 걸기

- 콜백 , 271 페이지
- 핫라인 , 283 페이지
- 단축 다이얼, 297 페이지
- WebDialer , 301 페이지
- 페이징 , 319 페이지
- 인터콤 , 341 페이지



22 장

콜백

- 콜백 개요, 271 페이지
- 콜백 사전 요건, 272 페이지
- 콜백 구성 작업 흐름, 272 페이지
- 콜백 상호 작용, 277 페이지
- 콜백 제한 사항, 279 페이지
- 콜백 문제 해결, 279 페이지

콜백 개요

콜백 기능을 사용하면 통화 중 내선 번호를 사용하여 통화를 받을 수 있는 경우 알림을 받을 수 있습니다.

전화기와 동일한 Unified Communications Manager 클러스터 내에 있거나 QSIG 트렁크 또는 QSIG 지원 인터클러스터 트렁크를 통해 원격 PINX(Private Integrated Network Exchange)에 있는 대상 전화에 대해 콜백을 활성화할 수 있습니다.

콜백 알림을 받으려면 통화 중 또는 통화 연결음이 수신되는 동안 콜백 소프트키 또는 기능 버튼을 누릅니다. 사용자는 응답 없음 타이머가 만료되면 트리거되는 다시걸기 신호음이 재생되는 동안에 콜백을 활성화할 수 있습니다.

일시 중지/보류해제

콜백 기능을 사용하면 콜백을 시작한 사용자가 통화 중인 경우 시스템에서 통화 완료 서비스를 일시 중단할 수 있습니다. 발신 사용자가 통화 가능 상태가 되면 통화 완료 서비스에서 해당 사용자에게 대한 보류를 해제합니다.



참고 콜백에서는 클러스터 내 및 클러스터 간 QSIG 트렁크 양쪽 모두 또는 QSIG 지원 기능이 있는 인터클러스터 트렁크에 대해 일시 중지/보류해제 콜백 알림을 지원합니다.

콜백 사전 요건

콜백 기능을 사용하려면 대상 전화기가 다음 위치 중 하나에 있어야 합니다.

- 사용자 전화기와 동일한 Unified Communications Manager 클러스터
- QSIG 트렁크를 통한 원격 PINX
- QSIG가 활성화된 클러스터 간 트렁크를 통한 원격 PINX

영어가 아닌 전화기 로캘 또는 국가별 신호음을 사용하려면 로캘을 설치해야 합니다.

- 다음 디바이스는 콜백 기능을 지원합니다.
 - Cisco Unified IP Phone 6900, 7900, 8900 및 9900 Series(6901 및 6911 제외)
 - Cisco IP 전화기 7800 및 8800 시리즈
 - Cisco VGC Phone(Cisco VG248 Gateway 사용)
 - Cisco ATA(Analog Telephone Adapter) 186 및 188
 - Cisco VG224 엔드포인트에 대한 통화 중 가입자
 - Cisco VG224 엔드포인트에 대한 응답 없음
- 지원되는 전화기로 통화를 착신 전환하는 CTI 라우트 포인트.

콜백 구성 작업 흐름

전화기에서 소프트키 또는 버튼을 지원하는지 여부에 따라 작업 흐름 중 하나를 완료합니다.

이 표를 사용하여 콜백 소프트키 또는 콜백 지원 IP 전화기에 대한 버튼을 구성할 지 여부를 결정합니다.

표 24: 콜백 소프트키 및 버튼을 사용하는 **Cisco IP** 전화기

Cisco 전화기 모델	콜백 소프트키	콜백 버튼
Cisco Unified IP Phone 6900 Series(6901 및 6911 제외)	X	X
Cisco Unified IP Phone 7900 시리즈	X	
Cisco IP 전화기 7800 및 8800 시리즈	X	X
Cisco Unified IP Phone 8900 시리즈	X	X
Cisco Unified IP Phone 9900 시리즈	X	X

Cisco 전화기 모델	콜백 소프트키	콜백 버튼
Cisco IP Communicator	X	

시작하기 전에

- [콜백 사전 요건, 272 페이지](#)을(를) 검토합니다.

프로시저

	명령 또는 동작	목적
단계 1	콜백에 대한 소프트키 템플릿 구성, 273 페이지	이 단계를 수행하여 콜백 소프트키를 템플릿에 추가하고 일반 디바이스 구성 또는 전화기를 사용하여 소프트키를 구성합니다.
단계 2	콜백 버튼 구성, 276 페이지	이 단계를 수행하여 전화기에 콜백 버튼을 추가하고 구성합니다.

콜백에 대한 소프트키 템플릿 구성

콜백 소프트키에는 다음과 같은 통화 상태가 있습니다.

- 온 훅
- 링아웃
- 호전환 연결됨

이 절차를 사용하여 콜백 소프트키를 사용할 수 있게 합니다.

시작하기 전에

전화기에서 콜백을 지원하는지 확인합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- a) 새로 추가를 클릭합니다.
 - b) 기본 템플릿을 선택하고 복사를 클릭합니다.
 - c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - d) 저장을 클릭합니다.
- 단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
- a) 찾기를 클릭하고 검색 기준을 입력합니다.

b) 필요한 기존 템플릿을 선택합니다.

단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.

참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.

단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.

단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.

단계 7 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.

단계 8 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.

단계 9 저장을 클릭합니다.

단계 10 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

다음에 수행할 작업

다음 절차 중 하나를 수행합니다.

- [콜백 소프트키 템플릿을 일반 디바이스 구성에 연결, 274 페이지](#)
- [콜백 소프트키 템플릿을 전화기에 연결, 276 페이지](#)

콜백 소프트키 템플릿을 일반 디바이스 구성에 연결

선택 사항. 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 [콜백 소프트키 템플릿을 전화기에 연결, 276 페이지](#)의 내용을 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 1	콜백 소프트키 템플릿을 일반 디바이스 구성에 추가, 275 페이지	이 단계에 따라 일반 디바이스 구성에 콜백 소프트키 템플릿을 추가합니다.
단계 2	일반 디바이스 구성을 전화기에 연결, 275 페이지	이 단계를 수행하여 콜백 소프트키 일반 디바이스 구성을 전화기에 연결합니다.

콜백 소프트키 템플릿을 일반 디바이스 구성에 추가

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성
- 단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성 하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.
- 새로 추가를 클릭합니다.
 - 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
 - 저장을 클릭합니다.
- 단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.
- 찾기를 클릭하고 검색 기준을 입력합니다.
 - 기존 일반 디바이스 구성을 클릭합니다.
- 단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.
- 단계 5 저장을 클릭합니다.
- 단계 6 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

일반 디바이스 구성을 전화기에 연결

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 재설정 을 클릭하여 전화기 설정을 업데이트합니다.

콜백 소프트키 템플릿을 전화기에 연결

선택 사항: 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하거나 일반 디바이스 구성과 함께 연결하는 대신 사용할 수 있습니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우 일반 디바이스 구성과 함께 이 절차를 사용합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 전화기

단계 2 찾기를 클릭하고 전화기를 선택하여 소프트키 템플릿을 추가합니다.

단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 재설정을 눌러 전화기 설정을 업데이트합니다.

콜백 버튼 구성

이 섹션의 절차에서는 콜백 버튼을 구성하는 방법을 설명합니다.

프로시저

	명령 또는 동작	목적
단계 1	콜백에 대한 전화기 버튼 템플릿 구성, 276 페이지	회선 또는 단축 다이얼 키에 콜백 버튼 기능을 할당하려면 이 단계를 수행합니다.
단계 2	버튼 템플릿을 전화기와 연결, 277 페이지	이 단계를 수행하여 전화기에 콜백 버튼을 구성합니다.

콜백에 대한 전화기 버튼 템플릿 구성

회선 또는 단축 다이얼 키에 기능을 할당하려는 경우 이 절차를 수행합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.

단계 2 [찾기] 를 클릭하여 지원 되는 전화기 템플릿 목록을 표시합니다.

단계 3 새 전화기 버튼 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.

- a) 전화기의 모델에 대한 기본 템플릿을 선택하고 복사를 클릭합니다.
- b) 전화기 버튼 템플릿 정보 필드에 템플릿의 새 이름을 입력합니다.
- c) 저장을 클릭합니다.

단계 4 기존 템플릿에 전화기 버튼을 추가하려는 경우 다음 단계를 수행합니다.

- a) 찾기를 클릭하고 검색 기준을 입력합니다.
- b) 기존 템플릿을 선택합니다.

단계 5 회전 드롭다운 목록에서 템플릿에 추가하려는 기능을 선택합니다.

단계 6 저장을 클릭합니다.

단계 7 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다.

버튼 템플릿을 전화기와 연결

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.

단계 3 전화기 버튼 템플릿을 추가할 전화기를 선택합니다.

단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

콜백 상호 작용

기능	상호 작용
통화 착신 전환	콜백 알림 화면에서 발신된 통화는 대상 DN에 구성된 모든 착신 전환 값을 무시합니다. 통화는 콜백 회수 타이머가 만료되기 전에 이루어져야 합니다. 그렇지 않으면 통화 착신 전환 구성된 값이 무시되지 않습니다.

기능	상호 작용
SIP 실행 전화기의 콜백 알림	<p>콜백 알림은 Cisco Unified IP Phone 7960 및 7940에 대해서만 다르게 작동합니다. 기타 모든 SIP 전화기 및 모든 SCCP 전화기는 온 훅 및 오프 훅 알림을 지원합니다.</p> <p>SIP 7960 또는 7940 전화기의 회선이 언제 사용 가능해지는지를 Unified Communications Manager에서 알 수 있는 유일한 방법은 INVITE Unified Communications Manager가 전화기에서 수신하는 SIP INVITE 메시지를 모니터링하는 것입니다. 전화기가 Unified Communications Manager로 SIP INVITE를 전송하고 전화기가 온 훅 상태가 되면 Unified Communications Manager에서 Cisco Unified IP Phone 7960 및 7940(SIP) 사용자에게 오디오 및 콜백 알림 화면을 전송할 수 있습니다.</p>
방해사절(DND)	<p>DND-Reject가 시작 또는 종료 측에서 끄기로 설정된 경우 콜백은 정상적으로 작동합니다. Dnd-Reject가 켜기로 설정된 경우에만 동작이 달라집니다.</p> <ul style="list-style-type: none"> 시작 측에서 DND-Reject 켜기 - 사용자 A가 사용자 B에게 전화를 걸어 콜백을 호출합니다. 사용자 A가 DND-R로 이동합니다. 사용자 B를 사용할 수 있게 되면 콜백 알림은 여전히 사용자 A에게 표시됩니다. 즉, 사용자에게 DND 상태와 관계 없이 다른 상대방의 가용성을 알릴 수 있습니다. 종료 측에서 DND-Reject 켜기 - 사용자 A가 사용자 B에게 전화를 걸고, 사용자 B가 DND-Reject를 켜기로 설정했습니다. 사용자 A는 통화 중 신호음을 빠르게 받을 수 있습니다. 사용자 A는 통화 중 엔드포인트에서 콜백을 시작할 수 있습니다. 사용자 B가 여전히 DND-Reject 상태이고 오프 훅 및 온 훅으로 전환되면 사용자 A는 “현재 사용자 B를 DND-R에서 사용할 수 있음”이라는 알림을 받고 다이얼 옵션이 표시되지 않습니다. 사용자 A를 취소하도록 선택하지 않으면 사용자 B가 DND-Reject가 끄기로 설정될 때까지 콜백에서 계속 사용자 B를 모니터링합니다.
Cisco Extension Mobility	<p>Cisco Extension Mobility 사용자가 로그인하거나 로그아웃하면 콜백과 연결된 모든 활성 통화 완료는 자동으로 취소됩니다. 전화기에서 콜백이 활성화된 후 시스템에서 착신 전화기가 제거된 경우 발신자가 [다이얼] 소프트키를 누르면 다시걸기 신호음을 받게 됩니다. 사용자는 콜백을 취소하거나 다시 활성화할 수 있습니다.</p>

콜백 제한 사항

기능	제한 사항
CUBE 간비디오를 사용하여 콜백	QSIG 사용 SIP 트렁크가 있는 CUBE를 통해 연결된 두 개의 Unified CM 클러스터 사이에 통화가 있는 경우에는 영상 통화로 통화 콜백 기능이 작동하지 않습니다. 자세한 정보는 CSCun46243을 참조하십시오.
SIP 트렁크	SIP 트렁크를 통한 콜백은 지원되지 않지만 QSIG 사용 SIP 트렁크를 통한 콜백은 지원됩니다.
발신자 또는 착신자의 이름이나 번호에 지원되는 문자	콜백은 발신자 또는 착신자의 이름 또는 번호로 공백과 0~9의 숫자만 지원합니다. 콜백을 사용하려면 발신자 또는 착신자의 이름 또는 번호에 #(파운드 기호) 또는 *(별표)를 포함할 수 없습니다.
음성 메일	통화를 모두 음성 메시징 시스템으로 착신 전환하는 경우에는 콜백을 활성화할 수 없습니다.

콜백 문제 해결

이 섹션에서는 다양한 시나리오에 대한 문제, 가능한 원인 및 해결 방법, 그리고 콜백용 IP 전화기에 표시되는 오류 메시지에 대해 설명합니다.

콜백 소프트키를 누른 후 콜백이 발생하기 전에 전화기 분리/재설정

문제

콜백 소프트키를 누른 후 콜백을 활성화하기 전에 전화를 분리하거나 재설정했습니다.

가능한 원인

Unified Communications Manager 콜백 활성화를 취소합니다.

해결 방법

발신자 전화기가 등록되면 발신자 전화기는 재설정 후에 콜백 활성화 창을 표시하지 않습니다. 발신자는 콜백 소프트키를 눌러 활성화 콜백 서비스를 확인해야 합니다. 전화기에서 콜백 알림이 발생합니다.

발신자가 전화기 재설정 전에 가용성 알림을 보지 못함

문제

클러스터 내 또는 클러스터 간 콜백 시나리오에서 발신자는 사용자(예: 사용할 수 없는 사용자 B)에 대해 콜백을 시작합니다. 사용자 B를 사용할 수 있게 되면 발신자 전화기에 사용 가능성 알림 화면이 표시되고 신호음이 재생됩니다. 발신자가 몇 가지 이유로 인해 가용성 알림이 누락되고 전화기가 재설정됩니다.

예를 들어 발신자는 다른 사용자(예: 사용자 C)에 연락하고 사용자 C가 통화 중으로 표시되므로 콜백 소프트웨어를 누릅니다. 발신자 전화기에는 바꾸기/유지 화면이 표시되지만 화면에는 사용자 B에 대한 사용 가능성 알림이 이미 발생한 상태가 아닙니다.

가능한 원인

사용자가 전화기를 재설정합니다.

해결 방법

전화기를 재설정했지만 활성 통화 중이 아닌 경우 전화기에서 콜백 알림을 검토합니다. 콜백 소프트웨어를 누릅니다.

콜백 오류 메시지

다음 섹션에서는 IP 전화기 화면에 표시되는 오류 메시지에 대해 설명합니다.

콜백이 활성 상태가 아님

문제

다음 오류 메시지가 표시됩니다.

```
CallBack is not active. Press Exit to quit this screen.
```

가능한 원인

사용자가 유휴 상태 중에 콜백 소프트웨어를 눌렀습니다.

해결 방법

오류 메시지에 제공된 권장 작업을 수행합니다.

콜백이 이미 활성 상태임

문제

다음 오류 메시지가 표시됩니다.

```
CallBack is already active on xxxx. Press OK to activate on yyyy. Press Exit to quit this screen.
```

가능한 원인

사용자가 콜백 활성화를 시도했지만 이미 활성 상태입니다.

문제

오류 메시지에 제공된 권장 작업을 수행합니다.

콜백을 활성화할 수 없음

문제

다음 오류 메시지가 표시됩니다.

```
CallBack cannot be activated for xxxx.
```

가능한 원인

사용자가 콜백 활성화를 시도했을 때 Unified Communications Manager 데이터베이스에서 내선 번호를 사용할 수 없거나 대상에 대한 QSIG 경로가 없는 경우(즉, 비 QSIG 트렁크를 통해 연결되는 원격 프록시에 내선 번호가 있는 경우) 데이터베이스에서 내선 번호를 찾을 수 없습니다.

해결 방법

사용자가 다시 시도해야 합니다. 그렇지 않으면 관리자가 디렉터리 번호를 Cisco Unified CM 관리에 추가해야 합니다.

키가 활성 상태가 아님

문제

통화 중에 콜백 소프트키가 전화기에 표시되고 전화기 벨이 울리기 전에 사용자가 콜백 소프트키를 누릅니다. 하지만 전화기에 다음 오류 메시지가 표시됩니다.

```
Key Not Active
```

가능한 원인

사용자가 적절한 시간에 콜백 소프트키를 누르지 않았을 수 있습니다.

해결 방법

사용자는 벨소리가 울리거나 통화 중 신호가 수신된 후에 콜백 소프트키를 눌러야 합니다. 잘못된 시간에 소프트키를 누르면 오류 메시지가 전화기에 표시될 수 있습니다.

키가 활성 상태가 아님



23 장

핫라인

- 핫라인 개요, 283 페이지
- 핫라인 시스템 요구 사항, 284 페이지
- 핫라인 구성 작업 흐름, 284 페이지
- 핫라인 문제 해결, 296 페이지

핫라인 개요

핫라인 기능을 통해 PLAR(개인 회선 자동 링다운) 기능을 확장할 수 있습니다. 그러면 사용자가 오프 훅되는 경우(또는 [전화걸기] 소프트키 또는 회선 키가 눌러진 경우) 전화기에서 즉시 미리 구성된 번호로 전화를 걸 수 있도록 전화기를 구성할 수 있습니다. 이 기능은 비상 전화 또는 "핫라인" 번호로 전화를 걸도록 지정된 전화에 유용합니다.

관리자는 최대 15초의 지연 시간을 구성할 수 있습니다. 이렇게 하면 전화기가 핫라인 번호로 기본 설정되기 전에 사용자가 전화를 걸 수 있습니다. 디바이스 > 디바이스 설정 > SIP 프로파일에서 타이머를 설정하도록 오프 훅에서 첫 번째 자릿수 타이머 간 간격 매개변수를 구성할 수 있습니다.

핫라인은 PLAR이 사용되는 전화기에 대해 다음과 같은 추가 제한 및 관리자 제어 기능을 추가합니다.

- 통화를 수신하는 핫라인 디바이스(핫라인을 사용하도록 구성된 디바이스)는 다른 핫라인 디바이스의 통화만 수신하고 핫라인 이외의 발신자를 거부합니다.
- 핫라인 전화를 걸기 전용, 받기 전용 또는 걸기와 받기 모두로 구성할 수 있습니다.
- 소프트키 템플릿을 전화기에 적용하여 핫라인 전화기에서 사용할 수 있는 기능을 제한할 수 있습니다.
- 아날로그 핫라인 전화기에서는 인바운드 훅 플래시 신호를 무시합니다.

라우트 클래스 신호 처리

핫라인에는 라우트 클래스 신호 처리가 사용되어 핫라인 전화기가 다른 핫라인 전화기에서 건 전화만 받도록 할 수 있습니다. 라우트 클래스는 통화에 대한 트래픽 클래스를 식별하는 DSN 코드입니다.

라우트 클래스는 다운스트림 디바이스에 특별 라우팅 또는 종료 요구 사항에 대해 알립니다. 핫라인 전화기는 동일한 라우트 클래스를 사용하는 통화만 허용할 수 있습니다.

통화 심사

핫라인은 또한 발신자 ID를 기반으로 구성 가능한 통화 심사를 제공합니다. 통화 가능한 통화 심사 기능을 사용하면 수신 핫라인 전화기에서 발신자 ID 정보에 따라 통화를 심사하여 심사 목록에 포함된 발신자만 연결되도록 할 수 있습니다.

핫라인 시스템 요구 사항

다음은 Unified Communications Manager에 대한 핫라인 시스템 요구 사항입니다.

- 클러스터의 각 서버에서 Unified Communications Manager 8.0(1) 이상
- MGCP Series POTS Phone(FXS)
- SCCP Series POTS Phone(FXS)



팁 Cisco Feature Navigator를 사용하여 특정 소프트웨어 릴리스, 기능 집합 또는 플랫폼을 지원하는 Cisco IOS 및 Catalyst OS 소프트웨어 이미지를 결정할 수 있습니다. Cisco Feature Navigator에 액세스하려면 <http://cfn.cloudapps.cisco.com/ITDIT/CFN/>로 이동합니다.

Cisco.com 계정이 없어도 Cisco Feature Navigator에 액세스할 수 있습니다.

핫라인 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	Cisco 통합 보고에 로그인하고 전화기 기능 목록 보고서를 실행하여 핫라인을 지원하는 전화기를 결정합니다.
단계 2	사용자 정의 소프트키 템플릿 만들기, 285 페이지	(선택 사항) 핫라인 전화기에서 기능을 제한하려면 원하는 기능만 허용하는 소프트키 템플릿을 만듭니다.
단계 3	전화기에서 핫라인 구성, 286 페이지	전화기를 핫라인 디바이스로 활성화합니다.
단계 4	라우트 클래스 신호 처리 작업 흐름 구성, 286 페이지	핫라인 기능을 지원 하도록 라우트 클래스 신호 처리를 구성합니다.

	명령 또는 동작	목적
단계 5	통화 전용 또는 수신 전용 핫라인 작업 흐름 구성, 290 페이지	선택 사항. 핫라인 전화를 발신 통화만 또는 종료 통화만으로 제한하려면 통화 및 수신 설정을 구성합니다.
단계 6	발신 검색 공간과 함께 통화 심사 구성, 293 페이지	선택 사항. 발신 검색 공간 및 파티션을 사용하여 핫라인 전화기에 대한 통화 차단 목록을 구성합니다.

사용자 정의 소프트키 템플릿 만들기

핫라인을 구성할 때 소프트키 템플릿을 사용자 정의하여 핫라인 전화기에서 사용하려는 기능만 표시할 수 있습니다.

Unified Communications Manager에는 통화 처리 및 애플리케이션을 위한 표준 소프트키 템플릿이 있습니다. 사용자 정의 소프트키 템플릿을 만드는 경우 표준 템플릿을 복사하고 필요한 대로 내용을 수정합니다.

시작하기 전에

[전화기 기능 목록 생성, 7 페이지](#)

프로시저

- 단계 1 장치 > 장치 설정 > 소프트키 템플릿을 선택합니다.
 - 단계 2 새로 추가를 클릭합니다.
 - 단계 3 드롭다운 목록에서 소프트키 템플릿을 선택하고 복사를 클릭하여 새 템플릿을 만듭니다.
 - 단계 4 소프트키 템플릿 이름 필드에 소프트키 템플릿을 식별하는 고유한 이름을 입력합니다.
 - 단계 5 템플릿 사용을 식별하는 설명을 입력합니다. 설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.
 - 단계 6 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.
- 참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.
- 단계 7 저장을 클릭합니다.
- 소프트키 템플릿이 복사되고 소프트키 템플릿 구성 창이 다시 표시됩니다.
- 단계 8 (선택 사항) 애플리케이션 추가 버튼을 클릭합니다.
 - 단계 9 Cisco Unified IP Phone LCD 화면에서 소프트키의 위치를 구성합니다.
 - 단계 10 구성을 저장하려면 저장을 클릭합니다.

전화기에서 핫라인 구성

이 절차를 사용하여 전화기를 핫라인 디바이스로 활성화합니다.

시작하기 전에

(선택 사항) 핫라인 전화기에서 사용할 수 있도록 설정할 기능만 표시하는 사용자 정의 소프트키 템플릿을 생성하려면 [사용자 정의 소프트키 템플릿 만들기, 285 페이지](#)의 내용을 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하고 핫라인 디바이스로 사용할 전화기를 선택합니다.

단계 3 핫라인 디바이스 확인란을 선택합니다.

단계 4 핫라인 전화기에 특별히 사용되는 사용자 정의 소프트키 템플릿을 만든 경우에는 소프트 템플릿 드롭다운 목록에서 소프트키 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

참고 디바이스폴에 소프트키 템플릿을 할당한 다음 해당 디바이스폴을 전화기에 할당할 수도 있습니다.

라우트 클래스 신호 처리 작업 흐름 구성

이 작업 흐름을 수행하여 핫라인 통화에 대한 라우트 클래스 신호 처리를 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	클러스터에서 라우트 클래스 신호 처리 활성화, 287 페이지	트렁크 및 게이트웨이의 라우트 클래스 신호 처리 기본값을 활성화로 설정합니다.
		참고 개별 트렁크 및 게이트웨이에 대한 설정은 클러스터 수준 기본값을 무시합니다. 이 서비스 매개 변수를 사용하여 클러스터에서 라우트 클래스 신호 처리를 활성화하는 경우에는 개별 트렁크 또는 게이트웨이에서도 라우트 클래스 신호 처리를 비활성화할 수 있습니다.

	명령 또는 동작	목적
단계 2	트렁크에서 라우트 클래스 신호 처리 활성화, 288 페이지	개별 트렁크에서 라우트 클래스 신호 처리를 활성화합니다.
단계 3	게이트웨이에서 라우트 클래스 신호 처리 활성화, 288 페이지	MGCP T1/CAS 또는 MGCP PRI 게이트웨이에서 라우트 클래스 신호 처리를 활성화합니다.
단계 4	핫라인 라우트 클래스에 대한 신호 처리 레이블 구성, 289 페이지	핫라인 라우트 클래스에 대한 SIP 신호 레이블을 구성합니다.
단계 5	핫라인 라우트 패턴에서 라우트 클래스 구성, 289 페이지	핫라인 통화를 라우팅하는 경로 패턴에 라우트 클래스를 구성합니다.
단계 6	핫라인 변환 패턴에서 라우트 클래스 구성, 290 페이지	선택 사항. 핫라인 통화에 변환 패턴을 사용하는 경우 변환 패턴에서 라우트 클래스를 구성합니다.

클러스터에서 라우트 클래스 신호 처리 활성화

라우트 클래스 트렁크 신호 처리 활성화 서비스 매개 변수를 **True**로 설정하는 경우 라우트 클래스 신호 처리를 지원하는 클러스터의 모든 트렁크 또는 게이트웨이에 대한 기본 라우트 클래스 신호 처리 설정이 활성화됨으로 설정됩니다.



참고 개별 트렁크 및 게이트웨이에 대한 설정은 클러스터 수준 기본값을 무시합니다. 이 서비스 매개 변수를 사용하여 클러스터에서 라우트 클래스 신호 처리를 활성화하는 경우에는 개별 트렁크 또는 게이트웨이에서도 라우트 클래스 신호 처리를 비활성화할 수 있습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 라우트 클래스 트렁크 신호 처리 활성화 서비스 매개 변수를 **True**로 설정합니다.
- 단계 3 저장을 클릭합니다.

다음에 수행할 작업

다음 절차를 사용하여 개별 트렁크 또는 게이트웨이에서 라우트 클래스 신호 처리를 구성합니다.

[트렁크에서 라우트 클래스 신호 처리 활성화, 288 페이지](#)

[게이트웨이에서 라우트 클래스 신호 처리 활성화, 288 페이지](#)

트렁크에서 라우트 클래스 신호 처리 활성화

이 절차를 사용하여 개별 트렁크에서 라우트 클래스 신호 처리를 활성화합니다. 개별 트렁크에 대한 구성은 클러스터 수준 서비스 매개 변수 설정을 무시합니다.

시작하기 전에

클러스터의 모든 트렁크에 대한 기본 라우트 클래스 신호 설정을 구성하려면 [클러스터에서 라우트 클래스 신호 처리 활성화, 287 페이지](#) 절차에 따라 클러스터 수준 서비스 매개 변수를 사용합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 트렁크.

단계 2 찾기를 클릭하고 라우트 클래스 신호 처리를 활성화할 SIP 트렁크를 선택합니다.

단계 3 라우트 클래스 신호 처리 활성화 드롭다운 목록 상자에서 다음 옵션 중 하나를 선택합니다.

- 기본값 - 이 트렁크는 라우트 클래스 신호 처리 활성화 서비스 매개 변수의 설정을 사용합니다.
- 끄기 - 이 트렁크에 대해 라우트 클래스 신호 처리가 비활성화됩니다.
- 켜기 - 이 트렁크에 대해 라우트 클래스 신호가 활성화됩니다.

단계 4 저장을 클릭합니다.

게이트웨이에서 라우트 클래스 신호 처리 활성화

이 절차를 사용하여 개별 MGCP PRI 또는 MGCP T1/CAS 게이트웨이에서 라우트 클래스 신호 처리를 활성화합니다. 개별 게이트웨이에 대한 구성은 클러스터 수준 서비스 매개 변수 설정을 무시합니다.

시작하기 전에

클러스터의 게이트웨이에 대한 기본 라우트 클래스 신호 설정을 구성하려면 [클러스터에서 라우트 클래스 신호 처리 활성화, 287 페이지](#) 절차에 따라 클러스터 수준 서비스 매개 변수를 사용합니다.

[트렁크에서 라우트 클래스 신호 처리 활성화, 288 페이지](#) 절차를 수행하여 개별 트렁크에 대한 라우트 클래스 신호 처리를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 게이트웨이

단계 2 찾기를 클릭하고 라우트 클래스 신호 처리를 구성할 게이트웨이를 선택합니다.

단계 3 라우트 클래스 신호 처리 활성화 드롭다운 목록 상자에서 다음 옵션 중 하나를 선택합니다.

- 기본값 - 이 게이트웨이는 클러스터 수준 라우트 클래스 신호 처리 활성화 서비스 매개 변수의 설정을 사용합니다.

- 끄기 - 이 게이트웨이에 대해 라우트 클래스 신호 처리가 비활성화됩니다.
- 켜기 - 이 게이트웨이에 대해 라우트 클래스 신호 처리가 활성화됩니다.

단계 4 음성 통화에 대한 음성 라우트 클래스를 인코딩하려면 음성 라우트 클래스 인코딩 확인란을 선택합니다.

단계 5 저장을 클릭합니다.

핫라인 라우트 클래스에 대한 신호 처리 레이블 구성

사용할 핫라인 라우트 클래스에 대한 SIP 신호 처리 레이블 값을 구성해야 합니다.

시작하기 전에

트렁크 및 게이트웨이에서 라우트 클래스 신호 처리를 활성화합니다. 자세한 내용은 [클러스터에서 라우트 클래스 신호 처리 활성화, 287 페이지](#)를 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 CallManager 서비스가 실행 중인 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 고급을 클릭합니다.

단계 5 **SIP** 라우트 클래스 명명 인증 기관 서비스 매개 변수 필드에 라우트 클래스를 나타내기 위해 SIP 신호 처리에 사용되는 레이블에 대한 명명 기관과 컨텍스트를 나타내는 값을 입력합니다. 기본값은 **cisco.com**입니다.

단계 6 **SIP** 핫라인 음성 라우트 클래스 레이블 서비스 매개 변수 필드에 핫라인 음성 라우트 클래스를 나타내는 레이블을 입력합니다. 기본값은 핫라인입니다.

단계 7 **SIP** 핫라인 데이터 라우트 클래스 레이블 서비스 매개 변수 필드에서 핫라인 데이터 라우트 클래스를 나타내는 레이블을 입력합니다. 기본값은 **ccdata**입니다.

단계 8 저장을 클릭합니다.

핫라인 라우트 패턴에서 라우트 클래스 구성

이 절차에서는 핫라인 디바이스와 관련된 통화 라우팅 지침에 대해 설명합니다. 네트워크에서 라우트 패턴 및 변환 패턴을 구성하는 방법에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 내용을 참조하십시오.

핫라인 통화를 라우팅할 것으로 예상되는 각 라우트 패턴에 대해 해당 라우트 패턴에 대한 라우트 클래스를 핫라인 음성 또는 핫라인 데이터로 설정해야 합니다.

시작하기 전에

[핫라인 라우트 클래스에 대한 신호 처리 레이블 구성, 289 페이지](#)

이 절차를 수행하기 전에 네트워크 통화 라우팅이 라우트 패턴을 사용하여 설정된 것으로 예상됩니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 라우트/헌트 > 라우트 패턴.

단계 **2** 찾기를 클릭하여 네트워크의 라우트 패턴 목록을 표시합니다.

단계 **3** 핫라인 통화를 라우팅하는 데 사용되는 각 TI/CAS 경로 패턴에 대해 다음을 수행합니다.

- a) 라우트 패턴 찾기 및 나열 창에서 라우트 패턴을 선택합니다.
 - b) 라우트 클래스 드롭다운 목록 상자에서 이 라우트 패턴에 대한 라우트 클래스로 핫라인 음성 또는 핫라인 데이터 중 하나를 선택합니다.
 - c) 저장을 클릭합니다.
-

핫라인 변환 패턴에서 라우트 클래스 구성

시작하기 전에

이 절차를 수행하기 전에 라우트 패턴 및 변환 패턴을 사용하여 네트워크 통화 라우팅을 설정해야 합니다.

[핫라인 라우트 패턴에서 라우트 클래스 구성, 289 페이지](#) 절차를 수행합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 변환 패턴.

단계 **2** 찾기를 클릭하여 클러스터의 변환 패턴을 표시합니다.

단계 **3** 핫라인 번호에서 사용하려는 각 변환 패턴에 대해 다음 단계를 수행합니다.

- a) 라우트 클래스 드롭다운 목록 상자에서 핫라인 음성 또는 핫라인 데이터 중 하나를 선택합니다.
 - b) 저장을 클릭합니다.
-

통화 전용 또는 수신 전용 핫라인 작업 흐름 구성

이 작업 흐름의 구성 예에서는 핫라인 전화기를 설정하여 전화를 걸거나 통화만 수신하는 방법에 대해 설명합니다.

프로시저

	명령 또는 동작	목적
단계 1	핫라인 통화 전용 수신 전용 파티션 구성, 291 페이지	두 개의 파티션을 만듭니다. 하나는 비어 있어야 하고 다른 하나는 새 CSS에 할당됩니다.
단계 2	핫라인 통화 전용 수신 전용 발신 검색 공간 구성, 291 페이지	새 발신 검색 공간을 만들고 새 파티션 중 하나를 이 CSS에 할당합니다. 이 CSS에는 다른 파티션이 포함되지 않습니다.
단계 3	다음 절차 중 하나를 수행합니다. <ul style="list-style-type: none"> • 핫라인 전화기에 통화 전용 구성, 292 페이지 • 핫라인 전화기에 수신 전용 구성, 292 페이지 	통화 전용으로 구성하려면 전화기 회선에 빈 파티션을 할당합니다. 수신만 구성하려면 새 CSS를 전화기에 할당합니다.

핫라인 통화 전용 수신 전용 파티션 구성

핫라인 전화기를 통화 전용으로 설정하거나 통화만 수신하도록 구성하려면 두 개의 파티션을 만들어야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 파티션.

단계 2 새로 추가를 클릭합니다.

단계 3 새 파티션을 만듭니다.

단계 4 파티션의 고유한 이름 및 설명을 입력합니다. 예를 들면 **IsolatedPartition**입니다.

참고 이 파티션은 CSS에 할당되지 않습니다.

단계 5 저장을 클릭합니다.

단계 6 2-5단계를 반복하여 두 번째 파티션을 만듭니다. 예를 들면 **EmptyPartition**입니다.

참고 이 파티션은 어떤 전화 회선에도 할당되지 않지만, NoRouteCSS에 할당됩니다.

핫라인 통화 전용 수신 전용 발신 검색 공간 구성

발신 검색을 생성하고 발신 검색 공간에 생성한 두 파티션 중 하나를 할당해야 합니다.

시작하기 전에

[핫라인 통화 전용 수신 전용 파티션 구성, 291 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 제어 클래스 > 발신 검색 공간.

단계 2 새로 추가를 클릭합니다.

단계 3 발신 검색 공간에 대한 이름 및 설명을 입력합니다.

단계 4 사용 가능한 파티션 목록 상자에서 화살표를 사용하여 빈 파티션 파티션을 선택합니다.

참고 파티션이 이 발신 검색 공간에만 할당되고 전화기 회선에 할당되지 않았는지 확인합니다.

단계 5 저장을 클릭합니다.

다음에 수행할 작업

다음 절차 중 하나를 수행합니다.

- [핫라인 전화기에 통화 전용 구성, 292 페이지](#)
- [핫라인 전화기에 수신 전용 구성, 292 페이지](#)

핫라인 전화기에 통화 전용 구성

파티션 및 발신 검색 공간을 설정한 경우 다음 단계를 수행하여 전화만 걸도록 핫라인 전화를 구성합니다.

시작하기 전에

[핫라인 통화 전용 수신 전용 발신 검색 공간 구성, 291 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 전화기.

단계 2 찾기를 클릭하고 핫라인 전화기를 선택합니다.

단계 3 왼쪽 탐색 창에서 전화 회선을 클릭합니다.

[디렉터리 번호 구성] 창이 표시됩니다.

단계 4 라우트 파티션드롭다운 목록에서 생성한 빈 파티션을 선택합니다.

단계 5 저장을 클릭합니다.

핫라인 전화기에 수신 전용 구성

발신 검색 공간 및 파티션을 이미 만든 경우에는 다음 단계를 수행하여 통화만 받도록 핫라인 전화기를 구성합니다.

시작하기 전에

[핫라인 통화 전용 수신 전용 발신 검색 공간 구성, 291 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하고 핫라인 전화기를 선택합니다.

단계 3 발신 검색 공간 드롭다운 목록에서 이전 절차에서 만든 새 CSS를 선택합니다.

단계 4 저장을 클릭합니다.

발신 검색 공간과 함께 통화 심사 구성

파티션에 있는 핫라인 전화기가 서로에게 전화를 걸 수 있도록 하려는 핫라인 전화기에만 해당하는 고유한 CSS를 할당하여 intra-switch(회선 간) 핫라인 통화에 대한 전화 조회를 구성합니다.



참고 각 패턴이 허용 또는 화면으로 표시할 각 번호 패턴과 일치하는 변환 패턴을 생성하여 전화 조회를 구성할 수도 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	핫라인 통화 심사에 대한 파티션 구성, 293 페이지	핫라인 전화 회선에 대한 새 파티션을 생성합니다.
단계 2	핫라인 통화 심사에 대한 발신 검색 공간 생성, 294 페이지	조회 목록에 대한 새 CSS를 만듭니다. CSS에는 허용하려는 핫라인 번호만 있는 파티션이 포함되어야 합니다.
단계 3	통화 심사에 대한 핫라인 전화기 구성, 295 페이지	새 CSS 및 파티션을 핫라인 전화기에 할당합니다.

핫라인 통화 심사에 대한 파티션 구성

발신 검색 공간을 사용하여 핫라인 전화기에서 통화 차단을 구성하려면 허용하려는 유일한 핫라인 번호를 가진 파티션을 설정해야 합니다.

핫라인 통화 차단 목록에 대한 새 파티션을 생성해야 하는 경우 다음 절차를 수행합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 파티션.

단계 2 새로 추가를 클릭하여 새 파티션을 생성합니다.

단계 3 파티션 이름, 설명 필드에 경로 플랜에 고유한 파티션 이름을 입력합니다.

파티션 이름에는 영숫자 문자는 물론 공백, 하이픈(-) 및 밑줄(_)을 사용할 수 있습니다. 파티션 이름에 대한 지침은 온라인 도움말을 참조하십시오.

단계 4 파티션 이름 뒤에 쉼표(,)를 입력하고 동일한 줄에 파티션 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\), 꺾쇠괄호(<>) 또는 대괄호([])는 사용할 수 없습니다.

설명을 입력하지 않으면 Cisco Unified Communications Manager에서 자동으로 이 필드에 파티션 이름을 입력합니다.

단계 5 여러 파티션을 생성하려면 각 파티션 항목마다 한 행을 사용합니다.

단계 6 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.

시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성 상태로 유지됩니다.

단계 7 구성할 다음 라디오 버튼 중 하나를 선택하고 시간대를 구성합니다.

- 시작 디바이스—이 라디오 버튼을 선택하면 시스템은 발신 디바이스의 표준 시간대를 시간 일정과 비교하여 파티션을 수신 통화를 받는 데 사용할 수 있는지 여부를 확인합니다.
- 특정 표준 시간대—이 라디오 버튼을 선택한 후에 드롭다운 목록에서 표준 시간대를 선택합니다. 시스템은 선택한 표준 시간대를 시간 일정과 비교하여 수신 통화를 받는 데 파티션을 사용할 수 있는지 여부를 확인합니다.

단계 8 저장을 클릭합니다.

핫라인 통화 심사에 대한 발신 검색 공간 생성

다음 절차를 수행하여 통화 차단 목록에서 핫라인 전화기에 대한 새 발신 검색 공간을 생성합니다. 이 CSS에 대해 선택하는 파티션의 유일한 핫라인 번호는 통화 차단 목록에 허용하려는 핫라인 번호여야 합니다. 이 CSS의 파티션에는 핫라인 번호를 포함하지 않아야 합니다.

시작하기 전에

[핫라인 통화 심사에 대한 파티션 구성, 293 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 발신 검색 공간.

단계 2 새로 추가를 클릭합니다.

단계 3 이름 필드에 이름을 입력합니다.

각 발신 검색 공간 이름은 시스템에 고유해야 합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.

단계 4 설명 필드에 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.

단계 5 사용 가능한 파티션 드롭다운 목록에서 다음 단계 중 하나를 수행합니다.

- 단일 파티션의 경우 해당 파티션을 선택합니다.
- 여러 파티션의 경우 컨트롤(**CTRL**) 키를 누른 상태에서 해당 파티션을 선택합니다.

단계 6 상자 사이에서 아래쪽 화살표를 선택하여 선택한 파티션 필드로 파티션을 이동합니다.

단계 7 (선택 사항) 선택한 파티션 상자 오른쪽의 화살표 키를 사용하여 선택한 파티션의 우선 순위를 변경합니다.

단계 8 저장을 클릭합니다.

통화 심사에 대한 핫라인 전화기 구성

핫라인 통화 차단에 대한 발신 검색 공간 및 파티션을 이미 구성한 경우 이 절차를 수행하여 발신 검색 공간 및 파티션을 핫라인 전화기에 할당합니다.

시작하기 전에

[핫라인 통화 심사에 대한 발신 검색 공간 생성, 294 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하고 핫라인 전화기를 선택합니다.

단계 3 발신 검색 공간 드롭다운 목록에서 핫라인 통화 차단 목록에 대해 생성한 새 발신 검색 공간을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 왼쪽 탐색 창에서 핫라인 통화에 사용할 전화 회선을 클릭합니다.

[디렉터리 번호 구성] 창이 표시됩니다.

단계 6 경로 파티션 드롭다운 목록에서 설정하는 발신 검색 공간에 포함되는 파티션을 선택합니다.

단계 7 저장을 클릭합니다.

핫라인 문제 해결

다음 표에서는 핫라인 통화가 올바르게 다이얼되지 않는 경우의 문제 해결 정보를 제공합니다.

표 25: 핫라인 문제 해결 - 통화가 올바르게 다이얼되지 않음

문제	해결 방법
다이얼톤	PLAR 구성을 확인합니다.
다시 걸기 신호음 또는 VCA(클러스터 내 통화)	<ul style="list-style-type: none"> • PLAR 구성을 확인합니다. • 양쪽 끝의 전화기가 모두 핫라인 전화기로 구성되어 있는지 확인합니다.
다시 걸기 신호음 또는 VCA(클러스터 간 또는 TDM 통화)	<ul style="list-style-type: none"> • PLAR 구성을 확인합니다. • 양쪽 끝의 전화기가 모두 핫라인 전화기로 구성되어 있는지 확인합니다. • 트렁크에서 라우트 클래스 신호 처리가 활성화되어 있는지 확인합니다. • CAS 게이트웨이에서 라우트 클래스 변환의 구성을 확인합니다.

다음 표에서는 발신자 ID를 기반으로 한 전화 조회가 작동하지 않는 경우의 문제 해결 정보를 제공합니다.

표 26: 문제 해결 핫라인 - 발신자 ID 문제를 기반으로 전화 조회

문제	해결 방법
통화 허용되지 않음	<ul style="list-style-type: none"> • 발신자 ID를 확인합니다. • 화면 CSS에 패턴을 추가합니다.
통화 허용됨	화면 CSS에서 패턴을 제거합니다.



24 장

단축 다이얼

- 단축 다이얼 개요, 297 페이지
- 단축 다이얼 구성 작업 흐름, 298 페이지

단축 다이얼 개요

관리자는 전화기의 단축 다이얼 번호를 구성하여 사용자에게 단축 다이얼 버튼을 제공하거나 특정 사용자가 할당되지 않은 전화기를 구성할 수 있습니다. 사용자는 Cisco Unified Communications 셀프 서비스 포털을 사용하여 전화기에서 단축 다이얼 버튼을 변경합니다. 단축 다이얼 항목을 구성할 때 일부 단축 다이얼 항목은 IP 전화기의 단축 다이얼 버튼에 할당됩니다. 나머지 단축 다이얼 항목은 단축 다이얼 지정에 사용됩니다. 사용자가 다이얼을 누르기 시작하면 단축 다이얼 소프트키가 표시되고, 사용자는 단축 다이얼의 해당 색인(코드)을 입력하여 모든 단축 다이얼 항목에 액세스할 수 있습니다.

전화기의 단축 다이얼 설정은 전화기의 물리적 버튼과 연결되는 반면, 단축 다이얼 설정은 전화기 버튼과 연결되지 않습니다.

일시 중지가 있는 단축 다이얼 프로그래밍

단축 다이얼에서 쉼표를 프로그래밍하여 FAC(Forced Authorization Code), CMC(Client Matter Code), 전화 걸기 일시 중지 또는 추가 숫자(예: 사용자 내선 번호, 회의 액세스 번호 또는 음성메일 암호)가 필요한 대상에 연결할 수 있습니다. 단축 다이얼 내에서 각 쉼표(.)는 다음을 나타냅니다.

- 대상 통화 주소를 FAC 또는 CMC 코드와 구분하는 구분 기호
- 사후 연결 DTMF 숫자를 보내기 2초 전 일시 중지

예를 들어 FAC 및 CMC 코드와, 그 다음에 IVR 프롬프트가 포함된 단축 다이얼을 원하는 경우 다음과 같이 입력합니다.

- 발신 번호는 91886543입니다.
- FAC 코드는 8787입니다.
- CMC 코드는 5656입니다.

- IVR 응답은 987989#이며 통화 연결 후 4초 내에 입력해야 합니다.

이 경우 **91886543,8787,5656,,987989#**을 단축 다이얼로 프로그래밍합니다.

단축 다이얼 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	단축 다이얼 기능을 지원하는 디바이스를 식별하는 보고서를 생성합니다.
단계 2	단축 다이얼 구성, 298 페이지	단축 다이얼 번호를 구성합니다.

단축 다이얼 구성

총 199개의 단축 다이얼 및 단축 다이얼 설정을 구성할 수 있습니다. 전화기의 실제 버튼에 대해 단축 다이얼 설정을 구성합니다. 단축 다이얼을 사용하여 액세스하는 단축 다이얼 번호에 대해 단축 다이얼 설정을 구성합니다. 동일한 창에서 단축 다이얼 항목과 단축 다이얼 색인을 구성할 수 있습니다.

또한 사후 연결 DTMF 숫자와 FAC, CMC 코드를 단축 다이얼의 일부로 구성할 수 있습니다.

단축 다이얼을 구성하려면 다음 단계를 수행합니다.



참고 일부 Cisco Unified IP Phone은 단축 다이얼을 지원하지 않습니다. 자세한 내용은 전화기 사용 설명서를 참조하십시오.

시작하기 전에

[전화기 기능 목록 생성, 7 페이지](#)

프로시저

- 단계 1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기 검색 기준을 입력하고 찾기를 클릭합니다. 단축 다이얼 버튼을 구성하려는 전화기를 선택합니다.
- 단계 2** 전화기 구성 창 맨 위의 관련 링크 드롭다운 목록 상자에서 단축 다이얼 추가/업데이트를 선택하고 이동을 클릭합니다.
전화기의 단축 다이얼 구성 창이 표시됩니다.
- 단계 3** 번호 필드에 사용자가 단축 다이얼 버튼 또는 단축 다이얼을 위한 단축 다이얼 색인을 누를 때 시스템에서 전화를 걸 번호를 입력합니다. 0~9의 숫자, *, #, 및 국제 이스케이프 문자에 해당하는 +를 입력할 수 있습니다. 단축 다이얼에 다이얼 일시 중지를 포함하려면 DTMF 숫자를 보내기 전에 구분 기

호로 사용할 수 있는 쉼표(.)를 입력할 수 있습니다. 포함하는 각 쉼표는 2초의 추가 일시 중지 시간을 나타냅니다. 예를 들어 두 개 쉼표(,,)는 일시 중지 시간 4초를 나타냅니다. 쉼표를 사용하면 단축 다이얼 문자열에서 FAC 및 CMC를 다른 숫자와 구분할 수 있습니다.

참고 단축 다이얼 문자열에 FAC 및 CMC를 포함할 때는 다음 요구 사항을 충족해야 합니다.

- FAC는 단축 다이얼 문자열에서 항상 CMC보다 앞에 있어야 합니다.
- FAC 및 DTMF 숫자가 있는 단축 다이얼에는 단축 다이얼 레이블이 필요합니다.
- 문자열의 FAC 숫자와 CMC 숫자 사이에는 쉼표 한 개만 허용됩니다.

단계 4 레이블 필드에 단축 다이얼 버튼 또는 단축 다이얼 번호에 표시할 텍스트를 입력합니다.

참고 일부 전화기에는 이 필드를 사용할 수 없습니다. Cisco Unified IP Phone에서 이 필드를 사용할 수 있는지 여부를 확인하려면 전화기 모델에 대한 사용자 설명서를 참조하십시오.

단계 5 (선택 사항) 단축 다이얼에 일시 중지를 구성하는 경우 FAC, CMC 및 DTMF 숫자가 전화기 화면에 표시되지 않도록 레이블을 추가해야 합니다.



25 장

WebDialer

- WebDialer 개요, 301 페이지
- WebDialer 사전 요건, 301 페이지
- WebDialer 구성 작업 흐름, 302 페이지
- WebDialer 상호 작용, 313 페이지
- WebDialer 제한 사항, 314 페이지
- WebDialer 문제 해결, 314 페이지

WebDialer 개요

Cisco WebDialer는 Unified Communications Manager노드에 설치되며 Unified Communications Manager와 함께 사용됩니다. Cisco Unified IP Phone 사용자가 웹 및 데스크톱 애플리케이션에서 전화를 걸 수 있습니다.

Cisco WebDialer는 회사 디렉터리의 하이퍼링크된 전화 번호를 사용하므로 사용자가 웹 페이지에서 통화할 사람의 전화 번호를 클릭하여 전화를 걸 수 있습니다. Cisco WebDialer는 IPv4 및 IPv6 주소 지정을 모두 지원합니다.

Cisco Unified Communications 셀프 서비스 포털에의 디렉터리 창에서 다음과 비슷한 URL을 사용하여 Cisco WebDialer를 시작합니다.

```
https://<IP address of Cisco Unified Communications Manager server>:8443/webdialer/  
Webdialer
```

Cisco WebDialer 화면에서 로그인을 클릭하여 WebdDialer 시스템에 로그인합니다. 새로운 팝업 창에서 Unified Communications Manager 사용자 **ID** 및 암호를 입력하여 필요한 전화 걸기 작업을 수행할 수 있습니다.

WebDialer 사전 요건

다음은 Cisco WebDialer에 필요한 소프트웨어 구성 요소입니다.

- C지원 TI Cisco Unified IP Phone

WebDialer 구성 작업 흐름

시작하기 전에

- [WebDialer 사전 요건, 301 페이지](#)을(를) 검토합니다.

프로시저

	명령 또는 동작	목적
단계 1	WebDialer 활성화, 303 페이지	Cisco WebDialer 서비스를 활성화합니다.
단계 2	(선택 사항) WebDialer 추적 활성화, 303 페이지	WebDialer 추적을 보려면 추적을 활성화합니다.
단계 3	(선택 사항) WebDialer 서블릿 구성, 304 페이지	WebDialer 서블릿을 구성합니다.
단계 4	(선택 사항) Redirector 서블릿 구성, 305 페이지	HTTPS 인터페이스를 통해 HTML을 사용하여 개발하는 다중 클러스터 애플리케이션을 사용하는 경우 리디렉터 서블릿을 구성합니다.
단계 5	(선택 사항) WebDialer 애플리케이션 서버 구성, 305 페이지	Cisco WebDialer에 대한 리디렉터를 구성합니다.
단계 6	(선택 사항) CTI에 보안 TLS 연결 구성, 306 페이지 에 대해 다음 하위 작업을 수행합니다. <ul style="list-style-type: none"> • WDSecureSysUser 애플리케이션 사용자 구성, 306 페이지 • CAPF 프로파일 구성, 197 페이지 • Cisco WebDialer 웹 서비스 구성, 199 페이지 	WebDialer는 WDSecureSysUser 애플리케이션 사용자 인증서를 사용하여 CTI에 보안 TLS 연결을 설정한 후 전화를 겁니다. 시스템을 혼합된 모드에서 실행하는 경우 이 절차를 수행합니다.
단계 7	Webdialer용 언어 로캘 구성, 309 페이지	Cisco 통합 커뮤니케이션 자가 관리 포털 메뉴에서 로캘 필드를 설정하여 Web Dialer에서 표시할 언어를 결정합니다.
단계 8	WebDialer 알람 구성, 309 페이지	Web Dialer 기능에 문제가 있는 경우 관리자에게 경고합니다.
단계 9	(선택 사항) 애플리케이션 다이얼 규칙 구성, 310 페이지	애플리케이션에 여러 클러스터가 필요한 경우 애플리케이션 다이얼 규칙을 구성합니다.
단계 10	표준 CCM 최종 사용자 그룹에 사용자 추가, 311 페이지	WebDialer 사용자를 Cisco Unified Communications Manager의 표준 최종 사용자 그룹에 추가합니다.

	명령 또는 동작	목적
단계 11	(선택 사항) 프록시 사용자 구성, 311 페이지 에 대해 다음 하위 작업을 수행합니다. <ul style="list-style-type: none"> • WebDialer 최종 사용자 추가, 312 페이지 • 인증 프록시 권한 할당, 312 페이지 	makeCallProxy HTML over HTTP 인터페이스를 사용하여 Cisco Web Dialer를 사용할 애플리케이션을 개발하는 경우 프록시 사용자를 만듭니다.

WebDialer 활성화

프로시저

- 단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다.도구 > 서비스 활성화.
- 단계 2 서버 그룹다운 목록에서 나열된 Unified Communications Manager 서버를 선택합니다.
- 단계 3 CTI 서비스에서 **Cisco WebDialer** 웹 서비스 확인란을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다.도구 > 제어 센터 - 기능 서비스를 선택하여 CTI 관리자 서비스가 활성 상태이며 시작 모드인지 확인합니다.
- Webdialer가 제대로 작동하려면 CTI 관리자 서비스를 활성화하고 시작 모드에 있어야합니다.

다음에 수행할 작업

[Webdialer용 언어 로캘 구성, 309 페이지](#) 또는 다음 선택적 작업 중 일부 또는 전부를 완료합니다.

- [WebDialer 추적 활성화, 303 페이지](#)
- [WebDialer 서블릿 구성, 304 페이지](#)
- [Redirector 서블릿 구성, 305 페이지](#)
- [WebDialer 애플리케이션 서버 구성, 305 페이지](#)
- [CTI에 보안 TLS 연결 구성, 306 페이지](#)

WebDialer 추적 활성화

Cisco WebDialer 추적을 활성화하려면 Cisco 유니파이드 Serviceability 관리 애플리케이션을 사용합니다. 추적 설정은 WebDialer 및 Redirector 서블릿 모두에 적용됩니다. 추적을 수집하려면 실시간 모니터링 도구(RTMT)를 사용합니다.

WebDialer 추적 파일에 액세스하려면 다음 CLI 명령을 사용합니다.

- `file get activelog tomcat/logs/webdialer/log4j`
- `file get activelog tomcat/logs/redirector/log4j`

추적에 대한 자세한 내용은 *Cisco Unified Serviceability* 관리 지침서를 참조하십시오.

시작하기 전에

[WebDialer 활성화, 303 페이지](#)

프로시저

단계 1 Cisco Unified Communications Manager 애플리케이션의 탐색 드롭다운 목록에서 **Cisco** 통합 서비스 가용성을 선택한 다음 이동을 클릭합니다.

단계 2 추적 > 구성을 클릭합니다.

단계 3 서버 드롭다운 목록에서 추적을 활성화할 서버를 선택합니다.

단계 4 서비스 그룹 드롭다운 목록에서 CTI 서비스를 선택합니다.

단계 5 서비스 드롭다운 목록에서 **Cisco WebDialer** 웹 서비스를 선택합니다.

단계 6 추적 구성 창에서 문제 해결 요구 사항에 따라 추적 설정을 변경합니다.

참고 WebDialer 추적 구성 설정에 대한 자세한 내용은 *Cisco Unified Serviceability* 관리 지침서를 참조하십시오.

단계 7 저장을 클릭합니다.

WebDialer 서버릿 구성

WebDialer 서버릿은 특정 클러스터의 Cisco Unified Communications Manager 사용자가 통화를 하고 완료할 수 있는 Java 서버릿입니다.

시작하기 전에

[WebDialer 활성화, 303 페이지](#)

프로시저

단계 1 시스템 > 서비스 매개 변수를 선택합니다.

단계 2 서버 드롭다운 목록에서 Cisco WebDialer 웹 서비스 매개 변수를 구성할 Cisco Unified Communications Manager 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco WebDialer** 웹 서비스를 선택합니다.

단계 4 관련 WebDialer Web Service 매개 변수를 구성합니다. 매개 변수에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 5 새 매개 변수 값을 적용하려면 Cisco WebDialer 웹 서비스를 다시 시작합니다.

Redirector 서블릿 구성

Redirector 서블릿은 Java 기반 Tomcat 서블릿입니다. Cisco WebDialer 사용자가 요청하면 Redirector 서블릿은 Cisco Unified Communications Manager 클러스터에서 해당 요청을 찾아 Cisco Unified Communications Manager 클러스터에 있는 특정 Cisco WebDialer 서버로 요청을 재전송합니다. Redirector 서블릿은 HTTPS 인터페이스를 통해 HTML을 사용하여 개발된 멀티 클러스터 애플리케이션에만 사용할 수 있습니다.

시작하기 전에

[WebDialer 활성화, 303 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
 - 단계 2 서버 드롭다운 목록에서 Redirector 서블릿을 구성할 Cisco Unified Communications Manager 서버를 선택합니다.
 - 단계 3 서비스 드롭다운 목록에서 Cisco WebDialer 웹 서비스를 선택합니다.
 - 단계 4 관련 WebDialer Web Service 매개 변수를 구성합니다. 매개 변수에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
 - 단계 5 새 매개 변수 값을 적용하려면 Cisco WebDialer 웹 서비스를 다시 시작합니다.

WebDialer Web Service에 대한 자세한 내용은 *Cisco Unified Serviceability* 관리 지침서를 참조하십시오.

WebDialer 애플리케이션 서버 구성

애플리케이션 서버는 Redirector 서블릿을 구성해야 합니다. 리디렉터는 클러스터에 Cisco Unified Communications Manager 서버가 여러 개 구성되어 있을 때만 필요합니다.

시작하기 전에

[WebDialer 활성화, 303 페이지](#)

프로시저

-
- 단계 1 Cisco Unified Communications Manager 관리 애플리케이션 서버 창에서 시스템 > 애플리케이션 서버를 선택합니다.
 - 단계 2 애플리케이션 서버 유형 드롭다운 목록에서 **Cisco WebDialer** 애플리케이션 서버를 선택합니다.

Cisco WebDialer 웹 서비스에 대한 서비스 매개 변수 구성 창 **WebDialers** 목록 필드에 서버가 나타납니다.

CTI에 보안 TLS 연결 구성

WebDialer는 WDSecureSysUser 애플리케이션 사용자 인증서를 사용하여 CTI에 보안 TLS 연결을 설정한 후 전화를 겁니다. WDSecureSysUser 애플리케이션 사용자를 구성하여 보안 TLS 연결을 설정하려면 다음 작업을 수행합니다.

시작하기 전에

- Cisco CTL 클라이언트를 설치하고 구성합니다. CTL 클라이언트에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 보안 설명서](#)의 내용을 참조하십시오.
- 엔터프라이즈 매개 변수 구성 창의 클러스터 보안 모드가 1(혼합 모드)인지 확인합니다. 시스템을 혼합 모드에서 작동하면 시스템의 다른 보안 기능에 영향을 미칩니다. 시스템이 현재 혼합 모드에서 실행되지 않으면, 이러한 상호 작용을 이해할 때까지 혼합 모드로 전환하지 마십시오. 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 보안 설명서](#)의 내용을 참조하십시오.
- 클러스터 SIPOAuth 모드 필드가 활성화됨으로 설정되어 있는지 확인합니다.
- 첫 번째 노드에서 Cisco Certificate Authority Proxy Function 서비스를 활성화합니다.
- [WebDialer 활성화, 303 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	WDSecureSysUser 애플리케이션 사용자 구성, 306 페이지	WDSecureSysUser 애플리케이션 사용자를 구성합니다.
단계 2	CAPF 프로파일 구성, 197 페이지	WDSecureSysUser 애플리케이션 사용자에 대한 CAPF 프로파일을 구성합니다.
단계 3	Cisco WebDialer 웹 서비스 구성, 199 페이지	Cisco WebDialer 웹 서비스에 대한 서비스 매개 변수를 구성합니다.

WDSecureSysUser 애플리케이션 사용자 구성

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 애플리케이션 사용자.

단계 2 찾기를 클릭합니다.

단계 3 애플리케이션 사용자 찾기 및 나열 창에서 **WDSecureSysUser**를 선택합니다.

단계 4 애플리케이션 사용자 구성 창의 필드를 구성하고 저장을 클릭합니다.

다음에 수행할 작업

[CAPF 프로파일 구성, 197 페이지](#)

CAPF 프로파일 구성

CAPF(Certificate Authority Proxy Function)는 보안 인증서를 발급하고 인증하는 작업을 수행하는 구성 요소입니다. 애플리케이션 사용자 CAPF 프로파일을 만들 때 프로파일은 구성 세부 정보를 사용하여 애플리케이션에 대한 보안 연결을 엮습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.사용자 관리 > 애플리케이션 사용자 CAPF 프로파일.

단계 2 다음 작업 중 하나를 수행합니다.

- 새 CAPF 프로파일을 추가하려면 찾기 창에서 새로 추가를 클릭합니다.
- 기존 프로파일을 복사하려면 적절한 프로파일 찾아 복사 열에 있는 해당 레코드에 대한 복사 아이콘을 클릭합니다.

기존 항목을 업데이트하려면 해당 프로파일을 찾아 표시합니다.

단계 3 관련 CAPF 프로파일 필드를 구성하거나 업데이트합니다. 필드 및 해당 구성 옵션에 대한 정보는 관련 항목 섹션을 참조하십시오.

단계 4 저장을 클릭합니다.

단계 5 보안을 사용하려는 각 애플리케이션 및 최종 사용자에 대해 절차를 반복합니다.

CAPF 프로파일 설정

설정	설명
애플리케이션 사용자	드롭다운 목록에서 CAPF 작업의 애플리케이션 사용자를 선택합니다. 이 설정은 이 설정은 최종 사용자 CAPF 프로파일 창에 나타나지 않습니다.
최종 사용자 ID	드롭다운 목록에서 CAPF 작업의 최종 사용자를 선택합니다. 이 설정은 구성된 이 설정은 애플리케이션 CAPF 프로파일 창에 나타나지 않습니다.

설정	설명
인스턴스 ID	1 ~ 128자의 영숫자(a-z, A-Z, 0-9)를 입력합니다. 인스턴스 ID는 인증서 작업의 사용 다중 애플리케이션 연결(인스턴스)을 구성할 수 있습니다. 애플리케이션과 CTIManager(우) 또는 서버(애플리케이션 사용자의 경우)에서 실행되는 각 인스턴스에 고유 인증서 ID가 할당됩니다. 이 필드는 웹 서비스 및 애플리케이션을 지원하는 CTIManager에 보안 연결(Secure Connection)을 설정할 때 필수 인스턴스 ID와 관련되어 있습니다.
인증서 작업	드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> 보류 중인 작업 없음 - 이 메시지는 인증서 작업이 발생하지 않을 때 표시됩니다. 설치/업그레이드 - 이 옵션은 새 인증서를 설치하거나 애플리케이션의 기존 LSC를 업데이트합니다.
인증 모드	설치/업그레이드 인증서 작업에 대한 인증 모드는 [인증 문자열별]이며, 이는 사용자 인증 문자열을 입력하는 경우에만 CAPF에서 LSC 설치/업그레이드 또는 문제 해결을 수행합니다.
인증 문자열	자체 인증 문자열을 생성하려면 고유 문자열을 입력합니다. 각 문자열은 4~10자를 포함해야 합니다. LSC 인증서를 설치 또는 업그레이드하려면 관리자가 애플리케이션 PC의 JTAPI/TSAPI 인증 문자열을 입력하는 경우에만 CAPF에서 LSC 설치/업그레이드 또는 문제 해결을 수행합니다. 인증 문자열은 일회용으로, 인스턴스에 대한 문자열을 사용한 후에는 다시 사용할 수 없습니다.
문자열 생성	인증 문자열을 자동으로 생성하려면 이 버튼을 클릭합니다. 4~10자리 인증 문자열이 생성됩니다.
키 크기(비트)	드롭다운 목록에서 인증서의 키 크기를 선택합니다. 기본 설정은 1024입니다. 기타 키 크기는 2048, 3072, 4096, 8192, 16384입니다. 키 생성은 우선 순위가 낮게 설정되어 있어, 작업이 수행되는 동안 애플리케이션이 사용할 수 없습니다.
작업 완료 시간	이 필드는 모든 인증서 작업을 지원하며, 해당 작업을 완료해야 하는 날짜 및 시간을 지정합니다. 표시되는 값이 첫 번째 노드에 적용됩니다. 이 설정은 인증서 작업을 완료해야 하는 기본 일수를 지정하는 CAPF 작업 유효 기간과 함께 사용됩니다. 이 매개 변수를 언제든지 업데이트할 수 있습니다.
인증서 작업 상태	이 필드에는 인증서 작업의 진행 상태(예: 보류 중, 실패 또는 성공)가 표시됩니다. 이 필드에 표시되는 정보를 변경할 수 없습니다.

Cisco IP 매니저 어시스턴트 (Cisco IPMA) 구성

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 Cisco WebDialer 웹 서비스가 활성화된 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco WebDialer** 웹 서비스를 선택합니다.

매개 변수 목록이 나타납니다.

단계 4 CTIManager 연결 보안 플래그 및 CAPF 프로파일 인스턴스 ID로 이동하고 보안 연결을 위해 CTIManager 매개 변수로 업데이트합니다.

매개 변수 설명을 보려면 매개 변수 이름 링크를 클릭합니다.

참고 CTIManager는 IPv4 및 IPv6 주소를 지원합니다.

단계 5 저장을 클릭합니다.

단계 6 서비스가 활성화된 각 서버에서 이 절차를 반복합니다.

다음에 수행할 작업

[공유 회선에 대한 Manager Assistant 작업 흐름, 188 페이지](#)를 참조하여 완료할 다음 작업을 결정합니다.

Webdialer용 언어 로캘 구성

Cisco Unified Communications 셀프 서비스 포털을 사용하여 Cisco WebDialer용 언어 로캘을 구성합니다. 기본 언어는 영어입니다.

시작하기 전에

[WebDialer 활성화, 303 페이지](#)

프로시저

단계 1 Cisco 통합 커뮤니케이션 자가 관리 포털에서 일반 설정 탭을 클릭합니다.

단계 2 언어를 클릭합니다.

단계 3 표시 언어 드롭다운 목록에서 언어 로캘을 선택한 다음 저장을 클릭합니다.

WebDialer 알람 구성

Cisco WebDialer 서비스는 Cisco Tomcat을 사용하여 알람을 생성합니다.

시작하기 전에

[Webdialer용 언어 로캘 구성, 309 페이지](#)

프로시저

-
- 단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다.알람 > 구성.
- 단계 2 서버 드롭다운 목록에서 알람을 구성하려는 서버를 선택한 다음 이동을 클릭합니다.
- 단계 3 서비스 그룹 드롭다운 목록에서 플랫폼 서비스를 선택한 다음 이동을 선택합니다.
- 단계 4 서비스 드롭다운 목록에서 **Cisco Tomcat**을 선택한 다음 이동을 클릭합니다.
- 단계 5 구성에서 클러스터를 지원하는 경우 모든 노드에 적용 확인란을 선택하여 클러스터의 모든 노드에 알람 구성을 적용합니다.
- 단계 6 모니터링 및 이벤트 수준에 대한 설명을 포함하는 알람 구성 설정에 설명된 대로 설정을 구성합니다.
- 참고 알람 구성 설정에 대한 자세한 내용은 *Cisco 통합 서비스 가용성* 설명서를 참조하십시오.
- 단계 7 저장을 클릭합니다.
-

다음에 수행할 작업

[표준 CCM 최종 사용자 그룹에 사용자 추가, 311 페이지](#) 또는 (선택 사항) 애플리케이션에 여러 개의 클러스터가 필요한 경우 [애플리케이션 다이얼 규칙 구성, 310 페이지](#)의 내용을 참조하십시오.

애플리케이션 다이얼 규칙 구성

시작하기 전에

[WebDialer 알람 구성, 309 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 다이얼 규칙 > 애플리케이션 다이얼 규칙.
- 단계 2 이름 필드에 다이얼 규칙의 이름을 입력합니다.
- 단계 3 설명 필드에 다이얼 규칙에 대한 설명을 입력합니다.
- 단계 4 시작 숫자 필드에 이 애플리케이션 다이얼 규칙을 적용할 디렉터리 번호의 첫 번째 숫자를 입력합니다.
- 단계 5 자릿수 필드에 애플리케이션 다이얼 규칙을 적용할 착신 번호의 길이를 입력합니다.
- 단계 6 제거할 총 자릿수 필드에 Unified Communications Manager가 이 다이얼 규칙에 적용되는 착신 번호 시작 부분에서 제거할 자릿수를 입력합니다.
- 단계 7 패턴 있는 접두사 필드에 이 애플리케이션 다이얼 규칙에 적용되는 착신 번호 앞에 추가할 패턴을 입력합니다.
- 단계 8 애플리케이션 다이얼 규칙에서 다이얼 규칙 우선 순위를 높음, 낮음 또는 중간으로 선택합니다.

단계 9 저장을 클릭합니다.

표준 CCM 최종 사용자 그룹에 사용자 추가

Unified Communications Manager의 사용자 디렉터리 창에서 Cisco WebDialer 링크를 사용하려면 각 사용자를 표준 Unified Communications Manager 최종 사용자 그룹에 추가해야 합니다.

프로시저

단계 1 사용자 관리 > 사용자 그룹을 선택합니다.

단계 2 사용자 그룹 찾기 및 나열 창에서 찾기를 클릭합니다.

단계 3 표준 CCM 최종 사용자를 클릭합니다.

단계 4 사용자 그룹 구성 창에서 그룹에 최종 사용자 추가를 클릭합니다.

단계 5 사용자 찾기 및 나열 창에서 찾기를 클릭합니다. 특정 사용자에 대한 조건을 입력할 수 있습니다.

단계 6 사용자 그룹에 한 명 이상의 사용자를 추가하려면 다음 단계 중 하나를 완료합니다.

- 한 명 이상의 사용자를 추가하려면 추가할 각 사용자 옆에 있는 확인란을 선택하고 선택한 항목 추가를 클릭합니다.
- 모든 사용자를 추가하려면 모두 선택을 클릭한 다음 선택한 항목 추가를 클릭합니다.

사용자 그룹 구성 창의 그룹 내 사용자 테이블에 사용자가 표시됩니다.

프록시 사용자 구성

makeCallProxy HTML over HTTP 인터페이스를 사용하여 Cisco Web Dialer를 사용할 애플리케이션을 개발하는 경우 프록시 사용자를 만듭니다. makeCallProxy 인터페이스에 대한 자세한 내용은 *Cisco WebDialer API* 참조 설명서에서 makeCallProxy 섹션을 참조하십시오.



참고 MakeCallProxy HTTP 메서드는 WebDialer 서비스의 서비스 매개 변수입니다. 이 매개 변수는 MakeCallProxy API가 받아들이는 HTTP 메서드를 제어합니다. HTTP GET은 API에 필요한 인증서가 HTTP GET 요청에 매개 변수로 포함되어 있으므로 안전하지 않은 것으로 간주됩니다. 따라서 이러한 HTTP GET 매개 변수는 애플리케이션 로그와 웹 브라우저의 기록에서 캡처할 수 있습니다.

서비스 매개 변수 MakeCallProxy HTTP 메서드가 보안으로 설정된 경우 HTTP GET에 의한 요청이 거부됩니다. 기본적으로 매개 변수 MakeCallProxy HTTP 메서드는 안전하지 않은 것으로 설정되어 있으므로, API에서 GET 및 POST 메서드를 모두 허용하고 이전 버전과의 호환성이 유지됩니다.

시작하기 전에

[표준 CCM 최종 사용자 그룹에 사용자 추가, 311 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	(선택 사항) WebDialer 최종 사용자 추가, 312 페이지	새 사용자를 추가합니다. 사용자가 존재하는 경우 다음 작업을 진행할 수 있습니다.
단계 2	인증 프록시 권한 할당, 312 페이지	최종 사용자에게 인증 프록시 권한을 할당합니다.

WebDialer 최종 사용자 추가

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 성을 입력합니다.
- 단계 4 암호를 입력하고 확인합니다.
- 단계 5 PIN을 입력하고 확인합니다.
- 단계 6 최종 사용자 구성 창의 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 7 저장을 클릭합니다.

인증 프록시 권한 할당

기존 사용자에게 인증 프록시 권한을 활성화하려면 다음 절차를 수행합니다.

프로시저

- 단계 1 사용자 관리 > 사용자 그룹을 선택합니다.
사용자 그룹 찾기 및 나열 창이 표시됩니다.
- 단계 2 찾기를 클릭합니다.
- 단계 3 표준 **EM** 인증 프록시 권한 링크를 클릭합니다.
사용자 그룹 구성 창이 나타납니다.
- 단계 4 그룹에 최종 사용자 추가를 클릭합니다.
사용자 찾기 및 나열 창이 표시됩니다.
- 단계 5 찾기를 클릭합니다. 특정 사용자에게 조건도 추가할 수 있습니다.
- 단계 6 한 명 이상의 사용자에게 프록시 권한을 할당하려면 다음 단계 중 하나를 완료합니다.
- 단계 7 단일 사용자를 추가하려면 사용자를 선택한 다음 선택한 항목 추가를 클릭합니다.

단계 8 목록에 나타나는 모든 사용자를 추가하려면 모두 선택을 클릭한 다음 선택한 항목 추가를 클릭합니다.

사용자 그룹 구성 창의 그룹 내 사용자 테이블에 사용자가 표시됩니다.

WebDialer 상호 작용

기능	상호 작용
CMC(Client Matter Code)	CMC를 사용하는 경우 신호음이 재생되면 사용자는 적절한 코드를 입력해야 합니다. 그렇지 않으면, IP 전화기 연결이 끊어지고 사용자는 다시걸기 신호음을 받습니다.
FAC(Forced Authorization Code)	FAC를 사용하는 경우 신호음이 재생되면 사용자는 적절한 코드를 입력해야 합니다. 그렇지 않으면, IP 전화기 연결이 끊어지고 사용자는 다시걸기 신호음을 받습니다.
ApplicationDialRule 테이블	Cisco Web Dialer에서는 애플리케이션 다이얼 규칙 데이터베이스 테이블의 변경 알림을 사용하여 업데이트된 다이얼 규칙을 추적하고 사용합니다.
클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC)	<p>Web Dialer는 다음과 같은 방법으로 CMC 및 FAC를 지원합니다.</p> <ul style="list-style-type: none"> • 사용자는 WD HTML 페이지 또는 SOAP 요청의 다이얼 텍스트 상자에 대상 번호를 입력한 다음 전화기에 CMC 또는 FAC를 수동으로 입력할 수 있습니다. • 사용자는 WD HTML 페이지 또는 SOAP 요청의 다이얼 텍스트 상자에 FAC 또는 CMC를 사용하여 대상 번호를 입력할 수 있습니다. <p>예를 들어, 대상 번호가 5555이고 FAC가 111이고 CMC가 222인 경우, 사용자는 5555111#(FAC), 5555222#(CMC) 또는 5555111222#(CMC 및 FAC)을 다이얼하여 전화를 걸 수 있습니다.</p> <p>참고</p> <ul style="list-style-type: none"> • WebDialer는 대상 번호에 대한 유효성 검사를 처리하지 않습니다. 전화기에서 필수 확인을 처리합니다. • 사용자가 코드를 제공하지 않거나 잘못된 코드를 제공하는 경우 통화는 실패합니다. • 사용자가 특수 문자를 포함하는 DN을 사용하여 WebApp에서 전화를 거는 경우 특수 문자를 제거한 후 통화가 성공적으로 수행됩니다. 동일한 규칙이 SOAP UI에서 작동하지 않습니다.

WebDialer 제한 사항

기능	제한 사항
전화기	<p>Cisco WebDialer는 Cisco CTI(Computer Telephony Integration)가 지원하는 SCCP(Skinny Client Control Protocol)와 SIP(Session Initiation Protocol)를 실행하는 전화기를 지원합니다.</p> <p>참고 일부 이전 전화기 모델에서는 SIP를 실행하는 Cisco Web Dialer를 지원하지 않습니다.</p>

WebDialer 문제 해결

인증 오류

문제

Cisco WebDialer에 다음 메시지가 표시됩니다.

인증에 실패 했습니다. 다시 시도하십시오.

가능한 원인

사용자가 잘못된 사용자 ID 또는 암호를 입력했습니다.

해결 방법

Unified Communications ManagerCisco Unified Communications Manager 사용자 ID 및 암호를 사용하여 로그인하는지 확인하십시오.

일시적으로 서비스를 사용할 수 없음

문제

Cisco WebDialer에 다음 메시지가 표시됩니다.

서비스를 일시적으로 사용할 수 없습니다. 나중에 다시 시도하십시오.

가능한 원인

Cisco 콜매니저 서비스는 세 개의 동시 CTI 세션의 스로틀 제한에 도달하여 오버로드 되었습니다.

해결 방법

잠시 후에 연결을 다시 시도하십시오.

디렉터리 서비스 다운

문제

Cisco WebDialer에 다음 메시지가 표시됩니다.

서비스를 일시적으로 사용할 수 없습니다. 나중에 다시 시도하십시오. 디렉터리 서비스가 중지되었습니다.

가능한 원인

Cisco Communications Manager 디렉터리 서비스가 다운되었을 수 있습니다.

해결 방법

잠시 후에 연결을 다시 시도하십시오.

Cisco CTIManager 다운

문제

Cisco WebDialer에 다음 메시지가 표시됩니다.

서비스를 일시적으로 사용할 수 없습니다. 나중에 다시 시도하십시오. Cisco CTIManager가 중지되었습니다.

가능한 원인

Cisco Web Dialer에 대해 구성된 Cisco CTIManager 서비스가 다운되었습니다.

해결 방법

잠시 후에 연결을 다시 시도하십시오.

세션이 만료되었습니다. 다시 로그인하십시오

문제

Cisco WebDialer에 다음 메시지가 표시됩니다.

세션이 만료되었습니다. 다시 로그인하십시오.

가능한 원인

Cisco Web Dialer 세션 만료:

- WebDialer 서블릿을 구성한 후
- Cisco Tomcat 서비스가 다시 시작된 경우.

해결 방법

Unified Communications Manager 사용자 ID 및 암호를 사용하여 로그인합니다.

어느 디바이스에도 로그인하지 않은 사용자

문제

Cisco WebDialer에 다음 메시지가 표시됩니다.

어느 디바이스에도 로그인하지 않은 사용자

가능한 원인

사용자는 Cisco WebDialer 기본 설정 창에서 Cisco Extension Mobility를 사용하도록 선택했지만 IP 전화기에 로그인하지는 않습니다.

해결 방법

- Cisco WebDialer를 사용하기 전에 전화기에 로그인합니다.
- **Extension Mobility** 사용 옵션을 선택하는 대신 대화 상자의 Cisco WebDialer 기본 설정 목록에서 디바이스를 선택합니다.

디바이스/회선 열기 실패

문제

사용자가 전화를 걸려고 하면 Cisco WebDialer에 다음 메시지가 표시됩니다.

어느 디바이스에도 로그인하지 않은 사용자

가능한 원인

- 사용자가 Unified Communications Manager에 등록되지 않은 Cisco Unified IP Phone을(를) 선택했습니다. 예를 들어, 사용자는 애플리케이션을 시작하기 전에 Cisco IP 소프트웨어를 기본 설정 디바이스로 선택합니다.
- 새 전화기가 있는 사용자가 더 이상 서비스 중이 아닌 이전 전화기를 선택합니다.

해결 방법

서비스 중이며 Unified Communications Manager에 등록된 전화기를 선택합니다.

대상에 연결할 수 없음

문제

Cisco WebDialer는 통화 종료 창에 다음 메시지를 표시합니다.

대상에 연결할 수 없음

가능한 원인

- 사용자가 잘못 된 번호로 전화를 겁니다.
- 올바른 다이얼 규칙이 적용되지 않았습니다. 예를 들어 사용자가 95550100 대신 5550100로 전화를 겁니다.

해결 방법

다이얼 규칙을 확인합니다.

■ 대상에 연결할 수 없음



26 장

페이징

- 페이징 개요, 319 페이지
- 페이징 사전 요건, 320 페이지
- 기본 페이징 작업 흐름에 대해 Cisco Unified Communications Manager 구성, 321 페이지
- 고급 알림 페이징 구성 작업 흐름, 332 페이지
- 페이징 상호 작용, 339 페이지

페이징 개요

Unified Communications Manager는 Cisco Paging Server와 통합하여 Cisco Unified IP Phone 및 다양한 엔드포인트에 대한 기본 페이징 서비스를 제공하도록 구성될 수 있습니다. Cisco Paging Server 제품은 InformaCast Virtual Appliance를 통해 제공되며, 다음과 같은 구축 옵션을 제공합니다.

InformaCast 기본 페이징

InformaCast 기본 페이징은 개별 Cisco IP 전화기 또는 최대 50대의 전화기 그룹에 동시에 전화기 간 라이브 오디오 페이징을 제공합니다. InformaCast 기본 페이징은 모든 Unified Communications Manager 고객과 모든 Cisco Business Edition 6000 및 Cisco Business Edition 7000 고객에게 무료로 제공됩니다.

InformaCast 고급 알림

InformaCast 고급 알림은 텍스트 및 오디오 메시지를 이용하여 무제한 수의 Cisco IP 전화기와 다양한 디바이스 및 시스템에 연결할 수 있는 완벽한 기능을 갖춘 비상 알림 및 페이징 솔루션입니다.

구성 프로세스를 간소화하기 위해 Unified Communications Manager에는 고급 알림 서비스를 신속하게 구성할 수 있는 프로비저닝 마법사가 제공됩니다.

일부 기능은 다음과 같습니다.

- Cisco IP 전화기 및 기타 엔드포인트에 대한 텍스트 및 오디오(라이브 또는 사전 녹음됨)
- 아날로그 및 IP 오버헤드 페이징 시스템 통합
- 911 또는 비상 통화 모니터링 또는 알림이나 녹음

- Cisco Jabber 통합
- Cisco Spark 통합
- 자동 날씨 알림
- 동적으로 트리거된 비상 전화회의 통화
- 사전 녹음 또는 예약된 브로드캐스트(학교 종소리 또는 교대조 변경)
- 메시지 확인 및 보고를 통한 이벤트 책임
- 컴퓨터 데스크톱(Windows 및 Mac OS)에 대한 알림
- 설비 통합(제어 조명, 문 잠금)
- 보안 통합(패닉 또는 감금 버튼, 모션 감지기, 화재)

InformaCast 고급 알림 기능에 액세스하려면 라이선스 키를 구입합니다.

InformaCast 모바일

InformaCast Mobile은 사용자가 iOS 또는 Android를 실행하는 모바일 디바이스에 이미지, 텍스트 및 미리 녹음된 오디오를 전송할 수 있는 클라우드 기반 서비스입니다. 또한 InformaCast 고급 알림과의 양방향 통합 기능이 있습니다.

일부 기능은 다음과 같습니다.

- iOS 또는 Android를 실행하는 모바일 디바이스를 통해 InformaCast 메시지를 전송하고 수신하는 기능
- InformaCast 고급 알림과의 양방향 통합 기능
- 메시지 확인 및 읽음 확인
- 통화 또는 SMS 메시징 요금 없음

InformaCast Mobile은 Singlewire 소프트웨어에서 직접 구입해야 합니다. 추가 세부 정보 및 다운로드에 대해서는 Singlewire 웹 사이트를 참조하십시오.

InformaCast 고급 알림과 통합하도록 Unified Communications Manager이 이미 구성된 경우에는 Unified Communications Manager의 추가 구성이 필요하지 않습니다.

페이징 사전 요건

Cisco Paging Server는 멀티캐스트 환경에서 작동하도록 설계되었습니다. 멀티캐스트에 맞게 네트워크를 구성해야 합니다.

페이징을 지원하는 Cisco Unified IP Phone 목록은 다음 웹 사이트에 있는 Singlewire 호환성 매트릭스의 **Cisco Unified IP Phones** 섹션을 참조하십시오.

<http://www.singlewire.com/compatibility-matrix.html>.

기본 페이징 작업 흐름에 대해 Cisco Unified Communications Manager 구성

InformaCast 기본 페이징 구축을 위해 Cisco Paging Server와 통합하도록 Unified Communications Manager를 구성하려면 다음 작업을 수행합니다.

시작하기 전에

- 다음을 검토하여 기능에 대해 알아 보십시오.
 - [페이징 개요, 319 페이지](#)
 - [InformaCast 기본 페이징, 319 페이지](#)
- [페이징 사전 요건, 320 페이지](#) 검토
- 이 섹션의 구성은 [고급 알림 페이징 구성 작업 흐름](#) 마법사를 사용하면 자동으로 구성됩니다.

프로시저

	명령 또는 동작	목적
단계 1	SNMP 서비스 활성화, 322 페이지	Unified Communications Manager에서 SNMP를 구성합니다.
단계 2	기본 코덱을 G.711로 설정, 324 페이지	기본 코덱을 G.711로 설정합니다.
단계 3	페이징에 대한 디바이스폴 구성, 324 페이지	디바이스폴을 구성합니다.
단계 4	InformaCast 페이징을 위한 경로 파티션 구성, 325 페이지	기본 페이징을 위한 라우트 파티션을 구성합니다.
단계 5	InformaCast 페이징을 위한 발신 검색 공간 구성, 325 페이지	기본 페이징을 위한 발신 검색 공간을 구성합니다.
단계 6	페이징을 위한 CTI 포트 구성, 326 페이지	CTI 포트를 구성합니다.
단계 7	AXL 액세스를 사용하여 액세스 컨트롤 그룹 구성, 327 페이지	AXL 액세스 컨트롤 그룹을 구성합니다.
단계 8	페이징을 위한 애플리케이션 사용자 구성, 327 페이지	애플리케이션 사용자를 구성합니다.
단계 9	다음 절차 중 하나를 사용하여 전화기에 대한 웹 액세스를 활성화합니다. <ul style="list-style-type: none"> • 전화기에 대한 웹 액세스 활성화, 328 페이지 	엔터프라이즈 전화기 구성을 사용하는 모든 전화기, 일반 전화 프로파일을 사용하는 전화기 그룹 또는 개별 전화기에서 웹 액세스를 활성화할 수 있습니다.

	명령 또는 동작	목적
	<ul style="list-style-type: none"> 일반 전화 프로파일에 대한 웹 액세스 활성화, 329 페이지 엔터프라이즈 전화기 구성에 대한 웹 액세스 활성화, 329 페이지 	
단계 10	인증 URL 구성, 330 페이지	InformaCast가 Cisco Unified IP Phone으로 브로드캐스트를 푸시할 때 전화기가 InformaCast를 인증하도록 Unified Communications Manager 인증 URL을 구성합니다.

Cisco Unified Communications Manager 및 Cisco Paging Serve를 구성하는 방법에 대한 자세한 절차는 *InformaCast Virtual Appliance* 기본 페이징 설치 및 사용자 설명서에서 확인하십시오.

페이징을 위한 SNMP 구성

다음 작업을 수행하여 기본 페이징 또는 고급 알림 구축을 위해 클러스터.

프로시저

	명령 또는 동작	목적
단계 1	SNMP 서비스 활성화, 322 페이지	클러스터에서 SNMP 및 기타 서비스를 활성화합니다.
단계 2	InformaCast SNMP 커뮤니티 문자열 생성, 323 페이지	SNMP 커뮤니티 문자열을 구성합니다.

SNMP 서비스 활성화

페이징을 구성하려면 클러스터의 모든 노드에서 SNMP를 활성화해야 합니다. 또한 다음 서비스도 활성화해야 합니다.

- Cisco CallManager SNMP 서비스 — 클러스터의 모든 노드에서 활성화합니다.
- Cisco CallManager — 하나 이상의 노드에서 활성화합니다.
- Cisco AXL 웹 서비스 — 하나 이상의 노드에서 활성화합니다.
- Cisco CTIManager - 하나 이상의 노드에서 활성화합니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. 도구 > 서비스 활성화.

단계 2 서버 드롭다운 목록에서 SNMP를 구성하려는 서버를 선택합니다.

단계 3 Cisco CallManager SNMP 서비스에 해당하는 확인란을 선택합니다.

단계 4 클러스터에 있는 하나 이상의 서버에 대해 Cisco CallManager, Cisco CTIManager 및 Cisco AXL 웹 서비스 서비스에 해당하는 확인란을 선택합니다.

단계 5 저장을 클릭합니다.

단계 6 확인을 클릭합니다.

단계 7 클러스터의 모든 네트워크에 대해 이전 단계를 반복합니다.

InformaCast SNMP 커뮤니티 문자열 생성

SNMP 커뮤니티 문자열을 설정하기 위한 기본 페이지에 이 절차를 수행합니다.

시작하기 전에

[SNMP 서비스 활성화, 322 페이지](#)

프로시저

단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. **SNMP > V1/V2c > 커뮤니티 문자열**.

단계 2 서버 드롭다운 목록 상자에서 서버를 선택하고 찾기를 클릭합니다.

단계 3 새로 추가를 클릭합니다.

단계 4 커뮤니티 문자열 이름 필드에 **ICVA**를 입력합니다.

단계 5 액세스 권한 드롭다운 목록에서 읽기 전용을 선택합니다.

단계 6 확인란이 활성화된 경우 모든 노드에 적용 확인란을 선택합니다.

단계 7 저장을 클릭합니다.

단계 8 확인을 클릭합니다.

다음에 수행할 작업

[기본 코덱을 G.711로 설정, 324 페이지](#)

페이징을 위한 지역 구성

기본 페이징의 경우 페이징 구축을 위한 지역을 설정해야 합니다.

프로시저

	명령 또는 동작	목적
단계 1	기본 코덱을 G.711로 설정, 324 페이지	다른 지역 통화를 위해 G.711 코덱을 사용하는 지역을 만듭니다.

	명령 또는 동작	목적
단계 2	페이징에 대한 디바이스폴 구성, 324 페이지	페이징에 대한 디바이스폴을 설정하고 생성한 지역을 해당 디바이스폴에 할당합니다.

기본 코덱을 G.711로 설정

다른 지역에 대한 통화의 기본 코덱으로 G.711을 사용하는 InformaCast 지역을 생성해야 합니다.

시작하기 전에

[페이징을 위한 SNMP 구성, 322 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 지역 정보 > 지역.

단계 2 새로 추가를 클릭합니다.

단계 3 이름 필드에 **ICVA**를 입력합니다.

단계 4 저장을 클릭합니다.

단계 5 지역 텍스트 상자에서 **CTRL** 키를 누르고 선택한 모든 지역을 클릭하여 모든 지역을 선택합니다.

단계 6 최대 오디오 비트 속도 드롭다운 목록에서 **64 kbps(G.722, G.711)**를 선택합니다.

단계 7 영상 통화에 대한 최대 세션 비트 속도 열에서 없음 라디오 버튼을 클릭합니다.

단계 8 저장을 클릭합니다.

페이징에 대한 디바이스폴 구성

이 절차를 수행하여 페이징 구축을 위한 디바이스폴을 구성합니다.

시작하기 전에

[기본 코덱을 G.711로 설정, 324 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 디바이스폴.

단계 2 새로 추가를 클릭합니다.

단계 3 디바이스폴 이름 필드에 **ICVA**를 입력합니다.

단계 4 **Cisco Unified Communications Manager Group** 드롭다운 목록에서 InformaCast 가상 어플라이언스가 통신할 Cisco Unified Communications Manager 클러스터를 포함하는 그룹을 선택합니다.

단계 5 날짜/시간 그룹 드롭다운 목록에서 날짜/시간 그룹을 선택합니다. 하루 중 시간까지 전화 걸기 제한을 수행하지 않는 한 **CMLocal**을 선택합니다.

단계 6 지역 드롭다운 목록에서 **ICVA**를 선택합니다.

단계 7 **SRST** 참조 드롭다운 목록에서 비활성화를 선택합니다.

단계 8 저장을 클릭합니다.

페이징을 위한 파티션 및 발신 검색 공간 구성

다음과 같이 페이징에 대한 파티션 및 CSS(발신 검색 공간)를 구성하려면 다음 작업을 수행합니다.

- 기본 페이징 구축의 경우 InformaCast 페이징을 위한 단일 파티션과 CSS를 생성합니다.

프로시저

	명령 또는 동작	목적
단계 1	InformaCast 페이징을 위한 경로 파티션 구성, 325 페이지	InformaCast 페이징을 위한 라우트 파티션을 구성합니다.
단계 2	InformaCast 페이징을 위한 발신 검색 공간 구성, 325 페이지	InformaCast 페이징을 위한 발신 검색 공간을 구성합니다.

InformaCast 페이징을 위한 경로 파티션 구성

기본 페이징 또는 고급 알림 구축에서 InformaCast 페이징.

시작하기 전에

[페이징에 대한 디바이스폴 구성, 324 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.콜 라우팅 > 제어 클래스 > 라우트 파티션.

단계 2 새로 추가를 클릭합니다.

단계 3 이름 필드에 파티션에 대한 다음 이름 및 설명을 입력합니다: **ICVA-CTIOutbound, ICVA-Do not add to any phone CSS.**

단계 4 저장을 클릭합니다.

InformaCast 페이징을 위한 발신 검색 공간 구성

이 절차를 수행하여 에서 InformaCast 페이징을 위한 발신 검색 공간을 구성합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 발신 검색 공간.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 이름 필드에 **ICVA**를 입력합니다.
- 단계 4 사용 가능한 파티션 목록 상자에서 화살표를 사용하여 다음 파티션을 선택한 파티션 목록 상자으로 이동합니다.
- InformaCast 페이징을 위해 생성한 파티션
 - 사용자의 내선 번호와 아날로그 페이징 확장이 포함된 파티션
- 단계 5 저장을 클릭합니다.
-

페이징을 위한 CTI 포트 구성

이 절차를 수행하여 페이징 구축에 대한 CTI 포트를 구성합니다. 필요한 CTI 포트 수는 구축 유형 및 애플리케이션에 사용되는 용도에 따라 달라집니다.

- 기본 페이징 구축의 경우 InformaCast 페이징을 위해 최소 두 개의 CTI 포트를 생성해야 합니다.

시작하기 전에

[InformaCast 페이징을 위한 발신 검색 공간 구성, 325 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 전화기 유형 드롭다운 목록에서 **CTI** 포트를 선택합니다.
- 단계 4 디바이스 이름 필드에 CTI 포트 이름을 입력합니다. 예를 들어, InformaCast 포트의 경우 **ICVA-IC-001**.
- 단계 5 설명 필드에 포트에 대한 설명을 입력합니다. 예를 들어 통화 모니터링용 **InformaCast** 보고 포트.
- 단계 6 디바이스폴 드롭다운 목록에서 **ICVA**를 선택합니다.
- 단계 7 발신 검색 공간 드롭다운 목록에서 **ICVA**를 선택합니다.
- 단계 8 디바이스 보안 프로파일 드롭다운 목록에서 **Cisco CTI 포트 - 표준 SCCP** 비보안 프로파일을 선택합니다.
- 단계 9 저장을 클릭합니다.
- 단계 10 확인을 클릭합니다.
- 단계 11 왼쪽 연결 영역에서 회선 [1] - 새 DN 추가를 클릭합니다.

- 단계 12 디렉터리 번호 필드에 디렉터리 번호를 입력합니다. 이 디렉터리 번호는 페이징 통화 외의 목적으로 사용해서는 안 됩니다. 전화기에 할당되어서는 안 되며 직접 내부 다이얼 범위 내에 있지 않아야 합니다.
- 단계 13 경로 파티션 드롭다운 목록에서 다음 포트 중 를 선택합니다.
- InformaCast 포트의 경우 **ICVA-CTIOutbound**를 선택합니다.
- 단계 14 표시(내부 발신자 ID) 텍스트 상자에서 구성하고 있는 포트 유형에 따라 **InformaCast**.
- 단계 15 **ASCII** 표시(내부 발신자 ID) 텍스트 상자에서 구성하고 있는 포트 유형에 따라 **InformaCast**.
- 단계 16 저장을 클릭합니다.
- 단계 17 필요한 각 CTI 포트에 대해 이 절차를 반복합니다.

다음에 수행할 작업

AXL 액세스를 사용하여 액세스 컨트롤 그룹 구성

AXL 액세스를 포함하는 액세스 컨트롤 그룹을 생성합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 사용자 설정 > 액세스 컨트롤 그룹.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 이름 텍스트 상자에 **ICVA** 사용자 그룹을 입력합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 관련 링크 드롭다운 목록에서 찾기/나열로 돌아가기를 선택한 다음 이동을 클릭합니다.
- 단계 6 역할 열에서 새 액세스 컨트롤 그룹에 해당하는 **i** 아이콘을 클릭합니다.
- 단계 7 그룹에 역할 할당을 클릭합니다.
- 단계 8 찾기를 클릭합니다.
- 단계 9 표준 **AXL API** 액세스 확인란을 선택하고 선택 항목 추가를 클릭합니다.
- 단계 10 저장을 클릭합니다.
-

페이징을 위한 애플리케이션 사용자 구성

애플리케이션 사용자를 구성하려면 이 절차를 수행합니다.

- 기본 페이징의 경우 InformaCast 애플리케이션 사용자를 구성합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 애플리케이션 사용자.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 사용자 ID 텍스트 상자에 애플리케이션 사용자의 사용자 ID를 입력합니다. 예를 들어 **ICVA InformaCast**를 입력합니다.
- 단계 4 암호 및 암호 확인 필드에 암호를 입력합니다.
- 단계 5 사용 가능한 디바이스 목록 상자에서 구축을 위해 생성한 CTI 포트를 클릭하고 화살표를 사용하여 디바이스를 제어된 디바이스 목록 상자로 이동합니다. 예를 들어, InformaCast의 경우 **ICVA-IC-001** 및 CallAware의 경우 **ICVA-CA-001**을 선택합니다.
- 단계 6 액세스 컨트롤 그룹에 추가를 클릭합니다.
- 단계 7 찾기를 클릭합니다.
- 단계 8 다음 확인란을 선택합니다(다르게 표시된 경우 이외에는 모든 애플리케이션 사용자에게 대해 이러한 권한을 선택).
- ICVA 사용자 그룹
 - 표준 CTI 모든 디바이스 제어 허용
 - 연결된 Xfer 및 conf를 지원하는 전화의 표준 CTI 컨트롤 허용
 - 표준 CTI 롤오버 모드를 지원하는 전화의 컨트롤 허용
 - 표준 CTI 활성화
- 단계 9 선택한 항목 추가를 클릭합니다.
- 단계 10 저장을 클릭합니다.
-

전화기에 대한 웹 액세스 활성화

기본 페이지ング에서 이 절차를 수행하여 Cisco Unified IP Phone에 대한 웹 액세스를 활성화합니다. 일반 전화 프로파일을 사용하여 해당 프로파일을 사용하는 전화기 그룹에 대해 웹 액세스를 활성화할 수도 있습니다. 자세한 내용은 [일반 전화 프로파일에 대한 웹 액세스 활성화, 329 페이지](#)를 참조하십시오.

시작하기 전에

[페이지ング을 위한 애플리케이션 사용자 구성, 327 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 웹 액세스를 활성화할 전화기를 선택합니다.
- 단계 3 제품별 구성 레이아웃 영역의 웹 액세스 드롭다운 목록에서 활성화됨을 선택합니다.

단계 4 저장을 클릭합니다.

다음에 수행할 작업

[인증 URL 구성, 330 페이지](#)(으)로 이동하십시오.

일반 전화 프로파일에 대한 웹 액세스 활성화

기본 페이지에서 이 절차를 수행하여 일반 전화 프로파일을 사용하는 Cisco Unified IP Phone 그룹에 대한 웹 액세스를 활성화합니다. 개별 전화기의 웹 액세스를 활성화할 수도 있습니다. 자세한 내용은 [전화기에 대한 웹 액세스 활성화, 328 페이지](#)를 참조하십시오.

시작하기 전에

[페이징을 위한 애플리케이션 사용자 구성, 327 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 전화 프로파일

단계 2 찾기를 클릭하고 웹 액세스를 활성화하려는 전화기 그룹에 적용되는 프로파일을 선택합니다.

단계 3 제품별 구성 레이아웃 영역의 웹 액세스 드롭다운 목록에서 활성화를 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 구성 적용을 클릭하여 일반 전화 프로파일을 사용하는 전화기를 재설정합니다.

단계 6 확인을 클릭합니다.

다음에 수행할 작업

[인증 URL 구성, 330 페이지](#)으로 이동하십시오.

엔터프라이즈 전화기 구성에 대한 웹 액세스 활성화

Unified Communications Manager에서 이 절차를 수행하여 일반 전화 프로파일을 사용하는 Cisco Unified IP Phone의 그룹에 대한 웹 액세스를 활성화합니다. 개별 전화기의 웹 액세스를 활성화할 수도 있습니다. 자세한 내용은 [전화기에 대한 웹 액세스 활성화, 328 페이지](#)를 참조하십시오.

시작하기 전에

[페이징을 위한 애플리케이션 사용자 구성, 327 페이지](#).

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 엔터프라이즈 전화기 설정.
- 단계 2 웹 액세스 드롭다운 목록에서 활성화를 선택합니다.
- 단계 3 저장을 클릭합니다.
- 단계 4 구성 적용을 클릭하여 일반 전화 프로파일을 사용하는 전화기를 재설정합니다.
- 단계 5 확인을 클릭합니다.

인증 URL 구성

다음 작업을 수행하여 InformaCast가 브로드캐스트를 Cisco Unified IP Phone으로 푸시할 때 전화기가 Unified Communications Manager 대신 InformaCast로 인증되도록 InformaCast를 가리키는 인증 URL을 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	인증 URL 설정, 330 페이지	Unified Communications Manager InformaCast를 가리키는 인증 URL을 설정합니다.
단계 2	전화기 재설정, 331 페이지	전화기에서 새 설정을 사용하도록 구축에서 전화기를 재설정합니다.
단계 3	전화기 테스트, 331 페이지	구축의 전화기에서 새 인증 URL 설정을 사용하는지 확인합니다.

인증 URL 설정

이 절차를 수행하여 InformaCast 가상 어플라이언스를 가리키도록 Unified Communications Manager 인증 URL을 설정합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 엔터프라이즈 매개 변수.
- 단계 2 전화기 URL 매개 변수 영역으로 스크롤하고 URL 인증 필드에 **http://<IP Address>:8081/InformaCast/phone/auth**를 입력합니다. <IP Address>는 InformaCast 가상 어플라이언스의 IP 주소입니다.
- 참고 URL 인증 필드에 기존 URL을 기록해 둡니다. InformaCast를 구성하는 경우 이 기능이 필요할 수 있습니다. 자세한 내용은 InformaCast 설명서를 참조하십시오.

단계 3 보안 전화기 **URL** 매개 변수 영역으로 스크롤하고 보안 인증 **URL** 필드에 **http://<IP Address>:8081/InformaCast/phone/auth**를 입력합니다. <IP Address>는 InformaCast 가상 어플라이언스의 IP 주소입니다.

단계 4 저장을 클릭합니다.

전화기 재설정

인증 URL을 설정하여 InformaCast 가상 어플라이언스를 가리키도록 한 후에는 전화기를 재설정해야 합니다. 이 절차에서는 디바이스폴에서 수동으로 전화기를 재설정하는 방법에 대해 설명합니다. 전화기를 재설정하는 방법에는 여러 가지가 있습니다. 예를 들어, 벌크 관리 도구를 사용하여 꺼져 있는 시간 동안 재설정을 예약할 수도 있습니다. 벌크 관리 도구에 대한 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 지침서를 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 전화기.

단계 2 수신 전화 위치 상자에서 디바이스폴을 선택합니다.

단계 3 다른 드롭다운 메뉴 및 필드 항목을 사용자 전화기가 포함된 디바이스폴을 불러오는 설정으로 설정합니다.

단계 4 찾기를 클릭합니다.

단계 5 재설정하려는 디바이스폴을 선택합니다.

단계 6 선택한 항목 재설정을 클릭합니다.

단계 7 재설정을 클릭합니다.

전화기 테스트

전화기가 InformaCast 가상 어플라이언스를 사용하여 인증되고 있는지 확인합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 전화기

단계 2 전화기 찾기 및 나열 창의 드롭다운 목록과 필드를 사용하여 새 인증 URL을 사용해야 하는 전화기에 대한 검색을 필터링하고 찾기를 클릭합니다.

단계 3 새 설정을 사용해야 하는 전화기의 경우 **IPv4** 주소 열에서 IP 주소 링크를 클릭합니다.

단계 4 네트워크 구성을 클릭합니다.

네트워크 구성 페이지가 나타납니다.

단계 5 인증 **URL** 필드에 **URL** 인증 엔터프라이즈 매개 변수에 입력한 InformaCast 가상 어플라이언스 IP 주소가 표시되는지 확인합니다. 올바른 URL이 표시되지 않는 경우에는 인증 URL을 설정해야 합니다.

고급 알림 페이지 구성 작업 흐름

다음 작업을 수행하여 IP 페이지 및 비상 통화 알림을 위해 InformaCast 페이지 서버를 Unified Communications Manager와 통합합니다. 여기에는 다음과 같은 기능이 포함됩니다.

- InformaCast 고급 알림
- 패닉 버튼 구성
- 사용자가 비상 서비스 번호로 전화를 걸 때 IP 전화기에 텍스트 및 오디오 알림(CallAware)

프로시저

	명령 또는 동작	목적
단계 1	InformaCast 가상 어플라이언스 설치, 332 페이지 .	Singlewire 웹 사이트에서 InformaCast OVA 파일을 다운로드하여 vSphere에 업로드합니다.
단계 2	InformaCast에 대한 연결 구성, 334 페이지 .	Unified Communications Manager 및 InformaCast를 구성합니다.
단계 3	패닉 버튼 구성, 336 페이지 .	IP 전화기로 텍스트 및 오디오 알림을 보내도록 패닉 버튼을 구성합니다.
단계 4	CallAware 비상 통화 알림 구성, 337 페이지 .	비상 통화 텍스트 및 오디오 알림을 구성합니다.

InformaCast 가상 어플라이언스 설치

Singlewire는 vSphere 클라이언트를 통해 관리되는 VMware ESXi 플랫폼에서 InformaCast Virtual Appliance를 지원합니다.



참고 Singlewire가 지원되는 VMware ESXi 버전의 목록을 보려면 <https://www.singlewire.com/compatibility-matrix> URL로 이동하여 InformaCast Platform 섹션 아래에서 서버 플랫폼 링크를 클릭합니다.



참고 라이선스를 구매한 경우 <https://www.singlewire.com/icva-kb-activate>를 참조하여 라이선스를 활성화합니다. 이렇게 하면 90일 평가판이 만료된 후 비상 알림이 활성 상태를 유지합니다.



참고 InformaCast 화면 캡처를 포함하여 설치에 대한 자세한 내용은 <https://www.singlewire.com/icva-kb-install> URL로 이동합니다.

시작하기 전에

vSphere 클라이언트를 사용하여 InformaCast Virtual Appliance를 가져옵니다. VMware 서버에서 다운로드할 수 있습니다.

프로시저

- 단계 1 [Singlewire](#) 웹 사이트에서 OVA 파일을 다운로드한 다음 vSphere 클라이언트에 로그인합니다.
참고 Communications Manager Business Edition 6000에서 InformaCast를 사용 중인 경우 패키지
에 OVA가 있는 DVD가 제공됩니다(물리적 미디어).

vSphere 클라이언트 창이 나타납니다.
- 단계 2 vSphere 클라이언트 창에서 파일 > **OVF** 템플릿 배포를 선택합니다.
OVF 템플릿 배포 대화 상자가 나타납니다.
- 단계 3 파일에서 배포 라디오 버튼을 클릭한 다음 찾아보기를 클릭하여 저장된 OVA 파일(또는 제공된 DVD
에 있는 OVA 파일)을 선택합니다. OVA 파일을 선택한 후 열기를 클릭합니다.
OVF 템플릿 배포 대화 상자에서 소스 위치가 선택됩니다.
- 단계 4 다음을 클릭하여 작업을 계속합니다.
OVF 템플릿 배포 대화 상자를 새로 고치면 **OVF** 템플릿 세부 정보가 나타납니다.
- 단계 5 다음을 클릭하여 이름과 위치를 확인한 후 다음을 클릭하여 새 가상 시스템 파일을 저장할 네트워크
를 선택합니다.

팁 가상 어플라이언스는 Cisco 통합 커뮤니케이션 매니저와 같은 VLAN에 설치하는 것이 좋
습니다.
- 단계 6 다음을 클릭하여 계속한 다음 완료를 누릅니다.
InformaCast Virtual Appliance가 가져오기를 시작합니다.
- 단계 7 vSphere 클라이언트 창에서 호스트 및 클러스터 아이콘을 클릭한 다음 호스트 서버를 선택합니다.
vSphere 클라이언트 창이 새로 고침됩니다.
- 단계 8 구성 탭을 클릭하고 소프트웨어 섹션에서 가상 시스템 시작/종료 링크를 선택합니다.
- 단계 9 속성 링크를 클릭합니다.
가상 머신 시작 및 종료 대화 상자가 나타납니다.
- 단계 10 시스템 설정 아래에서 시스템에서 가상 머신을 자동으로 시작 및 중지하도록 허용 확인란을 선택합
니다.
- 단계 11 시작 순서 아래에서 수동 시작 섹션으로 스크롤하여 가상 머신(기본적으로 Singlewire InformaCast
VM)을 선택한 다음 위로 이동 버튼을 사용하여 수동 시작 섹션에서 자동 시작 섹션으로 이동합니다.
이동한 후 확인을 클릭합니다.

호스팅되는 서버와 함께 InformaCast Virtual Appliance가 자동으로 시작되고 중단됩니다. 이제 InformaCast의 가상 머신을 켜고 해당 네트워크 구성을 설정합니다.

단계 12 보기 > 재고 > VM 및 템플릿을 선택한 다음 가상 머신을 선택합니다.

단계 13 재고 > 가상 머신 > 콘솔 열기를 선택합니다.
Singlewire InformaCast VM 콘솔 창이 나타납니다.

단계 14 InformaCast 구성이 처음으로 시작됩니다. 구성하는 동안 InformaCast Virtual Appliance에 대해 다음 작업을 수행합니다.

- a) Cisco 최종 사용자 라이선스 계약(EULA)에 동의
- b) Singlewire EULA 수락
- c) 호스트 이름 설정
- d) IP 주소, 서브넷 마스크 및 기본 게이트웨이 설정
- e) DNS 서버 IP 주소 및 도메인 이름 설정
- f) NTP 서버 IP 주소 또는 호스트 이름 설정
- g) 시간대 설정
- h) SSL(Secure Socket Layer) 인증서 파라미터 설정
- i) SSL 제목 대체 이름(선택 사항) 설정
- j) OS 관리자 암호 설정
- k) InformaCast 및 PTT(PushToTalk) 관리자 암호를 설정합니다. 이 암호는 Cisco Unified CM 관리의 고급 기능 > 비상 알림 페이지에서 Cisco Unified Communications Manager 및 InformaCast를 연결하는 데 필요합니다.
- l) 백업 및 통신을 위한 보안 암호 설정

성공적으로 구성되면 “Singlewire InformaCast 시작” 메시지가 표시됩니다.

단계 15 계속을 클릭하여 Singlewire InformaCast 작업을 수행합니다.

InformaCast에 대한 연결 구성

이 절차를 사용하여 InformaCast 인증서를 Unified Communications Manager Tomcat 신뢰 저장소에 로드합니다.

시작하기 전에

[InformaCast 가상 어플라이언스 설치, 332 페이지](#).

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > 비상 알림 페이지.

단계 2 InformaCast 비상 알림 소개 페이지에서 다음을 클릭하여 계속합니다.

InformaCast 가상 어플라이언스 설치 페이지가 나타납니다.

단계 3 InformaCast 가상 어플라이언스 설치 페이지에서 다음을 클릭하여 계속합니다.

참고 Unified Communications Manager를 사용하여 구성하려면 InformaCast 가상 어플라이언스를 설치해야 합니다.

Cisco Unified Communications Manager 및 **InformaCast** 연결 페이지가 나타납니다.

단계 4 InformaCast VM의 IP 주소 필드에 IP 주소 또는 호스트 이름을 입력합니다.

참고 기본적으로 사용자 이름은 **InformaCast** 필드에서 사용할 사용자 이름 필드에 admin으로 지정되며 편집할 수 없습니다.

단계 5 관리자 앱 사용자 암호 필드에 InformaCast 애플리케이션의 관리자 암호를 입력합니다.

InformaCast 인증서의 지문을 표시 하는 대화 상자가 표시됩니다.

단계 6 확인 을 클릭하여 InformaCast 인증서를 Unified Communications ManagerTomcat 신뢰 저장소에 로드합니다.

구성 프로세스가 시작됩니다.

참고 구성이 성공 하면 상태 필드에 완료 상태가 표시됩니다.

단계 7 다음을 클릭합니다.

마법사는 다음 작업을 수행합니다.

- SNMP 서비스 활성화
- 로컬로 생성된 임의 인증서를 사용하여 SNMP 서비스를 구성합니다.
- CTI 관리자 서비스 활성화
- InformaCast용으로 Unified Communications Manager 구성
 - 새 지역 생성(클러스터당 1개)
 - 새 디바이스풀 생성(클러스터당 1개)
 - SIP 트렁크 생성(클러스터당 1개)
 - 라우트 그룹 생성(클러스터당 1개)
 - 라우트 목록 생성
 - 역할 생성
 - 앱 사용자 생성
- Unified Communications Manager용 InformaCast 구성
 - 클러스터 생성
 - 받는 사람 그룹 새로 고침
 - SIP 액세스를 거부로 설정

- SIP 액세스 생성

패닉 버튼 구성

이 절차를 사용하여 텍스트 및 오디오 알람을 IP 전화기로 전송하는 패닉 버튼을 구성합니다. 이렇게 하면 응급 상황이 발생하는 경우 원클릭 알람을 시작할 수 있습니다.

시작하기 전에

[InformaCast에 대한 연결 구성, 334 페이지.](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > 비상 알람 페이지.
- 단계 2 InformaCast 비상 알람 소개 페이지에서 다음을 클릭하여 계속합니다.
- 단계 3 InformaCast 가상 어플라이언스 설치 페이지에서 다음을 클릭하여 계속합니다.
- 단계 4 Cisco Unified Communications Manager 및 InformaCast 연결 페이지에서 다음을 클릭하여 계속합니다.
패닉 버튼 구성 페이지가 나타납니다.
- 단계 5 사전 녹음된 메시지를 이름으로 선택합니다) 드롭다운 목록에서 Cisco Unified IP phone 및 비상 시 다양한 디바이스 및 시스템에 표시될 사전 녹음된 메시지를 선택합니다.
참고 필요에 따라 InformaCast 관리에서 미리 녹음된 메시지를 변경할 수 있습니다.
- 단계 6 DN을 입력하여 패닉 버튼 트리거 필드에 0에서 9까지의 숫자, 별표(*) 및 파운드 기호(#)가 포함된 디렉터리 번호(DN)를 입력합니다. 기본값은 ***5입니다.
- 단계 7 라우트 파티션 드롭다운 목록에서 라우트 패턴에 대한 액세스를 제한할 파티션을 선택합니다.
참고 라우트 패턴에 대한 액세스를 제한하지 않으려면 파티션에 대해 <없음>을 선택합니다.
- 단계 8 알람을 전송할 전화기 선택 버튼을 클릭합니다.
알람을 전송할 전화기 대화 상자가 나타납니다.
- 단계 9 알람을 전송할 전화기 대화 상자에서 Cisco Unified IP Phone을 선택하여 사전 녹음된 메시지를 전송합니다. 사용자가 입력한 다이얼 패턴(예: ***5)이 선택한 전화기의 단축 다이얼로 구성됩니다. 선택한 Cisco Unified IP Phone 항목은 알람 전송하도록 선택된 전화기 목록 상자에 표시됩니다.
- 단계 10 규칙 추가를 클릭하여 선택된 Cisco Unified IP Phone에서 알람을 받도록 새 규칙을 만듭니다.
 - a) 드롭다운 목록에서 매개 변수 중 하나를 선택합니다. 사용 가능한 옵션은 디바이스폴, 설명 및 디렉터리 번호입니다.
 - b) 두 번째 드롭다운 목록에서 다음 조건 옵션 중 하나를 선택합니다.

- 수행

- 수행하지 않음

c) 세 번째 드롭다운 목록에서 다음 조건 옵션 중 하나를 선택합니다.

- 다음으로 시작
- 다음으로 종료
- 포함

d) 텍스트 상자에 검색 조건을 입력합니다.

참고 새 규칙은 최소 1개, 최대 5개까지 구성할 수 있습니다. 5개의 규칙이 구성된 경우 규칙 추가 버튼이 비활성화됩니다.

참고 규칙을 삭제하려면 규칙 삭제를 클릭합니다.

e) 규칙 테스트를 클릭하여 생성된 규칙의 유효성을 확인합니다. 0개 이상의 전화기로 테스트 규칙을 완료하면 다음 버튼이 활성화됩니다.

참고 나중에 이 규칙과 일치하는 Cisco Unified Communications Manager에 추가된 전화기는 이 그룹에 대한 알림에 수신자로 포함됩니다.

단계 11 다음을 클릭합니다.

마법사는 다음 작업을 수행합니다.

- 선택된 전화기에 입력한 DN에 대한 단축 다이얼을 추가합니다. 선택된 전화기에 사용되지 않은 단축 다이얼이 기존 전화기 버튼 템플릿에 할당된 경우 이 단축 다이얼이 선택된 전화기에 직접 나타납니다. 선택된 전화기에 사용하지 않는 단축 다이얼 버튼이 없는 경우 패닉 버튼 단축 다이얼이 생성되지만 전화기에 나타나지 않습니다.
- 생성된 라우트 목록을 사용하여 선택한 파티션의 입력된 DN에 대한 라우트 패턴을 추가합니다.
- 입력한 DN에 대한 InformaCast DialCast 항목을 만들어 선택한 메시지를 선택한 규칙과 일치하는 전화기로 보냅니다.

CallAware 비상 통화 알림 구성

이 절차를 사용하여 CallAware 비상 통화 알림 세부 정보를 구성합니다. 이렇게 하면 비상 번호로 전화를 걸 때 IP 전화기로 텍스트 및 오디오 알림을 보냅니다. 또한 911 이외의 번호로 통화를 검색할 수도 있습니다.

시작하기 전에

[패닉 버튼 구성, 336 페이지](#).

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > 비상 알림 페이지.
- 단계 2 InformaCast 비상 알림 소개 페이지에서 다음을 클릭하여 계속합니다.
- 단계 3 InformaCast 가상 어플라이언스 설치 페이지에서 다음을 클릭하여 계속합니다.
- 단계 4 Cisco Unified Communications Manager 및 InformaCast 연결 페이지에서 다음을 클릭하여 계속합니다.
- 단계 5 패닉 버튼 구성 페이지에서 다음을 클릭하여 계속합니다.
CallAware 비상 통화 알림 구성 페이지가 나타납니다.
- 단계 6 사전 녹음된 메시지를 이름으로 선택합니다) 드롭다운 목록에서 Cisco Unified IP phone 및 비상 시 다양한 디바이스 및 시스템에 표시될 사전 녹음된 메시지를 선택합니다.
- 참고 필요에 따라 InformaCast 관리에서 미리 녹음된 메시지를 변경할 수 있습니다.
- 단계 7 비상 라우트 패턴 선택 버튼을 클릭합니다.
라우트 패턴 대화 상자가 나타납니다.
- 단계 8 라우트 패턴 대화 상자에서 원하는 패턴 옆의 상자를 선택하여 라우트 패턴을 선택합니다.
- a) 선택 항목/변경 사항 저장 버튼을 클릭합니다.
선택한 라우트 패턴은 선택한 라우트 패턴 목록 상자에 표시됩니다.
- 단계 9 규칙 추가를 클릭하여 선택된 Cisco Unified IP Phone에서 알림을 받도록 새 규칙을 만듭니다.
- a) 드롭다운 목록에서 매개 변수 중 하나를 선택합니다. 사용 가능한 옵션은 디바이스폴, 설명 및 디렉터리 번호입니다.
- b) 두 번째 드롭다운 목록에서 다음 조건 옵션 중 하나를 선택합니다.
- 수행
 - 수행하지 않음
- c) 세 번째 드롭다운 목록에서 다음 조건 옵션 중 하나를 선택합니다.
- 다음으로 시작
 - 다음으로 종료
 - 포함
- d) 텍스트 상자에 검색 조건을 입력합니다.
- 참고 새 규칙은 최소 1개, 최대 5개까지 구성할 수 있습니다. 5개의 규칙이 구성된 경우 규칙 추가 버튼이 비활성화됩니다.
- 참고 규칙을 삭제하려면 규칙 삭제를 클릭합니다.
- e) 규칙 테스트를 클릭하여 생성된 규칙의 유효성을 확인합니다. 0개 이상의 전화기로 테스트 규칙을 완료하면 완료 버튼이 활성화됩니다.

참고 이 규칙과 일치하는 이후 날짜에 Unified Communications Manager에 추가된 전화기는 이 그룹에 대한 알림에서 수신자로 포함됩니다.

단계 10 마침을 클릭합니다.

마법사는 다음 작업을 수행합니다.

- InformaCast에 대한 외부 전화 제어 프로파일 추가
- 선택한 각 라우트 패턴에 대해 외부 전화 제어 프로파일을 참조하도록 라우트 패턴을 수정합니다.
- 전화기와 일치하는 규칙을 사용하여 알림을 수신할 수신자 그룹을 생성합니다.
- 선택한 메시지 및 수신자 그룹을 사용하여 InformaCast 라우팅 요청을 생성합니다.

요약 페이지가 나타나면 Unified Communications Manager를 이용해 InformaCast를 성공적으로 구성했는지 확인합니다. 자세한 내용은 <https://www.singlewire.com>을 참조하십시오.

페이징 상호 작용

- 고급 알림 페이징 상호 작용, 339 페이지

고급 알림 페이징 상호 작용

표 27: 고급 알림 페이징 상호 작용

기능	상호 작용
비상 알림 페이징	<p>기본 페이징 모드에서만 InformaCast 릴리스 11.5(1)SU3 이상 버전을 사용하여 비상 알림 페이징 마법사를 구성할 수 있습니다.</p> <p>비상 알림 페이징 마법사에 숫자를 포함하는 라우트 패턴에 대한 통화 모니터링을 구성할 수 있습니다. 와일드카드 문자를 포함하는 라우트 패턴의 경우 InformaCast에서 구성합니다.</p>



27 장

인터콤

- 인터콤 개요, 341 페이지
- 인터콤 사전 요건, 342 페이지
- 인터콤 구성 작업 흐름, 342 페이지
- 인터콤 상호 작용, 346 페이지
- 인터콤 제한 사항, 347 페이지
- 인터콤 문제 해결, 348 페이지

인터콤 개요

인터콤은 기존 회선과 단축 다이얼 기능이 결합되어 있는 일종의 전화 회선입니다. 인터콤 회선을 통해 사용자는 단방향 오디오 껏속말에 자동으로 응답하는 다른 사용자의 인터콤 회선에 전화를 걸 수 있습니다. 그러면 수신자는 껏속말 통화를 확인하고 양방향 인터콤 통화를 시작할 수 있습니다.

사용자는 인터콤 회선을 사용하여 인터콤 파티션의 다른 인터콤 회선으로 전화를 걸거나, 인터콤 파티션 외부의 인터콤 회선을 대상으로 회선을 미리 구성할 수 있습니다.

인터콤을 통해 사용자는 미리 정의된 대상으로 전화를 걸 수 있습니다. 착신 대상은 음소거를 활성화한 상태로 스피커폰 모드에서 자동 응답합니다. 이렇게 하면 개시자와 대상 간에 단방향 음성 경로가 설정되므로 개시자는 착신자가 통화 중이거나 휴휴 상태인 경우에도 간단한 메시지를 전달할 수 있습니다.

인터콤 전화를 자동으로 받을 때 착신자의 음성이 발신자에게 반환되지 않도록 하기 위해 Unified Communications Manager는 껏속말 인터콤 기능을 구현합니다. 껏속말 인터콤은 발신자와 착신자 사이에 단방향 오디오만 있음을 의미합니다. 착신자가 발신자와 대화하려면 수동으로 키를 눌러야 합니다.

자동 응답 신호음이 들리면 송신자와 수신자 모두에 대해 껏속말 인터콤 상태가 시작되었음을 나타냅니다.

인터콤 및 기본 디바이스

각 인터콤 회선을 사용하려면 기본 디바이스가 필요합니다. 인터콤 회선은 지정된 기본 디바이스에만 표시됩니다.

관리자가 인터콤 회선을 디바이스에 할당하면 시스템에서 그 디바이스를 인터콤 회선의 기본 디바이스로 설정합니다(이전에 설정되지 않은 경우). 관리자는 인터콤 회선의 기본 디바이스를 수정할 수 있습니다. 관리자가 기본 디바이스를 다른 디바이스로 변경하면 인터콤 회선이 여전히 원래 디바이스에 할당되어 있는 경우에도 인터콤 회선이 원래 디바이스에서 제거됩니다.

인터콤 회선을 디바이스 프로파일에 할당할 수 있습니다. 사용자가 디바이스 프로파일을 사용하여 인터콤 회선의 기본 디바이스와 일치하는 기본 디바이스에 로그인하는 경우에만 인터콤 회선을 사용할 수 있습니다. 그렇지 않으면, 사용자가 로그인할 때 인터콤 회선이 표시되지 않습니다.

인터콤 사전 요건

인터콤 기능을 위한 시스템 요구 사항은 다음과 같습니다.

- Cisco Unified IP Phone 펌웨어 릴리스 8.3(1) 이상

인터콤 구성 작업 흐름

시작하기 전에

- [인터콤 사전 요건, 342 페이지](#)(를) 검토합니다.

프로시저

	명령 또는 동작	목적
단계 1	인터콤 파티션 구성, 342 페이지	새 인터콤 파티션을 추가하거나 기존 파티션을 구성합니다.
단계 2	인터콤 발신 검색 공간 구성, 343 페이지	새 인터콤 발신 검색 공간을 추가합니다.
단계 3	인터콤 변환 패턴 구성, 344 페이지	새 인터콤 변환 패턴을 추가하거나 기존 인터콤 변환 패턴을 구성합니다.
단계 4	인터콤 디렉터리 번호 구성, 344 페이지	인터콤 디렉터리 번호를 추가하거나 업데이트합니다.
단계 5	인터콤 회선 및 단축 다이얼 구성, 345 페이지	인터콤 회선 및 단축 다이얼을 구성합니다.

인터콤 파티션 구성

시작하기 전에

특정 릴리스 및 디바이스 팩에 대해 전화기 모델이 인터콤 기능을 지원하는 확인하십시오. [전화기 기능 목록 생성, 7 페이지](#)

프로시저

-
- 단계 1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 인터콤 > 인터콤 경로 파티션. 인터콤 파티션 패턴 찾기 및 나열 창이 나타납니다.
- 단계 2** 새로 추가를 클릭합니다.
새 인터콤 파티션 추가 창이 나타납니다.
- 단계 3** 인터콤 파티션 정보 섹션의 이름 상자에, 추가할 인터콤 파티션의 이름 및 설명을 입력합니다.
- 참고 여러 파티션을 입력하려면 각 파티션 항목마다 하나의 회선을 사용합니다. 최대 75개의 파티션을 입력할 수 있습니다. 이름과 설명으로 최대 총 1,475자를 사용할 수 있습니다. 파티션 이름은 50자를 초과할 수 없습니다. 각 줄에서 쉼표(.)를 사용하여 파티션 이름과 설명을 구분하십시오. 설명을 입력하지 않으면 Unified Communications Manager에서 파티션 이름을 설명으로 사용합니다.
- 단계 4** 저장을 클릭합니다.
- 단계 5** 구성할 파티션을 찾습니다.
인터콤 파티션 구성 창이 표시됩니다.
- 단계 6** [인터콤 파티션 구성] 필드 영역에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 7** 저장을 클릭합니다.
인터콤 파티션 구성 창이 나타납니다.
- 단계 8** 설정을 적절히 입력합니다. 인터콤 파티션 구성 매개 변수에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 9** 저장을 클릭합니다.
- 단계 10** 구성 적용을 클릭합니다.
-

인터콤 발신 검색 공간 구성

시작하기 전에

[인터콤 파티션 구성, 342 페이지](#)

프로시저

-
- 단계 1** 메뉴 모음에서 통화 라우팅 > 인터콤 > 인터콤 발신 검색 공간을 선택합니다.
- 단계 2** 새로 추가를 클릭합니다.

단계 3 [인터콤 발신 검색 공간] 필드 영역에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

인터콤 변환 패턴 구성

시작하기 전에

[인터콤 발신 검색 공간 구성, 343 페이지](#)

프로시저

단계 1 통화 라우팅 > 인터콤 > 인터콤 변환 패턴을 선택합니다.

인터콤 변환 패턴 찾기 및 나열 창이 나타납니다.

단계 2 다음 작업 중 하나를 수행합니다.

- a) 기존 인터콤 변환 패턴을 복사하려면 구성할 파티션을 찾아 복사할 인터콤 변환 패턴 옆에 있는 복사 버튼을 클릭합니다.
- b) 새 인터콤 변환 패턴을 추가하려면 새로 추가를 클릭합니다.

단계 3 [인터콤 변환 패턴 구성] 필드 영역에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

선택한 파티션, 경로 패턴 및 번호 지정 플랜 조합을 사용하는 인터콤 변환 패턴이 고유한지 확인합니다. 중복 항목을 나타내는 오류 메시지가 표시되는 경우 경로 패턴이나 헌트 파일럿, 변환 패턴, 디렉터리 번호, 통화 지정 보류 번호, 통화 당겨 받기 번호 또는 Meet-Me 구성 창을 확인합니다.

인터콤 변환 패턴 구성 창에는 새로 구성된 인터콤 변환 패턴이 표시됩니다.

인터콤 디렉터리 번호 구성

인터콤 디렉터리 번호에 패턴을 할당할 수 있습니다(예: 352XX). 패턴을 인터콤 디렉터리 번호에 할당할 때 사용자가 혼동되지 않게하려면 텍스트 또는 숫자를 인터콤 DN 구성 필드, 회선 텍스트 레이블, 표시(내부 발신자 ID) 및 외부 전화 번호 마스크를 추가합니다. 이러한 필드는 인터콤 디렉터리 번호를 추가하고 인터콤 디렉터리 번호를 전화기와 연결한 경우에만 인터콤 디렉터리 번호에 표시됩니다.

예를 들어 사용자 이름을 회선 텍스트 레이블 및 내부 발신자 ID에 추가하고 외부 회선 번호를 외부 번호 마스크에 추가한다고 가정합니다. 그러면 발신 정보가 표시될 때 352XX가 아니라 John Chan으로 표시됩니다.

프로시저

단계 1 통화 라우팅 > 인터콤 > 인터콤 디렉터리 번호를 선택합니다.

인터콤 디렉터리 번호 찾기 및 나열 창이 표시됩니다.

단계 2 특정 인터콤 디렉터리 번호를 찾으려면 검색 조건을 입력하고 찾기를 클릭합니다.

검색 조건과 일치하는 인터콤 디렉터리 번호 목록이 표시됩니다.

단계 3 다음 작업 중 하나를 수행합니다.

a) 인터콤 디렉터리 번호를 추가하려면 새로 추가 버튼을 클릭합니다.

b) 인터콤 디렉터리 번호를 업데이트하려면 업데이트할 인터콤 디렉터리 번호를 클릭합니다.

인터콤 디렉터리 번호 구성 창이 표시됩니다.

단계 4 [인터콤 디렉터리 번호 구성] 필드 영역에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

단계 6 구성 적용을 클릭합니다.

단계 7 전화 재설정을 클릭합니다.

단계 8 디바이스를 재시작합니다.

다시 시작하는 동안 게이트웨이의 전화가 끊어질 수 있습니다.

인터콤 회선 및 단축 다이얼 구성

시작하기 전에

[인터콤 디렉터리 번호 구성, 344 페이지](#)

프로시저

단계 1 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿을 선택하고 기존 전화기 버튼 템플릿에 인터콤 회선을 추가하거나 새 템플릿을 만듭니다.

참고 인터콤 회선은 기본 회선으로 구성할 수 없습니다.

단계 2 버튼 정보 영역의 기능 드롭다운 목록에서 인터콤을 선택합니다.

단계 3 버튼 정보 영역의 기능 드롭다운 목록에서 단축 다이얼을 선택합니다.

참고 미리 정의된 대상(바로 호출)을 사용하는 인터콤 회선을 구성하여 빠른 액세스를 지원할 수 있습니다.

단계 4 저장을 클릭합니다.

단계 5 구성 적용을 클릭합니다.

인터콤 상호 작용

기능	상호 작용
벌크 관리 도구	Unified Communications Manager 관리자는 벌크 관리 도구를 사용하여 사용자를 개별적으로 추가하는 대신 여러 인터콤 사용자를 한 번에 추가할 수 있습니다. 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서 의 내용을 참조하십시오.
참여	인터콤 대상이 참여 대상인 경우에도 Cisco Unified IP Phone은 껏속말 인터콤을 지원할 수 있습니다. 대상 발신자가 인터콤 버튼을 눌러 인터콤 발신자와 대화하려고 하면 원래 통화가 보류되고 참여 개시자가 해제됩니다.
방해사절(DND)	대상 전화기에서 인터콤 통화가 DND를 무시합니다.
통화 유지	통화가 유지된 경우 최종 사용자는 전화기가 Unified Communications Manager에 등록되기 전에 통화를 끊어야 합니다. 인터콤 회선이 껏속말 모드인 경우 일방 미디어를 나타내며, 종료 측에는 사용자가 전혀 없을 수 있습니다. 따라서, 토크백 모드의 인터콤 통화만 유지됩니다. (껏속말 인터콤은 유지되지 않습니다.)
Cisco Unified Survivable Remote Site Telephony(SRST)	Cisco Unified IP Phone에 SRST를 등록할 경우 전화기가 인터콤 회선을 등록하지 않습니다. 따라서 전화기에 SRST를 등록하면 이 기능을 사용할 수 없습니다.
Cisco Unified Communications Manager Assistant	Unified Communications Manager Assistant 구성 마법사를 사용하면 Cisco Unified Communications Manager Assistant 구성 시간이 더 적게 소요되고 오류를 제거할 수 있습니다. 관리자가 구성 마법사를 성공적으로 실행하고 완료하면 파티션, 발신 검색 공간, 라우트 포인트 및 변환 패턴이 자동으로 생성됩니다.
CTI	CTI/JTAPI/TSP를 사용하여 인터콤 회선의 사전 구성된 대상 디렉터리 번호를 설정 또는 수정할 수 있습니다. 대상 디렉터리 번호가 업데이트 또는 재구성될 경우 Cisco 통합 커뮤니케이션 매니저 관리를 통해 알람을 수신합니다. 애플리케이션에서 인터콤 회선을 제어하도록 구성되지 않은 경우에는 CTI/JTAPI/TSP가 역호환됩니다. 애플리케이션 사용자 목록에 인터콤 회선이 구성된 경우 변경 사항을 지정하고 호환성을 테스트해야 합니다.

기능	상호 작용
Cisco Extension Mobility	인터콤 기능은 Cisco Extension Mobility와 상호 작용합니다. 사용자가 로그인에 사용하는 디바이스 프로파일에 프로비저닝된 인터콤 회선이 있는 경우 Cisco Extension Mobility 사용자는 시스템에서 표시하는 인터콤 회선을 사용하여 기능을 지원하는 전화기에 로그인할 수 있습니다. 전화기는 해당 인터콤 회선의 기본 디바이스여야 합니다.
IPv6(Internet Protocol Version 6)	인터콤은 IP 주소 지정 모드가 IPv4 전용 또는 IPv4 및 IPv6인 전화기를 지원할 수 있습니다. 인터콤 통화 중에 토크백 모드는 발신자가 인터콤을 시작할 때 사용되는 미디어 스트림과 IP 버전이 동일한 미디어 스트림을 설정합니다.
인터콤 디렉토리 번호 (회선)	인터콤 디렉토리 번호(회선)는 인터콤 회선당 하나의 디바이스로 제한되어 있습니다. Cisco Extension Mobility는 광범위하게 사용되므로 모바일 사용자에게 인터콤 기능이 필요한 경우 단일 디바이스에서만 사용할 수 있도록 해야 합니다. 인터콤 회선을 일반 디바이스 또는 Extension Mobility 프로파일에 할당할 수 있지만 시스템에서 인터콤 회선을 일반 디바이스 또는 Extension Mobility 프로파일에 연결시켜야 합니다.
익스텐션 모빌리티 프로파일	익스텐션 모빌리티 프로파일을 동시에 두 개 이상의 전화기에서 사용할 수 있습니다. 인터콤 디렉토리 번호 구성 창(Cisco Unified CM 관리 > 통화 라우팅 > 인터콤 > Intercom Directory Number Configuration (인터콤 디렉토리 번호 구성))의 기본 활성화된 디바이스 필드를 사용하여 이 인터콤 회선을 표시할 수 있는 디바이스를 지정합니다. Extension Mobility에 사용되지 않는 인터콤 회선의 경우에도 기본 활성화된 디바이스 필드를 구성해야 합니다.

인터콤 제한 사항

다음 제한 사항이 인터콤 기능에 적용됩니다.

기능	제한 사항
보류	이 시스템은 인터콤 통화가 보류되도록 허용하지 않습니다.
착신 전환	인터콤 통화는 착신 전환될 수 없습니다.
호전환	이 시스템은 인터콤 통화가 호전환되도록 허용하지 않습니다.
전환	이 시스템은 인터콤 통화가 전환되도록 허용하지 않습니다.
당겨 받기/직접 당겨 받기	당겨받기 그룹에는 인터콤 통화가 포함되지 않습니다.
방해사절	인터콤이 DND(방해사절)를 무시합니다.

기능	제한 사항
대역폭	충분한 대역폭이 존재하지 않을 경우, 인터콤 통화가 실패합니다.
통화 대상	두 개의 인터콤 통화가 하나의 대상으로 전송될 경우, 첫 번째 통화가 연결되고, 두 번째 통화는 통화음이 들리며 끊어집니다.
참여 및 회의끼기	인터콤은 참여 및 회의끼기를 지원하지 않습니다.
전화회의	이 시스템은 인터콤 통화가 전화회의에 사용되도록 허용하지 않습니다.
모니터링 및 녹음	활성 통화가 모니터링되고 있거나 녹음되고 있는 경우, 해당 사용자는 인터콤 전화를 받거나 걸 수 없습니다.
영상	비디오는 인터콤에서 지원되지 않습니다.
인터콤 파티션	발신 검색 공간 또는 라우트 패턴과 같은 항목에 할당된 인터콤 파티션은 삭제할 수 없습니다.
Extension Mobility	디바이스, 회선(DN), 변환 패턴 또는 기타 항목에서 사용 중인 인터콤 발신 검색 공간은 삭제할 수 없습니다.

인터콤 문제 해결

인터콤 회선에서 전화를 걸 때 통화 중 신호음

문제

사용자가 인터콤 회선에서 전화를 걸 때 전화기가 통화 중 신호음을 재생합니다.

가능한 원인

DN이 발신 번호와 동일한 인터콤 파티션에 있지 않습니다.

해결 방법

- DN이 발신 번호와 동일한 인터콤 파티션에 있는지 확인합니다.

• I

이 경우, 전화를 거는 DN이 다른 전화기에 구성되어 있고 전화기가 동일한 Unified Communications Manager 클러스터에 등록되어 있는지 확인합니다.

인터콤 통화에서 스피커, 핸드셋 또는 헤드셋과 함께 **Talkback**를 사용할 수 없음

문제

사용자는 헤드셋, 핸드셋 또는 스피커를 사용하여 인터콤 통화에 대해 TalkBack 모드로 전환할 수 없습니다.

가능한 원인

이러한 상황은 의도적인 것입니다. 해당 회선 버튼을 눌러 인터콤 통화에 대해 연결됨 상태로 전환하는 유일한 방법은 해당 회선 버튼을 누르는 것입니다.

해결 방법

사용자는 스피커, 핸드셋 또는 헤드셋을 사용하여 통화를 종료할 수 있습니다.

SCCP 문제 해결

전화기에 인터콤 회선이 표시되지 않음

문제

전화기에 인터콤 회선이 표시되지 않습니다.

가능한 원인

전화기 버전이 8.3(1) 이전일 수 있거나 버튼 템플릿이 전화기에 할당되지 않았을 수 있습니다.

해결 방법

- 전화기 버전을 확인합니다. 8.3(1) 이상인지 확인합니다.
- 버튼 템플릿이 전화기에 할당되었는지 여부를 확인합니다.
- Cisco Unified Communications Manager와 전화기 간의 스니퍼 추적을 캡처합니다. 버튼 템플릿 응답에서 인터콤 회선이 전화기로 전송되는지 여부를 확인합니다(버튼 정의 = Ox17).

전화기가 **SRST**로 폴백할 때 인터콤 회선이 표시되지 않음

문제

Unified Communications Manager 릴리스 6.0(x) 이상으로 구성된 전화기에는 두 개의 인터콤 회선이 포함되어 있습니다. Unified Communications Manager가 중지되고 SRST로 폴백합니다. 인터콤 회선은 표시되지 않습니다.

가능한 원인

SRST의 SCCP 버전은 SCCP 버전 12를 지원하지 않습니다.

해결 방법

- SRST의 SCCP 버전을 확인합니다. SRST가 SCCP 버전 12를 지원하는 경우 인터콤 회선을 지원 합니다.
- SRST가 SCCP 버전 12를 지원하는 경우 스니퍼 추적을 캡처하고 전화기가 보낸 버튼 템플릿에 인터콤 회선이 포함되어 있는지 확인합니다.

SIP 문제 해결

SIP를 실행하는 전화기 디버그

Debug sip-messages sip-task gsmfsmIsM sip-adapter 디버그 명령을 사용합니다.

SIP를 실행하는 전화기의 구성

구성 표시 — 인터콤 회선이 featureid--> 23이 포함된 일반 회선으로 구성된 경우 전화기에 명령이 표시 됩니다.

Cisco Extension Mobility 사용자가 로그인했지만 인터콤 회선이 표시되지 않음

문제

Cisco Extension Mobility 사용자는 전화기에 로그인되어 있지만 사용자 인터콤 회선이 표시되지 않습니다.

가능한 원인

기본 활성화된 디바이스가 잘못 구성되었습니다.

해결 방법

- 기본 활성화된 디바이스가 인터콤 디렉터리 번호에 구성되어 있는지 확인합니다.
- 기본 활성화된 디바이스가 사용자가 로그인되어 있는 디바이스와 일치하는지 확인합니다.

인터콤 회선이 전화기에 표시되지 않음

문제

인터콤 회선이 구성되고 전화기에 할당되었지만 전화기에는 표시되지 않습니다.

가능한 원인

기본 활성화된 디바이스 값이 이 디바이스의 인터콤 회선으로 설정됩니다.

해결 방법

구성이 완료되었으면 전화기를 재설정합니다.

■ 인터콤 회선이 전화기에 표시되지 않음



X 부

통화 수신

- 기본 회선 지원 , 355 페이지
- 착신 전환 , 359 페이지
- 통화 당겨받기 , 385 페이지
- 통화 대기 및 직접 통화, 409 페이지
- Extension Mobility , 439 페이지
- 클러스터 간 Extension Mobility , 457 페이지
- 클러스터 간 Extension Mobility 로밍, 493 페이지
- 보류 복귀 , 507 페이지
- 헛트 그룹 액세스 , 515 페이지
- 악성 전화 식별 , 525 페이지
- 통화 전환 , 537 페이지
- 외부 호전환 제한 , 551 페이지



28 장

기본 회선 지원

- 기본 회선 지원 개요, 355 페이지
- 기본 회선 지원 사전 요건, 355 페이지
- 기본 회선 지원 구성 작업 흐름, 355 페이지
- 기본 회선 지원 상호 작용, 357 페이지
- 기본 회선 지원 문제 해결, 358 페이지

기본 회선 지원 개요

전화기가 오프 hook 상태이고 모든 회선의 통화를 수신할 때 시스템에서 항상 통화에 대한 기본 회선을 선택하도록 Cisco Unified CM 관리에서 기본 회선 지원을 구성할 수 있습니다.

기본 회선 지원 사전 요건

다음 디바이스는 기본 회선 지원 기능과 호환됩니다.

Cisco Unified IP Phone 7900 시리즈, 8900 시리즈 및 9900 시리즈

지원되는 디바이스에 대한 자세한 내용은 최신 버전의 *Cisco Unified IP Phone* 설명서 및 *Cisco Unified IP Phone* 관리 지침서를 참조하십시오.

기본 회선 지원 구성 작업 흐름

Cisco CallManager 서비스 또는 디바이스 및 디바이스 프로파일에 대한 기본 회선 지원 기능을 구성하려면 다음 절차 중 하나를 수행합니다.

시작하기 전에

- 기본 회선 지원 사전 요건, 355 페이지을(를) 검토합니다.

프로시저

	명령 또는 동작	목적
단계 1	클러스터 수준 기본 회선 지원 구성, 356 페이지	(선택 사항). 전체 클러스터에 적용되는 Cisco CallManager 서비스에 대한 기본 회선 지원 기능을 구성합니다.
단계 2	디바이스에 대한 기본 회선 지원 구성, 357 페이지	(선택 사항). 기능 클러스터 전체를 활성화하지 않으려면 클러스터 내의 특정 디바이스에 대해 기본 회선 지원 기능을 구성합니다. 참고 이 매개 변수를 구성하면 통화가 전화기의 다른 회선에서 울리는 경우에도 오프 혹은으로 전환하면 전화기에서 활성화된 첫 번째 회선이 활성화됩니다. 따라서 통화는 다른 회선에서 응답되지 않습니다.

클러스터 수준 기본 회선 지원 구성

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 항상 기본 회선 사용 클러스터 수준 서비스 매개 변수를 사용하여 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **True**- 전화기가 오프 혹은 상태로 전환될 때 기본 회선이 선택되고 활성화 회선이 됩니다.
- **False**- 전화기가 오프 혹은 상태로 전환될 때 IP 전화기에서 사용 가능한 회선을 활성화 회선으로 자동 선택합니다.

이 서비스 매개 변수의 기본값은 **False**입니다.

단계 5 이 변경 내용을 SIP 전화에 적용하려면 Cisco Unified CM 관리에서 구성 적용 버튼을 클릭합니다(예: 디바이스 구성 창, 디바이스풀 구성 창 또는 적용 구성이 옵션인 다른 창).

참고 SIP 전화기에 새 구성이 적용되지 않으면 Cisco CallManager 서비스를 다음에 재설정하거나 영향을 받는 각 디바이스를 재설정할 때까지 SIP 기본 회선 지원 기능 변경 사항이 구현되지 않습니다.

디바이스에 대한 기본 회선 지원 구성

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 일반 전화 프로필.

단계 2 찾기 및 나열 창에서 항상 기본 회선 사용 설정을 변경하려는 전화기를 선택합니다.
전화기 구성 창이 나타납니다.

단계 3 항상 기본 회선 사용 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 끄기 - 전화기가 유휴 상태이고 한 회선에서 통화가 수신되는 경우 전화기 사용자는 통화가 수신된 회선에서 통화에 응답합니다.
- 켜기 - 전화기가 유휴(오프 후) 상태이고 한 회선에서 통화가 수신되는 경우 통화를 위해 기본 회선이 선택됩니다. 다른 회선의 전화는 계속 울리므로 전화기 사용자가 해당 전화를 받으려면 다른 회선을 선택해야 합니다.
- 기본값 - Unified Communications Manager에서 Cisco CallManager 서비스를 지원하는 항상 기본 회선 사용 서비스 매개 변수의 구성을 사용합니다.

단계 4 저장을 클릭합니다.

기본 회선 지원 상호 작용

기능	상호 작용
항상 기본 회선 사용	디바이스 프로필 또는 기본 디바이스 프로필 구성 창에서 항상 기본 회선 사용 매개 변수에 대해 켜기를 선택하는 경우 Cisco Extension Mobility 사용자는 Cisco Extension Mobility를 지원하는 디바이스에 로그인한 후에 이 기능을 사용할 수 있습니다.
최대 통화 수 및 통화 중 트리거 설정	전화기가 회선에 이미 전화를 건 경우에는 Unified Communications Manager는 최대 통화 수 및 통화 중 트리거 설정에 대한 구성을 사용하여 통화를 라우팅하는 방법을 결정합니다.
자동 응답	Cisco Unified CM 관리의 자동 응답 드롭다운 목록에서 헤드셋을 사용하여 자동 응답 옵션을 선택하거나 스피커폰 옵션을 자동 응답으로 선택하는 경우 자동 응답 구성은 항상 프라임 회선 사용 매개 변수에 대한 구성을 무시합니다.

기본 회선 지원 문제 해결

True로 설정되면 기본 회선 지원이 작동하지 않음

문제 클러스터 수준 서비스 매개 변수에서 항상 기본 회선 사용을 **True**로 설정하고 IP 전화기가 오프 hook 상태가 되면 기본 회선이 활성 회선이 됩니다. 통화가 두 번째 회선에서 울릴 때도 사용자가 오프 hook 상태로 전환될 때 첫 번째 회선만 활성화됩니다. 전화기는 두 번째 회선의 통화에 응답하지 않습니다. 그러나 여러 회선 표시가 있는 IP 전화기가 7.1.2 전화기 로드와 함께 사용되는 경우 두 번째 회선이 울릴 때 전화기에서 기본 회선을 사용하지 않습니다. 사용자가 핸드셋을 들면 전화기는 두 번째 회선의 통화에 응답합니다.

해결 방법 통화가 시작될 때 보조 회선이 연결되지 않도록 기본 회선에 대한 회선 버튼을 누릅니다.

착신 전화에 응답할 수 없음

문제 사용자는 IP 전화기에서 오프 hook으로 전환된 후 자동으로 착신 전화를 받을 수 없으며 응답 소프트키를 눌러 통화에 응답해야 합니다.

해결 방법 문제를 해결하려면 다음 절차를 수행합니다.

1. Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 서비스 매개 변수.
2. 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 서버를 선택합니다.
3. 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
4. 클러스터 수준 매개 변수(디바이스 전화)에서 항상 프라임 회선 사용을 **False**로 설정합니다.

착신 전화가 자동으로 응답됨

문제 IP 전화기의 공유 회선에서 인바운드 통화가 수신되면, 해당 통화에 응답하거나 발신 전화를 걸 수 있는 옵션 없이, 핸드셋을 들면 통화가 즉시 응답됩니다. 자동 회선 선택이 비활성화로 설정된 경우에도 이 동작은 변경되지 않습니다.

해결 방법 문제를 해결하려면 다음 절차를 수행합니다.

1. Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 서비스 매개 변수.
2. 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 서버를 선택합니다.
3. 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
4. 클러스터 수준 매개 변수(디바이스 전화)에서 항상 프라임 회선 사용을 **False**로 설정합니다.



29 장

착신 전환

- 착신 전환 개요, 359 페이지
- 통화 착신 전환 구성 작업 흐름, 361 페이지
- 착신 전환 상호 작용, 379 페이지
- 착신 전환 제한 사항, 383 페이지

착신 전환 개요

사용자는 통화를 다른 전화기로 착신 전환하도록 Cisco Unified IP Phone을 구성할 수 있습니다. 다음과 같은 통화 착신 전환 유형이 지원됩니다.

- 착신 전환 대역폭 없음 - 대역폭이 부족하여 디렉터리 번호에 대한 통화가 실패하면 통화를 착신 전환하고, PSTN(공중 전화 교환망)을 대체 경로 또는 음성 메일 시스템으로 사용하여 자동으로 전달 기능을 AAR(자동 대체 라우팅) 대상에 제공합니다.
- 대체 대상으로 착신 전환 - 디렉터리 번호에 대한 통화 및 착신 전환된 대상에 대한 통화가 응답하지 않을 때 통화를 착신 전환합니다. 통화가 마지막 수단으로 대체 대상으로 전환됩니다. 이 착신 전환 유형은 “MLPP 대체 상대 대상”으로도 불립니다.
- CFA(모두 착신 전환) - 모든 통화를 디렉터리 번호로 착신 전환합니다.
- CFB(통화 시 착신 전환) - 회선이 사용 중이고 구성된 착신 전환 트리거 값에 도달하는 경우에만 통화를 착신 전환합니다.
- CFNA(부재중 착신 전환) - 구성된 응답 없음 벨소리 지속 기간 타이머가 초과되거나 대상이 등록 해제된 후 전화기가 응답하지 않을 때 통화를 착신 전환합니다.
- 통화권이 아닌 경우 착신 전환(CFNC) - 헌트 목록이 소모되거나 시간이 초과될 때 통화를 착신 전환하며, 관련 헌트 파일럿은 최종 호 전환에 대한 “개인 기본 설정 사용”을 지정합니다.
- 등록되지 않은 착신 전환(CFU) - 원격 WAN 링크 실패로 인해 전화기가 등록되지 않은 경우 통화를 착신 전환하고, PSTN(공중 전화 교환망)을 통해 자동으로 경로 전환을 제공합니다. 발신자 유형(내부 또는 외부)을 기준으로 통화를 착신 전환할 수도 있습니다.

- **CFA 대상 무시** - 통화를 착신 전환할 사용자(대상)가 착신 전환된 통화(이니시에이터)에게 전화를 걸 때 통화를 착신 전환합니다. 대상으로 돌아가는 통화 착신 전환 대신 이니시에이터의 전화기가 울립니다.

CFA 루프 예방 및 CFA 루프 차단을 포함하여 모두 착신 전환

CFA(모두 착신 전환)를 사용하면 전화기 사용자가 모든 통화를 디렉터리 번호로 착신 전환할 수 있습니다.

내부 및 외부 통화에 대한 CFA를 구성하고, 발신 검색 공간(CSS)을 구성하여 음성 메일 시스템 또는 전화 건 대상 번호로 통화를 전달할 수 있습니다. Unified Communications Manager에는 CFA에 대한 보조 발신 검색 공간 구성 필드가 포함되어 있습니다. CFA의 보조 CSS는 CFA의 기존 CSS와 결합하여 대체 CSS 시스템 구성 지원을 허용합니다. CFA를 활성화하면 CFA의 기본 및 보조 CSS만 사용하여 CFA 대상의 유효성을 확인하고 통화를 CFA 대상으로 재전송합니다. 이러한 필드가 비어 있는 경우에는 널 CSS가 사용됩니다. CFA의 기본 CSS 및 CFA 필드의 보조 CSS에 구성된 CSS 필드만 사용됩니다. 전화기에서 CFA가 활성화된 경우 CFA의 CSS와 CFA의 보조 CSS를 사용하여 CFA 대상의 유효성을 검사하고 CFA 대상이 데이터베이스에 기록됩니다. CFA가 활성화되면 CFA의 CSS와 CFA의 보조 CSS에 대해 CFA 대상의 유효성이 항상 확인됩니다.

Unified Communications Manager CFA 루프가 식별되면 전화기에서 CFA 활성화를 방지합니다. 예를 들어, Unified Communications Manager는 사용자 디렉터리 번호 1000을 사용하여 전화기에서 착신 전환 소프트웨어를 누르고 CFA 대상으로 1001을 입력하고, 1001이 모든 통화를 디렉터리 번호 1002로 착신 전환하고, 모든 통화를 디렉터리 번호 1003으로 착신 전환하고, 모든 통화를 1000으로 착신 전환하는 경우 착신 전환 루프를 식별합니다. 이 경우 Unified Communications Manager는 루프가 발생했음을 식별하고 디렉터리 번호 1000으로 전화기에서 CFA를 활성화하는 것을 방지합니다.



팁 서로 다른 파티션에 동일한 디렉터리 번호가 존재하는 경우(예: 파티션 1과 2에 디렉터리 번호 1000이 존재하는 경우) Unified Communications Manager는 전화기에서 CFA 활성화를 허용합니다.

Unified Communications Manager에서 CFA 루프 차단을 지원하므로 CFA 루프는 통화 처리에 영향을 주지 않습니다. 이는 CFA 루프가 식별되는 경우 통화가 전체 착신 전환 체인을 통과하여 모두 통화 착신 전환 루프를 차단하고, CFNA, CFB 또는 기타 착신 전환 옵션이 착신 전환 체인에 있는 디렉터리 번호 중 하나에 대해 CFA와 함께 구성된 경우에도 루프가 예상대로 완료될 수 있도록 해줍니다.

예를 들어, 디렉터리 번호 1000을 사용하는 전화기의 사용자는 모든 통화를 디렉터리 번호 1001로 착신 전환하고, 이어서 모든 통화를 디렉터리 번호 1002로 착신 전환한 후, 모든 통화를 디렉터리 번호 1000으로 착신 전환하여 CFA 루프를 생성합니다. 또한 디렉터리 번호 1002에서 디렉터리 번호 1004로 CFNA를 구성했습니다. 디렉터리 번호 1003을 사용하는 전화기의 사용자가 디렉터리 번호 1000으로 전화를 걸면, 1001로 착신 전환하고, 1002로 착신 전환합니다. Unified Communications Manager에서 CFA 루프를 식별하고 루프를 차단하고 디렉터리 번호 1002에 연결을 시도합니다. 디렉터리 번호 1002를 사용하는 전화기의 사용자가 통화 응답하기 전에 응답 없음 벨소리 지속 시간 타이머가 만료되면 Unified Communications Manager는 통화를 디렉터리 번호 1004로 착신 전환합니다.

단일 통화의 경우 Unified Communications Manager는 여러 CFA 루프를 식별하고 각 루프가 식별된 후 통화 연결을 시도할 수 있습니다.

통화 착신 전환 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	착신 전환에 대한 파티션 구성, 361 페이지	관리자는 파티션을 구성하여 통화 착신 전환을 설계 기준 및 요구 사항에 따라 특정 번호로 제한할 수 있습니다.
단계 2	착신 전환에 대한 발신 검색 공간 구성, 363 페이지	관리자는 설계 기준 및 요구 사항을 기반으로 하여 통화 착신 전환을 특정 번호로 제한하도록 발신 검색 공간을 구성할 수 있습니다.
단계 3	헌트 목록이 소모되었거나 헌트 타이머가 만료되면 착신 전환 구성, 364 페이지	헌팅이 실패할 경우(즉, 목록에서 헌트 번호를 선택하지 않았거나 헌트 타이머가 초과되어 헌트 상대방 응답 없이 헌팅이 종료된 경우) 통화를 착신 전환할 수 있습니다.
단계 4	착신 전환(대역폭 없음) 구성, 366 페이지	대역폭 부족으로 인해 착신 디렉터리 번호에 대한 통화가 실패할 경우 PSTN(공중 전화망)을 대체 경로로 사용하여 AAR(자동 대체 라우팅) 대상으로 통화를 착신 전환하거나 음성 메일 시스템으로 통화를 전달할 수 있습니다.
단계 5	착신 전환 대체 대상 구성, 367 페이지	응답하지 않는 통화를 디렉터리 번호와 착신 대상으로 착신 전환할 수 있습니다. 통화는 마지막 수단으로 대체 대상으로 전환됩니다.
단계 6	다른 착신 전환 유형 구성, 368 페이지	CFA, CFB, CFNA, CFNA 및 CFU와 같은 추가 착신 전환 유형을 구성할 수 있습니다. 디렉터리 번호 구성 창에서 이러한 착신 전환 유형을 모두 구성할 수 있습니다.
단계 7	통화 착신 전환에 대한 대상 오버라이드 활성화, 378 페이지	관리자는 CFA의 대상이 CFA의 이니시에이터에게 전화를 걸 때 CFA를 무시할 수 있습니다. 이 기능을 사용하면 CFA 대상이 중요한 통화에 대해 이니시에이터에게 연락할 수 있습니다.

착신 전환에 대한 파티션 구성

연결성 특성이 비슷한 디렉터리 번호(DN) 및 라우트 패턴의 논리적 그룹을 만들기 위해 파티션을 구성합니다. 파티션은 조직, 위치 및 통화 유형에 따라 라우트 플랜을 논리적 하위 집합으로 나눔으로써 콜 라우팅을 지원합니다. 여러 파티션을 구성할 수 있습니다.

파티션을 구성하여 통화 착신 전환을 설계 기준과 요구 사항에 따라 특정 번호로 제한합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 파티션.

단계 2 새로 추가를 클릭하여 새 파티션을 생성합니다.

단계 3 파티션 이름, 설명 필드에 경로 플랜에 고유한 파티션 이름을 입력합니다.

파티션 이름에는 영숫자 문자는 물론 공백, 하이픈(-) 및 밑줄(_)을 사용할 수 있습니다. 파티션 이름에 대한 지침은 온라인 도움말을 참조하십시오.

단계 4 파티션 이름 뒤에 쉼표(.)를 입력하고 동일한 줄에 파티션 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\), 꺾쇠괄호(<>) 또는 대괄호([])는 사용할 수 없습니다.

설명을 입력하지 않으면 Cisco Unified Communications Manager에서 자동으로 이 필드에 파티션 이름을 입력합니다.

단계 5 여러 파티션을 생성하려면 각 파티션 항목마다 한 행을 사용합니다.

단계 6 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.

시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성 상태로 유지됩니다.

단계 7 구성할 다음 라디오 버튼 중 하나를 선택하고 시간대를 구성합니다.

- 시작 디바이스—이 라디오 버튼을 선택하면 시스템은 발신 디바이스의 표준 시간대를 시간 일정과 비교하여 파티션을 수신 통화를 받는 데 사용할 수 있는지 여부를 확인합니다.
- 특정 표준 시간대—이 라디오 버튼을 선택한 후에 드롭다운 목록에서 표준 시간대를 선택합니다. 시스템은 선택한 표준 시간대를 시간 일정과 비교하여 수신 통화를 받는 데 파티션을 사용할 수 있는지 여부를 확인합니다.

단계 8 저장을 클릭합니다.

착신 전환에 대한 파티션 이름 지침

발신 검색 공간의 파티션 목록에서 최대 문자 수는 1024자로 제한됩니다. 즉, CSS의 최대 파티션 수는 파티션 이름의 길이에 따라 달라집니다. 다음 표를 사용하여 파티션 이름이 고정 길이인 경우 발신 검색 공간에 추가할 수 있는 최대 파티션 수를 결정합니다.

표 28: 파티션 이름 지침

파티션 이름 길이	최대 파티션 수
2자	340
3자	256
4자	204

파티션 이름 길이	최대 파티션 수
5자	172
...	...
10자	92
15자	64

착신 전환에 대한 발신 검색 공간 구성

발신 검색 공간은 일반적으로 디바이스에 할당되어 있는 정렬된 경로 파티션 목록입니다. 발신 검색 공간은 통화를 완료하려고 시도할 때 발신 디바이스에서 검색할 수 있는 파티션을 결정합니다.

설계 기준 및 요구 사항을 기반으로 하여 착신 전환을 특정 번호로 제한하도록 발신 검색 공간을 구성합니다.

시작하기 전에

[착신 전환에 대한 파티션 구성, 361 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 제어 클래스 > 발신 검색 공간.

단계 2 새로 추가를 클릭합니다.

단계 3 이름 필드에 이름을 입력합니다.

각 발신 검색 공간 이름은 시스템에 고유해야 합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.

단계 4 설명 필드에 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.

단계 5 사용 가능한 파티션 드롭다운 목록에서 다음 단계 중 하나를 수행합니다.

- 단일 파티션의 경우 해당 파티션을 선택합니다.
- 여러 파티션의 경우 컨트롤(**CTRL**) 키를 누른 상태에서 해당 파티션을 선택합니다.

단계 6 상자 사이에서 아래쪽 화살표를 선택하여 선택한 파티션 필드로 파티션을 이동합니다.

단계 7 (선택 사항) 선택한 파티션 상자 오른쪽의 화살표 키를 사용하여 선택한 파티션의 우선 순위를 변경합니다.

단계 8 저장을 클릭합니다.

힌트 목록이 소모되었거나 힌트 타이머가 만료되면 착신 전환 구성

힌트의 개념은 착신 전환의 개념과 다릅니다. 힌트를 사용하면 Unified Communications Manager에서 하나 이상의 숫자 목록으로 통화를 확장할 수 있습니다. 여기서 각 목록은 고정된 알고리즘 집합에서 선택되는 힌트 순서를 지정합니다. 통화가 이러한 목록에서 힌트 상대방으로 확장되고 상대방이 응답하지 않거나 통화 중인 경우에는 다음 힌트 상대방과의 힌트를 다시 시작합니다. (다음 힌트 상대방은 현재 힌트 알고리즘에 따라 달라집니다.) 그런 다음 응답 없음 착신 전환(CFNA), CFB(통화 시 착신 전환) 또는 시도된 상대방에 대해 구성된 CFA(모두 착신 전환) 값을 무시합니다.

착신 전환을 사용하면 착신자가 응답에 실패하거나 통화 중이고 힌트가 발생하지 않을 때 통화를 확장(전환 또는 재전송)하는 방법에 대한 세부 제어가 가능합니다. 예를 들어, 회선의 CFNA 값이 힌트 파일럿 번호로 설정된 경우 응답되지 않은 해당 회선에 대한 통화는 힌트 파일럿 번호로 전환되어 힌트를 시작합니다.

시작하기 전에

[착신 전환에 대한 발신 검색 공간 구성, 363 페이지](#)

프로시저

-
- 단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 경로/힌트 > 힌트 파일럿. 힌트 파일럿 찾기 및 나열 창이 표시됩니다.
 - 단계 **2** 찾기를 클릭합니다.
구성된 힌트 파일럿 목록이 표시됩니다.
 - 단계 **3** 힌트에 실패한 경우 통화 처리를 구성하려는 패턴을 선택합니다.
힌트 파일럿 구성 창이 표시됩니다.
 - 단계 **4** 힌트 통화 처리 설정 영역에 대한 힌트 파일럿 구성에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
 - 단계 **5** 저장을 클릭합니다.
-

착신 전환에 대한 힌트 통화 처리 필드

필드	설명
힌트 통화 취급 설정	
참고	<p>힌트 응답 없음 착신 전환 또는 힌트 통화 중 착신 전환 필드는 라우트 목록에서 통화를 이동하는 데 사용됩니다. 대기는 라우트 목록에서 발신자를 보류하는 데 사용됩니다. 따라서 대기를 활성화하는 경우 힌트 응답 없음 착신 전환과 힌트 통화 중 착신 전환이 모두 자동으로 비활성화됩니다. 반대로 힌트 응답 없음 착신 전환이나 힌트 통화 중 착신 전환을 활성화하는 경우 대기가 자동으로 비활성화됩니다.</p>

필드	설명
헛통 응답 없음 착신 전환	<p>헛통 목록을 통해 분배되는 전화를 특정 기간 내에 받지 않는 경우 이 필드에는 통화가 착신 전환되는 대상을 지정합니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 응답하지 않는 통화를 착신 전환하지 않음 • 회선 그룹 구성원의 착신 전환 설정 사용(개인 기본 설정 사용 확인란 대체) • 응답하지 않는 통화의 착신 전환 대상 <ul style="list-style-type: none"> • 대상 - 통화를 착신 전환해야 하는 디렉터리 번호를 입력합니다. • 발신 검색 공간 - 이 디렉터리 번호를 사용하는 모든 디바이스에 적용되는 드롭다운 목록에서 발신 검색 공간을 선택합니다. • 최대 헛통 타이머 - 대기 없는 헛통에 대한 최대 시간을 지정하는 값(초)을 입력합니다. 유효한 값은 1~3600입니다. 기본값은 1800초(30분)입니다. <p>주의 연결된 회선 그룹의 RNA 복귀 시간 초과 및 최대 헛통 타이머에 동일한 값을 지정하지 마십시오.</p> <p> 응답 없음 착신 전환 타이머는 회선 그룹의 RNA 타이머보다 커야합니다.</p> <p> 응답 없음 착신 전환 타이머는 회선 그룹의 RNA 타이머의 배수가 아니어야합니다.</p> <p>헛통 구성원이 전화를 받거나 타이머가 만료되기 전에 헛통 목록이 모두 사용되는 경우 이 타이머는 취소됩니다. 이 타이머의 값을 지정하지 않은 경우에는 헛통 구성원이 전화를 받거나 헛통이 모두 사용될 때까지 헛통이 계속됩니다. 어느 이벤트도 발생하지 않는 경우 30분 동안 헛통이 계속된 후에 통화가 최종 처리를 위해 수신됩니다.</p> <p>참고 헛통이 착신 전환 최대 홉 수 서비스 매개 변수에 지정된 홉 수를 초과하는 경우 30분 최대 헛통 타이머 값 이전에 헛통이 만료되고 발신자에게 다시걸기 신호음이 들립니다.</p>

착신 전환(대역폭 없음) 구성

프로시저

- 단계 1 Cisco Unified CM 관리자에서 다음 메뉴를 선택합니다.통화 라우팅 > 디렉터리 번호 구성.
디렉터리 번호 찾기 및 나열 창이 표시됩니다.
- 단계 2 찾기를 클릭합니다.
구성된 디렉터리 번호 목록이 표시됩니다.
- 단계 3 대역폭이 충분하지 않을 때 착신 전환을 구성할 디렉터리 번호를 선택합니다.
디렉터리 번호 구성 창이 표시됩니다.
- 단계 4 **AAR** 설정 영역에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [착신 전환에 대한 디렉터리 번호 구성 필드, 367 페이지](#)를 참조하십시오.
- 단계 5 저장을 클릭합니다.

착신 전환에 대한 디렉터리 번호 구성 필드

필드	설명
음성 메일	<p>통화를 음성 메일로 착신 전환하려면 이 확인란을 선택합니다.</p> <p>참고 이 확인란을 선택하면 Unified Communications Manager가 대상 및 발신 검색 공간 필드의 값을 무시합니다.</p>
AAR 대상 마스크	전화 걸 AAR 대상을 결정하려면 외부 전화 번호 마스크 대신 이 설정을 사용합니다.
AAR 그룹	<p>드롭다운 목록에서 AAR 그룹을 선택합니다. AAR 그룹은 불충분한 대역폭으로 인해 차단될 수 있는 통화를 라우팅하는 데 사용되는 접두사 번호를 제공합니다. 없음을 선택하면 서버에서 차단된 통화를 다시 라우팅하려는 시도를 하지 않습니다.</p> <p>또한 시스템 시스템 > 서비스 매개 변수의 우선 순위 대체 상대 시간 초과 서비스 매개 변수에서 이 값을 구성할 수 있습니다.</p>
통화 착신 전환 내역에 이 대상 보존	<p>기본적으로 디렉터리 번호 구성에서 통화의 AAR 레그를 통화 기록에 유지하므로, AAR이 음성 메일 시스템으로 착신 전환되어 사용자에게 음성 메시지를 남기라는 메시지를 표시합니다.</p> <p>이 확인란을 선택하면 AAR 통화 레그가 착신 전환 기록에 표시됩니다.</p>

착신 전환 대체 대상 구성

시작하기 전에

[착신 전환\(대역폭 없음\) 구성, 366 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 디렉터리 번호 구성. 디렉터리 번호 찾기 및 나열 창이 표시됩니다.
- 단계 2 찾기를 클릭합니다. 구성된 디렉터리 번호 목록이 표시됩니다.

단계 3 대체 대상을 구성할 디렉터리 번호를 선택합니다.

디렉터리 번호 구성 창이 표시됩니다.

단계 4 MLPP 대체 상대 및 기밀 액세스 수준 설정 영역에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [착신 전환에 대한 MLPP 대체 상대 및 기밀 액세스 수준 설정 필드](#), 368 페이지를 참조하십시오.

단계 5 저장을 클릭합니다.

착신 전환에 대한 MLPP 대체 상대 및 기밀 액세스 수준 설정 필드

필드	설명
대상	이 디렉터리 번호에서 우선 순위 통화를 수신하였는데 이 번호도, 이 번호의 착신 전환 대상도 우선 순위 통화를 받지 않을 때 MLPP 우선 순위 통화를 전환해야 하는 번호를 입력합니다. 값에는 숫자, 파운드 기호(#) 및 별표(*)가 포함될 수 있습니다.
MLPP 발신 검색 공간	드롭다운 목록에서 MLPP 대체 상대 대상 번호와 연결할 발신 검색 공간을 선택합니다.
MLPP 응답 없음 벨소리 지속 기간(초)	이 디렉터리 번호와 해당 통화 착신 전환 대상에서 우선 순위 통화에 응답하지 않을 경우 MLPP 우선 순위 통화가 이 디렉터리 번호 대체 상대로 전송되기까지 대기하는 시간을 초 단위(4~60)로 입력합니다. 또한 Cisco Unified CM 관리에서 시스템 > 서비스 매개 변수의 우선 순위 대체 상대 시간 초과 서비스 매개 변수에서 이 값을 구성할 수 있습니다.

다른 착신 전환 유형 구성

디렉터리 번호 구성 창에서 모두 착신 전환(CFA), 통화 시 착신 전환(CFB), 부재 중 착신 전환(CFNA), 통화권이 아닌 경우 착신 전환(CFNC) 및 등록되지 않은 착신 전환(CFU) 등을 구성할 수 있습니다.

시작하기 전에

- 통화 착신 전환 기능이 의도한 대로 작동하려면 구성된 전화기와 디렉터리 번호를 다양한 파티션에서 구성하는 것이 좋습니다. 그러면 통화 착신 전환 발신 검색 공간도 구성되거나 다른 착신 전환이 실패할 수 있습니다. 통화가 통화 착신 전환 대상으로 전환되거나 재전송되는 경우 통화를 착신 전환하도록 구성된 통화 착신 전환 발신 검색 공간이 사용됩니다.
- [착신 전환 대체 대상 구성](#), 367 페이지

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 디렉터리 번호 구성.

디렉터리 번호 찾기 및 나열 창이 표시됩니다.

단계 2 디렉터리 번호 구성 창에서 통화 착신 전환 및 통화 당겨받기 설정 필드를 구성하여 CFA, CFB, CFNA, CFNC 및 CFU를 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 [착신 전환 필드, 369 페이지](#)를 참조하십시오.

단계 3 저장을 클릭합니다.

착신 전환 필드

필드	설명
통화 착신 전환 및 통화 당겨받기 설정	

설명

이 옵션에 사용할 수 있는 값으로는 다음 3가지가 있습니다.

- 시스템 기본값 사용 - **CFA CSS** 활성화 정책 서비스 매개 변수는 통화 착신 전환에 사용할 모두 착신 전환 발신 검색 공간을 결정합니다. **CFA CSS** 활성화 정책 서비스 매개 변수를 구성된 **CSS** 사용으로 설정한 경우 모두 착신 전환 발신 검색 공간 및 모두 착신 전환용 보조 발신 검색 공간이 통화 착신 전환에 사용됩니다. 이 값이 기본 설정입니다.
- 구성된 **CSS** 사용 - 디렉터리 번호 구성 창에서 명시적으로 구성된 모두 착신 전환 발신 검색 공간이 착신 전환 활성화 및 통화 착신 전환을 제어합니다.

모두 착신 전환 발신 검색 공간을 없음으로 설정하면 착신 전환에 대한 **CSS**가 구성되지 않습니다. 파티션의 디렉터리 번호에 대한 모두 착신 전환 활성화 시도가 실패합니다. 모두 착신 전환 활성화 중에는 모두 착신 전환 발신 검색 공간 및 모두 착신 전환용 보조 발신 검색 공간의 변경이 적용되지 않습니다.

- 디바이스/회선 **CSS** 사용 - 디렉터리 번호 발신 검색 공간과 디바이스 발신 검색 공간의 조합은 모두 착신 전환 발신 검색 공간을 명시적으로 구성하지 않고 모두 착신 전환 활성화 및 착신 전환을 제어합니다.

전화기에서 모두 착신 전환이 활성화되면, 모두 착신 전환 발신 검색 공간 및 모두 착신 전환용 보조 발신 검색 공간이 활성화 디바이스에 대한 디렉터리 번호 발신 검색 공간 및 디바이스 발신 검색 공간으로 자동으로 채워집니다.

모두 착신 전환 발신 검색 공간이 없음으로 설정된 경우, 전화기를 통해 착신 전환이 활성화되면 디렉터리 번호 발신 검색 공간과 활성화 디바이스 발신 검색 공간 조합이 모두 착신 전환 시도를 제어합니다.

CFA CSS 활성화 정책—서비스 매개 변수 구성 창에서 의도한 대로 모두 착신 전환에 대해 이 서비스 매개 변수를 올바르게 구성해야 합니다. 이 서비스 매개 변수에서 사용할 수 있는 값은 다음 2가지입니다.

- 구성된 **CSS** 사용 — 기본 및 보조 CFA 발신 검색 공간이 통화 착신 전환 시도를 제어합니다.
- 디바이스/회선 **CSS** 활성화 - 기본 및 보조 CFA 발신 검색 공간이 기본 회선 발신 검색 공간 및 활성화 디바이스 발신 검색 공간으로 업데이트됩니다.

로밍—동일한 디바이스 모빌리티 그룹에서 디바이스가 로밍 중인 경우 Cisco Unified Communications Manager는 디바이스 모빌리티 **CSS**를 사용하여 로컬 게이트웨이에 연결합니다. 사용자가 전화기에 모든 통화 착신 전환을 설정하는 경우 CFA **CSS**가 없음으로 설정되고 CFA **CSS** 활성화 정책이 디바이스/회선 **CSS** 활성화로 설정되어 있으면 다음과 같은 현상이 발생합니다.

- 디바이스가 홈 위치에 있는 경우 디바이스 **CSS** 및 회선 **CSS**가 CFA **CSS**로 사용됩니다.
- 동일한 디바이스 모빌리티 그룹에서 디바이스가 로밍 중인 경우 로밍 디바이스폴의 디바이스 모빌리티 **CSS** 및 회선 **CSS**가 CFA **CSS**로 사용됩니다.
- 디바이스가 다른 디바이스 모빌리티 그룹에서 로밍 중인 경우 디바이스 **CSS** 및 회선 **CSS**가 CFA **CSS**로 사용됩니다.

필드	설명
모두 착신 전환	<p>이 필드 행의 필드는 디렉터리 번호가 모두 착신 전환으로 설정된 경우 이 디렉터리 번호에 대한 통화의 착신 전환 처리를 지정합니다. 발신 검색 공간 필드는 사용자가 전화기에서 모든 통화 착신 전환을 활성화한 경우 입력되는 모두 착신 전환 대상을 확인하는 데 사용됩니다. 또한 이 필드는 통화를 모두 착신 전환 대상으로 재전송하는 데에도 사용됩니다.</p> <p>다음과 같은 값을 구성합니다.</p> <ul style="list-style-type: none"> 음성 메일 - 음성 메일 프로필 구성 창의 설정을 사용하려면 이 확인란을 선택합니다. <p>참고 이 확인란을 선택하면 Unified Communications Manager가 대상 및 발신 검색 공간 필드의 값을 무시합니다.</p> <ul style="list-style-type: none"> 대상 - 이 필드는 모든 통화가 착신 전환되는 디렉터리 번호를 나타냅니다. 외부 대상을 포함하여 걸 수 있는 전화 번호를 사용합니다. 발신 검색 공간 - 이 설정은 이 디렉터리 번호를 사용하는 모든 디바이스에 적용됩니다. 착신 전환 최대 홉 수 - Cisco Unified CM 관리자에서 이 매개 변수를 구성하고 시스템 > 서비스 매개 변수를 선택합니다. <p>이 서비스 매개 변수는 단일 통화를 착신 전환하거나 전환할 수 있는 최대 홉수를 지정하며 QSIG 통화에 대한 특별한 고려 사항이 있습니다. 수신 QSIG 통화의 경우 최대값은 15(ISO 사양당)입니다. 이 필드에 더 큰 값을 지정하면 지정된 값이 비 QSIG 통화 및 수신 QSIG 통화에 적용되고, 통화는 최대 15 번만 전환됩니다. QSIG 트렁크를 구성하는 경우 이 매개 변수를 15로 설정하는 것이 좋습니다.</p> <p>예를 들어, 이 매개 변수의 값이 7이고, 7개의 홉으로 구성되는 디렉터리 번호 1000부터 007까지 연속적으로 모든 체인의 착신 전환이 발생하는 경우에는 Cisco Unified Communications Manager는 단일 통화에 대해 착신 전환 홉이 7개 이상 지원되지 않으므로 디렉터리 번호가 2000인 전화기 사용자가 디렉터리 번호 1000으로 CFA를 활성화할 수 없습니다.</p>
모두 착신 전환용 보조 발신 검색 공간	<p>통화 착신 전환은 회선 기반 기능이므로 디바이스 발신 검색 공간을 알 수 없는 경우 시스템에서 통화를 착신 전환하는 데 회선 발신 검색 공간만 사용합니다. 회선 발신 검색 공간이 제한적이며 전송할 수 없는 경우 착신 전환 시도가 실패합니다.</p> <p>모든 통화 착신 전환용 보조 발신 검색 공간을 추가하면 착신 전환을 활성화할 수 있는 해결책이 제공됩니다. 모든 통화 착신 전환용 기본 발신 검색 공간과 모든 통화 착신 전환용 보조 발신 검색 공간은 연결(기본 CFA CSS + 보조 CFA CSS)됩니다. Unified Communications Manager는 이 조합을 사용하여 CFA 대상을 확인하고 통화를 착신 전환합니다.</p>

질문	
	<p>이 필드 행의 필드에서는 디렉터리 번호가 통화 중인 경우 이 디렉터리 번호로의 내부 통화에 대한 착신 전환 처리를 지정합니다. 대상 및 발신 검색 공간 필드의 값은 착신 전환 대상으로 통화를 재전송하는 데 사용됩니다. 다음과 같은 값을 구성합니다.</p>
• 음성 메일 - 내부 통화에 대해 음성 메일 프로필 구성 창에 구성된 값을 사용하려면 이 확인란을 선택합니다.	
참고	<p>이 확인란을 선택하면 음성 메일 파일럿의 발신 검색 공간이 사용됩니다. Unified Communications Manager는 대상 및 발신 검색 공간 필드의 값을 무시합니다.</p>
참고	<p>내부 통화에 대해 이 확인란을 선택한 경우 외부 통화에 대해 자동으로 음성 메일 확인란이 선택됩니다. 음성 메일 시스템으로 외부 통화를 착신 전환하지 않으려면 외부 통화에 대해 음성 메일 확인란을 선택 취소해야 합니다.</p>
• 대상 - 이 필드는 내부 통화에 대한 통화 중 착신 전환 대상을 나타냅니다. 외부 대상을 포함하여 걸 수 있는 전화 번호를 사용합니다.	
참고	<p>내부 통화의 대상 값을 입력하는 경우 이 값은 시스템에서 자동으로 외부 통화의 대상 필드로 복사됩니다. 다른 대상으로 외부 통화를 착신 전환하려는 경우 외부 통화에 대한 대상 필드에 다른 값을 입력해야 합니다.</p>
• 발신 검색 공간 - 통화 중 내부 착신 전환 발신 검색 공간은 통화 중 내부 착신 전환 대상으로 통화를 착신 전환하는 데 사용됩니다. 이 디렉터리 번호를 사용하는 모든 디바이스에 적용됩니다.	
참고	<p>시스템에서 파티션 및 발신 검색 공간을 사용하고 있는 경우 착신 전환 발신 검색 공간을 구성하는 것이 좋습니다. 통화가 통화 착신 전환 대상으로 전환되거나 재전송되는 경우 통화를 착신 전환하도록 구성된 통화 착신 전환 발신 검색 공간이 사용됩니다. 발신 검색 공간 필드가 없음인 경우 시스템에서 파티션 및 발신 검색 공간을 사용 중이면 착신 전환 작업은 실패합니다. 예를 들어 통화 중 착신 전환 대상을 구성하는 경우 통화 중 착신 전환 발신 검색 공간도 구성해야 합니다. 통화 중 착신 전환 발신 검색 공간을 구성하지 않은 경우 통화 중 착신 전환 대상이 파티션에 있으면 착신 전환 작업이 실패합니다.</p>
참고	<p>내부 통화에 대한 발신 검색 공간을 선택하는 경우 외부 통화에 대한 발신 검색 공간 설정으로 이 값이 자동으로 복사됩니다. 외부 통화를 다른 발신 검색 공간으로 착신 전환하려면 발신 검색 공간에서 외부 통화에 대해 다른 값을 선택해야 합니다.</p>
통화 중 착신 전환 트리거는 각 회선 형태에 대해 구성되어 있으며 회선 형태에 대해 구성된 최대 통화 수를 초과할 수 없습니다. 통화 중 착신 전환 트리거는 통화 중 착신 전환 설정이 활성화되기 전에 회선에 존재하는 활성 통화 수를 결정합니다(예: 10개 통화).	
팁	<p>사용자가 발신 전화를 걸고 호 전환을 수행할 수 있도록 통화 중 트리거를 최대 통화 수보다 조금 작게 유지합니다.</p>
팁	<p>통화 중인 디렉터리 번호로 통화를 착신 전환하면 통화가 완료되지 않습니다.</p>

필드	설명
통화 중 외부 착신 전환	<p>이 필드 행의 필드에서는 디렉터리 번호가 통화 중인 경우 이 디렉터리 번호로의 외부 통화에 대한 착신 전환 처리를 지정합니다. 대상 및 발신 검색 공간 필드는 착신 전환 대상으로 통화를 재전송하는 데 사용됩니다.</p> <p>다음과 같은 값을 구성합니다.</p> <ul style="list-style-type: none"> 음성 메일 - 외부 통화에 대해 음성 메일 프로필 구성 창에 구성된 값을 사용하려면 이 확인란을 선택합니다. <ul style="list-style-type: none"> 참고 이 확인란을 선택하면 음성 메일 파일럿의 발신 검색 공간이 사용됩니다. Unified Communications Manager는 대상 및 발신 검색 공간 필드의 값을 무시합니다. 참고 내부 통화에 대해 이 확인란을 선택한 경우 외부 통화에 대해 자동으로 음성 메일 확인란이 선택됩니다. 음성 메일 시스템으로 외부 통화를 착신 전환하지 않으려면 외부 통화에 대해 음성 메일 확인란을 선택 취소해야 합니다. 대상 - 이 필드는 외부 통화에 대한 통화 중 착신 전환 대상을 나타냅니다. 외부 대상을 포함하여 걸 수 있는 전화 번호를 사용합니다. <ul style="list-style-type: none"> 참고 내부 통화의 대상 값을 입력하는 경우 이 값은 시스템에서 자동으로 외부 통화의 대상 필드로 복사됩니다. 다른 대상으로 외부 통화를 착신 전환하려는 경우 외부 통화에 대한 대상 필드에 다른 값을 입력해야 합니다. 발신 검색 공간 - 통화 중 외부 착신 전환 발신 검색 공간은 통화 중 외부 착신 전환 대상으로 통화를 착신 전환합니다. 이 디렉터리 번호를 사용하는 모든 디바이스에 적용됩니다. <ul style="list-style-type: none"> 참고 시스템에서 파티션 및 발신 검색 공간을 사용하고 있는 경우 착신 전환 발신 검색 공간을 구성하는 것이 좋습니다. 통화가 통화 착신 전환 대상으로 전환되거나 재전송되는 경우 통화를 착신 전환하도록 구성된 통화 착신 전환 발신 검색 공간이 사용됩니다. 발신 검색 공간 필드가 없음인 경우 시스템에서 파티션 및 발신 검색 공간을 사용 중이면 착신 전환 작업은 실패합니다. 예를 들어 통화 중 착신 전환 대상을 구성하는 경우 통화 중 착신 전환 발신 검색 공간도 구성해야 합니다. 통화 중 착신 전환 발신 검색 공간을 구성하지 않은 경우 통화 중 착신 전환 대상이 파티션에 있으면 착신 전환 작업이 실패합니다. 참고 내부 통화에 대한 발신 검색 공간을 선택하는 경우 외부 통화에 대한 발신 검색 공간 설정으로 이 값이 자동으로 복사됩니다. 외부 통화를 다른 발신 검색 공간으로 착신 전환하려면 발신 검색 공간에서 외부 통화에 대해 다른 값을 선택해야 합니다.

- 음성 메일 - 음성 메일 프로필 구성 창에 구성된 값을 사용하려면 이 확인란을 선택합니다.
- 참고 이 확인란을 선택하면 음성 메일 파일럿의 발신 검색 공간이 사용됩니다. Unified Communications Manager는 대상 및 발신 검색 공간 필드의 값을 무시합니다.
- 참고 내부 통화에 대해 이 확인란을 선택한 경우 외부 통화에 대해 자동으로 음성 메일 확인란이 선택됩니다. 음성 메일 시스템으로 외부 통화를 착신 전환하지 않으려면 외부 통화에 대해 음성 메일 확인란을 선택 취소해야 합니다.
- 대상 - 이 필드는 통화에 응답하지 않을 경우 내부 통화가 착신 전환되는 디렉터리 번호를 나타냅니다. 외부 대상을 포함하여 걸 수 있는 전화 번호를 사용합니다.
- 참고 내부 통화의 대상 값을 입력하는 경우 이 값은 시스템에서 자동으로 외부 통화의 대상 필드로 복사됩니다. 다른 대상으로 외부 통화를 착신 전환하려는 경우 외부 통화에 대한 대상 필드에 다른 값을 입력해야 합니다.
- 발신 검색 공간 - 응답 없음 내부 착신 전환 발신 검색 공간은 응답 없음 내부 착신 전환 대상으로 통화를 착신 전환하는 데 사용됩니다. 이 디렉터리 번호를 사용하는 모든 디바이스에 적용됩니다.
- 참고 시스템에서 파티션 및 발신 검색 공간을 사용하고 있는 경우 착신 전환 발신 검색 공간을 구성하는 것이 좋습니다. 통화가 통화 착신 전환 대상으로 전환되거나 재전송되는 경우 통화를 착신 전환하도록 구성된 통화 착신 전환 발신 검색 공간이 사용됩니다. 발신 검색 공간 필드가 없음인 경우 시스템에서 파티션 및 발신 검색 공간을 사용 중이면 착신 전환 작업은 실패합니다. 예를 들어 응답 없음 착신 전환 대상을 구성하는 경우 응답 없음 착신 전환 발신 검색 공간도 구성해야 합니다. 응답 없음 착신 전환 발신 검색 공간을 구성하지 않은 경우 응답 없음 착신 전환 대상이 파티션에 있으면 착신 전환 작업이 실패합니다.
- 참고 내부 통화에 대한 발신 검색 공간을 선택하는 경우 외부 통화에 대한 발신 검색 공간 설정으로 이 값이 자동으로 복사됩니다. 외부 통화를 다른 발신 검색 공간으로 착신 전환하려면 발신 검색 공간에서 외부 통화에 대해 다른 값을 선택해야 합니다.

필드	설명
응답 없음 외부 착신 전환	<p>이 필드 행의 필드에서는 디렉터리 번호가 응답하지 않는 경우 이 디렉터리 번호로의 외부 통화에 대한 착신 전환 처리를 지정합니다. 대상 및 발신 검색 공간 필드는 착신 전환 대상으로 통화를 재전송하는 데 사용됩니다.</p> <p>다음과 같은 값을 구성합니다.</p> <ul style="list-style-type: none"> • 음성 메일 - 음성 메일 프로필 구성 창에 구성된 값을 사용하려면 이 확인란을 선택합니다. <ul style="list-style-type: none"> 참고 이 확인란을 선택하면 음성 메일 파일럿의 발신 검색 공간이 사용됩니다. Unified Communications Manager는 대상 및 발신 검색 공간 필드의 값을 무시합니다. 참고 내부 통화에 대해 이 확인란을 선택한 경우 외부 통화에 대해 자동으로 음성 메일 확인란이 선택됩니다. 음성 메일 시스템으로 외부 통화를 착신 전환하지 않으려면 외부 통화에 대해 음성 메일 확인란을 선택 취소해야 합니다. • 대상 - 이 필드는 통화에 응답하지 않을 경우 외부 통화가 착신 전환되는 디렉터리 번호를 나타냅니다. 외부 대상을 포함하여 걸 수 있는 전화 번호를 사용합니다. <ul style="list-style-type: none"> 참고 내부 통화의 대상 값을 입력하는 경우 이 값은 시스템에서 자동으로 외부 통화의 대상 필드로 복사됩니다. 다른 대상으로 외부 통화를 착신 전환하려는 경우 외부 통화에 대한 대상 필드에 다른 값을 입력해야 합니다. • 발신 검색 공간 - 응답 없음 외부 착신 전환 발신 검색 공간은 응답 없음 외부 착신 전환 대상으로 통화를 착신 전환하는 데 사용됩니다. 이 디렉터리 번호를 사용하는 모든 디바이스에 적용됩니다. <ul style="list-style-type: none"> 참고 시스템에서 파티션 및 발신 검색 공간을 사용하고 있는 경우 착신 전환 발신 검색 공간을 구성하는 것이 좋습니다. 통화가 통화 착신 전환 대상으로 전환되거나 재전송되는 경우 통화를 착신 전환하도록 구성된 통화 착신 전환 발신 검색 공간이 사용됩니다. 발신 검색 공간 필드가 없음인 경우 시스템에서 파티션 및 발신 검색 공간을 사용 중이면 착신 전환 작업은 실패합니다. 예를 들어 통화 중 착신 전환 대상을 구성하는 경우 응답 없음 착신 전환 발신 검색 공간도 구성해야 합니다. 응답 없음 착신 전환 발신 검색 공간을 구성하지 않은 경우 응답 없음 착신 전환 대상이 파티션에 있으면 착신 전환 작업이 실패합니다. 참고 내부 통화에 대한 발신 검색 공간을 선택하는 경우 외부 통화에 대한 발신 검색 공간 설정으로 이 값이 자동으로 복사됩니다. 외부 통화를 다른 발신 검색 공간으로 착신 전환하려면 발신 검색 공간에서 외부 통화에 대해 다른 값을 선택해야 합니다.

필드	설명
통화권 아님 작신 전환 내부	<p>대상 및 발신 검색 공간 필드는 작신 전환 대상으로 통화를 재전송하는 데 사용됩니다.</p> <p>다음과 같은 값을 구성합니다.</p> <ul style="list-style-type: none"> 음성 메일 - 음성 메일 프로필 구성 창에 구성된 값을 사용하려면 이 확인란을 선택합니다. <p>참고 이 확인란을 선택하면 Unified Communications Manager가 대상 및 발신 검색 공간 필드의 값을 무시합니다. 내부 통화에 대해 이 확인란을 선택한 경우 외부 통화에 대해 자동으로 음성 메일 확인란이 선택됩니다. 음성 메시징 시스템으로 외부 통화를 작신 전환하지 않으려면 외부 통화에 대해 음성 메일 확인란을 선택 취소해야 합니다.</p> <ul style="list-style-type: none"> 대상 - 이 필드는 디렉터리 번호를 제어하는 애플리케이션에 장애가 발생하는 경우 연결되지 않은 내부 통화를 작신 전환할 디렉터리 번호를 지정합니다. 외부 대상을 포함하여 걸 수 있는 전화 번호를 사용합니다. <p>참고 내부 통화의 대상 값을 입력하는 경우 이 값은 시스템에서 자동으로 외부 통화의 대상 필드로 복사됩니다. 다른 대상으로 외부 통화를 작신 전환하려는 경우 외부 통화에 대한 대상 필드에 다른 값을 입력해야 합니다.</p> <ul style="list-style-type: none"> 발신 검색 공간 - 통화권 아님 작신 전환 내부 발신 검색 공간은 통화권 아님 작신 전환 내부 대상으로 통화를 작신 전환하는 데 사용됩니다. 이 값은 이 디렉터리 번호를 사용하는 모든 디바이스에 적용됩니다. <p>참고 시스템에서 파티션 및 발신 검색 공간을 사용하고 있는 경우 작신 전환 발신 검색 공간을 구성하는 것이 좋습니다. 통화가 통화 작신 전환 대상으로 전환되거나 재전송되는 경우 통화를 작신 전환하도록 구성된 통화 작신 전환 발신 검색 공간이 사용됩니다. 발신 검색 공간 필드가 없음인 경우 시스템에서 파티션 및 발신 검색 공간을 사용 중이면 작신 전환 작업은 실패합니다. 예를 들어 통화 중 작신 전환 대상을 구성하는 경우 통화권 아님 작신 전환 발신 검색 공간도 구성해야 합니다. 통화권 아님 작신 전환 발신 검색 공간을 구성하지 않은 경우 통화 중 작신 전환 대상이 파티션에 있으면 작신 전환 작업이 실패합니다.</p> <p>참고 내부 통화에 대한 발신 검색 공간을 선택하는 경우 외부 통화에 대한 발신 검색 공간 설정으로 이 값이 자동으로 복사됩니다. 외부 통화를 다른 발신 검색 공간으로 작신 전환하려면 발신 검색 공간에서 외부 통화에 대해 다른 값을 선택해야 합니다.</p>

필드	설명
통화권 아님 착신 전환 외부	<p>대상 및 발신 검색 공간 필드는 착신 전환 대상으로 통화를 재전송하는 데 사용됩니다.</p> <p>다음 값을 지정합니다.</p> <ul style="list-style-type: none"> 음성 메일 - 음성 메일 프로필 구성 창에 구성된 값을 사용하려면 이 확인란을 선택합니다. <p>참고 이 확인란을 선택하면 Unified Communications Manager에서 대상 상자 및 발신 검색 공간 필드의 값을 무시합니다. 내부 통화에 대해 이 확인란을 선택한 경우 외부 통화에 대해 자동으로 음성 메일 확인란이 선택됩니다. 음성 메시징 시스템으로 외부 통화를 착신 전환하지 않으려면 외부 통화에 대해 음성 메일 확인란을 선택 취소해야 합니다.</p> <ul style="list-style-type: none"> 대상 - 이 필드는 디렉터리 번호를 제어하는 애플리케이션에 장애가 발생하는 경우 연결되지 않은 내부 통화를 착신 전환할 디렉터리 번호를 지정합니다. 외부 대상을 포함하여 걸 수 있는 전화 번호를 사용합니다. <p>참고 내부 통화의 대상 값을 입력하는 경우 이 값은 시스템에서 자동으로 외부 통화의 대상 필드로 복사됩니다. 다른 대상으로 외부 통화를 착신 전환하려는 경우 외부 통화에 대한 대상 필드에 다른 값을 입력해야 합니다.</p> <ul style="list-style-type: none"> 발신 검색 공간 - 통화권 아님 착신 전환 외부 발신 검색 공간은 통화권 아님 착신 전환 외부 대상으로 통화를 착신 전환하는 데 사용됩니다. 이 값은 이 디렉터리 번호를 사용하는 모든 디바이스에 적용됩니다. <p>참고 시스템에서 파티션 및 발신 검색 공간을 사용하고 있는 경우 착신 전환 발신 검색 공간을 구성하는 것이 좋습니다. 통화가 통화 착신 전환 대상으로 전환되거나 재전송되는 경우 통화를 착신 전환하도록 구성된 통화 착신 전환 발신 검색 공간이 사용됩니다. 발신 검색 공간이 없음인 경우 시스템에서 파티션 및 발신 검색 공간을 사용 중이면 착신 전환 작업은 실패할 수 있습니다. 예를 들어 통화권 아님 착신 전환 대상을 구성하는 경우 통화권 아님 착신 전환 발신 검색 공간도 구성해야 합니다. 통화권 아님 착신 전환 발신 검색 공간을 구성하지 않은 경우 통화권 아님 착신 전환 대상이 파티션에 있으면 착신 전환 작업이 실패할 수 있습니다.</p> <p>참고 내부 통화에 대한 발신 검색 공간을 선택하는 경우 외부 통화에 대한 발신 검색 공간 설정으로 이 값이 자동으로 복사됩니다. 외부 통화를 다른 발신 검색 공간으로 착신 전환하려면 발신 검색 공간에서 외부 통화에 대해 다른 설정을 선택해야 합니다.</p>
CTI 실패 시 착신 전환	<p>이 필드는 CTI 라우트 포인트 및 CTI 포트에만 적용됩니다. 이 행의 필드에서는 CTI 라우트 포인트 또는 CTI 포트가 실패하는 경우 이 CTI 라우트 포인트 또는 CTI 포트의 외부 통화에 대한 착신 전환 처리를 지정합니다.</p> <p>다음과 같은 값을 구성합니다.</p> <ul style="list-style-type: none"> 음성 메일 - 음성 메일 프로필 구성 창에 구성된 값을 사용하려면 이 확인란을 선택합니다. <p>참고 이 확인란을 선택하면 Unified Communications Manager가 대상 및 발신 검색 공간 필드의 값을 무시합니다.</p> <ul style="list-style-type: none"> 대상 - 이 필드는 디렉터리 번호를 제어하는 애플리케이션에 장애가 발생하는 경우 연결되지 않은 내부 통화를 착신 전환할 디렉터리 번호를 지정합니다. 외부 대상을 포함하여 걸 수 있는 전화 번호를 사용합니다. 발신 검색 공간 - 이 설정은 이 디렉터리 번호를 사용하는 모든 디바이스에 적용됩니다.

필드	설명
등록되지 않은 내부 착신 전환	<p>이 필드는 등록되지 않은 내부 DN 통화에 적용됩니다. 통화가 지정된 대상 또는 음성 메일로 재전송됩니다.</p> <p>참고 DN으로의 등록되지 않은 착신 전환 최대 홉 수 서비스 매개 변수의 디렉터리 번호에 대한 서비스 매개 변수 구성 창에서 최대 착신 전환 수도 지정해야 합니다.</p> <p>이 매개 변수는 디렉터리 번호에 대해 동시에 허용되는 등록되지 않은 착신 전환의 최대 수를 지정합니다. 이 매개 변수는 착신 전환 루프가 발생하는 경우 등록되지 않은 DN으로 인해 통화를 착신 전환할 수 있는 횟수를 제한합니다. 이 수를 사용하여 착신 전환 등록되지 않은 외부 통화에 대한 착신 전환 루프를 중지합니다. Unified Communications Manager는 서비스 매개 변수에 지정된 값이 초과될 때 통화를 종료합니다.</p>
등록되지 않은 외부 착신 전환	<p>이 필드는 등록되지 않은 외부 DN 통화에 적용됩니다. 통화가 지정된 대상 또는 음성 메일로 재전송됩니다.</p> <p>참고 DN으로의 등록되지 않은 착신 전환 최대 홉 수 서비스 매개 변수의 디렉터리 번호에 대한 서비스 매개 변수 구성 창에서 최대 착신 전환 수도 지정해야 합니다.</p> <p>이 매개 변수는 디렉터리 번호에 대해 동시에 허용되는 등록되지 않은 착신 전환의 최대 수를 지정합니다. 이 매개 변수는 착신 전환 루프가 발생하는 경우 등록되지 않은 DN으로 인해 통화를 착신 전환할 수 있는 횟수를 제한합니다. 이 수를 사용하여 착신 전환 등록되지 않은 외부 통화에 대한 착신 전환 루프를 중지합니다. Unified Communications Manager는 서비스 매개 변수에 지정된 값이 초과될 때 통화를 종료합니다.</p>
응답 없음 벨소리 지속 기간(초)	<p>이 필드는 지정된 경우 응답되지 않은 통화를 응답 없음 착신 전환 대상으로 착신 전환하기 전에 대기 하는 시간(초)을 지정합니다. 이 매개 변수에 지정된 값이 T301 타이머 서비스 매개 변수에 지정된 값보다 작은지 확인하십시오. 응답 없음 착신 전환 타이머 서비스 매개 변수의 값이 T301 타이머 서비스 매개 변수에 지정된 값보다 크면 통화가 착신 전환되지 않고 발신자가 통화 중 신호를 수신합니다.</p> <p>Cisco Unified Communications Manager 응답 없음 착신 전환 타이머 서비스 매개 변수에 값을 설정하려면 이 필드를 비워 둡니다.</p>

통화 착신 전환에 대한 대상 오버라이드 활성화

착신전환에 대해 대상 재정의의를 활성화합니다. **Unified Communications Manager**는 CFA 대상이 착신자 번호와 일치할 경우 CFA 대상을 무시합니다. 오버라이드는 내부 및 외부 통화 모두에 적용됩니다. 발신자 번호가 변환된 경우 발신자 번호가 CFA 대상과 일치하지 않으면 재정의가 발생하지 않습니다.

시작하기 전에

[다른 착신 전환 유형 구성, 368 페이지](#)

프로시저

단계 1 **Cisco Unified CM** 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수. 서비스 매개 변수 구성 창이 표시됩니다.

단계 2 클러스터 수준 매개 변수(기능 - 보류 복귀) 영역에서 **CFA** 대상 무시 서비스 매개 변수 값을 **True**로 설정합니다.

착신 전환 상호 작용

기능	상호 작용
콜백	콜백 알림 화면에서 발신된 통화는 대상 DN에 구성된 모든 착신 전환 값을 무시합니다. 통화는 콜백 회수 타이머가 만료되기 전에 이루어져야 합니다. 그렇지 않으면 통화 착신 전환 구성된 값이 무시되지 않습니다.
통화 표시 제한	연결 번호 표시 제한은 시스템의 모든 발신 통화에 적용됩니다. 이 값을 True 로 설정하면 이 필드는 기존의 Unified Communications Manager 애플리케이션, 기능 및 통화 처리와 투명하게 상호 작용합니다. 해당 값은 시스템 내부 또는 외부의 모든 착신 통화에 적용됩니다. 통화가 모두 착신 전환 또는 통화 중 착신 전환 대상으로 라우팅되거나 착신 전환 또는 CTI 애플리케이션을 통해 재전송되는 경우 연결된 번호 표시가 업데이트되어 수정된 번호나 재전송된 번호가 표시됩니다.
DND(Do Not Disturb)	Cisco Unified IP Phone에서는 DND(방해사절) 기능이 활성임을 나타내는 메시지가 사용자에게 새 음성 메시지가 있음을 나타내는 메시지보다 우선합니다. 하지만, 모두 착신 전환 기능이 활성임을 나타내는 메시지는 방해사절보다 우선 순위가 높습니다.
외부 전화 제어	외부 전화 제어에서는 변환 패턴 수준에서 통화를 차단하지만, 통화 착신 전환에서는 디렉터리 번호 수준에서 통화를 차단합니다. 외부 전화 제어의 우선 순위가 더 높습니다. 즉, 통화 착신 전환이 호출되는 통화의 경우 변환 패턴에 외부 통화 제어 프로파일이 할당되어 있는 경우 Unified Communications Manager는 라우팅 쿼리를 보조 라우트 서버에 보냅니다. 통화 착신 전환은 보조 라우트 서버에서 계속 외부와 함께 허용 결정을 Unified Communications Manager로 보내는 경우에만 트리거됩니다. 참고 외부 통화 제어를 지원하는 통화 전환 흡수 서비스 매개 변수 및 통화 착신 전환을 지원하는 통화 착신 전환 통화 흡수 서비스 매개 변수는 별개입니다. 따라서 개별적으로 작동합니다.
클러스터 간 Extension Mobility	Cisco Extension Mobility Cross Cluster는 착신 전환을 지원합니다.
확장 및 연결	확장 및 연결은 모두 착신 전환을 지원합니다.

기능	상호 작용
지정전환	<p>디렉터리 번호 구성 창에 응답 없음 착신 전환 필드가 구성되지 않은 경우 착신 전환은 클러스터 전체의 CFNA 타이머 서비스 매개 변수인 응답 없음 착신 전환 타이머를 사용합니다.</p> <p>통화가 착신 전환됨과 동시에 사용자가 [전환] 소프트키를 누르면 (타이머에 설정된 시간이 너무 짧았기 때문에) 통화가 음성 메일로 전환되지 않고 할당된 착신 전환 디렉터리 번호로 전환됩니다. 이 상황을 해결하려면 CFNA 타이머 서비스 매개 변수에 충분한 시간을 설정하십시오(예: 60초).</p>
논리적 파티션	Unified Communications Manager는 수신 및 전환된 디바이스와 연결된 지오로케이션 식별자 정보를 사용하여 논리적 파티셔닝 정책 검사를 수행합니다. 이 처리는 모든 유형의 통화 착신 전환에 적용됩니다.

기능	상호 작용
MLPP(Multilevel Precedence and Preemption)	<p>통화 중 착신 전환</p> <ul style="list-style-type: none"> • MLPP 활성화 스테이션에 대해 사전 구성된 [우선 대체 상대] 대상을 구성할 수 있습니다. • Cisco Unified Communications Manager는 통화 중 착신 전환 기능을 적용하여 통화 [우선 대체 상대 전환] 절차를 적용하기 전에 우선 순위 통화를 일반 방식으로 착신 전환합니다. • 시스템에서 착신 전환된 여러 통화에 대해 우선 순위 통화를 유지합니다. • 착신되는 우선 순위 통화가 기존 통화보다 우선 순위가 높은 경우 선점이 발생합니다. 활성 통화에서 선점된 상대는 우선 순위 통화가 지정된 스테이션에서 통화를 끊을 때까지 연속적 선점 신호음을 수신합니다. 통화를 끊으면 우선 순위 통화가 지정된 스테이션에서 선점 벨소리를 수신합니다. 스테이션이 오프 홀스로 전환되면 대상 스테이션이 선점 통화에 연결됩니다. <p>응답 없음 착신 전환</p> <ul style="list-style-type: none"> • [우선] 우선 순위 이상의 통화의 경우 착신 전환 프로세스 중 통화 처리에서 통화의 우선 수준을 유지하고 착신 전환 대상 사용자를 선점할 수 있습니다. • 우선 순위 통화 대상에 [대체 상대]가 구성된 경우 [우선 순위 통화 대체 상대] 시간 초과가 만료된 이후 통화 처리에서 우선 순위 통화를 [대체 상대]로 전환합니다. 우선 순위 통화 대상에 [대체 상대] 값이 구성되지 않은 경우 통화 처리에서 우선 순위 통화를 [응답 없음 착신 전환] 값으로 전환합니다. • 일반적으로, 우선 순위 통화는 음성 메일 시스템이 아닌 사용자로 통화를 전송합니다. 관리자는 우선 순위 통화가 음성 메일 시스템으로 전송되지 않도록 우선 순위 통화에 표준 VM 처리 사용 엔터프라이즈 매개 변수를 설정합니다. <p>착신되는 우선 순위 통화가 기존 통화보다 우선순위가 낮거나 같은 경우 통화 처리에서 일반 통화 착신 전환 동작을 호출합니다. 우선 순위 통화에 대한 대상 스테이션을 선점할 수 없는 경우(즉, MLPP가 구성되지 않은 경우) 통화 처리에서 통화 착신 전환 동작을 호출합니다.</p> <p>대체 상대 전환(APD)은 특수한 유형의 통화 착신 전환으로 구성됩니다. 사용자가 APD에 대해 구성된 경우, 우선 순위 통화가 통화 중이거나 전화를 받지 않는 디렉터리 번호(DN)로 전송될 때 APD가 이루어 집니다. MLPP APD는 우선 순위 통화에만 적용됩니다. MLPP APD 통화는 우선 순위 통화에 대한 DN 응답 없음 착신 전환 값을 비활성화합니다.</p>

기능	상호 작용
발신 통화 기록의 원래 착신자 이름	프라이버시를 착신자 디바이스의 프로파일에만 구성하거나 CFA(모든 통화 착신 전환) 또는 CFB(통화 중 착신 전환) 또는 CFUR(등록되지 않은 통화 착신 전환)가 활성화된 경우 “전용번호”가 아닌 구성된 경고 이름이 표시됩니다. 통화 착신 전환 시 “전용번호”를 표시하려면 SIP 프로파일이 아닌 변환 패턴 또는 경로 패턴에 이름 표시 제한을 구성해야 합니다.
롤오버 회선	<p>통화 착신 전환 설정을 사용하여 공유 회선에 대한 롤오버 회선을 만들 수 있습니다. 이는 일부 콜 센터 상황에서 유용할 수 있습니다.</p> <p>롤오버 회선을 사용하는 경우 누군가가 번호(예: 1-800-HOTLINE)로 전화를 걸면 통화는 항상 특정 전화 회선으로 라우팅됩니다. 이는 여러 전화기에서 공유하는 공유 회선일 수 있습니다. 회선 1이 통화 중인 경우 통화는 회선 2로 롤오버되고 회선 2가 통화 중인 경우 회선 3으로 롤오버됩니다. 회선 1이 통화 중인 경우에만 회선 2 또는 3을 사용할 수 있습니다.</p> <p>이 유형의 통화 기능은 통화 착신 전환 설정 및 통화 중 트리거를 통해 다음과 같이 할 수 있습니다.</p> <ul style="list-style-type: none"> • 회선 1에서 통화 중 트리거를 1로 설정하고 통화 착신 전환을 체인의 두 번째 회선으로 구성합니다. • 회선 2에서 통화 중 트리거를 1로 설정하고 통화 착신 전환을 체인의 세 번째 회선으로 구성합니다. • 사용자의 요구에 맞는 많은 회선에 대해 이 작업을 계속합니다.
보안 신호음	모두 착신 전환은 보호된 전화기에서 지원됩니다.
세션 전환	사용자가 통화를 전환하면 사무실 전화기에 새 통화가 표시됩니다. 데스크폰이 깜박이는 동안에는 데스크폰에서 핸드오프된 통화에 대해 모두 착신 전환이 트리거되지 않습니다.
공유 회선	모두 착신전환(CFA) 설정이 있는 공유 회선을 사용하고 발신 트렁크에서 '발신 번호'를 '리디렉션된 상대방의 외부 전화 번호' 표시로 선택하면 공유 회선에 서로 다른 E164 번호가 구성되어 있으면 표시되는 리디렉션 번호가 일치하지 않을 수 있습니다. 따라서 공유 회선 간에 동일한 E164 번호를 사용하는 것이 좋습니다.

착신 전환 제한 사항

기능	제한 사항
착신 전환	<ul style="list-style-type: none"> 모두 착신 전환이 Unified Communications Manager 또는 Cisco 통합 커뮤니케이션 자가 관리 포털에서 발생하는 경우 Unified Communications Manager는 CFA 루프를 방지하지 않습니다. Unified Communications Manager는 CFA가 전화기에서 활성화되고, 모두 착신 전환 통화에 대한 홉 수가 착신 전환 최대 홉 수 서비스 매개 변수에 대해 지정된 값을 초과하고, 착신 체인의 모든 전화기에 CFA 활성화된 경우(CFB, CFNA 또는 기타 착신 전환 옵션) 모두 착신 전환 루프를 방지합니다. <p>예를 들어, 디렉터리 번호가 1000인 사용자가 디렉터리 번호 1001(CFB와 CFNA가 디렉터리 번호 1002으로 구성되고, CFA가 디렉터리 번호 1001로 구성됨)로 모두 착신 전환하는 경우 디렉터리 번호 1002는 디렉터리 번호 1001에 대해 CFB 및 CFNA(CFA가 아님) 대상으로 작동하기 때문에 Unified Communications Manager는 통화가 발생하도록 허용합니다.</p> <ul style="list-style-type: none"> 통화를 모두 음성 메시징 시스템으로 착신 전환하는 경우에는 콜백을 활성화할 수 없습니다. iDivert(음성 전환) 소프트키를 누를 때 응답 없음 착신 전환 시간 초과와 관련된 일반적이지 않은 조건이 존재합니다. 예를 들어, 관리자가 응답 없음 착신 전환 시간 초과 후 즉시 [전환] 소프트키를 누를 경우, 통화 착신 전환이 해당 통화를 사전 구성된 디렉터리 번호로 착신 전환합니다. 그러나, 관리자가 응답 없음 착신 전환 시간 초과 전에 [전환] 소프트키를 누를 경우, 음성 전환이 해당 통화를 관리자의 보이스메일로 전환합니다.
지정전환	CFA(모든 통화 착신 전환)와 CFB(통화 중 착신 전환)가 활성화된 경우, 시스템은 음성전환을 지원하지 않습니다(CFA와 CFB가 음성 전환보다 우선).
인터콤	인터콤 통화는 착신 전환할 수 없습니다.
힌트 그룹 로그아웃	<p>SIP(7906, 7911, 7941, 7961)를 실행하는 전화기가 힌트 그룹에 로그인되고 모두 착신 전환이 활성화되면 SIP를 실행하는 전화기에 통화가 표시됩니다.</p> <p>SIP를 실행하는 7940 및 7960 전화기가 힌트 그룹에 로그인되고 모두 착신 전환이 활성화되면 전화기가 생략되고 회선 그룹의 다음 전화기가 올립니다.</p>

기능	제한 사항
논리적 파티션	<p>다음과 같은 경우에 논리적 파티션 처리가 발생하지 않습니다.</p> <ul style="list-style-type: none"> • 발신 및 착신 전환된 디바이스 모두 VoIP(Voice over IP) 전화기인 경우. • 지오로케이션 또는 지오로케이션 필터가 어떤 디바이스와도 연결되지 않은 경우.
MLPP(Multilevel Precedence and Preemption)	<p>보조 서비스에 대한 MLPP(다단계 우선 순위 및 선점) 지원은 착신 전환에 대해 다음과 같은 제한 사항을 지정합니다.</p> <ul style="list-style-type: none"> • 착신 MLPP 통화에 대한 CFA(모든 통화 착신 전환) 지원 기능은 착신자의 MLPP 대체 상대(MAP) 대상이 구성된 경우 항상 해당 대상으로 통화를 착신 전환합니다. 구성이 잘못된 경우(즉, MAP 대상이 지정되지 않은 경우), 통화가 거부되고, 발신자는 다시 걸기 신호음을 받게 됩니다. • 착신 MLPP 통화에 대한 CFNA(응답 없음 착신 전환) 지원 기능은 CFNA 대상으로 한 번 통화를 착신 전환합니다. 첫 번째 호출 후, 통화의 응답이 계속 이루어지지 않을 경우, 원래 착신자의 MAP 대상이 구성되면 통화가 해당 대상으로 전송됩니다. 구성이 잘못된 경우(즉, MAP 대상이 지정되지 않은 경우), 통화가 거부되고, 발신자는 다시 걸기 신호음을 받게 됩니다. • 착신 MLPP 통화에 대한 CFB(통화 중 착신 전환) 지원 기능은 착신 전환 호출에 대해 구성된 최대 숫자까지 통화를 착신 전환합니다. 최대 호출 수에 도달할 경우, 원래 착신자의 MAP 대상이 구성되면 해당 대상으로 통화가 전송됩니다. 구성이 잘못된 경우(즉, MAP 대상이 지정되지 않은 경우), 통화가 거부되고, 발신자는 다시 걸기 신호음을 받게 됩니다.
호 전환으로 착신 전환 분류	<p>통화가 호 전환될 때 통화 분류는 원래 레그가 아니라 호 전환된 레그에 대한 분류를 수행합니다. 예:</p> <ul style="list-style-type: none"> • PSTN에서 수신되는 통화는 접수 담당자가 수신합니다. 이는 외부 통화입니다. • 접수 담당자는 내선 번호 3100으로 통화를 호전환합니다. 호전환된 통화는 이제 내부 통화입니다. • 내선 번호 3100의 사용자가 통화 중이지만 외부 통화를 접수 담당자에게 돌려 보내기 위해 외부 통화 착신 전환 기능이 구성되어 있습니다. 그러나 통화가 두 번째 레그(내부)의 분류를 수행하기 때문에 통화가 보이스메일로 이동합니다.



30 장

통화 당겨받기

- 당겨 받기 개요, 385 페이지
- 당겨받기 구성 작업 흐름, 387 페이지
- 당겨받기 상호 작용, 405 페이지
- 당겨받기 제한 사항, 406 페이지

당겨 받기 개요

통화 당겨받기 기능을 사용하면 사용자가 자신의 디렉터리 번호가 아닌 디렉토리 번호로 걸려오는 전화를 받을 수 있습니다.

그룹 당겨받기 개요

그룹 통화 당겨받기 기능을 사용하여 사용자는 다른 그룹의 수신 통화를 당겨받을 수 있습니다. 사용자는 Cisco Unified IP Phone에서 이 기능이 활성화된 경우 적절한 통화 당겨받기 그룹 번호로 전화를 걸어야 합니다. 이 유형의 통화 당겨받기에는 [그룹픽업] 소프트웨어를 사용합니다. 당겨받기 그룹에 여러 통의 통화가 수신되는 동안 사용자가 그룹 통화 당겨받기 전화 기능을 호출하면 벨소리가 가장 오래 울린 수신 통화에 연결됩니다. 전화기 모델에 따라 사용자는 그룹 당겨받기 프로그램 가능 기능 버튼 또는 그룹 당겨받기 소프트웨어를 사용하여 수신 통화를 당겨 받을 수 있습니다. 자동 그룹 통화 당겨받기를 사용하지 않는 경우에는 사용자가 그룹픽업 소프트웨어를 누르고 다른 당겨받기 그룹의 그룹 번호를 누른 후 전화를 받아야 연결됩니다.

기타 그룹 당겨받기 개요

기타 그룹 당겨받기 기능을 통해 사용자는 자신의 그룹과 연결된 그룹의 수신 통화를 당겨받을 수 있습니다. Unified Communications Manager는 연결된 그룹에서 수신 통화를 자동으로 검색하여 사용자가 Cisco Unified IP Phone에서 이 기능을 활성화할 때 통화를 연결합니다. 이 유형의 통화 당겨받기에는 [기타픽업] 소프트웨어를 사용합니다. 자동 기타 그룹 당겨받기를 사용하지 않는 경우에는 사용자가 [기타픽업] 및 [전화받기] 소프트웨어를 눌러 통화를 연결해야 합니다. 전화기 모델에 따라 사용자는 통화 당겨받기 프로그램 가능 기능 버튼 또는 통화 당겨받기 소프트웨어를 사용하여 수신 통화를 당겨 받을 수 있습니다.

연결된 그룹이 둘 이상인 경우 연결된 그룹에 대한 통화 응답 우선 순위는 첫 번째 연결된 그룹이 가장 높습니다. 예를 들어 그룹 A, B 및 C가 그룹 X와 연결되면 그룹 A는 가장 높은 우선 순위를 가지며 그룹 C는 통화에 응답하는 우선 순위가 가장 낮습니다. 그룹 X가 그룹 A의 수신 통화를 당겨 받고, 통화가 그룹 A의 수신 통화보다 그룹 C에서 더 일찍 발생했을 수 있습니다.



참고 해당 그룹에서 수신 통화가 여러 개 발생할 경우 가장 오래 벨이 울린 통화를 먼저 당겨받습니다. 기타 그룹 통화 당겨받기의 경우 연결된 당겨받기 그룹이 여러 개 구성되어 있으면 우선 순위가 벨소리 시간보다 우선 적용됩니다.

직접 당겨 받기 개요

직접 통화 당겨받기 기능을 사용하면 [그룹픽업] 또는 [그룹 픽업] 소프트키를 누르고 벨소리가 울리는 디바이스의 디렉터리 번호를 입력하여 벨소리가 울리는 통화를 DN에서 직접 당겨받을 수 있습니다. 자동 직접 당겨받기가 활성화되지 않은 경우 사용자는 그룹픽업 소프트키를 누르고, 벨소리가 울리는 전화기의 DN을 다이얼한 다음, 사용자 전화기에서 지금 울리는 통화를 받아 연결해야 합니다. Unified Communications Manager는 연결된 그룹 메커니즘을 사용하여 직접 당겨받기를 사용하여 수신 통화를 선택하려는 사용자의 권한을 제어합니다. 사용자의 관련 그룹은 사용자가 속하는 당겨받기 그룹과 관련된 하나 이상의 통화 당겨받기 그룹을 지정합니다.

사용자가 벨소리가 울리는 통화를 DN에서 직접 당겨받으려는 경우 사용자의 관련 그룹에 DN이 속하는 당겨받기 그룹이 포함되어 있어야 합니다. 두 명의 사용자가 다른 통화 당겨받기 그룹에 속해 있고 사용자의 관련 그룹에 상대방의 통화 당겨받기 그룹이 포함되어 있지 않은 경우 사용자가 [직접 통화 당겨받기]를 호출하여 서로의 통화를 당겨받을 수 없습니다.

사용자가 직접 통화 당겨받기 기능을 호출하고 수신 통화를 당겨받을 DN을 입력할 경우 지정된 전화기로 수신되는 통화에 연결되며, 해당 통화가 DN이 속한 통화 당겨받기 그룹에서 가장 오래 울린 통화인지 여부는 무관합니다. 특정 DN에서 여러 통화가 울리고 사용자가 [직접 통화 당겨받기]를 호출하여 DN에서 통화를 당겨받을 경우 지정된 DN에서 가장 오래 울린 수신 통화로 연결됩니다.

BLF 당겨받기 개요

BLF 당겨받기 기능을 사용하면 BLF DN에서 통화가 선택될 때 Unified Communications Manager에서 전화기 사용자에게 알릴 수 있습니다. BLF 당겨받기 이니시에이터(통화를 당겨받는 전화기)는 사용 가능한 다음 회선 또는 지정된 회선으로 선택됩니다. 지정된 회선을 사용하려면 BLF SD 버튼을 누르기 전까지 회선이 오프 훅 상태로 유지되어야 합니다. 힌트 목록 구성원 DN을 BLF DN으로 구성하여 힌트 목록 구성원으로의 수신 통화를 BLF 통화 당겨받기 개시자가 당겨 받을 수 있도록 할 수 있습니다. 힌트 목록 구성원의 수신 통화는 힌트 목록에서 오거나 직접 통화일 수 있습니다. 각 사례의 동작은 힌트 목록 구성원 DN, BLF DN 및 힌트 파일럿 구성원에 대해 통화 당겨받기를 구성하는 방식에 따라 다릅니다. 자동 통화 당겨받기 활성화 서비스 매개 변수가 False로 설정된 상태로 당겨받기가 발생하는 경우 전화기가 오프 상태를 유지해야 하거나 사용자가 전화받기 키를 눌러 통화를 당겨 받아야 합니다.

전화기의 BLF SD 버튼은 다음 상태 중 하나에서 있을 수 있습니다.

- 유힬 - BLF DN에 통화가 없음을 나타냅니다.

- 통화 중 - BLF DN에 활성 통화가 하나 이상 있지만 경고가 없음을 나타냅니다.
- 알림 - BLF DN에 수신 통화가 하나 이상 있음을 깜박여서 나타냅니다.

BLF DN에 대한 수신 통화가 있을 때 BLF 당겨받기 이니시에이터 전화기의 BLF SD 버튼이 깜박여 BLF DN으로의 수신 통화가 있음을 나타냅니다. 자동 통화 당겨받기가 구성된 경우에는 사용자가 통화 당겨받기 개시자 전화기의 BLF SD 버튼을 눌러 수신 통화를 당겨 받습니다. 자동 통화 당겨받기가 구성되지 않은 경우에는 전화기가 오프 hook 상태로 유지되어야 하거나 사용자가 전화받기 키를 눌러 통화를 당겨 받아야 합니다.

당겨받기 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	통화 당겨받기 그룹 구성, 389 페이지	<p>사용하려는 각 당겨받기 기능에 대한 당겨받기 그룹을 구성합니다.</p> <ul style="list-style-type: none"> • 통화 당겨받기 • 그룹 통화 당겨받기 • 기타 통화 당겨받기 • 직접 통화 당겨받기 • BLF 통화 당겨받기 <p>고유한 이름 및 번호를 사용하여 그룹을 정의해야 합니다.</p>
단계 2	디렉터리 번호에 통화 당겨받기 그룹 할당, 390 페이지	<p>통화 당겨받기를 활성화할 전화기와 연결된 디렉터리 번호에 위에서 만든 각 통화 당겨받기 그룹을 할당합니다. 이 기능을 사용하려면 통화 당겨받기 그룹에 디렉터리 번호를 할당해야 합니다.</p> <p>생성하는 각 통화 당겨받기 그룹에 대해 이 절차를 반복합니다.</p>
단계 3	통화 당겨받기 그룹을 또 하나 만들고 단계 1, 387 페이지에서 만든 BLF 통화 당겨받기 그룹에 연결합니다. 통화 당겨받기 그룹을 여	BLF 통화 당겨받기를 구성하는 경우 이 단계를 수행합니다.

	명령 또는 동작	목적
	러 BLF DN 통화 당겨받기 그룹에 연결할 수 있습니다.	참고 또 하나의 통화 당겨받기 그룹을 항상 만들 필요는 없습니다. 예를 들어 이니시에이터 DN과 대상 DN을 모두 포함하는 단일 통화 당겨받기 그룹을 가질 수 있습니다. 이러한 경우 BLF 통화 당겨받기 그룹을 자신과 연결합니다.
단계 4	당겨받기에 대한 파티션 구성, 391 페이지	연결성 특성이 비슷한 디렉터리 번호(DN)의 논리적 그룹을 만들기 위해 파티션을 구성합니다. 파티션을 사용하여 통화 당겨받기 그룹에 대한 액세스를 제한할 수 있습니다. 통화 당겨받기 그룹 번호를 파티션에 할당하는 경우 해당 파티션의 번호로 전화를 걸 수 있는 전화기만이 통화 당겨받기 그룹을 사용할 수 있습니다. 직접 당겨받기에 대해 이 절차를 완료해야 합니다. 다른 유형의 통화 당겨받기에는 선택 사항입니다.
단계 5	발신 검색 공간 구성, 392 페이지	파티션을 구성하는 경우 발신 검색 공간도 구성해야 합니다. 발신 검색 공간을 구성하여 발신 디바이스에서 통화를 완료하려고 할 때 검색할 수 있는 파티션을 식별합니다. 모든 당겨받기에 대해 이 절차를 완료해야 합니다. 다른 유형의 통화 당겨받기에는 선택 사항입니다.
단계 6	헌트 파일럿에 통화 당겨받기 그룹 할당, 392 페이지	(선택 사항). 사용자가 회선 그룹 구성원에서 경고 중인 통화를 당겨 받을 수 있도록 헌트 파일럿 DN에 통화 당겨받기 그룹을 할당합니다. 통화 당겨받기 그룹에 할당된 헌트 목록은 통화 당겨받기, 그룹 통화 당겨받기, BLF 통화 당겨받기, 다른 그룹 당겨받기 및 작업 당겨받기를 사용할 수 있습니다.
단계 7	구성 알림: <ul style="list-style-type: none"> 당겨받기 알림 구성, 393 페이지 디렉터리 번호에 대한 당겨받기 알림 구성, 394 페이지 BLF 당겨받기 알림 구성, 395 페이지 	(선택 사항). 당겨받기 그룹의 다른 구성원이 통화를 수신하는 경우 알림을 구성합니다. 오디오 알림이나 시각적 알림 또는 둘 다 구성할 수 있습니다.

	명령 또는 동작	목적
단계 8	직접 당겨 받기 구성: <ul style="list-style-type: none"> • 기간 구성, 397 페이지 • 시간 일정 구성, 397 페이지 • 시간 일정을 파티션에 연결, 398 페이지 	직접 통화 당겨 받기를 구성하기 전에 파티션 및 발신 검색 공간을 구성해야 합니다. 직접 통화 당겨받기 기능을 사용하여 직접 통화 당겨받기 기능을 요청하는 사용자의 발신 검색 공간에는 사용자가 통화를 당겨받으려는 DN의 파티션이 포함되어야 합니다. 시간 기간 및 시간 일정은 연결된 그룹의 구성원이 통화를 수신하는 데 사용할 수 있는 시간을 지정합니다.
단계 9	자동 통화 응답 구성: <ul style="list-style-type: none"> • 자동 통화 당겨받기 구성, 398 페이지 • BLF 자동 당겨받기 구성, 399 페이지 	(선택 사항). 자동 통화 응답을 활성화하고 자동 통화 응답에 대한 타이머를 구성합니다.
단계 10	전화기 버튼 템플릿 구성: <ul style="list-style-type: none"> • 당겨받기 전화기 버튼 템플릿 구성, 400 페이지 • 당겨받기 버튼 템플릿을 전화기와 연결, 401 페이지 • BLF 당겨받기 이니시에이터에 대한 BLF 단축 다이얼 번호 구성, 401 페이지 	사용하려는 통화 당겨받기 기능에 대한 전화기 버튼 템플릿을 구성합니다. <ul style="list-style-type: none"> • 단축 다이얼 BLF • 통화 당겨받기 • 그룹 통화 당겨받기 • 기타 그룹 당겨받기 직접 통화 당겨 받기의 경우 그룹 통화 당겨받기 버튼을 사용합니다.
단계 11	당겨받기에 대한 소프트키 구성, 402 페이지 <ul style="list-style-type: none"> • 통화 당겨 받기에 대한 소프트키 템플릿 구성, 402 페이지 • 소프트키 템플릿을 일반 디바이스에 연결, 404 페이지 • 소프트키 템플릿을 전화기에 연결, 405 페이지 	사용하려는 통화 당겨받기 기능 중 하나에 대해 소프트키를 구성합니다. <ul style="list-style-type: none"> • 통화 당겨받기(픽업) • 그룹 당겨받기(그룹픽업) • 기타 당겨받기(기타픽업) 직접 통화 당겨 받기의 경우 그룹 통화 당겨받기 소프트키를 사용합니다.

통화 당겨받기 그룹 구성

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 그룹 당겨받기.

통화 당겨받기 그룹 찾기 및 나열 창이 나타납니다.

단계 2 새로 추가를 클릭합니다.

통화 당겨받기 그룹 구성 창이 나타납니다.

단계 3 통화 당겨받기 그룹 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

디렉터리 번호에 통화 당겨받기 그룹 할당

이 섹션에서는 통화 당겨받기 그룹을 디렉터리 번호에 할당하는 방법을 설명합니다. 통화 당겨받기 그룹에 할당된 디렉터리 번호에 한해서만 통화 당겨받기, 그룹 통화 당겨받기, BLF 통화 당겨받기, 다른 그룹 당겨받기 및 지정보류 통화 당겨받기를 사용할 수 있습니다. 통화 당겨받기 번호와 함께 파티션을 사용하는 경우에는 통화 당겨받기 그룹에 할당된 디렉터리 번호에 적절한 파티션을 포함하는 발신 검색 공간이 있는지 확인합니다.

시작하기 전에

[통화 당겨받기 그룹 구성, 389 페이지](#)

프로시저

단계 1 디바이스 > 전화기 또는 통화 라우팅 > 디렉터리 번호를 선택합니다.

단계 2 통화 당겨받기 그룹에 할당하려는 전화기 또는 디렉터리 번호를 찾는 데 적합한 검색 조건을 입력하고 찾기를 클릭합니다.

검색 조건과 일치하는 전화기 또는 디렉터리 번호 목록이 표시됩니다.

단계 3 통화 당겨받기 그룹을 할당할 전화기 또는 디렉터리 번호를 선택합니다.

단계 4 전화기 구성 창의 연결 정보 목록에서, 통화 당겨받기 그룹에 할당할 디렉터리 번호를 선택합니다.

단계 5 통화 착신 전환 및 통화 당겨받기 설정 영역에 표시되는 통화 당겨받기 그룹 드롭다운 목록에서 원하는 통화 당겨받기 그룹을 선택합니다.

단계 6 데이터베이스에 변경 사항을 저장하려면 저장을 클릭합니다.

다음에 수행할 작업

다음 작업을 수행하십시오.

- [당겨받기에 대한 파티션 구성, 391 페이지](#)
- [발신 검색 공간 구성, 392 페이지](#)

당겨받기에 대한 파티션 구성

통화 당겨받기 그룹 번호에 파티션을 할당하여 통화 당겨받기 그룹에 대한 액세스를 제한할 수 있습니다. 이 구성을 사용하는 경우 발신 검색 공간에 파티션과 통화 당겨받기 그룹 번호가 포함된 전화기만이 통화 당겨받기 그룹에 참가할 수 있습니다. 파티션 및 그룹 번호 조합은 시스템 전체에서 고유해야 합니다. 여러 파티션을 만들 수 있습니다.

통화 당겨받기 그룹 번호를 파티션에 할당하는 경우 해당 파티션의 번호로 전화를 걸 수 있는 전화기만이 통화 당겨받기 그룹을 사용할 수 있습니다. 파티션이 멀티테넌트 구성의 테넌트를 나타내는 경우 당겨받기 그룹이 각 테넌트의 해당 파티션에 할당되었는지 확인합니다.

시작하기 전에

[디렉터리 번호에 통화 당겨받기 그룹 할당, 390 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 파티션.

단계 2 파티션 이름, 설명 필드에 경로 플랜에 고유한 파티션 이름을 입력합니다.

파티션 이름에는 영숫자 문자는 물론 공백, 하이픈(-) 및 밑줄(_)을 사용할 수 있습니다. 파티션 이름에 대한 지침은 온라인 도움말을 참조하십시오.

단계 3 파티션 이름 뒤에 쉼표(.)를 입력하고 동일한 줄에 파티션 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\), 꺾쇠괄호(<>) 또는 대괄호([])는 사용할 수 없습니다.

설명을 입력하지 않으면 Cisco Unified Communications Manager에서 자동으로 이 필드에 파티션 이름을 입력합니다.

단계 4 여러 파티션을 생성하려면 각 파티션 항목마다 한 행을 사용합니다.

단계 5 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.

시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성화 상태로 유지됩니다.

단계 6 구성할 다음 라디오 버튼 중 하나를 선택하고 시간대를 구성합니다.

- 시작 디바이스—이 라디오 버튼을 선택하면 시스템은 발신 디바이스의 표준 시간대를 시간 일정과 비교하여 파티션을 수신 통화를 받는 데 사용할 수 있는지 여부를 확인합니다.
- 특정 표준 시간대—이 라디오 버튼을 선택한 후에 드롭다운 목록에서 표준 시간대를 선택합니다. 시스템은 선택한 표준 시간대를 시간 일정과 비교하여 수신 통화를 받는 데 파티션을 사용할 수 있는지 여부를 확인합니다.

단계 7 저장을 클릭합니다.

발신 검색 공간 구성

발신 검색 공간은 일반적으로 디바이스에 할당되어 있는 정렬된 경로 파티션 목록입니다. 발신 검색 공간은 통화를 완료하려고 시도할 때 발신 디바이스에서 검색할 수 있는 파티션을 결정합니다.

시작하기 전에

[당겨받기에 대한 파티션 구성, 391 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 발신 검색 공간.

단계 2 새로 추가를 클릭합니다.

단계 3 이름 필드에 이름을 입력합니다.

각 발신 검색 공간 이름은 시스템에 고유해야 합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.

단계 4 설명 필드에 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.

단계 5 사용 가능한 파티션 드롭다운 목록에서 다음 단계 중 하나를 수행합니다.

- 단일 파티션의 경우 해당 파티션을 선택합니다.
- 여러 파티션의 경우 컨트롤(CTRL) 키를 누른 상태에서 해당 파티션을 선택합니다.

단계 6 상자 사이에서 아래쪽 화살표를 선택하여 선택한 파티션 필드로 파티션을 이동합니다.

단계 7 (선택 사항) 선택한 파티션 상자 오른쪽의 화살표 키를 사용하여 선택한 파티션의 우선 순위를 변경합니다.

단계 8 저장을 클릭합니다.

헌트 파일럿에 통화 당겨받기 그룹 할당

통화 당겨받기 그룹에 할당된 헌트 목록에 한해서만 통화 당겨받기, 그룹 통화 당겨받기, BLF 통화 당겨받기, 다른 그룹 당겨받기 및 지정보류 통화 당겨받기를 사용할 수 있습니다. 다음 단계에 따라 헌트 파일럿에 그룹 당겨받기를 할당합니다.

시작하기 전에

[발신 검색 공간 구성, 392 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 경로/힌트 > 힌트 파일럿.
- 단계 2 통화 당겨받기 그룹에 할당하려는 힌트 파일럿을 찾는 데 적합한 검색 조건을 입력하고 찾기를 클릭합니다. 검색 조건과 일치하는 힌트 파일럿 목록이 표시됩니다.
- 단계 3 통화 당겨받기 그룹을 할당할 힌트 파일럿을 선택합니다.
- 단계 4 힌트 착신 전환 설정 영역에 표시되는 통화 당겨받기 그룹 드롭다운 목록에서 원하는 그룹 당겨받기를 선택합니다.
- 단계 5 저장을 클릭합니다.

당겨받기 알림 구성

시스템 수준, 통화 당겨 받기 그룹 수준 또는 개별 전화기 수준에서 통화 당겨 받기 알림을 구성할 수 있습니다.

시작하기 전에

[힌트 파일럿에 통화 당겨받기 그룹 할당, 392 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	그룹 당겨받기에 대한 당겨받기 알림 구성, 393 페이지	이렇게 하면 오디오 및/또는 시각적 경고가 당겨받기 그룹으로 전송되기 전에 원래 착신자가 통화를 당겨받기할 수 있습니다.
단계 2	디렉터리 번호에 대한 당겨받기 알림 구성, 394 페이지	사용자는 전화기가 유휴 상태이거나 활성 통화가 있는 경우 제공할 오디오 경고의 유형을 구성합니다.
단계 3	BLF 당겨받기 알림 구성, 395 페이지	

그룹 당겨받기에 대한 당겨받기 알림 구성

시작하기 전에

[힌트 파일럿에 통화 당겨받기 그룹 할당, 392 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 그룹 당겨받기. 그룹 당겨받기 창이 나타납니다.

단계 2 통화 당겨받기 그룹 구성 창에서 그룹 당겨받기 알림 설정 섹션의 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [당겨받기에 대한 당겨받기 알림 필드, 394 페이지](#)의 내용을 참조하십시오.

참고 통화 당겨받기 구성에 영향을 줄 수 있는 기능 상호 작용 및 제한 사항에 대한 통화 당겨받기 상호 작용 및 제한 사항을 참조하십시오.

당겨받기에 대한 당겨받기 알림 필드

필드	설명
통화 당겨받기 그룹 알림 정책	드롭다운 목록에서 알림 정책을 선택합니다. 사용할 수 있는 옵션은 알림 없음, 오디오 알림, 시각적 알림, 오디오와 시각적 알림입니다.
그룹 당겨받기 알림 타이머	원래 착신자에게 처음 전화가 걸려오는 시간과 통화 당겨받기 그룹의 나머지 구성원에게 알리는 시간 사이의 지연을 초 단위(1-300의 정수)로 입력합니다.
발신자 정보	그룹 당겨받기에 대한 시각적 알림 메시지에 발신자 ID가 포함되도록하려면 이 확인란을 선택합니다. 그룹 당겨받기 알림 정책이 시각적 알림 또는 오디오 및 시각적 알림으로 설정되어 있을 때만 이 설정을 사용할 수 있습니다. 참고 알림은 디바이스의 기본 회선에만 전송됩니다.
착신자 정보	그룹 당겨받기에 대한 시각적 알림 메시지에 원래 착신자의 ID가 포함되도록하려면 이 확인란을 선택합니다. 이 설정은 그룹 당겨받기 알림 정책이 시각적 알림 또는 오디오 및 시각적 알림으로 설정되어 있을 때 사용할 수 있습니다.

디렉터리 번호에 대한 당겨받기 알림 구성

전화기가 유휴 상태이거나 사용 중일 때 제공되는 오디오 알림 유형을 구성하려면 다음 단계를 수행합니다.

시작하기 전에

[그룹 당겨받기에 대한 당겨받기 알림 구성, 393 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 디렉터리 번호.
디렉터리 번호 찾기 및 나열 창이 나타납니다.
- 단계 2 검색 기준을 입력하고 찾기를 클릭합니다.
- 단계 3 통화 당겨 받기 알림을 구성하려는 디렉터리 번호를 클릭합니다.
디렉터리 번호 구성 창이 나타납니다.
- 단계 4 연결된 디바이스 창에서 디바이스 이름을 선택하고 회선 형태 편집 버튼을 클릭합니다.
디렉터리 번호 구성 창이 새로 고쳐지며 선택한 디바이스에서 이 DN의 회선 형태가 표시됩니다.
- 단계 5 통화 당겨 받기 그룹 오디오 경고 설정(전화기 유휴) 드롭다운 목록에서 다음 중 하나를 선택합니다.
- 시스템 기본값 사용
 - 비활성화
 - 한 번 울림
- 단계 6 통화 당겨 받기 그룹 오디오 경고 설정(전화기 활성화) 드롭다운 목록에서 다음 중 하나를 선택합니다.
- 시스템 기본값 사용
 - 비활성화
 - 경고음만
- 단계 7 저장을 클릭합니다.
-

BLF 당겨받기 알림 구성

시작하기 전에

[디렉터리 번호에 대한 당겨받기 알림 구성, 394 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- 단계 4 서비스 매개 변수 구성 창의 클러스터 수준 매개 변수(디바이스 - 전화기) 섹션에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [BLF 당겨받기 알림에 대한 서비스 매개 변수 필드, 396 페이지](#)를 참조하십시오.
-

BLF 당겨받기 알림에 대한 서비스 매개 변수 필드

필드	설명
유티 스테이션에 대한 그룹 당겨받기 오디오 경고 설정	<p>이 매개 변수는 전화기가 유티 상태(사용하고 있지 않음) 상태일 때 제공되는 오디오 알림 종류를 결정 하며 그룹 당겨받기의 수신 통화와 관련하여 알림을 받아야 합니다. 유효한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 비활성화 • 한 번 울림
통화 중 스테이션에 대한 그룹 당겨받기 오디오 경고 설정	<p>이 매개 변수는 통화 중일 때(사용 중) 제공되는 오디오 알림의 종류를 결정하며, 그룹 당겨받기의 수신 통화와 관련하여 알림을 받아야 합니다. 유효한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 비활성화 • 경고음만
유티 스테이션에 대한 BLF 당겨받기 오디오 경고 설정	<p>이 매개 변수는 전화기가 유티 상태이고 BLF 당겨받기 버튼의 수신 통화와 관련하여 알림을 받아야 하는 경우 제공되는 오디오 알림 종류를 결정합니다. 유효한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 벨소리 없음 • 한 번 울림
통화 중 스테이션에 대한 BLF 그룹 당겨받기 오디오 경고 설정	<p>이 매개 변수는 전화기가 통화 중일 때 제공되는 오디오 알림의 종류를 결정하며 BLF 당겨받기 버튼의 수신 통화에 대한 알림이 있어야 합니다. 유효한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 벨소리 없음 • 경고음만

직접 통화 당겨받기 구성

프로시저

	명령 또는 동작	목적
단계 1	기간 구성, 397 페이지	그룹에 연결된 그룹의 구성원에 대한 시간 기간을 구성합니다.
단계 2	시간 일정 구성, 397 페이지	그룹에 연결된 그룹의 구성원에 대한 시간 일정을 구성합니다.
단계 3	시간 일정을 파티션에 연결, 398 페이지	일정을 파티션과 연결하여 발신 디바이스에서 특정 시간 동안 통화를 완료하려고 시도할 때 어디를 검색하는지 확인합니다.

기간 구성

이 절차를 사용하여 기간을 정의합니다. 시작 시간과 종료 시간을 정의할 수 있고, 또한 반복 간격을 연간 달력에 요일이나 지정된 날짜로 지정할 수도 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 콜 라우팅 > 제어 클래스 > 기간을 선택합니다.

단계 2 기간기 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 3 저장을 클릭합니다.

시간 일정 구성

시작하기 전에

[기간 구성, 397 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 시간 일정.

단계 2 시간 일정 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

시간 일정을 파티션에 연결

일정을 파티션과 연결하여 발신 디바이스에서 특정 시간 동안 통화를 완료하려고 시도할 때 어디를 검색하는지 확인합니다.

시작하기 전에

[시간 일정 구성, 397 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 콜 라우팅 > 제어 클래스 > 파티션을 선택합니다.

단계 2 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.

시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성 상태로 유지됩니다.

단계 3 저장을 클릭합니다.

자동 통화 응답 구성

프로시저

	명령 또는 동작	목적
단계 1	자동 통화 당겨받기 구성, 398 페이지	통화 당겨받기, 그룹 당겨받기, 기타 그룹 당겨받기, 직접 당겨받기 및 BLF 통화 당겨받기를 자동으로 수행할 수 있습니다. 자동 통화 응답을 활성화하지 않으면 사용자가 추가 소프트키나 다이얼 그룹 번호를 눌러 연결을 완료해야 합니다.
단계 2	BLF 자동 당겨받기 구성, 399 페이지	

자동 통화 당겨받기 구성

자동 통화 당겨받기는 수신 통화에 사용자를 연결합니다. 사용자가 전화기에서 소프트키를 누르면 Unified Communications Manager에서 그룹에 수신되는 통화를 찾아 통화 연결을 완료합니다. 통화 당겨받기, 그룹 당겨받기, 기타 그룹 당겨받기, 직접 당겨받기 및 BLF 통화 당겨받기를 자동으로 수행할 수 있습니다. 자동 통화 응답을 활성화하지 않으면 사용자가 추가 소프트키나 다이얼 그룹 번호를 눌러 연결을 완료해야 합니다.

시작하기 전에

[시간 일정을 파티션에 연결, 398 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- 단계 4 클러스터 수준 매개 변수(기능 - 당겨받기) 섹션의 자동 응답 활성화 드롭다운 목록에서 **True** 또는 **False**를 선택하여 그룹 당겨받기에 대한 자동 통화 응답을 활성화하거나 비활성화합니다.
- 단계 5 자동 응답 활성화 서비스 매개 변수가 False인 경우 통화 당겨받기 응답 없음 타이머 필드에 12~300의 값을 입력합니다. 이 매개 변수는 통화를 당겨받지만 통화 당겨받기, 그룹 통화 당겨받기 또는 기타 그룹 통화 당겨받기를 사용하여 통화에 응답하지 않는 경우 통화가 복원되는 데 걸리는 시간을 제어합니다.
- 단계 6 당겨받기 타이머 필드에 1에서 5 사이의 값을 입력합니다. 이 서비스 매개 변수는 Cisco Unified Communications Manager가 클러스터의 모든 노드에서 모든 경고 통화를 식별하는 데 필요한 최대 시간(초)을 지정합니다. 그런 다음 이 정보는 대기열에서 가장 오래 대기한 통화가 당겨 받기, 그룹당겨 받기 또는 기타 당겨받기 소프트웨어를 누르는 다음 사용자에게 전달되도록 하는 데 사용됩니다.
- 단계 7 저장을 클릭합니다.
-

BLF 자동 당겨받기 구성

시작하기 전에

[자동 통화 당겨받기 구성, 398 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- 단계 4 다음 클러스터 수준 서비스 매개 변수에 대한 값을 구성합니다.
- 유휴 스테이션의 BLF 당겨받기 오디오 알림 설정 - 드롭다운 목록에서 **True** 또는 **False**를 선택하여 그룹 당겨받기에 대한 자동 통화 응답을 활성화하거나 비활성화합니다. 이 서비스 매개 변수의 기본값은 False입니다.
 - 통화 중인 스테이션의 BLF 당겨받기 오디오 알림 설정 - 자동 통화 당겨받기 활성화 서비스 매개 변수가 False이면 12~300(포함)의 값을 입력합니다. 이 매개 변수는 통화를 당겨받지만 통화 당겨받기, 그룹 통화 당겨받기 또는 기타 그룹 통화 당겨받기를 사용하여 통화에 응답하지 않는 경우 통화가 복원되는 데 걸리는 시간을 제어합니다.
-

당겨 받기 전화기 버튼 구성

프로시저

	명령 또는 동작	목적
단계 1	당겨받기 전화기 버튼 템플릿 구성, 400 페이지	전화기 버튼 템플릿에 당겨 받기 기능을 추가합니다.
단계 2	당겨받기 버튼 템플릿을 전화기와 연결, 401 페이지	
단계 3	BLF 당겨받기 이니시에이터에 대한 BLF 단축 다이얼 번호 구성, 401 페이지	

당겨받기 전화기 버튼 템플릿 구성

다음 단계에 따라 전화기 버튼 템플릿에 통화 당겨 받기 기능을 추가합니다.

시작하기 전에

[자동 통화 응답 구성, 398 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.

단계 2 [찾기]를 클릭하여 지원 되는 전화기 템플릿 목록을 표시합니다.

단계 3 새 전화기 버튼 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.

- 전화기의 모델에 대한 기본 템플릿을 선택하고 복사를 클릭합니다.
- 전화기 버튼 템플릿 정보 필드에 템플릿의 새 이름을 입력합니다.
- 저장을 클릭합니다.

단계 4 기존 템플릿에 전화기 버튼을 추가하려는 경우 다음 단계를 수행합니다.

- 찾기를 클릭하고 검색 기준을 입력합니다.
- 기존 템플릿을 선택합니다.

단계 5 회선 드롭다운 목록에서 템플릿에 추가하려는 기능을 선택합니다.

단계 6 저장을 클릭합니다.

단계 7 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다.

당겨받기 버튼 템플릿을 전화기와 연결

시작하기 전에

[당겨받기 전화기 버튼 템플릿 구성, 400 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.

단계 3 전화기 버튼 템플릿을 추가할 전화기를 선택합니다.

단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

BLF 당겨받기 이니시에이터에 대한 BLF 단축 다이얼 번호 구성

시작하기 전에

[당겨받기 버튼 템플릿을 전화기와 연결, 401 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 BLF 당겨받기 이니시에이터로 사용할 전화기를 선택합니다.

단계 3 연결 창에서 새 **BLF SD** 링크를 추가합니다.

통화 상태 감시(BLF) 다이얼 구성 창이 표시됩니다.

단계 4 BLF SD 버튼으로 모니터링할 디렉토리 번호(BLF DN)를 선택합니다.

단계 5 BLF 통화 당겨받기 및 BLF 단축 다이얼에 대한 BLF SD 버튼을 사용하려면 통화 당겨받기 확인란을 선택합니다. 이 확인란을 선택 취소하는 경우 BLF 단축 다이얼에만 BLF SD 버튼이 사용됩니다.

단계 6 저장을 클릭합니다.

당겨받기에 대한 소프트키 구성

프로시저

	명령 또는 동작	목적
단계 1	통화 당겨받기에 대한 소프트키 템플릿 구성, 402 페이지	당겨받기, 그룹 당겨받기 받기 및 기타 당겨받기 소프트키를 소프트키 템플릿에 추가합니다.
단계 2	소프트키 템플릿을 일반 디바이스 구성에 연결, 404 페이지에 대해 다음 하위 작업을 수행합니다. <ul style="list-style-type: none"> 소프트키 템플릿을 일반 디바이스 구성에 추가, 404 페이지 일반 디바이스 구성을 전화기에 연결, 405 페이지 	선택 사항. 전화기에서 소프트키 템플릿을 사용할 수 있게 하려면 이 단계 또는 다음 단계를 완료해야 합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 이 단계를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.
단계 3	소프트키 템플릿을 전화기에 연결, 405 페이지	선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하거나 일반 디바이스 구성과 함께 연결하는 대신 사용할 수 있습니다. 일반 디바이스 구성 또는 다른 기본 소프트키에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우 일반 디바이스 구성과 함께 이 절차를 사용합니다.

통화 당겨받기에 대한 소프트키 템플릿 구성

이 절차를 사용하여 다음과 같은 당겨받기 소프트키를 사용할 수 있습니다.

소프트키	설명	통화 상태
통화 당겨받기(당겨받기)	그룹 내의 다른 내선 번호에서 통화에 응답할 수 있습니다.	온 혹은 오프
그룹 당겨받기(그룹픽업)	그룹 외부의 내선 번호에서 통화에 응답할 수 있습니다.	온 혹은 오프
기타 당겨받기(기타픽업)	그룹과 연결된 다른 통화 그룹에서 울리는 전화를 받을 수 있습니다.	온 혹은 오프

시작하기 전에

당겨받기 전화기 버튼 구성, 400 페이지

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- a) 새로 추가를 클릭합니다.
 - b) 기본 템플릿을 선택하고 복사를 클릭합니다.
 - c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - d) 저장을 클릭합니다.
- 단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
- a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 필요한 기존 템플릿을 선택합니다.
- 단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.
- 참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.
- 단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
- 단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.
- 단계 7 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.
- 단계 8 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.
- 단계 9 저장을 클릭합니다.
- 단계 10 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

다음에 수행할 작업

다음 작업 중 하나를 수행합니다.

- [소프트키 템플릿을 일반 디바이스 구성에 연결, 404 페이지](#)
- [소프트키 템플릿을 전화기에 연결, 405 페이지](#)

소프트키 템플릿을 일반 디바이스 구성에 연결

선택 사항. 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 [소프트키 템플릿을 전화기에 연결, 405 페이지](#)의 내용을 참조하십시오.

프로시저

단계 1 [소프트키 템플릿을 일반 디바이스 구성에 추가, 404 페이지](#)

단계 2 [일반 디바이스 구성을 전화기에 연결, 405 페이지](#)

소프트키 템플릿을 일반 디바이스 구성에 추가

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성

단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.

- a) 새로 추가를 클릭합니다.
- b) 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
- c) 저장을 클릭합니다.

단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.

- a) 찾기를 클릭하고 검색 기준을 입력합니다.
- b) 기존 일반 디바이스 구성을 클릭합니다.

단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

단계 6 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.

- 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

일반 디바이스 구성을 전화기에 연결

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정 을 클릭하여 전화기 설정을 업데이트합니다.

소프트키 템플릿을 전화기에 연결

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.
- 단계 4 저장을 클릭합니다.

당겨받기 상호 작용

기능	상호 작용
경로 플랜 보고서	라우트 계획 보고서에는 Unified Communications Manager에서 구성된 패턴과 DN이 표시됩니다. 통화 당겨받기 그룹에 DN을 할당하기 전에, 경로 플랜 보고서를 사용하여 중첩된 패턴과 DN을 검색하십시오.
발신 검색 공간 및 파티션	디바이스 발신 검색 공간을 기준으로 사용자에게 대한 통화 당겨받기 액세스를 제한하려면 통화 당겨받기 그룹 번호에 파티션을 할당합니다.
시간(TOD)	연결된 그룹의 구성원에 대한 시간(TOD) 매개 변수를 사용하면 해당 그룹의 동일한 기간 내에 있는 통화를 받을 수 있습니다. TOD는 타임스탬프를 발신 검색 공간 및 파티션과 연결합니다.

기능	상호 작용
통화 회계	<p>전화 받기가 자동 응답을 통해 발생할 경우 시스템에서 2개의 CDR(통화 세부 정보 레코드)을 생성합니다. 한 CDR은 지워지는 원래 통화에 적용되고 다른 CDR은 연결 요청 통화에 적용됩니다.</p> <p>통화 당겨받기가 비자동 통화 당겨받기를 통해 발생할 경우에는 시스템에서 연결 요청 통화에 적용되는 하나의 통화 세부 정보 레코드를 생성합니다.</p> <p>CDR 검색은 특정 시간 범위와 일치하는 CDR과 다른 검색 기준과 일치하는 CDR을 모두 반환합니다. 특정 CDR과 연결된 통화 유형을 검색할 수도 있습니다. 검색 결과에는 통화가 당겨받기 통화인지 여부를 나타내는 통화 유형 필드가 표시됩니다.</p>
착신 전환	<p>자동 통화 당겨받기 활성화(Auto Call Pickup Enabled) 서비스 매개 변수가 [거짓]으로 설정된 상태에서 통화 당겨받기가 발생할 경우 당겨받기 소프트웨어 중 하나를 누르면 전화기에 구성된 통화 착신 전환이 무시됩니다. 통화 당겨받기 요청자가 응답하지 않을 경우 [통화 당겨받기 응답 없음 타이머]가 만료되면 원래 통화가 복원됩니다.</p>

당겨받기 제한 사항

제한 사항	설명
다른 통화 당겨받기 그룹에 대한 다른 전화 회선	한 대의 전화기에서 서로 다른 회선이 서로 다른 통화 당겨받기 그룹에 할당될 수 있지만, 사용자에게 혼란을 줄 수 있으므로 Cisco는 이 설정을 권장하지 않습니다.
통화 당겨받기 그룹 번호	<ul style="list-style-type: none"> 통화 당겨받기 그룹이 회선 또는 DN과 연결되어 있을 때에는 해당 그룹을 삭제할 수 없습니다. 통화 당겨받기 그룹 번호를 사용 중인 회선을 파악하려면, 통화 당겨받기 구성 창에서 종속성 레코드를 사용합니다. 통화 당겨받기 그룹 번호를 삭제하려면, 각 회선 또는 DN에 새 통화 당겨받기 그룹 번호를 재할당합니다. 통화 당겨받기 그룹 번호를 업데이트하면 Cisco Unified Communications Manager가 해당 통화 당겨받기 그룹에 할당된 모든 디렉터리 번호를 자동으로 업데이트합니다.
SIP 전화기	<ul style="list-style-type: none"> 시스템은 SIP를 실행하는 몇몇 Cisco Unified IP Phone에서 통화 당겨받기 알림을 지원하지 않습니다. 통화 당겨받기 알림은 SIP를 실행하는 사용이 허가된 타사 전화기에서만 지원됩니다.

제한 사항	설명
직접 통화 당겨받기	<ul style="list-style-type: none"> • 힌트 파일럿 번호로 전화를 걸어 이루어진 통화로 인해 힌트 목록에 속하는 디바이스에서 벨소리가 울릴 경우, 사용자는 직접 통화 당겨받기 기능을 사용하여 그러한 통화를 당겨받을 수 없습니다. • 사용자는 회선 그룹에 속하는 DN에 대한 통화를 직접 통화 당겨받기 기능을 사용하여 당겨받을 수 없습니다.
BLF 당겨받기	시스템은 SIP를 실행하는 몇몇 Cisco Unified IP Phone에서 통화 당겨받기 알림을 지원하지 않습니다.
발신자 수신 국제 번호 접두사 - 전화기	“수신 발신자 국제 번호 접두사 - 전화기” 서비스 매개 변수에서 접두사를 구성하고 통화 당겨받기 그룹의 다른 구성원에게 국제 전화를 거는 경우 통화 당겨받기 그룹의 다른 구성원이 통화를 당겨받지 않으면 발신자 필드에서 해당 접두사가 호출되지 않습니다.



31 장

통화 대기 및 직접 통화

- 통화 대기 개요, 409 페이지
- 통화 지정 보류 사전 요건, 410 페이지
- 통화 대기 구성 작업 흐름, 411 페이지
- 통화 지정 보류 상호 작용, 426 페이지
- 통화 대기 제한 사항, 427 페이지
- 통화 대기 문제 해결, 428 페이지
- 통화 전환 보류 개요, 428 페이지
- 통화 전환 보류 사전 요건, 429 페이지
- 통화 전환 보류 구성 작업 흐름, 429 페이지
- 통화 전환 보류 상호 작용, 433 페이지
- 통화 전환 보류 제한 사항, 435 페이지
- 통화 전환 보류 문제 해결, 436 페이지

통화 대기 개요

통화 지정보류 기능을 사용하면 통화를 대기 중으로 설정하여 Unified Communications Manager 시스템의 다른 전화기에서 통화가 검색되도록 할 수 있습니다(예: 다른 사무실 또는 회의실의 전화기). 활성 통화 중인 경우 지정보류 소프트키를 눌러서 통화 지정보류 내선으로 통화를 지정보류할 수 있습니다. 그런 다음 시스템의 다른 전화기가 통화 지정보류 내선 번호로 전화를 걸어 통화를 검색할 수 있습니다.

통화 지정보류 내선 번호로 사용하도록 단일 디렉터리 번호 또는 디렉터리 번호 범위를 정의할 수 있습니다. 각 통화 지정보류 내선 번호에서 한 개의 통화만 지정보류할 수 있습니다.

통화 지정보류 기능은 Unified Communications Manager 클러스터 안에서 작동하며 클러스터의 각 Unified Communications Manager는 통화 지정보류 내선 번호가 정의되어 있어야 합니다. 통화 지정보류 내선 번호로 사용하도록 단일 디렉터리 번호 또는 디렉터리 번호 범위를 정의할 수 있습니다. 디렉터리 번호 또는 번호 범위가 고유한지 확인하십시오.

사용자는 할당된 경로 패턴(예: ICT(Intercluster Trunk)에 대한 경로 패턴은 80XX일 수 있음) 및 통화 지정보류 번호(예: 8022)로 전화를 걸어 다른 Unified Communications Manager 클러스터에서 지정보류

류된 통화를 가져올 수 있습니다. 발신 검색 공간 및 파티션이 적절히 구성되어 있는지 확인해야 합니다. 통화 지정보류는 전체 클러스터에서 작동합니다.

유효한 통화 지정보류 내선 번호는 정수와 와일드카드 문자 X로 구성됩니다. 통화 지정보류 내선 번호에는 최대 XX를 구성할 수 있으며(예: 80XX) 이 경우 최대 100개의 통화 지정보류 내선 번호가 제공됩니다. 통화가 지정보류될 경우 Unified Communications Manager는 사용 가능한 다음 통화 지정보류 내선 번호를 선택하고 전화기에 해당 번호를 표시합니다.

지정보류 모니터링

통화 지정보류 모니터링은 타이머가 만료될 때까지 지정 보류된 통화의 상태를 Cisco Unified Communications Manager에서 모니터링하는 선택적 통화 지정보류 기능입니다. 타이머가 만료되면 통화가 미리 할당된 번호로 착신 전환되거나, 음성 메일로 전송되거나, 통화 지정보류자에게 반환됩니다. 전화기 회선과 헌트 파일럿에 지정 보류 모니터링을 적용할 수 있습니다.

통화 지정 보류 사전 요건

클러스터 간에 통화 지정 보류를 사용하는 경우에는 파티션 및 발신 검색 공간을 구성해야 합니다.

표 29: 지정 보류 소프트키 템플릿 및 통화 지정 보류 버튼 템플릿을 지원하는 **Cisco Unified IP Phone**

전화기 모델	지원되는 소프트키 템플릿	지원되는 전화기 버튼 템플릿
Cisco Unified IP Phone 6900 시리즈(6901 및 6911 제외)	X	X
Cisco IP 전화기 7800 시리즈	X	X
Cisco Unified IP Phone 7900 시리즈(7921, 7925, 7936, 7937 제외)	X	
Cisco IP 전화기 8800 시리즈	X	X
Cisco Unified IP Phone 8900 시리즈	X	X
Cisco Unified IP Phone 9900 시리즈	X	X
Cisco Unified IP Phone 7900 시리즈(7906, 7911, 7921, 7925, 7936, 7937 제외)		X



참고 프로그램 가능 회선 키 기능을 사용하여 모든 회선(회선 1 제외)이나 버튼에 통화 지정보류를 구성할 수 있습니다.

통화 대기 구성 작업 흐름

시작하기 전에

- [통화 지정 보류 사전 요건, 410 페이지](#) 검토

프로시저

	명령 또는 동작	목적
단계 1	클러스터 수준 통화 대기 구성, 412 페이지	(선택 사항). 전체 클러스터에 대해 통화 대기를 구성하거나 3단계의 절차에 따라 클러스터 내 서버에서 통화 대기를 구성합니다.
단계 2	통화 지정 보류에 대한 파티션 구성, 413 페이지	통화 대기 번호를 추가하기 위한 파티션을 만듭니다.
단계 3	통화 지정보류 번호 구성, 413 페이지	클러스터의 여러 서버에 걸쳐 통화 대기를 사용하도록 통화 대기 번호를 구성합니다.
단계 4	통화 대기를 위한 소프트키 템플릿 구성, 416 페이지	지정 보류 소프트키를 소프트키 템플릿에 추가합니다.
단계 5	소프트키 템플릿을 일반 디바이스 구성에 연결, 417 페이지 에 대해 다음 하위 작업을 수행합니다. <ul style="list-style-type: none"> • 소프트키 템플릿을 일반 디바이스 구성에 추가, 418 페이지 • 일반 디바이스 구성을 전화기에 연결, 418 페이지 	(선택 사항) 전화기에서 소프트키 템플릿을 사용할 수 있게 하려면 이 단계 또는 다음 단계를 완료해야 합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 이 단계를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.
단계 6	소프트키를 전화기와 연결, 419 페이지	(선택 사항) 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하거나 일반 디바이스 구성과 함께 연결하는 대신 사용할 수 있습니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우 일반 디바이스 구성과 함께 이 절차를 사용합니다.
단계 7	통화 대기 버튼 구성, 419 페이지 에 대해 다음 하위 작업을 수행합니다. <ul style="list-style-type: none"> • 통화 대기를 위한 전화기 버튼 템플릿 구성, 419 페이지 • 버튼 템플릿을 전화기와 연결, 420 페이지 	

	명령 또는 동작	목적
단계 8	지정보류 모니터링 구성, 420 페이지	이 선택적 작업 흐름을 완료하여 통화 대기 구성에 지정 보류 모니터링을 추가합니다.

클러스터 수준 통화 대기 구성

프로시저

단계 1 시스템 > 서비스 매개 변수를 선택합니다.

단계 2 원하는 노드를 서버로, 서비스를 **Cisco CallManager**(활성)로 선택합니다.

단계 3 고급을 클릭합니다.

창에 고급 서비스 매개 변수가 표시됩니다.

단계 4 클러스터 수준 매개 변수(기능 - 일반) 섹션에서 클러스터 수준 통화 지정보류 번호/범위 활성화를 **True**로 설정합니다.

기본값은 false입니다. 이 매개 변수는 통화 지정보류 기능이 클러스터 수준으로 구현되었는지 또는 특정 Unified CM 노드로 제한되는지 여부를 결정합니다.

단계 5 Cisco CallManager 서비스 및 통화 지정보류가 구성된 클러스터의 각 서버에 대해 통화 지정보류 표시 타이머를 설정합니다.

기본값은 10초입니다. 이 매개 변수는 통화 지정보류 번호가 통화를 지정보류한 전화기에 표시되는 시간을 결정합니다.

단계 6 Unified Communications Manager 서비스 및 통화 지정보류가 구성된 클러스터의 각 서버에 대해 통화 지정보류 복귀 타이머를 설정합니다.

기본값은 60초입니다. 이 매개 변수는 통화가 지정보류 상태를 유지하는 시간을 결정합니다. 이 타이머가 만료되면 지정보류된 통화가 통화를 지정보류한 디바이스로 돌아갑니다. 헌트 그룹 구성원이 헌트 파일럿을 통해 오는 통화를 지정보류하는 경우에는 통화 지정보류 복귀 타이머 만료 시 통화가 헌트 파일럿으로 돌아갑니다.

참고 통화 지정보류 복귀 타이머(Call Park Reversion Timer) 값을 통화 지정보류 표시 타이머(Call Park Display Timer)보다 작게 설정할 경우, 통화 지정보류 번호가 전화기에 표시되지 않을 수 있습니다.

단계 7 저장을 클릭합니다.

단계 8 모든 Unified Communications Manager 및 CTI 관리자 서비스를 다시 시작합니다.

통화 지정 보류에 대한 파티션 구성

연결성 특성이 비슷한 디렉터리 번호(DN) 및 라우트 패턴의 논리적 그룹을 만들기 위해 파티션을 구성합니다. 파티션은 조직, 위치 및 통화 유형에 따라 라우트 플랜을 논리적 하위 집합으로 나눔으로써 콜 라우팅을 지원합니다. 여러 파티션을 구성할 수 있습니다.

시작하기 전에

(선택사항) [클러스터 수준 통화 대기 구성, 412 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 파티션.

단계 2 새로 추가를 클릭하여 새 파티션을 생성합니다.

단계 3 파티션 이름, 설명 필드에 경로 플랜에 고유한 파티션 이름을 입력합니다.

파티션 이름에는 영숫자 문자는 물론 공백, 하이픈(-) 및 밑줄(_)을 사용할 수 있습니다. 파티션 이름에 대한 지침은 온라인 도움말을 참조하십시오.

단계 4 파티션 이름 뒤에 쉼표(,)를 입력하고 동일한 줄에 파티션 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\), 꺾쇠괄호(<>) 또는 대괄호([])는 사용할 수 없습니다.

설명을 입력하지 않으면 Cisco Unified Communications Manager에서 자동으로 이 필드에 파티션 이름을 입력합니다.

단계 5 여러 파티션을 생성하려면 각 파티션 항목마다 한 행을 사용합니다.

단계 6 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.

시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성 상태로 유지됩니다.

단계 7 구성할 다음 라디오 버튼 중 하나를 선택하고 시간대를 구성합니다.

- 시작 디바이스—이 라디오 버튼을 선택하면 시스템은 발신 디바이스의 표준 시간대를 시간 일정과 비교하여 파티션을 수신 통화를 받는 데 사용할 수 있는지 여부를 확인합니다.
- 특정 표준 시간대—이 라디오 버튼을 선택한 후에 드롭다운 목록에서 표준 시간대를 선택합니다. 시스템은 선택한 표준 시간대를 시간 일정과 비교하여 수신 통화를 받는 데 파티션을 사용할 수 있는지 여부를 확인합니다.

단계 8 저장을 클릭합니다.

통화 지정보류 번호 구성

클러스터의 서버 간에 통화 지정보류를 사용하려면 각 서버에 통화 지정보류 내선 번호를 구성해야 합니다.

각 통화 지정보류 디렉터리 번호, 파티션 및 범위가 Unified Communications Manager 내에서 고유한지 확인하십시오. 디바이스를 등록하는 각 Unified Communications Manager에는 고유한 통화 지정보류 디렉터리 번호와 범위가 필요합니다. Cisco 통합 커뮤니케이션 매니저 관리에서는 통화 지정보류를 구성하는 데 사용하는 통화 지정보류 번호 또는 범위를 확인하지 않습니다. 유효한 번호 또는 범위와 범위 중첩 가능성을 식별하는 데 도움을 받으려면, Unified Communications Manager Dialed Number Analyzer 도구를 사용하십시오.

시작하기 전에

[통화 지정 보류에 대한 파티션 구성, 413 페이지](#)

프로시저

단계 1 통화 라우팅 > 통화 지정보류를 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 새 통화 지정보류 번호를 추가하려면 새로 추가를 클릭합니다.
- 통화 지정보류 번호를 복사하려면 통화 지정보류 번호 또는 번호 범위를 찾은 다음 복사 아이콘을 클릭합니다.
- 통화 지정보류 번호를 업데이트하려면 통화 지정보류 번호 또는 번호 범위를 찾습니다.

통화 지정보류 번호 구성 창이 표시됩니다.

단계 3 통화 지정보류 구성 필드에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [통화 지정보류 구성 필드, 415 페이지](#)를 참조하십시오.

단계 4 새로 추가하거나 변경한 통화 지정보류 번호를 데이터베이스에 저장하려면 저장을 클릭합니다.

통화 지정정보류 구성 필드

필드	설명
통화 지정정보류 번호/범위	<p>통화 지정정보류 내선 번호를 입력합니다. 숫자 또는 와일드카드 문자 X를 입력할 수 있습니다(1개 또는 2개의 X가 허용됨). 예를 들어, 5555의 단일 통화 지정정보류 내선 번호를 정의하려면 5555를 입력하고 5500부터 5599까지 통화 지정정보류 내선 번호 범위를 정의하려면 55XX를 입력합니다.</p> <p>참고 하나의 통화 지정정보류 범위 정의를 사용하여 최대 100개의 통화 지정정보류 번호를 만들 수 있습니다. 통화 지정정보류 번호는 고유하게 지정해야 합니다.</p> <p>참고 Unified Communications Manager 서버와 통화 지정정보류 번호를 중복할 수 없습니다. 각 Unified Communications Manager 서버에 고유한 번호 범위가 있는지 확인하십시오.</p> <p>참고 통화가 시작되는 서버 목록에서 통화 지정정보류 범위를 선택합니다. 예를 들어, 전화기 A(노드 A에 등록)가 전화기 B(노드 B에 등록)에 전화를 걸고 전화기 B 사용자가 [지정보류]를 누를 경우 전화기 B는 노드 A에 상주하는 CSS의 통화 지정정보류 범위가 필요합니다. 전화기와 게이트웨이가 다양한 노드를 사용하여 통신하고 임의 서버에서 시작된 통화를 지정정보류해야 하는 멀티노드 환경에서는 전화기에 모든 서버의 통화 지정정보류 범위가 포함된 CSS가 필요합니다.</p>
설명	이 통화 지정정보류 번호에 대한 간략한 설명을 입력합니다. 설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&) 또는 꺾쇠괄호(<>)는 사용할 수 없습니다.

필드	설명
파티션	<p>통화 지정보류 번호에 대한 액세스를 제한하기 위해 파티션을 사용하려는 경우 드롭다운 목록에서 원하는 파티션을 선택합니다. 통화 지정보류 번호에 대한 액세스를 제한하지 않으려면 파티션에 대해 <None>을 선택합니다.</p> <p>참고 통화 지정보류 내선 번호와 파티션과의 조합이 Unified Communications Manager 내에서 고유한지 확인하십시오.</p>
Unified Communications Manager	드롭다운 목록을 사용하여 이러한 통화 지정보류 번호가 적용되는 Cisco Unified Communications Manager를 선택합니다.

통화 대기를 위한 소프트키 템플릿 구성

이 절차를 사용하여 지정 보류 소프트키를 사용할 수 있게 합니다.

지정 보류 소프트키에는 다음과 같은 통화 상태가 있습니다.

- 온 훅
- 링아웃
- 호전환 연결됨

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
 - a) 새로 추가를 클릭합니다.
 - b) 기본 템플릿을 선택하고 복사를 클릭합니다.
 - c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - d) 저장을 클릭합니다.
- 단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
 - a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 필요한 기존 템플릿을 선택합니다.
- 단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.

참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.

- 단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
- 단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.
- 단계 7 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.
- 단계 8 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.
- 단계 9 저장을 클릭합니다.
- 단계 10 다음 작업 중 하나를 수행합니다.
 - 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

소프트키 템플릿을 일반 디바이스 구성에 연결

선택 사항. 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면, 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

프로시저

- 단계 1 [소프트키 템플릿을 일반 디바이스 구성에 추가, 418 페이지](#)
- 단계 2 [일반 디바이스 구성을 전화기에 연결, 418 페이지](#)

소프트키 템플릿을 일반 디바이스 구성에 추가

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성
- 단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.
- a) 새로 추가를 클릭합니다.
 - b) 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
 - c) 저장을 클릭합니다.
- 단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.
- a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 기존 일반 디바이스 구성을 클릭합니다.
- 단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.
- 단계 5 저장을 클릭합니다.
- 단계 6 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.
-

일반 디바이스 구성을 전화기에 연결

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정을 클릭하여 전화기 설정을 업데이트합니다.
-

소프트키를 전화기와 연결

선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성과 연결할 수 있습니다. 이 절차는 일반 디바이스 구성과 함께 작동합니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우에 사용할 수 있습니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
 - 단계 2 찾기를 클릭하고 전화기를 선택하여 소프트키 템플릿을 추가합니다.
 - 단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.
 - 단계 4 저장을 클릭합니다.
 - 단계 5 재설정을 눌러 전화기 설정을 업데이트합니다.
-

통화 대기 버튼 구성

통화 대기를 위한 전화기 버튼 템플릿 구성

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.
 - 단계 2 [찾기] 를 클릭하여 지원 되는 전화기 템플릿 목록을 표시합니다.
 - 단계 3 새 전화기 버튼 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
 - a) 전화기의 모델에 대한 기본 템플릿을 선택하고 복사를 클릭합니다.
 - b) 전화기 버튼 템플릿 정보 필드에 템플릿의 새 이름을 입력합니다.
 - c) 저장을 클릭합니다.
 - 단계 4 기존 템플릿에 전화기 버튼을 추가하려는 경우 다음 단계를 수행합니다.
 - a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 기존 템플릿을 선택합니다.
 - 단계 5 회선 드롭다운 목록에서 템플릿에 추가하려는 기능을 선택합니다.
 - 단계 6 저장을 클릭합니다.
 - 단계 7 다음 작업 중 하나를 수행합니다.
 - 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.

- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다.

버튼 템플릿을 전화기와 연결

시작하기 전에

통화 대기를 위한 전화기 버튼 템플릿 구성, [419 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.

단계 3 전화기 버튼 템플릿을 추가할 전화를 선택합니다.

단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

지정보류 모니터링 구성

이러한 선택적 작업을 완료하여 통화지정 보류 구성에 지정보류 모니터링을 추가합니다.

시작하기 전에

지정보류 모니터링은 통화 지정보류를 지원하는 전화기의 하위 집합에서만 지원됩니다. 다음 Cisco Unified IP Phone은 지정보류 모니터링을 지원합니다.

- Cisco IP 전화기 8811
- Cisco IP 전화기 8841
- Cisco IP 전화기 8845
- Cisco IP 전화기 8851
- Cisco IP 전화기 8851NR
- Cisco IP 전화기 8861
- Cisco IP 전화기 8865
- Cisco IP 전화기 8865NR
- Cisco Unified IP Phone 8961

- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

프로시저

	명령 또는 동작	목적
단계 1	지정보류 모니터링 시스템 타이머 구성, 421 페이지	지정보류 모니터링 기능에 대한 시스템 수준 타이머를 구성합니다.
단계 2	헌트 파일럿에 대한 지정보류 모니터링 구성, 422 페이지	(선택 사항) 헌트 파일럿이 구축된 경우 지정보류 모니터링 대상을 헌트 파일럿에 할당합니다.
단계 3	디렉터리 번호에 대한 지정보류 모니터링 구성, 423 페이지	개별 전화 회선에 대한 지정보류 모니터링 대상을 할당합니다.
단계 4	유니버설 회선 템플릿을 통한 지정보류 모니터링 구성, 424 페이지	LDAP 디렉터리 동기화가 구성된 경우에는 범용 회선 템플릿을 사용하여 지정보류 모니터링이 구성된 여러 사용자에 대한 디렉터리 번호 설정을 프로비저닝할 수 있습니다.

지정보류 모니터링 시스템 타이머 구성

이 절차를 사용하여 지정보류 모니터링 기능에 대한 시스템 수준 타이머를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 퍼블리셔 노드를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 다음 서비스 매개 변수에 대한 값을 구성합니다.

- 지정보류 모니터링 복귀 타이머—Cisco Unified Communications Manager에서 사용자에게 지정보류한 통화를 검색하라는 메시지를 표시하기 전까지 대기하는 시간(초)입니다. 개별 전화 회선의 경우 디렉터리 번호 구성 창에서 동일한 설정으로 이 설정을 재정의할 수 있습니다. 통화 지정보류 복귀 타이머가 만료되면 통화가 헌트 파일럿으로 착신 전환됩니다.
- 지정보류 모니터링 주기적 복귀 타이머 — 통화가 지정보류 되었을 때 복귀 시도 사이의 시간(초)입니다. Cisco Unified Communications Manager는 지정보류 전화기 벨소리를 울리거나 경고를 내거나 깜박여서 지정 보류된 통화에 대해 사용자에게 알립니다. 지정보류 모니터링 복귀 타이머가 만료되면 통화가 헌트 파일럿이 아닌 지정 보류된 상대방에게 착신 전환됩니다.
- 지정보류 모니터링 착신 전환 검색 없음 타이머—지정보류된 통화가 통화 지정보류의 디렉터리 번호 구성에 지정된 지정보류 모니터링 착신 전환 검색 없음 대상으로 전달되기 전에 통화 대기

미리 알림이 발생하는 시간(초)입니다. 지정정보류 모니터링 착신 전환 검색 없음 타이머가 만료되면 통화가 헌트 파일럿으로 착신 전환됩니다.

참고 이러한 필드에 대한 자세한 내용은 서비스 매개 변수 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

다음에 수행할 작업

이러한 선택적 작업을 사용하여 개별 전화기 회선 및 헌트 파일럿에 대해 만료된 타이머가 처리되는 방식을 할당합니다.

- [헌트 파일럿에 대한 지정정보류 모니터링 구성, 422 페이지](#)
- [디렉터리 번호에 대한 지정정보류 모니터링 구성, 423 페이지](#)
- [유니버설 회선 템플릿을 통한 지정정보류 모니터링 구성, 424 페이지](#)

헌트 파일럿에 대한 지정정보류 모니터링 구성

구축에서 헌트 파일럿을 사용하는 경우 이 옵션 절차를 사용하여 헌트 파일럿에 지정정보류 모니터링 대상을 할당합니다.



참고 헌트 파일럿 설정에 대한 일반적인 정보는 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "헌트 파일럿 구성" 장을 참조하십시오.

시작하기 전에

[지정정보류 모니터링 시스템 타이머 구성, 421 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 경로/헌트 > 헌트 파일럿.

단계 2 찾기를 클릭하고 지정정보류 모니터링 대상을 구성하려는 헌트 파일럿을 선택합니다.

단계 3 지정정보류 모니터링 검색 대상 없음 필드에서 대상 디렉터리 번호 및 발신 검색 공간을 할당합니다.

단계 4 헌트 파일럿 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

디렉터리 번호에 대한 지정보류 모니터링 구성

이 절차를 사용하여 개별 전화 회선에 대한 지정 보류 모니터링 대상을 할당합니다. 다른 번호로 통화를 착신 전환하거나, 음성 메일로 보내거나, 통화 지정 보류로 돌아갈 수 있습니다.



참고 다음 도구는 여러 전화 회선에 대한 설정을 프로비저닝하는 데 사용할 수 있습니다.

- 범용 회선 템플릿을 사용하여 LDAP 디렉터리 동기화를 통해 여러 전화 회선에 대한 지정 보류 모니터링 설정을 프로비저닝합니다. 자세한 내용은 [유니버설 회선 템플릿을 통한 지정보류 모니터링 구성, 424 페이지](#)를 참조하십시오.
- 벌크 관리 도구를 사용하여 많은 수의 전화 회선에 대한 설정을 포함하는 CSV 파일을 가져옵니다. 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서](#)를 참조하십시오.

시작하기 전에

[지정보류 모니터링 시스템 타이머 구성, 421 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 디렉터리 번호.

단계 2 찾기를 클릭하고 구성된 디렉터리 번호를 선택합니다.

단계 3 다음 지정보류 모니터링 필드에 값을 입력합니다.

- 지정보류 모니터링 착신 전환 검색 없음 외부 대상—지정보류 모니터링 착신 전환 검색 없음 타이머가 만료되고 피지정보류자가 외부 당사자인 경우, 통화는 음성 메일 또는 지정된 디렉토리 번호로 전달됩니다. 이 필드가 비어 있는 경우 통화가 지정보류자의 회선으로 재전송됩니다.
- 지정보류 모니터링 착신 전환 검색 없음 내부 대상—지정보류 모니터링 착신 전환 검색 없음 타이머가 만료되고 피지정보류자가 내부 당사자인 경우, 통화는 음성 메일 또는 지정된 디렉토리 번호로 전달됩니다. 이 필드가 비어 있는 경우 통화가 지정보류자의 회선으로 재전송됩니다.
- 지정보류 모니터링 복귀 타이머—Cisco Unified Communications Manager에서 사용자에게 이 전화 회선에서 지정보류한 통화를 검색하라는 메시지를 표시하기 전까지 대기하는 시간(초)입니다. 값이 0이거나 비어 있으면 Cisco Unified Communications Manager는 지정 보류 모니터 복귀 타이머 서비스 매개 변수의 값을 사용합니다.

단계 4 디렉터리 번호 구성 창의 나머지 필드를 완료합니다.필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

유니버설 회선 템플릿을 통한 지정보류 모니터링 구성

이 절차를 사용하여 범용 회선 템플릿에 지정보류 모니터링 설정을 할당합니다. LDAP 디렉터리 동기화가 구성되어 있는 경우에는 범용 회선 템플릿 구성을 사용하여 여러 사용자에게 대해 구성된 지정보류 모니터링을 사용하여 디렉터리 번호 설정을 프로비저닝할 수 있습니다.

시작하기 전에

[지정보류 모니터링 시스템 타이머 구성, 421 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 사용자 전화/추가 > 범용 회선 템플릿.

단계 2 다음 단계 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 템플릿을 선택합니다.
- 새로 추가를 클릭하여 새 템플릿을 만듭니다.

단계 3 지정보류 모니터링 설정 섹션을 확장하고 필드를 완성합니다. 필드 설명은 [유니버설 회선 템플릿에 대한 지정보류 모니터링 설정, 424 페이지](#)를 참조하십시오.

단계 4 저장을 클릭합니다.

다음에 수행할 작업

범용 회선 템플릿을 개별 디렉터리 번호에 적용하려면 사용자 프로파일, 기능 그룹 템플릿 및 LDAP 디렉터리 동기화에 템플릿을 할당해야 합니다. 동기화가 발생하면 해당 템플릿 설정이 동기화의 일부인 전화기 회선에 적용됩니다. LDAP 설정에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 "최종 사용자 구성" 장을 참조하십시오.

유니버설 회선 템플릿에 대한 지정보류 모니터링 설정

다음 표에는 Cisco Unified Communications Manager의 유니버설 회선 템플릿 구성 창에 있는 지정보류 모니터링 필드가 포함되어 있습니다.

표 30: 유니버설 회선 템플릿에 대한 지정보류 모니터링 설정

필드	설명
검색되지 않을 때 외부 통화의 착신 전환 대상	<p>통화가 지정 보류된 사용자가 외부 상대방이고 지정 보류 모니터링 착신 전환 없음 타이머가 만료되면 시스템에서 다음 대상 중 하나로 통화를 전송합니다.</p> <ul style="list-style-type: none"> • 보이스메일 - 음성 메일 프로필의 구성을 사용하여 통화를 전송할 위치를 결정합니다. • 발신자에게로 복귀 - 통화를 통화 지정 보류 반환합니다. • 다른 번호로 통화를 착신 전환하려면 텍스트 상자에 다른 번호를 입력합니다. <p>옵션을 선택하지 않으면 통화가 통화 지정 보류 반환됩니다.</p>
검색되지 않을 때 외부 통화 착신 전환용 발신 검색 공간	지정 보류된 통화를 구성된 번호로 재전송하도록 구성한 경우에는 착신 전환 대상에 대한 발신 검색 공간을 선택합니다.
검색되지 않을 때 내부 통화의 착신 전환 대상	<p>통화가 지정 보류된 사용자가 내부 상대방이고 지정 보류 모니터링 착신 전환 없음 타이머가 만료되면 시스템에서 다음 대상 중 하나로 통화를 전송합니다.</p> <ul style="list-style-type: none"> • 보이스메일 - 음성 메일 프로필의 구성을 사용하여 통화를 전송할 위치를 결정합니다. • 발신자에게로 복귀 - 통화를 통화 지정 보류 반환합니다. • 다른 번호로 통화를 착신 전환하려면 텍스트 상자에 다른 번호를 입력합니다. <p>옵션을 선택하지 않으면 통화가 통화 지정 보류 반환됩니다.</p>
검색되지 않을 때 내부 통화 착신 전환용 발신 검색 공간	지정 보류된 통화를 구성된 번호로 재전송하도록 구성한 경우에는 착신 전환 대상에 대한 발신 검색 공간을 선택합니다.
지정 보류 복귀 타이머(초)	<p>이 타이머는 Unified Communications Manager에서 사용자가 지정 보류한 통화를 검색하라는 메시지를 표시하기 전에 대기하는 시간(초)을 결정하는 데 사용됩니다. 이 타이머는 사용자가 전화기에서 [지정보류] 소프트키를 누르면 시작되고, 타이머가 만료되면 미리 알림이 발행됩니다. 기본값은 60초입니다.</p> <p>참고 타이머에 대해 0을 선택하는 경우 이 템플릿을 사용하는 전화 회선은 지정 보류 모니터 복귀 타이머 클러스터 수준 서비스 매개 변수 값을 사용합니다.</p>

통화 지정 보류 상호 작용

기능	상호 작용
CTI 애플리케이션	CTI 애플리케이션은 통화 지정보류 DN에 대한 활동 모니터링을 포함한 통화 지정보류 기능에 액세스합니다. 통화 지정보류 DN을 모니터링하려면 CTI 애플리케이션과 연결된 애플리케이션 또는 최종 사용자를 표준 CTI 통화 지정보류 모니터링 허용 사용자 그룹에 추가합니다.
대기 중 음악	대기 중 음악을 사용하여 사용자는 스트리밍 소스에서 제공하는 음악으로 통화를 보류할 수 있습니다. 통화 중 음악 대기 오디오 소스는 전화기 구성 창의 네트워크 보류 MOH 오디오 소스 설정에 의해 선택됩니다. 디바이스 구성 내에서 오디오 소스를 선택하지 않는 경우 Cisco Unified CM에서는 디바이스폴에 정의된 오디오 소스를 사용하거나 디바이스폴에서 오디오 소스 ID를 지정하지 않은 경우 시스템 기본값을 사용합니다.
경로 플랜 보고서	라우트 플랜 보고서에는 Unified Communications Manager에서 구성된 패턴과 디렉터리 번호가 표시됩니다. 통화 지정보류에 디렉터리 번호를 할당하기 전에, 라우트 플랜 보고서를 사용하여 중첩된 패턴과 디렉터리 번호를 검색하십시오.
발신 검색 공간 및 파티션	디바이스 발신 검색 공간을 기준으로 사용자에게 통화 지정보류 액세스를 제한하려면 통화 지정보류 디렉터리 번호 또는 범위를 파티션에 할당하십시오.
지정전환	통화 지정보류에서는 음성전환([즉시 전환] 또는 [전환] 소프트키)을 지원합니다. 예를 들어 사용자 A가 사용자 B에게 전화를 걸고 사용자 B가 통화 지정을 보류합니다. 사용자 B가 통화를 검색하고 [전환] 또는 [전환] 소프트키를 눌러 통화를 음성 메시징 사서함으로 보낼지 결정합니다. 사용자 A가 사용자 B의 음성 메일 인사말을 받습니다.
참여	<ul style="list-style-type: none"> 참여와 통화 지정보류-대상 전화기(참여 중인 전화기)가 통화를 제어합니다. 참여 이니시에이터는 대상 전화기에 “피기백”합니다. 대상이 참여되는 경우에도 대상 전화기에 일반 기능이 대부분 포함되므로 참여 개시자는 기능에 액세스할 수 없습니다. 대상이 통화를 지정보류하는 경우 참여 개시자는 통화를 해지해야 합니다(참여) 회의끼기와 통화 지정보류-대상과 참여 이니시에이터는 피어 역할을 합니다. 회의끼기 기능은 컨퍼런스 브리지를 사용하므로 회의개설 전화회의처럼 동작합니다. 두 전화기(대상 및 참여 개시자) 모두 기능에 대한 모든 권한을 가집니다.
통화 전환 보류	통화 지정보류에 대해 [직접 통화 지정보류]와 [지정보류] 소프트 키를 둘 다 구성하지 않는 것이 좋지만, 둘 다 구성하는 것은 가능합니다. 둘 다 구성할 경우 통화 지정보류와 통화 전환 보류 번호가 중복되지 않도록 해야 합니다.

기능	상호 작용
QSIG 클러스터 간 트렁크	사용자가 QSIG 클러스터 간 트렁크 또는 QSIG 게이트웨이 트렁크 전반에서 통화를 지정보류할 경우, 지정보류된 발신자(피지정보류자)에게는 '지정보류된 번호로' 메시지가 표시되지 않습니다. 전화기에 원래 연결된 번호가 계속 표시됩니다. 통화는 지정보류되었고, 통화를 보류한 사용자는 해당 통화를 다시 가져올 수 있습니다. 지정보류된 상태에서 통화를 다시 가져오면, 통화는 계속되지만 지정보류된 발신자에게는 새로 연결된 번호가 표시되지 않습니다.

통화 대기 제한 사항

기능	제한 사항
통화 지정보류	Unified Communications Manager에서는 각 통화 보류 내선 번호에서 한 개의 통화만 지정보류할 수 있습니다.
공유 회선	노드 전반의 공유 회선 디바이스의 경우, 먼저 디바이스가 등록된 노드에 회선이 등록됩니다. 예를 들어, 가입자2의 디바이스가 먼저 등록된 후, 가입자2 및 퍼블리셔 노드에서 회선이 생성되는 경우, 해당 회선은 가입자2에 속합니다. 각 노드는 통화 지정보류 번호와 함께 구성해야 합니다.
백업	장애 조치 또는 폴백을 달성하려면, 게시자 노드와 가입자 노드에서 통화 지정보류 번호를 구성하십시오. 이를 구성하면 기본 노드가 작동하지 않을 때, 해당 회선 디바이스 연결이 보조 노드로 변경되고, 보조 노드 통화 지정보류 번호가 사용됩니다.
통화 전환 보류	직접 통화 지정보류(또는 통화 지정보류)가 공유 회선에서 시작되고, 어떤 디바이스에서도 해당 통화를 가져오지 않을 경우, 지정보류된 해당 통화가 공유 회선(지정보류 회선)의 수신자에게 복귀되지 않을 수 있습니다.
전화회의	두 공유 회선과 지정보류 복귀 중인 발신자 간에 전화회의 통화가 설정되거나 지정보류가 실패하면 양자간(다른 공유 회선과 발신자 간) 통화가 이루어집니다. 이유가 지정보류 복귀 중이면, Unified Communications Manager는 회선을 공유하는 두 디바이스로 통화를 확장하고 한쪽 당사자를 전화회의에 추가하려고 시도합니다(이미 전화회의에 참여하고 있거나 지정보류를 누른 당사자). 상대방이 이미 전화회의에 있는 상대방을 먼저 추가하려고 시도하면 지정 보류 복귀가 실패합니다. 지정보류 복귀가 실패하면, 해당 공유 회선은 정상시와 같이 통화에 참여할 수 있습니다.
서버 삭제	Unified Communications Manager에 대해 통화 지정보류 번호가 구성된 노드를 서버 구성 창(시스템 > 서버)에서 삭제하려고 할 경우, 노드 삭제가 실패합니다. 노드를 삭제하려면 먼저 Cisco 통합 커뮤니케이션 매니저 관리에서 해당 통화 지정보류 번호를 삭제해야 합니다.

통화 대기 문제 해결

사용자가 통화 대기를 할 수 없음

문제

사용자가 통화 대기를 할 수 없습니다. 사용자가 지정보류 소프트키 또는 기능 버튼을 누르면 통화가 지정보류되지 않습니다.

해결 방법

고유한 통화 지정 보류 번호가 클러스터의 Unified Communications Manager에 할당되었는지 확인합니다.

통화 지정 보류 번호에 할당된 파티션이 전화기 디렉터리 번호에 할당된 파티션과 일치하지 않습니다. 파티션에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 내용을 참조하십시오.

통화 대기 번호가 충분히 길게 표시되지 않음

문제

통화 지정 보류 번호가 사용자를 위해 충분히 길게 표시되지 않습니다.

해결 방법

통화 지정 보류 표시 타이머를 더 긴 기간으로 설정합니다. 타이머에 대한 자세한 내용은 [클러스터 수준 통화 대기 구성, 412 페이지](#)의 내용을 참조하십시오.

통화 전환 보류 개요

통화 전환 보류를 통해 사용자는 사용자가 선택한 사용 가능한 통화 전환 보류 번호로 통화를 호전환할 수 있습니다. 구성된 통화 전환 보류 번호는 클러스터 전체에 존재합니다. 직접 통화 지정보류 통화 상태 감시(BLF)를 지원하는 전화기를 특정 직접 통화 지정보류 번호의 통화 중 또는 유휴 상태를 모니터링하도록 구성할 수 있습니다. 사용자는 BLF를 사용하여 통화 전환 보류 번호를 바로 호출할 수도 있습니다.

Unified Communications Manager는 각 통화 전환 보류 번호에서 하나의 통화만 보류할 수 있습니다. 지정보류된 통화를 검색하려면 사용자는 구성된 검색 접두사 다음에 통화가 지정보류된 통화 전환 보류 번호를 사용하여 전화를 걸어야 합니다.

통화 전환 보류 사전 요건

구축의 전화기가 통화 전환 보류를 지원하는지 확인합니다. 지원되는 전화기 목록을 보려면 Cisco 통합 보고에서 전화기 기능 목록 보고서를 실행하고 기능으로 지원되는 통화 전환 보류를 선택합니다. 자세한 내용은 [전화기 기능 목록 생성, 7 페이지](#)를 참조하십시오.

통화 전환 보류 구성 작업 흐름

시작하기 전에

- [통화 전환 보류 사전 요건, 429 페이지](#) 검토

프로시저

	명령 또는 동작	목적
단계 1	클러스터 수준 통화 전환 보류 구성, 429 페이지	통화 전환 보류에 대한 클러스터 수준 매개 변수를 구성합니다.
단계 2	통화 전환 보류 번호 구성, 430 페이지	통화 전환 보류 내선 번호 하나 또는 다양한 내선 번호를 추가, 복사 및 업데이트합니다.
단계 3	BLF/통화 전환 보류 버튼 구성, 431 페이지	BLF/통화 전환 보류에 대한 전화기 버튼 템플릿을 구성합니다.
단계 4	영향을 받는 디바이스와 통화 전환 보류 동기화, 433 페이지	영향을 받는 디바이스와 통화 전환 보류 동기화

클러스터 수준 통화 전환 보류 구성

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 타이머를 설정하려면 클러스터 수준 매개 변수(기능 - 일반) 섹션에서 통화 지정보류 복귀 타이머 필드를 업데이트합니다.

기본값은 60초입니다. 이 매개 변수는 통화가 지정보류 상태를 유지하는 시간을 결정합니다. 타이머가 만료되면 통화 전환 보류 구성 창에서 구성하는 설정에 따라 지정보류된 통화가 통화를 지정보류한 디바이스나 지정된 다른 번호로 반환됩니다.

통화 전환 보류 번호 구성

시작하기 전에

각 통화 전환 보류 디렉터리 번호, 파티션 및 범위가 Unified Communications Manager 내에서 고유한지 확인하십시오. 시작하기 전에 라우트 계획 보고서를 생성합니다. [지정보류] 소프트키도 활성화할 경우(권장되지 않음), 통화 지정보류 번호와 통화 전환 보류 번호 사이에 중첩이 존재하지 않는지 확인하십시오. 복귀 번호가 구성되지 않은 경우, 해당 통화는 통화 지정보류 복귀 타이머가 만료된 후 지정보류자(지정보류 당사자)에게 복귀됩니다.

[클러스터 수준 통화 전환 보류 구성, 429 페이지](#)

프로시저

단계 1 통화 라우팅 > 통화 전환 보류를 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 통화 전환 보류 번호를 새로 추가하려면 새로 추가를 클릭합니다.
- 통화 전환 보류 번호를 복사하려면, 해당 통화 전환 보류 번호 또는 여러 개의 번호를 찾은 다음 복사 아이콘을 클릭합니다.
- 통화 전환 보류 번호를 업데이트하려면 통화 전환 보류 번호나 번호 범위를 찾습니다.

통화 전환 보류 번호 구성 창이 표시됩니다.

단계 3 통화 전환 보류 설정 영역에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [통화 전환 보류 구성 설정, 431 페이지](#)를 참조하십시오.

단계 4 새로 추가하거나 변경한 통화 지정보류 번호를 데이터베이스에 저장하려면 저장을 클릭합니다.

통화 전환 보류 번호를 업데이트하는 경우 Unified Communications Manager는 해당 번호에 대해 지정 보류된 통화를 통화 대기 복귀 타이머가 만료된 후에만 복귀시킵니다.

단계 5 구성 적용을 클릭합니다.

구성 정보 적용 대화 상자가 표시됩니다.

단계 6 **OK(확인)**를 클릭합니다.

단계 7 BLF를 사용하여 통화 전환 보류 번호를 모니터링하는 경우 통화 전환 보류 구성 창에서 디바이스 다시 시작을 클릭합니다. 이 단계는 변경 알림을 사용하는 경우 선택 사항입니다.

통화 전환 보류 구성 설정

필드	설명
번호	통화 전환 보류 번호를 입력합니다. 숫자(0-9) 또는 와일드카드 문자([, -, *, ^, #) 및 X(1개 또는 2개의 X가 허용됨)를 입력할 수 있습니다. 예를 들어, 5555의 단일 통화 지정보류 번호를 정의하려면 5555를 입력하고 5500부터 5599까지 통화 전환 보류 내선 번호 범위를 정의하려면 55XX를 입력합니다. 통화 전환 보류 번호는 고유하고 통화 지정보류 번호와 중첩되지 않아야 합니다.
설명	통화 전환 보류 번호 또는 범위에 대해 간략히 설명합니다. 설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&) 또는 꺾쇠괄호(<>)와 탭은 사용할 수 없습니다.
파티션	직접 통화 지정보류 번호에 대한 액세스를 제한하기 위해 파티션을 사용하려는 경우 드롭다운 목록에서 원하는 파티션을 선택합니다. 통화 전환 보류 번호에 대한 액세스를 제한하지 않으려면 파티션을 기본값 <None>으로 유지합니다. 참고 통화 지정보류 번호와 파티션과의 조합이 Unified Communications Manager 내에서 고유한지 확인하십시오.
복귀 번호	지정보류된 통화를 가져올 수 없을 경우 복귀할 번호를 입력하거나 필드를 비워둡니다. 참고 복귀 번호는 숫자만 포함할 수 있으며 와일드카드를 사용할 수 없습니다.
복귀 발신 검색 공간	드롭다운 목록을 사용하여 발신 검색 공간을 선택하거나 발신 검색 공간을 기본값 <None>으로 유지합니다.
검색 접두사	이 필수 필드에는 지정보류된 통화를 가져오기 위한 접두사를 입력합니다. 시스템은 지정보류된 통화를 가져오려는 시도와 직접 지정보류를 시작하려는 시도를 구분하기 위해 검색 접두사가 필요합니다.

BLF/통화 전환 보류 버튼 구성

시작하기 전에

[클러스터 수준 통화 전환 보류 구성, 429 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.

단계 2 구성 창이 표시되면 연결 정보 창에서 새 **BLF** 직접 통화 지정보류 추가 링크를 클릭합니다.

참고 전화기 또는 디바이스 프로파일에 적용한 전화기 버튼 템플릿에서 [BLF/통화 전환 보류]를 지원하지 않는 경우에는 [연결 정보] 창에 해당 링크가 표시되지 않습니다.

단계 3 BLF/통화 지정 보류 필드 영역에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [BLF/통화 전환 보류 구성 필드, 432 페이지](#)를 참조하십시오.

단계 4 구성을 완료한 후에 저장을 클릭하고 창을 닫습니다.

전화기 구성 창의 연결 정보 창에 디렉터리 번호가 표시됩니다.

BLF/통화 전환 보류 구성 필드

표 31: BLF/통화 전환 보류 버튼 구성 필드

필드	설명
디렉터리 번호	디렉터리 번호 드롭다운 목록에는 Unified Communications Manager 데이터 베이스에 있는 통화 전환 보류 번호 목록이 표시됩니다. SCCP를 실행하는 전화기 또는 SIP를 실행하는 전화기의 경우 사용자가 [바로 호출] 버튼을 누를 때 전화를 걸 번호(및 표시되는 경우 해당 파티션)를 선택합니다(예: 6002 in 3). 특정 파티션 없이 표시되는 디렉터리 번호는 기본 파티션에 속합니다.
레이블	[BLF/통화 전환 보류] 버튼에 표시할 텍스트를 입력합니다. 이 필드는 국제화를 지원합니다. 전화기에서 국제화를 지원하지 않는 경우 시스템은 [레이블 ASCII] 필드에 표시되는 텍스트를 사용합니다.
레이블 ASCII	[BLF/통화 전환 보류] 버튼에 표시할 텍스트를 입력합니다. ASCII 레이블은 사용자가 [레이블] 필드에 입력하는 국제화되지 않은 텍스트 버전을 나타냅니다. 전화기가 국제화를 지원하지 않는 경우, 시스템은 이 필드에 표시되는 텍스트를 사용합니다. 참고 [레이블 ASCII] 필드에 [레이블] 필드의 텍스트와는 다른 텍스트를 입력하면 Cisco 통합 커뮤니케이션 매니저 관리는 두 텍스트가 서로 다르더라도 양쪽 필드에 대한 구성을 모두 허용합니다.

영향을 받는 디바이스와 통화 전환 보류 동기화

프로시저

단계 1 통화 라우팅 > 통화 전환 보류를 선택합니다.

직접 통화 지정보류 찾기 및 나열 창이 표시됩니다.

단계 2 사용할 검색 조건을 선택합니다.

단계 3 찾기를 클릭합니다.

창에 검색 조건과 일치하는 통화 전환 보류의 목록이 표시됩니다.

단계 4 적용 가능한 디바이스를 동기화할 통화 전환 보류를 클릭합니다. 직접 통화 지정보류 구성 창이 표시됩니다.

단계 5 구성을 추가로 변경합니다.

단계 6 저장을 클릭합니다.

단계 7 구성 적용을 클릭합니다.

구성 정보 적용 대화 상자가 표시됩니다.

단계 8 **OK**(확인)를 클릭합니다.

통화 전환 보류 상호 작용

다음 표에서는 직접 통화 지정 보류 기능과 기능 상호 작용에 대해 설명합니다.

기능	상호 작용
대기 중 음악	<p>직접 통화 지정 보류에 대한 대기 중 음악 오디오 소스는 기본 네트워크 보류 MOH 오디오 소스 서비스 매개 변수를 통해 할당됩니다. 매개 변수를 할당하려면:</p> <ol style="list-style-type: none"> 1. Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다. 2. 서버 드롭다운 목록에서 Unified Communications Manager 클러스터 노드를 선택합니다. 3. 서비스 드롭다운 목록에서 Cisco CallManager를 선택합니다. 4. 클러스터 수준 매개 변수(서비스)에서 MOH 오디오 소스를 기본 네트워크 보류 MOH 오디오 소스 ID 매개 변수에 할당합니다. 기본값은 1입니다. 5. 저장을 클릭합니다. <p>참고 MOH 오디오 소스를 시스템에 추가하는 방법에 대한 자세한 내용은 이 설명서의 "대기 중 음악 구성" 섹션을 참조하십시오.</p>
발신 검색 공간 및 파티션	디바이스 발신 검색 공간에 따라 파티션에 직접 통화 지정보류 디렉터리 번호 또는 범위를 할당하여 사용자에게 대한 직접 통화 지정보류 액세스를 제한할 수 있습니다.
지정전환	통화 전환 보류에서는 음성전환([전환] 또는 [전환] 소프트키)을 지원합니다. 예를 들어 사용자 A가 사용자 B에게 전화를 걸고 사용자 B가 통화 지정을 보류합니다. 사용자 B가 통화를 검색하고 [전환] 또는 [전환] 소프트키를 눌러 통화를 음성 메시징 사서함으로 보낼지 결정합니다. 사용자 A가 사용자 B의 음성 메일 인사말을 받습니다.
참여	<ul style="list-style-type: none"> • 참여와 직접 통화 전환 보류 - 대상 전화기(참여 중인 전화기)가 통화를 제어합니다. 참여 이니시에이터는 대상 전화기에 “피기백”합니다. 대상이 참여되는 경우에도 대상 전화기에 일반 기능이 대부분 포함되므로 참여 개시자는 기능에 액세스할 수 없습니다. 대상이 통화 전환 보류를 사용하여 통화를 지정보류하는 경우 참여 개시자는 통화(참여)를 해제해야 합니다. • 회의끼기와 직접 통화 전환 보류-대상과 참여 이니시에이터는 피어 역할을 합니다. 회의끼기 기능은 컨퍼런스 브리지를 사용하므로 지금 미팅 전화회의와 유사하게 동작합니다. 두 전화기(대상 및 참여 개시자) 모두 기능에 대한 모든 권한을 가집니다.

기능	상호 작용
통화 지정보류	<p>통화 지정보류에 대해 [직접 통화 지정보류]와 [지정보류] 소프트 키를 둘 다 구성하지 않는 것이 좋지만, 둘 다 구성하는 것은 가능합니다. 둘 다 구성할 경우 통화 지정보류와 통화 전환 보류 번호가 중복되지 않도록 해야 합니다.</p> <p>통화 전환 보류 기능을 사용하여 지정보류된 발신자(피지정보류자)는 지정보류된 동안 표준 통화 지정보류 기능을 사용할 수 없습니다.</p>

통화 전환 보류 제한 사항

기능	제한 사항
통화 전환 보류 번호	<p>Unified Communications Manager 한 당사자는 각 통화 전환 보류 번호에서 하나의 통화만 보류할 수 있습니다.</p> <p>BLF 버튼을 사용하여 디바이스에서 모니터링하도록 구성된 통화 전환 보류 번호는 삭제할 수 없습니다. 통화 전환 보류 번호 또는 범위가 사용 중이어서 삭제할 수 없다는 메시지가 표시됩니다. 해당 번호를 사용 중인 디바이스를 파악하려면 통화 전환 보류 구성 창에서 종속성 레코드 링크를 클릭합니다.</p>
표준 통화 대기 기능	통화 전환 보류 기능을 사용하여 지정보류된 발신자(피지정보류자)는 지정보류된 동안 표준 통화 지정보류 기능을 사용할 수 없습니다.
통화 전환 보류 기능	전송 및 통화 전환 보류가 모두 실패할 수 있으므로 전송 및 통화 전환 보류 버튼을 동시에 누르지 않는 것이 좋습니다.
통화 전환 보류 BLF	통화 전환 보류 BLF는 여러 통화 전환 보류 번호를 모니터링할 수 없습니다. 사용자는 통화 전환 보류 BLF를 사용하여 개별 통화 전환 보류 번호를 모니터링할 수 있습니다. Extension Mobility
SIP를 실행하는 전화기에 대한 통화 전환 보류	<p>SIP를 실행하는 전화기에 대한 통화 전환 보류에는 다음 제한 사항이 적용됩니다.</p> <ul style="list-style-type: none"> 통화 전환 보류는 SIP를 실행하는 Cisco Unified IP Phone 7940 및 7960에서 호전환 소프트키를 사용하여 호출됩니다. SIP를 실행하는 Cisco Unified IP Phone 7940 및 7960에서 비공개 전환 소프트키가 사용되는 경우, 시스템은 통화 전환 보류를 지원하지 않습니다. SIP를 실행하는 Cisco Unified IP Phone 7940 및 7960과 SIP를 실행하는 타사 전화기에서 통화 전환 보류 BLF를 지원하지 않습니다.

통화 전환 보류 문제 해결

사용자가 통화 지정보류를 검색할 수 없음

사용자가 지정보류된 통화를 검색할 수 없습니다. 지정보류된 통화를 검색하기 위해 지정보류된 통화 번호를 다이얼한 후 사용자는 통화 중 신호음을 수신하고 IP 전화기에 "지정 보류 슬롯을 사용할 수 없음" 메시지가 표시됩니다.

사용자가 검색 접두사 다음에 직접 통화 지정 보류 번호를 입력했는지 확인합니다.

사용자가 통화 대기를 할 수 없음

사용자가 통화 대기를 할 수 없습니다. 전환 소프트키(또는 사용 가능한 경우 전환 버튼)를 누르고 통화 전환 보류 번호를 다이얼하면 통화가 전환 보류되지 않습니다.

통화 대기 번호에 할당된 파티션이 전화기 디렉터리 번호에 할당된 파티션과 일치하는지 확인합니다. 파티션 및 발신 검색 공간이 디바이스에 맞게 올바르게 구성되었는지 확인합니다. 파티션에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.

복귀 타이머가 만료된 후 사용자가 다시 걸기 신호음을 수신함

사용자가 통화 대기를 할 수 없습니다. 사용자는 복귀 타이머가 만료되면 다시 걸기 신호음을 수신합니다.

통화 전환 보류 번호로 전화를 걸기 전에 사용자가 전환 소프트키(또는 사용 가능한 경우 전환 버튼)를 누른 다음, 통화 전환 보류 번호로 전화를 건 후에는 전환 소프트키(또는 전환 버튼)를 다시 누르거나 온훅으로 전환합니다. 통화 전환 보류는 호 전환 기능이므로 통화 전환 보류 번호는 단독으로 전화를 걸 수 없습니다.



참고 온 훅 호 전환 활성화 서비스 매개 변수가 **True**로 설정된 경우 전환 소프트키(또는 전환 버튼)를 두 번 누르지 않고 온 훅으로 전환하는 것만으로 전환을 완료할 수 있습니다.

사용자가 다시 걸기 신호음 또는 알림 수신

사용자가 통화 대기를 할 수 없습니다. 전송 소프트키(또는 [사용 가능한 경우 호 전환] 버튼)를 누르고 직접 통화 지정 보류 번호로 전화를 걸면 사용자는 다시 걸기 신호음 또는 알림을 수신합니다.

다이얼한 번호가 직접 통화 지정 보류 번호로 구성되어 있는지 확인합니다.

사용자가 범위 내의 번호에서 통화를 지정보류할 수 없음

통화 전환 보류 번호의 범위를 구성한 후에는 사용자가 범위 내의 번호에서 통화를 지정 보류할 수 없습니다.

통화 전환 보류 번호의 범위를 입력하는 구문을 검토합니다. 잘못된 구문을 사용하는 경우 실제로는 그렇지 않은 범위를 시스템이 구성하는 것처럼 보일 수 있습니다.

통화 지정 보류가 너무 빠르게 복귀함

지정 보류된 통화가 너무 빨리 복귀됩니다.

통화 지정 보류 복귀 타이머를 더 긴 기간으로 설정합니다.

지정보류 슬롯 사용할 수 없음

사용자가 통화 대기를 할 수 없습니다. 전송 소프트키(또는 사용 가능한 경우 호 전환 버튼)를 누르고 직접 통화 지정 보류 번호로 전화를 걸면 사용자는 통화 중 신호음을 수신하고, IP 전화기에 "지정 보류 슬롯을 사용할 수 없음" 메시지가 표시됩니다.

다이얼한 직접 통화 지정 보류 번호가 지정 보류된 통화에서 이미 사용되고 있지 않은지 확인하거나 다른 직접 통화 지정 보류 번호로 통화를 지정 보류합니다.

통화 지정보류가 통화 지정보류 번호로 복귀되지 않음

지정 보류된 통화는 통화가 지정 보류한 번호로 복귀되지 않습니다.

직접 통화 지정 보류 번호의 구성을 확인하여 다른 디렉터리 번호가 아닌 통화를 지정 보류한 번호로 복귀하도록 구성되어 있는지 확인합니다.

번호 또는 범위가 사용 중 이므로 삭제할 수 없음

통화 전환 보류 번호 또는 범위를 삭제하려고 하면 사용 중이어서 해당 번호 또는 범위를 삭제할 수 없다는 메시지가 표시됩니다.

디바이스에서 모니터링하도록 구성된 통화 전환 보류 번호는 BLF 버튼을 사용하여 삭제할 수 없습니다. 번호를 사용 중인 디바이스를 확인하려면 [통화 전환 보류 구성] 창에서 [종속성 레코드] 링크를 클릭합니다.

번호 또는 범위가 사용 중 이므로 삭제할 수 없음



32 장

Extension Mobility

- Extension Mobility 개요, 439 페이지
- Extension Mobility 사전 요건, 439 페이지
- Extension Mobility 구성 작업 흐름, 440 페이지
- Cisco Extension Mobility 상호 작용, 449 페이지
- Cisco Extension Mobility 제한 사항, 451 페이지
- Extension Mobility 문제 해결, 452 페이지

Extension Mobility 개요

Cisco Extension Mobility를 사용하면 시스템 내에 있는 다른 전화기에서 회선 표시, 서비스 및 단축 다이얼과 같은 전화기 설정을 일시적으로 액세스할 수 있습니다. 예를 들어, 하나의 전화기를 여러 근로자가 사용할 경우 개별 사용자가 전화기에 로그인하고 다른 사용자 계정에 영향을 주지 않고 자신의 설정에 액세스할 수 있도록 Extension Mobility를 구성할 수 있습니다.

사용자가 Extension Mobility를 사용하여 로그인하고 Extension Mobility 프로파일이 이미 애플리케이션 사용자와 연결된 경우 CTI 애플리케이션에서 장치 관련 정보를 전송합니다.

CTI 애플리케이션에는 장치를 직접 제어하지 않고도 사용자가 로그인한 장치(Extension Mobility 프로파일 사용)를 제어할 수 있습니다. 따라서, 애플리케이션 사용자에게 대한 디바이스 프로파일 연결을 사용하는 녹음은 장치를 직접 연결하지 않은 경우에만 작동합니다.

Extension Mobility 사전 요건

- 연결할 수 있는 TFTP 서버.
- Extension Mobility 기능은 대부분의 Cisco Unified IP Phone에 제공됩니다. 전화기 설명서를 참조하여 Cisco Extension Mobility가 지원되는지 확인하십시오.

Extension Mobility 구성 작업 흐름

시작하기 전에

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	Extension Mobility 기능을 지원하는 디바이스를 식별하는 보고서를 생성합니다.
단계 2	Extension Mobility 서비스 활성화, 441 페이지	
단계 3	Cisco Extension Mobility 전화 서비스 구성, 441 페이지	사용자가 나중에 가입하여 내선 기능에 액세스할 수 있는 Extension Mobility IP 전화 서비스를 구성합니다.
단계 4	사용자에 대한 Extension Mobility 디바이스 프로파일 생성, 442 페이지	Extension Mobility 디바이스 프로파일을 구성합니다. 이 프로파일은 사용자가 Extension Mobility에 로그인할 때 실제 디바이스에 매핑하는 가상 디바이스의 역할을 합니다. 물리적 디바이스는 이 프로파일의 특성에 적용됩니다.
단계 5	사용자에 디바이스 프로파일 연결, 443 페이지	설정을 다른 전화기에서 액세스할 수 있도록 디바이스 프로파일을 사용자와 연결합니다. 실제 디바이스를 연결하는 것과 동일한 방법으로 사용자 디바이스 프로파일을 사용자와 연결합니다.
단계 6	Extension Mobility에 구독, 443 페이지	사용자가 Extension Mobility에 로그인하고, 로그아웃할 수 있도록 IP 전화기 및 디바이스 프로파일을 Extension Mobility 서비스에 가입합니다.
단계 7	인증서 변경 IP 전화 서비스 구성, 444 페이지	사용자가 전화기에서 PIN을 변경할 수 있도록 Cisco Unified IP Phone 서비스의 자격 증명 변경을 구성하고 사용자, 디바이스 프로파일 또는 IP 전화기를 전화 서비스 자격 증명 변경과 연결해야 합니다.
단계 8	(선택 사항) Extension Mobility에 대한 서비스 매개 변수 구성, 444 페이지	Extension Mobility의 동작을 수정하려면 서비스 매개 변수를 구성합니다.

Extension Mobility 서비스 활성화

프로시저

단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. 도구 > 서비스 활성화.

단계 2 서버 그룹다운 목록에서 필요한 노드를 선택합니다.

단계 3 다음과 같은 서비스를 활성화합니다.

- a) Cisco CallManager
- b) Cisco Tftp
- c) Cisco Extension Mobility
- d) ILS 서비스

참고 ILS 서비스를 활성화하려면 퍼블리셔 노드를 선택해야 합니다.

단계 4 저장을 클릭합니다.

단계 5 확인을 클릭합니다.

Cisco Extension Mobility 전화 서비스 구성

사용자가 나중에 가입하여 내선 기능에 액세스할 수 있는 Extension Mobility IP 전화 서비스를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화 서비스.

단계 2 새로 추가를 클릭합니다.

단계 3 서비스 이름 필드에 서비스의 이름을 입력합니다.

단계 4 서비스 URL 필드에 서비스 URL을 입력합니다.

형식은 `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#`입니다. IP 주소는 Cisco Extension Mobility가 활성화되어 실행되고 있는 Unified Communications Manager의 IP 주소입니다.

IPv4 또는 IPv6 주소일 수 있습니다.

예제:

`http://123.45.67.89:8080/emapp/EMAppServlet?device=#DEVICENAME#`

예제:

`http://[2001:0001:0001:0067:0000:0000:0000:0134]:8080/emapp/EMAppServlet?device=#DEVICENAME#`

이 형식은 사용자 ID 및 PIN을 사용하여 로그인하도록 허용합니다. Extension Mobility 서비스에 가입한 IP 전화 사용자의 경우 추가 로그인 옵션을 구성할 수 있습니다. 추가 로그인 옵션을 구성하려면 loginType 매개 변수를 서비스 URL에 다음 형식으로 추가합니다.

- loginType=DN을 사용하면 기본 내선 번호와 PIN을 사용하여 로그인할 수 있습니다.

서비스 URL 형식: http://<IP

Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=DN.

- loginType=SP를 사용하면 셀프 서비스 사용자 ID와 PIN을 사용하여 로그인할 수 있습니다.

서비스 URL 형식: http://<IP

Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=SP.

- loginType=UID를 사용하면 사용자 ID와 PIN을 사용하여 로그인할 수 있습니다.

서비스 URL 형식: http://<IP

Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=UID.

loginType을 URL의 끝에 추가하지 않는 경우 표시된 기본 로그인 옵션은 사용자 ID 및 PIN입니다.

단계 5 서비스 유형 필드에서 서비스를 [서비스], [디렉터리] 또는 [메시지] 버튼 중 어떤 항목으로 설정할지 선택합니다.

단계 6 저장을 클릭합니다.

사용자에 대한 **Extension Mobility** 디바이스 프로파일 생성

Extension Mobility 디바이스 프로파일을 구성합니다. 이 프로파일은 사용자가 Extension Mobility에 로그인할 때 실제 디바이스에 매핑하는 가상 디바이스의 역할을 합니다. 물리적 디바이스는 이 프로파일의 특성에 적용됩니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 디바이스 프로파일.

단계 2 다음 작업 중 하나를 수행합니다.

- 찾기 를 클릭하여 설정을 수정하고 결과 목록에서 기존 디바이스 프로파일을 선택합니다.
- 새 디바이스 프로파일을 추가하려면 새로 추가를 클릭하고 디바이스 프로파일 유형에서 옵션을 선택합니다. 다음을 클릭합니다.
- 디바이스 프로토콜 드롭다운 목록에서 디바이스 프로토콜을 선택하고 다음을 클릭합니다.

단계 3 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

단계 5 연결 정보 섹션에서 새 **DN** 추가를 클릭합니다.

단계 6 디렉터리 번호 필드에 디렉터리 번호를 입력하고 저장을 클릭합니다.

단계 7 재설정을 클릭하고 프롬프트에 따릅니다.

사용자에 디바이스 프로파일 연결

설정을 다른 전화기에서 액세스할 수 있도록 디바이스 프로파일을 사용자와 연결합니다. 실제 디바이스를 연결하는 것과 동일한 방법으로 사용자 디바이스 프로파일을 사용자와 연결합니다.



팁 BAT(벌크 관리 도구)를 사용하여 Cisco Extension Mobility의 사용자 디바이스 프로파일을 한 번에 여러 개 추가하거나 삭제할 수 있습니다. [Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서](#)를 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 사용자에 대한 설정을 수정하려면 찾기를 클릭하고 검색 기준을 입력한 후 결과 목록에서 기존 사용자를 선택합니다.
- 새로 추가를 클릭하여 새 사용자를 추가합니다.

단계 3 **Extension Mobility**에서 사용자가 만든 디바이스 프로파일을 찾아 사용 가능한 프로파일을 제어되는 프로파일로 이동합니다.

단계 4 홈 클러스터 확인란을 선택합니다.

단계 5 저장을 클릭합니다.

Extension Mobility에 구독

사용자가 Extension Mobility에 로그인하고, 로그아웃할 수 있도록 IP 전화기 및 디바이스 프로파일을 Extension Mobility 서비스에 가입합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 작업 중 하나를 수행합니다.

- 디바이스 > 전화기를 선택하고 검색 조건을 지정한 후 찾기를 클릭하고 Extension Mobility에 사용할 전화기를 선택합니다.
- 디바이스 > 디바이스 설정 > 디바이스 프로파일을 선택하고 검색 조건을 지정하고 찾기를 클릭하고 사용자가 만든 디바이스 프로파일을 선택합니다.

단계 2 관련 링크 드롭다운 목록에서 서비스 가입/가입 해지를 선택하고 이동을 클릭합니다.

단계 3 서비스 선택 드롭다운 목록 상자에서 **Extension Mobility** 서비스를 선택합니다.

단계 4 다음을 클릭합니다.

단계 5 가입을 클릭합니다.

단계 6 저장을 클릭하고 팝업 창을 닫습니다.

인증서 변경 IP 전화 서비스 구성

사용자가 전화기에서 PIN을 변경할 수 있도록 Cisco Unified IP Phone 서비스의 자격 증명 변경을 구성하고 사용자, 디바이스 프로파일 또는 IP 전화기를 전화 서비스 자격 증명 변경과 연결해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화 서비스.

단계 2 새로 추가를 클릭합니다.

단계 3 서비스 이름 필드에 인증서 변경을 입력합니다.

단계 4 서비스 **URL** 필드에 다음 값을 입력합니다. 여기서 **server**는 인증서 변경 IP 전화 서비스가 실행되는 서버를 나타냅니다.

`http://server:8080/changecredential/ChangeCredentialServlet?device=#DEVICENAME#`

단계 5 (선택 사항) 보안 서비스 **URL** 필드에 다음 값을 입력합니다. 여기서 **server**는 인증서 변경 IP 전화 서비스가 실행되는 서버입니다.

`https://server:8443/changecredential/ChangeCredentialServlet?device=#DEVICENAME#`

단계 6 **IP** 전화 서비스 구성 창에서 나머지 필드를 구성하고 저장을 선택합니다.

단계 7 Cisco Unified IP Phone을 인증서 변경 IP 전화 서비스에 가입하려면 디바이스 > 전화기를 선택합니다.

단계 8 전화기 구성 창에서 관련 링크 드롭다운 목록으로 이동하고 서비스 가입/가입 해지를 선택합니다.

단계 9 이동을 클릭합니다.

단계 10 서비스 선택 드롭다운 목록 상자에서 인증서 변경 **IP** 전화 서비스를 선택합니다.

단계 11 다음을 클릭합니다.

단계 12 가입을 클릭합니다.

단계 13 저장을 클릭합니다.

Extension Mobility에 대한 서비스 매개 변수 구성

(선택사항)

Extension Mobility의 동작을 수정하려면 서비스 매개 변수를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 필드에서 Cisco Extension Mobility 서비스를 실행하는 노드를 선택합니다.

단계 3 서비스 필드에서 **Cisco Extension Mobility**를 선택합니다.

단계 4 고급을 클릭하여 모든 서비스 매개 변수를 표시합니다.

이러한 서비스 매개 변수 및 해당 구성 옵션에 대한 자세한 내용은 [Extension Mobility 서비스 매개 변수, 445 페이지](#)를 참조하십시오.

단계 5 저장을 클릭합니다.

Extension Mobility 서비스 매개 변수

표 32: Extension Mobility 서비스 매개 변수

서비스 매개 변수	설명
클러스터 내 최대 로그인 시간 적용	<p>로컬 로그인에 대한 최대 시간을 지정하려면 True를 선택합니다. 이 시간이 지나면 시스템이 디바이스를 자동으로 로그아웃합니다. 기본값인 False를 선택하면 최대 로그인 시간이 없습니다.</p> <p>자동 로그아웃을 설정하려면 클러스터 내 최대 로그인 시간 서비스 매개 변수를 True로 선택하고, 이 서비스 매개 변수에도 시스템 최대 로그인 시간을 지정해야 합니다. 그러면 Cisco Unified Communications Manager에서 모든 로그인에 자동 로그아웃 서비스를 사용합니다.</p> <p>클러스터 내 최대 로그인 시간 적용 값이 False로 설정되고 클러스터 내 최대 로그인 시간 서비스 매개 변수에 유효한 최대 로그인 시간을 지정하는 경우 클러스터 내 최대 로그인 시간 적용 값이 자동으로 True로 변경됩니다.</p>

서비스 매개 변수	설명
클러스터 내 최대 로그인 시간	<p>이 매개 변수는 사용자가 디바이스에 로컬로 로그인할 수 있는 최대 시간 (예: 8:00(8시간) 또는 :30(30분))을 설정합니다.</p> <p>클러스터 내 최대 로그인 시간 적용 매개 변수가 False로 설정되어 있으면 시스템은 이 매개 변수를 무시하고 최대 로그인 시간을 0:00으로 설정합니다.</p> <p>올바른 값은 HHH:MM 형식의 0:00~168:00 사이의 값입니다. 여기서 HHH는 시간을 나타내고 MM은 분을 나타냅니다.</p> <p>참고 사용자 프로파일 구성의 최종 사용자가 내선 이동을 최대 로그인 시간을 설정하도록 허용 확인란을 통해 구성된 Extension Mobility 최대 로그인 시간을 설정하도록 사용자에게 액세스 권한을 부여하는 경우 셀프 서비스 포털의 사용자 구성이 클러스터 내 최대 로그인 시간 서비스 매개 변수의 값보다 우선합니다.</p>
최대 동시 요청 수	<p>동시에 발생할 수 있는 최대 로그인 또는 로그아웃 작업 수를 지정합니다. 이 숫자는 Cisco Extension Mobility 서비스에서 시스템 리소스를 과도하게 사용하지 않도록 합니다. 대부분의 경우 기본값 5가 적합합니다.</p>
멀티 로그인 동작	<p>하나의 전화기에 로그인한 다음 동일한 클러스터 또는 다른 클러스터에서 두 번째 전화기에 로그인하면 사용자는 서비스 매개 변수 구성 페이지에 정의된 다중 로그인 동작 설정을 기반으로 두 번째 전화기에서 로그인 동작을 볼 수 있습니다.</p> <p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 멀티 로그인 허용—동시에 두 개 이상의 디바이스에 로그인할 수 있습니다. • 멀티 로그인 허용 안 함—하나의 디바이스에만 로그인할 수 있습니다. 두 번째 디바이스에 대한 로그인 시도는 실패하고 전화기에 오류 코드 “25”(멀티 로그인 허용 안 함)가 표시됩니다. 첫 번째 디바이스에서 로그아웃한 경우에만 성공적으로 로그인할 수 있습니다. 이는 기본값입니다. • 자동 로그 아웃—두 번째 디바이스에 로그인하려고 하면(Extension Mobility 또는 클러스터 간 Extension Mobility), Cisco Unified Communications Manager가 첫 번째 디바이스에서 자동으로 로그아웃됩니다. <p>이것은 필수 필드입니다.</p> <p>참고 멀티 로그인 동작은 두 클러스터 간 Extension Mobility 로그인 간에도 적용됩니다.</p>

서비스 매개 변수	설명
영숫자 사용자 ID	<p>사용자 ID에 영숫자 문자가 포함되도록하려면 True를 선택합니다. 사용자 ID에 숫자만 포함되도록하려면 False를 선택합니다.</p> <p>참고 영숫자 사용자 ID 매개 변수는 시스템 전체에 적용됩니다. 영숫자 및 숫자 사용자 ID를 혼합하여 사용할 수 있습니다. 영숫자 키패드를 사용하여 입력할 수 있는 사용자 ID만 지원됩니다. 대소문자 구분 사용자 ID 필드에는 문자를 소문자로 입력해야 합니다.</p>
마지막으로 로그인한 사용자 기억	<p>False를 선택하면 시스템은 전화기에 로그인한 마지막 사용자를 기억하지 않습니다. 사용자가 전화기에 일시적으로 액세스하는 경우에만 이 옵션을 사용합니다. 전화기에 로그인한 마지막 사용자를 기억하도록하려면 True를 선택합니다. 전화기에 한 사용자만 있을 때 이 옵션을 사용합니다.</p> <p>예를 들면, Cisco Extension Mobility를 사용하여 전화기에 허용된 통화 유형을 활성화합니다. 로그인하지 않고 사무실 전화를 사용하고 있는 개인은 내부 또는 비상 전화만 걸 수 있습니다. 그러나 Cisco Extension Mobility를 사용하여 로그인하면 로컬, 장거리 및 국제 전화도 걸 수 있습니다. 이 시나리오에서는 이 사용자만 해당 전화기에 정기적으로 로그인합니다. Cisco Extension Mobility에서 로그인한 마지막 사용자 ID를 기억하도록 하는 것이 좋습니다.</p>
클러스터 내 EM의 통화 로그 지우기	<p>Cisco Extension Mobility 수동 로그인 및 로그아웃 프로세스 중 통화 로그를 지우도록 지정하려면 True를 선택합니다.</p> <p>사용자가 IP 전화기에서 Cisco Extension Mobility 서비스를 사용하는 동안에는 모든 통화(발신, 수신 또는 부재 중)가 통화 로그에 표시되며, IP 전화기 디스플레이에서 검색 및 확인할 수 있습니다. 프라이버시를 보장하려면, 통화 로그 지우기 서비스 매개 변수를 True로 설정합니다. 그러면 사용자가 로그아웃하고 다른 사용자가 로그인하면 통화 로그가 지워집니다.</p> <p>EMCC(클러스터 간 Extension Mobility)의 경우 사용자가 전화기에서 로그인하거나 로그아웃하면 통화 로그가 항상 지워집니다.</p> <p>참고 수동 로그인/로그아웃하는 동안에만 통화 로그가 지워집니다. Cisco Extension Mobility가 자동 로그아웃 또는 수동 로그아웃이 아닌 다른 작업으로 인해 로그아웃되면 통화 로그가 지워지지 않습니다.</p>

서비스 매개 변수	설명
IP 주소 확인	<p>이 매개 변수는 로그인 또는 로그아웃을 요청하고있는 소스의 IP 주소를 확인할지 여부를 설정합니다.</p> <p>매개 변수를 True로 지정하면 Cisco Extension Mobility 로그인 또는 로그아웃을 요청하는 IP 주소를 확인하여 신뢰할 수 있는지 확인합니다.</p> <p>먼저 로그인 또는 로그아웃할 디바이스의 캐시를 확인합니다.</p> <p>IP 주소가 캐시 또는 신뢰할 수 있는 IP 주소 목록에 있거나 등록된 디바이스인 경우 디바이스에 로그인하거나 로그아웃할 수 있습니다. IP 주소가 없으면 로그인 또는 로그아웃이 차단됩니다.</p> <p>매개 변수를 False로 설정하면 Cisco Extension Mobility 로그인 또는 로그아웃 요청을 확인하지 않습니다.</p> <p>IP 주소 확인은 디바이스를 로그인 또는 로그아웃하는 데 필요한 시간에 영향을 줄 수 있지만 무단 로그인 또는 로그아웃 시도를 방지하는 추가 보안을 제공합니다. 특히 원격 디바이스의 경우 별도의 신뢰할 수 있는 프록시 서버에서 로그인하는 기능과 함께 이 기능을 사용하는 것이 좋습니다.</p>
신뢰할 수 있는 IP 목록	<p>이 매개 변수는 텍스트 상자(최대 길이: 1024자)로 표시됩니다. 텍스트 상자에 신뢰할 수 있는 IP 주소 또는 호스트 이름 문자열을 세미콜론으로 구분하여 입력하면 됩니다. IP 주소 범위 및 정규식은 지원되지 않습니다.</p>
프록시 허용	<p>이 매개 변수가 True이면 웹 프록시를 사용하여 Cisco Extension Mobility 로그인 및 로그아웃 작업을 수행할 수 있습니다.</p> <p>이 매개 변수가 False이면 프록시를 통해 들어오는 Cisco Extension Mobility 로그인 및 로그아웃 요청을 거부합니다.</p> <p>선택하는 설정은 IP 주소 확인 매개 변수를 true로 지정하는 경우에만 적용됩니다.</p>
Extension Mobility 캐시 크기	<p>이 필드에서는 Cisco Extension Mobility가 유지 관리하는 디바이스의 캐시 크기를 입력합니다. 이 필드의 최소값은 1000이고 최대값은 20000입니다. 기본값은 10000입니다.</p> <p>입력하는 값은 IP 주소 확인 매개 변수가 True인 경우에만 적용됩니다.</p>

Cisco Extension Mobility 상호 작용

표 33: Cisco Extension Mobility 상호 작용

기능	상호 작용
보조자	Cisco Extension Mobility를 사용하는 관리자는 Cisco Unified Communications Manager Assistant도 사용할 수 있습니다. 관리자가 Cisco Extension Mobility를 사용하여 Cisco Unified IP Phone에 로그인한 다음 Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스를 선택합니다. Cisco IP 매니저 어시스턴트 (Cisco IPMA) 서비스가 시작되면 관리자는 Assistant 및 모든 Cisco Unified Communications Manager Assistant 기능(예: 통화 필터링 및 방해사절)에 액세스할 수 있습니다.
BLF 프리젠프스	<p>사용자 디바이스 프로파일에서 [BLF/단축 다이얼] 버튼을 구성하면 Cisco Extension Mobility를 지원하는 전화기에 로그인한 후 [BLF/단축 다이얼] 버튼에 BLF 프리젠프스 상태가 표시될 수 있습니다.</p> <p>Extension Mobility 사용자가 로그아웃하면 Cisco Extension Mobility를 지원하는 전화기의 [BLF/단축 다이얼] 버튼에는 구성된 로그아웃 프로파일에 대한 BLF 프리젠프스 상태가 표시됩니다.</p>
통화 표시 제한	<p>통화 표시 제한 기능을 활성화하면 Cisco Extension Mobility가 정상적으로 작동합니다. 통화 정보의 표시 또는 제한은 사용자가 디바이스에 로그인하면 해당 사용자와 연결된 사용자 디바이스 프로파일에 따라 다릅니다. 사용자가 로그아웃할 경우에는 전화기 구성 창에서 해당 전화기 유형에 정의된 구성에 따라 통화 정보가 표시 또는 제한됩니다.</p> <p>Cisco Extension Mobility에서 통화 표시 제한을 사용하려면 디바이스 프로파일 구성 창 및 전화기 구성 창에서 발신자 표시기 무시(내부 통화만 해당) 확인란을 선택합니다.</p>
모두 착신 전환 발신 검색 공간	<p>모두 착신 전환 발신 검색 공간(CSS)의 향상된 기능을 사용하면 기능 손실 없이 이후 릴리스의 Cisco Unified Communications Manager로 업그레이드할 수 있습니다.</p> <p>CFA CSS 활성화 정책서비스 매개 변수는 이 향상된 기능을 지원합니다. 서비스 매개 변수 구성 창에서 이 매개 변수는 클러스터 수준 매개 변수(기능 - 착신 전환) 섹션에 두 가지 옵션과 함께 표시됩니다.</p> <ul style="list-style-type: none"> • 구성된 CSS 사용(기본값) • 디바이스/회선 CSS 활성화

기능	상호 작용
DND(Do Not Disturb)	<p>Extension Mobility의 경우 디바이스 프로파일 설정에 방해 사절(DND) 수신 통화 경고 및 DND 상태가 포함됩니다. 사용자가 로그인하고 DND를 활성화하는 경우 DND 수신 통화 경고 및 DND 상태 설정이 저장되며 이러한 설정은 사용자가 다시 로그인할 때 사용됩니다.</p> <p>참고 Extension Mobility에 로그인된 사용자가 DND 수신 통화 경고나 DND 상태 설정을 수정하는 경우 이 작업은 실제 디바이스 설정에는 적용되지 않습니다.</p>
인터콤	<p>Cisco Extension Mobility는 인터콤 기능을 지원합니다. 인터콤 기능을 지원하기 위해 Cisco Extension Mobility는 인터콤 회선에 대해 구성된 기본 디바이스를 사용합니다. 인터콤 회선은 기본 디바이스에서만 표시됩니다.</p> <p>인터콤 회선을 디바이스 프로파일에 할당할 수 있습니다. 사용자가 기본 디바이스가 아닌 디바이스에 로그인하면 인터콤 회선이 표시되지 않습니다.</p> <p>다음 추가 고려 사항은 Cisco Extension Mobility의 인터콤에 적용됩니다.</p> <ul style="list-style-type: none"> • Unified Communications Manager가 인터콤 회선을 디바이스에 할당하고 기본 디바이스 값이 비어 있으면 현재 디바이스가 기본 디바이스로 선택됩니다. • AXL이 인터콤 DN을 프로그래밍 방식으로 할당하면 개별적으로 Cisco Unified Communications Manager 관리를 사용하여 인터콤 DN을 개별적으로 업데이트하여 기본 디바이스를 설정해야 합니다. • 인터콤 회선에 대해 인터콤 기본 디바이스로 설정된 디바이스를 삭제하면 인터콤 기본 디바이스는 더 이상 삭제된 디바이스로 설정되지 않습니다.
IPv6(Internet Protocol Version 6)	<p>Cisco Extension Mobility는 IPv6를 지원합니다. IP 주소 지정 모드가 IPv6 또는 듀얼 스택(IPv4 및 IPv6)인 전화기를 사용할 수 있습니다.</p>
기본 회선	<p>디바이스 프로파일 또는 기본 디바이스 프로파일 구성 창에서 항상 기본 회선 사용 매개 변수에 대해 켜기를 선택하는 경우 Cisco Extension Mobility 사용자는 Cisco Extension Mobility를 지원하는 디바이스에 로그인한 후에 이 기능을 사용할 수 있습니다.</p>

Cisco Extension Mobility 제한 사항

표 34: Cisco Extension Mobility 제한 사항

기능	제한 사항
캐시	Cisco Extension Mobility는 모든 로그인 사용자 정보에 대한 캐시를 2분 동안 유지합니다. 캐시에 있는 사용자에게 관련 Extension Mobility 요청이 들어올 경우, 해당 사용자는 캐시의 정보로 검증됩니다. 예를 들어, 사용자가 암호를 변경하고 로그아웃한 후 2분 내에 다시 로그인할 경우, 기존 암호와 새 암호가 모두 인식됩니다.
콜백	Cisco Extension Mobility 사용자가 디바이스에서 로그아웃하면, 해당 Cisco Extension Mobility 사용자에게 대해 활성 상태인 모든 콜백 서비스가 자동으로 취소됩니다.
문자 디스플레이	사용자가 로그인했을 때 표시되는 문자는 전화기의 현재 로캘에 따라 달라집니다. 예를 들어, 전화기가 현재 영어 로캘에 있을 경우(전화기의 로그아웃 프로파일에 기반하여), 사용자는 UserID에 영어 문자만 입력할 수 있습니다.
보류 복귀	Cisco Extension Mobility는 보류 복귀 기능을 지원하지 않습니다.
IP 전화	Cisco Extension Mobility에 로그인하려면 실제 Cisco Unified IP Phone이 있어야 합니다. Cisco Extension Mobility로 구성된 사무실 전화기의 사용자는 해당 전화기에 원격으로 로그인할 수 없습니다.
로캘	사용자 또는 프로파일과 연결된 사용자 로캘이 해당 로캘 또는 디바이스와 동일하지 않을 경우, 성공적으로 로그인한 후, 전화기가 재시작되고 재설정됩니다. 이 동작은 전화기 구성 파일이 다시 빌드되기 때문에 발생합니다. 프로파일과 디바이스 간의 추가 모듈 불일치도 동일한 동작을 일으킬 수 있습니다.
로그아웃	Cisco Extension Mobility가 중단되거나 재시작될 경우, 이미 로그인한 사용자는 로그아웃 간격 만료 후 자동으로 로그아웃되지 않습니다. 이러한 전화기는 하루에 한 번만 사용자를 자동으로 로그아웃합니다. 전화기 또는 Cisco Unified CM 관리에서 수동으로 해당 사용자를 로그아웃시킬 수 있습니다.
보안 신호음	Cisco Extension Mobility 및 회선 간 참가 서비스는 보호된 전화기에서 비활성화됩니다.
사용자 그룹	사용자를 표준 EM 인증 프로시 켄한 사용자 그룹에 추가할 수 있지만, 해당 사용자는 프로시에 의해 인증될 권한을 얻지 못합니다.
마지막으로 로그인한 사용자 기억	서비스 매개 변수 마지막으로 로그인한 사용자 기억은 기본 Extension Mobility 서비스 URL 또는 loginType이 UID인 Extension Mobility 서비스 URL의 경우에만 적용됩니다.

Extension Mobility 문제 해결

Extension Mobility 문제 해결

프로시저

- Cisco Extension Mobility 추적 디렉터리를 구성하고 다음 단계를 수행하여 디버그 추적을 활성화합니다.
 - a) Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다.추적 > 추적 설정.
 - b) 서버 드롭다운 목록에서 서버를 선택합니다.
 - c) 구성된 서비스 드롭다운 목록에서 **Cisco Extension Mobility**를 선택합니다.
- Cisco Extension Mobility 서비스에 대해 올바른 URL을 입력했는지 확인합니다. URL은 대/소문자를 구분합니다.
- 모든 구성 절차가 완벽하고 올바르게 수행되었는지 확인합니다.
- Cisco Extension Mobility 사용자 인증에 문제가 발생하는 경우 사용자 페이지로 이동하여 PIN을 확인합니다.

인증 오류

문제 “오류 201 인증 오류”가 전화기에 표시됩니다.

해결 방법 사용자는 올바른 사용자 ID와 PIN이 입력되었는지 확인하고 시스템 관리자에게 사용자 ID 및 PIN이 올바른지 확인해야 합니다.

빈 사용자 ID 또는 PIN

문제 “오류 202 빈 사용자 ID 또는 PIN”이 전화기에 나타납니다.

해결 방법 올바른 사용자 ID 및 PIN을 입력합니다.

통화 중입니다. 다시 시도하십시오.

문제 “오류 26 통화 중. 다시 하십시오”가 전화기에 나타납니다.

해결 방법 동시 로그인 및 로그아웃 요청 수가 최대 동시 요청 서비스 매개 변수보다 큰지 확인합니다. 이 경우, 동시 요청 수를 줄입니다.



참고

동시 로그인 및 로그아웃 요청 수를 확인하려면 Cisco Unified Real-Time Monitoring Tool을 사용하여 Extension Mobility 개체의 진행 중인 요청 카운터를 봅니다. 자세한 내용은 다음 위치에서 Cisco Unified Real Time Monitoring Tool 관리 지침서를 참조하십시오. <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

데이터베이스 오류

문제 “오류 6 데이터베이스 오류”가 전화기에 표시됩니다.

해결 방법 많은 수의 요청이 있는지 여부를 확인합니다. 많은 수의 요청이 있는 경우 **Extension Mobility** 개체 카운터에서 진행 중인 요청 카운터가 높은 값을 표시합니다. 많은 수의 동시 요청으로 인해 요청이 거부되는 경우 조정된 요청도 높은 값을 표시합니다. 자세한 데이터베이스 로그를 수집합니다.

디바이스에 로그인할 수 없음

문제 “오류 22 디바이스에 로그인할 수 없음”이 전화기에 나타납니다.

해결 방법 전화기 구성 창에서 **Extension Mobility** 활성화 확인란을 선택했는지 확인합니다(디바이스 > 전화기).

빈 디바이스 이름

문제 “오류 207 빈 디바이스 이름”이 전화기에 나타납니다.

해결 방법 Cisco Extension Mobility에 대해 구성된 URL이 올바른지 확인합니다. 자세한 내용은 관련 항목 섹션을 참조하십시오.

관련 항목

[Cisco Extension Mobility 전화 서비스 구성](#), 441 페이지

EMService 연결 오류

문제 “오류 207 EMService 연결 오류”가 전화기에 나타납니다.

해결 방법 Cisco Unified에 Serviceability에서 도구 > 제어 센터 - 기능을 선택하여 Cisco Extension Mobility 서비스가 실행되고 있는지 확인합니다.

업그레이드 중 **Extension Mobility** 성능

문제 업그레이드 후 게시자 버전 전환 중 **Extension Mobility(EM)** 로그인 성능.

해결 방법 **Extension Mobility(EM)** 사용자가 통합 커뮤니케이션 관리자 게시자의 버전 전환 업그레이드 중에 로그인되어 있고 게시자가 비활성화된 경우에는 버전 전환 중에 EM 로그인 데이터가 손실되고 EM 프로파일이 로그아웃됩니다.



참고 EM 로그인 프로파일이 로그아웃된 경우 사용자가 다시 로그인하거나 버전 전환 후에 Unified Communications Manager가 활성화된 경우에만 로그인할 수 있습니다.

호스트를 찾을 수 없음

문제 “호스트를 찾을 수 없음” 오류 메시지가 전화기에 나타납니다.

해결 방법 Cisco Unified에 Serviceability에서 도구 > 제어 센터 - 네트워크 서비스를 선택하여 Cisco Tomcat 서비스가 실행되고 있는지 확인합니다.

HTTP 오류

문제 HTTP 오류 (503)가 전화기에 표시됩니다.

해결 방법

- 서비스 버튼을 누르면 이 오류가 발생하는 경우 Cisco Unified Serviceability에서 도구 > 제어 센터 - 네트워크 서비스를 선택하여 Cisco IP Phone Services 서비스가 실행 중인지 확인합니다.
- Extension Mobility 서비스를 선택하면 이 오류가 발생하는 경우 Cisco Unified Serviceability에서 도구 > 제어 센터 - 네트워크 서비스를 선택하여 Cisco Extension Mobility Application 서비스가 실행 중인지 확인합니다.

전화기 재설정

문제 사용자가 로그인 또는 로그아웃 하면 전화는 다시 시작하는 대신에 재설정합니다.

가능한 원인 로컬 변경이 재설정의 가능한 원인입니다.

해결 방법 추가 작업은 필요하지 않습니다. 로그인한 사용자 또는 프로파일과 연결된 사용자 로컬이 해당 로컬 또는 디바이스와 동일하지 않을 경우, 성공적으로 로그인한 후, 전화기가 재시작되고 재설정됩니다. 이 패턴은 전화기 구성 파일이 다시 빌드되기 때문에 발생합니다.

로그인한 후 전화 서비스를 사용할 수 없음

문제 로그인 후 사용자가 전화 서비스를 사용할 수 없습니다.

가능한 원인 이 문제는 사용자 프로파일이 전화기에 로드되었을 때 연결된 서비스가 없기 때문에 발생합니다.

해결 방법

- 사용자 프로파일에 Cisco Extension Mobility 서비스가 포함되어 있는지 확인하십시오.
- 사용자가 로그인하는 전화기의 구성을 Cisco Extension Mobility를 포함하도록 변경합니다. 전화를 업데이트한 후 사용자가 전화 서비스에 액세스할 수 있습니다.

로그아웃한 후 전화 서비스를 사용할 수 없음

문제 사용자가 로그아웃하고 전화기가 기본 디바이스 프로파일로 전환되면 전화 서비스를 더 이상 사용할 수 없게 됩니다.

해결 방법

- 자동 디바이스 프로파일과 전화기 구성 간에 동기화 엔터프라이즈 매개 변수가 **True**로 설정되었는지합니다.
- 전화기를 Cisco Extension Mobility 서비스에 가입합니다.

사용자가 다른 위치에서 로그인

문제 “오류 25 사용자가 다른 위치에서 로그인”이 전화기에 표시됩니다.

해결 방법 사용자가 다른 전화기로 로그인했는지 여부를 확인하십시오. 멀티 로그인을 허용해야 하는 경우 멀티 로그인 동작 서비스 매개 변수가 멀티 로그인 허용으로 설정되었는지 확인합니다.

사용자 프로파일 부재

문제 “오류 205 사용자 프로파일 부재”가 전화기에 나타납니다.

해결 방법 사용자에게 디바이스 프로파일을 연결합니다.



33 장

클러스터 간 **Extension Mobility**

- [Extension Mobility Cross Cluster 개요, 457 페이지](#)
- [클러스터 간 Extension Mobility 사전 요건, 457 페이지](#)
- [클러스터 간 Extension Mobility 구성 작업 흐름, 458 페이지](#)
- [클러스터 간 Extension Mobility 상호 작용, 481 페이지](#)
- [클러스터 간 Extension Mobility 제한, 482 페이지](#)
- [클러스터 간 Extension Mobility 문제 해결, 486 페이지](#)

Extension Mobility Cross Cluster 개요

EMCC(Extension Mobility Cross Cluster) 기능은 사용자에게 Extension Mobility와 동일한 기능을 제공하지만 한 클러스터(홈 클러스터)에서 이동하여 다른 원격 클러스터(방문 클러스터)의 임시 전화기에 로그인 할 수도 있습니다. 이곳에서 마치 본사에서 IP 전화기를 사용하는 것처럼 모든 위치에서 해당 전화 설정에 액세스할 수 있습니다.

클러스터 간 **Extension Mobility** 사전 요건

- EMCC(Extension Mobility Cross Cluster) 구성을 지원 및 사용하는 기타 통화 제어 엔티티(예: 기타 Cisco Unified Communications Manager 클러스터, EMCC 클러스터 간 서비스 프로파일 및 EMCC 원격 클러스터 서비스)
- 비보안 또는 혼합 모드로 설정된 클러스터입니다. 자세한 내용은 [다양한 클러스터 버전을 위한 익스텐션 모빌리티 크로스 클러스터\(EMCC\) 및 보안 모드, 484 페이지](#)를 참조하십시오.
- 보안 또는 비보안 모드에서 지원되는 전화기

클러스터 간 Extension Mobility 구성 작업 흐름

시작하기 전에

- 클러스터 간 Extension Mobility 사전 요건, 457 페이지 검토
- 클러스터 간 내선 이동 상호 작용 및 제한 사항을 검토합니다.

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	클러스터 간 Extension Mobility 기능을 지원하는 디바이스를 식별하는 보고서를 생성합니다.
단계 2	<p>Configure Extension Mobility, 459 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> • 클러스터 간 Extension Mobility를 위해 서비스 활성화, 460 페이지 • Extension Mobility 전화 서비스 구성, 460 페이지 • 클러스터 간 Extension Mobility를 위한 디바이스 프로파일 구성, 462 페이지 • 사용자에게 Extension Mobility 상호 클러스터 활성화, 469 페이지 • 디바이스를 Extension Mobility에 구독, 469 페이지 	Extension Mobility를 구성하면 한 클러스터에 있는 다른 전화기에서 회선 표시, 서비스 및 단축 다이얼과 같은 전화기 설정을 일시적으로 액세스할 수 있습니다. 홈 및 원격 클러스터 모두에서 이 작업 흐름을 수행하면 사용자가 홈 및 방문 클러스터에서 설정에 액세스할 수 있습니다.
단계 3	<p>클러스터 간 Extension Mobility에 대한 인증서 구성, 470 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> • Bulk Provisioning Service 활성화, 470 페이지 • 벌크 인증서 관리 구성 및 인증서 내보내기, 471 페이지 • 인증서 통합, 472 페이지 • 클러스터로 인증서 가져오기, 472 페이지 	홈 및 원격 클러스터를 적절하게 구성하려면 각 클러스터에서 인증서를 동일한 SFTP 서버 및 SFTP 디렉터리로 내보내고 참여 클러스터 중 하나에서 이를 통합해야 합니다. 이 절차는 두 클러스터 사이에 신뢰가 설정되어 있는지 확인합니다.
단계 4	<p>클러스터 간 Extension Mobility 디바이스 및 템플릿 구성, 473 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> • 일반 디바이스 구성 만들기, 474 페이지 	

	명령 또는 동작	목적
	<ul style="list-style-type: none"> 클러스터 간 Extension Mobility 템플릿 구성, 474 페이지 기본 템플릿 설정, 474 페이지 클러스터 간 Extension Mobility 디바이스 추가, 475 페이지 	
단계 5	클러스터 간 Extension Mobility를 위한 지오로케이션 필터 구성, 475 페이지	지오로케이션 필터를 구성하여 국가, 시/도 및 구/군/시 같이 일치하는 디바이스 위치에 대한 기준을 지정합니다. 지오로케이션은 디바이스의 위치를 식별하는 데 사용되고 필터는 지오로케이션의 어느 부분이 중요한지를 나타냅니다.
단계 6	클러스터 간 Extension Mobility에 대한 기능 매개 변수 구성, 476 페이지	지오로케이션 필터와 같이 사용자가 구성한 기능 매개 변수에 대한 값을 선택합니다.
단계 7	클러스터 간 Extension Mobility에 대한 클러스터 간 SIP 트렁크 구성, 479 페이지	클러스터 간 PSTN 액세스 및 RSVP 에이전트 서비스에 대한 착신 또는 발신 트래픽을 처리하도록 트렁크를 구성합니다. 두 PSTN 액세스 및 RSVP 에이전트 서비스에 대해 트렁크 하나를 구성하거나 각 서비스에 대해 트렁크를 하나씩 구성할 수 있습니다. 클러스터 간 Extension Mobility를 위해 SIP 트렁크가 두 개 이상 필요하지 않습니다.
단계 8	클러스터 간 Extension Mobility를 위한 클러스터 간 서비스 프로파일 구성, 480 페이지	클러스터 간 서비스 프로파일을 구성하여 클러스터 간 Extension Mobility를 활성화합니다. 프로파일은 이전의 모든 구성을 수집하고 결과 보고서를 제공합니다.
단계 9	원격 클러스터 서비스 구성, 480 페이지	클러스터 간 Extension Mobility에 대한 원격 클러스터를 구성합니다. 이 단계는 원격(방문) 클러스터와 홈 클러스터 간 연결을 완료합니다.

Configure Extension Mobility

Extension Mobility를 구성하면 한 클러스터에 있는 다른 전화기에서 회선 표시, 서비스 및 단축 다이얼과 같은 전화기 설정을 일시적으로 액세스할 수 있습니다. 홈 및 원격 클러스터 모두에서 이 작업 흐름을 수행하면 사용자가 홈 및 방문 클러스터에서 설정에 액세스할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	클러스터 간 Extension Mobility 를 위해 서비스 활성화, 460 페이지	
단계 2	Extension Mobility 전화 서비스 구성, 460 페이지	사용자가 가입할 수 있는 Extension Mobility 전화 서비스를 만듭니다.
단계 3	클러스터 간 Extension Mobility 를 위한 디바이스 프로파일 구성, 462 페이지	사용자가 익스텐션 모빌리티 크로스 클러스터 (EMCC)에 로그인할 때 실제 디바이스에 설정을 매핑하는 디바이스 프로파일을 만듭니다.
단계 4	사용자에 대해 Extension Mobility 상호 클러스터 활성화, 469 페이지	
단계 5	디바이스를 Extension Mobility 에 구독, 469 페이지	모든 디바이스에 대해 엔터프라이즈 가입을 설정하지 않은 경우 디바이스에서 Extension Mobility 를 활성화하고 서비스에 가입합니다.

클러스터 간 **Extension Mobility**를 위해 서비스 활성화

프로시저

단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. 도구 > 서비스 활성화.

단계 2 서버 드롭다운 목록에서 필요한 노드를 선택합니다.

단계 3 다음과 같은 서비스를 활성화합니다.

- a) Cisco CallManager
- b) Cisco Tftp
- c) Cisco Extension Mobility
- d) ILS 서비스

참고 ILS 서비스를 활성화하려면 퍼블리셔 노드를 선택해야 합니다.

단계 4 저장을 클릭합니다.

단계 5 확인을 클릭합니다.

Extension Mobility 전화 서비스 구성

사용자가 가입할 수 있는 **Extension Mobility** 전화 서비스를 만듭니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화 서비스.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 서비스 이름 필드에 서비스의 이름을 입력합니다.
- 예를 들어, Extension Mobility 또는 EM 같은 이름을 입력합니다. Java MIDlet 서비스의 서비스 이름은 JAD(Java Application Descriptor) 파일에 정의된 이름과 정확히 일치해야 합니다.
- 단계 4 서비스 URL 필드에 서비스 URL을 다음 형식으로 입력합니다.
- ```
http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#.
```
- 단계 5 (선택 사항) HTTPS를 사용하는 보안 URL을 만들려는 경우 보안 서비스 URL을 다음 형식으로 입력합니다.
- ```
https://<IP Address>:8443/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#
```
- 단계 6 (선택 사항) 추가 로그인 옵션을 구성하려면 loginType 매개 변수를 서비스 URL에 다음 형식으로 추가합니다.
- loginType=DN을 사용하면 사용자가 기본 내선 번호와 PIN을 사용하여 로그인할 수 있습니다. 서비스 URL 형식: `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#&loginType=DN`
 - loginType=SP를 사용하면 셀프 서비스 사용자 ID와 PIN을 사용하여 로그인할 수 있습니다. 서비스 URL 형식: `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#&loginType=SP.`
 - loginType=UID를 사용하면 사용자 ID와 PIN을 사용하여 로그인할 수 있습니다. 서비스 URL 형식: `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#&loginType=UID.`
- loginType 매개 변수를 보안 URL에 추가할 수도 있습니다. loginType을 URL의 끝에 추가하지 않는 경우 표시된 기본 로그인 옵션은 사용자 ID 및 PIN입니다.
- 단계 7 서비스 범주 및 서비스 유형 필드에 대해 기본값을 사용합니다.
- 단계 8 활성화 확인란을 체크합니다.
- 단계 9 (선택 사항) 엔터프라이즈 가입 확인란을 선택하여 이 전화 서비스에 모든 전화기 및 디바이스 프로파일을 가입합니다.
- 참고 서비스를 처음으로 구성할 때 이 확인란을 선택하는 경우 이 IP 전화 서비스를 엔터프라이즈 가입 서비스로 설정합니다. 엔터프라이즈의 모든 전화기 및 디바이스 프로파일은 이 IP 전화 서비스에 자동으로 가입되므로 개별적으로 가입할 필요가 없습니다.
- 단계 10 저장을 클릭합니다.

클러스터 간 **Extension Mobility**를 위한 디바이스 프로파일 구성

사용자가 익스텐션 모빌리티 크로스 클러스터 (EMCC)에 로그인할 때 실제 디바이스에 설정을 매핑하는 디바이스 프로파일을 만듭니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 디바이스 프로파일.

단계 2 다음 작업 중 하나를 수행합니다.

- 찾기를 클릭하여 기존 디바이스 프로파일을 수정하고 검색 기준을 입력합니다. 결과 목록에서 디바이스 프로파일 이름을 클릭합니다.
- 새 디바이스 프로파일을 추가하려면 새로 추가를 클릭하고 다음을 클릭하여 디바이스 프로파일 유형을 선택합니다. 다음을 클릭하여 프로토콜을 선택하고 다음을 클릭합니다.

단계 3 디바이스 프로파일 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [클러스터 간 Extension Mobility를 위한 디바이스 프로파일 필드, 462 페이지](#)를 참조하십시오.

단계 4 저장을 클릭합니다.

단계 5 새 디바이스 프로파일에 DN(디렉터리 번호)을 추가합니다.

클러스터 간 **Extension Mobility**를 위한 디바이스 프로파일 필드

표 35: 디바이스 프로파일 설정

필드	설명
제품 유형	이 디바이스 프로파일 적용되는 제품 유형을 표시합니다.
디바이스 프로토콜	이 디바이스 프로파일 적용되는 디바이스 프로토콜을 표시합니다.
디바이스 프로파일 이름	고유한 이름을 입력합니다. 이 이름은 최대 50자로 구성될 수 있습니다.
설명	디바이스 프로파일에 대한 설명을 입력합니다. 이 특정 사용자 디바이스 프로파일을 설명하는 모든 정보가 텍스트로 사용됩니다.
사용자 보류 MOH 오디오 소스	<p>사용자가 보류 작업을 시작할 때 재생되는 오디오 소스를 지정하고, [사용자 보류 MOH 오디오 소스] 드롭다운 목록에서 오디오 소스를 선택합니다.</p> <p>오디오 소스를 선택하지 않는 경우 Unified Communications Manager에서 디바이스폴에 정의되어 있는 오디오 소스를 사용하거나, 디바이스폴에 오디오 소스 ID가 지정되어 있지 않으면 시스템 기본값을 사용합니다.</p> <p>참고 [대기 중 음악 오디오 소스 구성] 창에서 오디오 소스를 정의합니다. 액세스하려면 미디어 리소스 > 대기 중 음악 오디오 소스를 선택합니다.</p>

필드	설명
사용자 로케일	<p>드롭다운 목록에서 전화기 사용자 인터페이스와 연결된 로케일을 선택합니다. 사용자 로케일은 언어 및 글꼴을 비롯하여 사용자를 지원하기 위한 일련의 세부 정보를 식별합니다.</p> <p>Unified Communications Manager 지역화를 지원하는 전화기 모델에만 이 필드를 사용할 수 있습니다.</p> <p>참고 사용자 로케일을 지정하지 않은 경우 Unified Communications Manager에서는 디바이스폴과 연결된 사용자 로케일을 사용합니다.</p> <p>사용자가 전화기에서 영어 외의 언어로 정보를 표시해야 하는 경우 사용자 로케일을 구성하기 전에 로케일 설치 관리자가 설치되어 있는지 확인합니다. Unified Communications Manager 로케일 설치 관리자 설명서를 참조하십시오.</p>
전화기 버튼 템플릿	<p>[전화기 버튼 템플릿] 드롭다운 목록표에서 전화기 버튼 템플릿을 선택합니다.</p> <p>팁 프레즌스 모니터링을 위해 프로필에 BLF/바로 호출을 구성하려면 BLF/바로 호출을 위해 구성된 전화기 버튼 템플릿을 선택합니다. 구성을 저장하면 [연결 정보] 창에 [새 BLF SD 추가] 링크가 표시됩니다. BLF/SpeedDials에 관한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서 항목을 참조하십시오.</p>
소프트키 템플릿	[소프트키 템플릿] 드롭다운 목록에서 목록에 있는 소프트키 템플릿을 선택합니다.
프라이버시	[프라이버시] 드롭다운 목록에서 프라이버시가 필요한 각 전화기에 대해 [켜기]를 선택합니다. 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서 를 참조하십시오.

필드	설명
참여 단일 버튼	<p>드롭다운 목록의 다음 옵션 중에서 선택합니다.</p> <ul style="list-style-type: none"> • 끄기 - 이 디바이스에서 사용자가 참여/회의끼기 단일 버튼 기능을 사용할 수 없습니다. • 참여 - 이 옵션을 선택하면 사용자가 전화기에서 [참여 단일 버튼] 공유 회선 버튼을 누르고 [참여]를 사용하여 통화에 참여할 수 있습니다. • 기본값 - 이 디바이스는 서비스 파라미터 및 디바이스풀 설정에서 [참여/회의끼기 단일 버튼] 설정을 상속합니다. <p>참고 서버 파라미터와 디바이스풀 설정이 다른 경우 디바이스는 서비스 파라미터 설정에서 설정을 상속받습니다.</p> <p>자세한 내용은 Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서를 참조하십시오.</p>
회선 간 통화 참가	<p>드롭다운 목록의 다음 옵션 중에서 선택합니다.</p> <ul style="list-style-type: none"> • 끄기 - 이 디바이스에서 사용자가 회선 간 통화 참가 기능을 사용할 수 없습니다. • 켜기 - 이 디바이스에서 사용자가 여러 회선 간 통화에 참가할 수 있습니다. • 기본값 - 이 디바이스는 서비스 파라미터 및 디바이스풀 설정에서 [회선 간 통화 참가] 설정을 상속합니다. <p>참고 서버 파라미터와 디바이스풀 설정이 다른 경우 디바이스는 서비스 파라미터 설정에서 설정을 상속받습니다.</p> <p>자세한 내용은 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서를 참조하십시오.</p>
항상 기본 회선 사용	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 끄기 - 전화기가 유휴 상태이고 한 회선에서 통화가 수신되는 경우 전화기 사용자는 통화가 수신된 회선에서 통화에 응답합니다. • 켜기 - 전화기가 유휴(오프 후) 상태이고 한 회선에서 통화가 수신되는 경우 통화를 위해 기본 회선이 선택됩니다. 다른 회선의 전화는 계속 울리므로 전화기 사용자가 해당 전화를 받으려면 다른 회선을 선택해야 합니다. • 기본값 - Unified Communications Manager에서 Cisco CallManager 서비스를 지원하는 항상 기본 회선 사용(Always Use Prime Line) 서비스 파라미터의 구성을 사용합니다.

필드	설명
음성 메시지에 항상 기본 회선 사용	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 켜기 - 전화기가 유휴 상태인 경우 전화기 사용자 전화기에서 [메시지] 버튼을 누르면 전화기의 기본 회선이 음성 메시지를 가져오기 위한 활성 회선이 됩니다. • 끄기 - 전화기가 유휴 상태인 경우 전화기에서 [메시지] 버튼을 누르면 자동으로 음성 메시지가 있는 회선에서 음성 메시징 시스템으로 전화가 걸립니다. Unified Communications Manager에서는 음성 메시지가 있는 첫 번째 라인을 항상 선택합니다. 음성 메시지가 있는 회선이 없는 경우 전화기 사용자가 [메시지] 버튼을 누르면 기본 회선이 사용됩니다. • 기본값 - Unified Communications Manager에서 Cisco CallManager 서비스를 지원하는 항상 기본 회선 사용(Always Use Prime Line) 서비스 파라미터의 구성을 사용합니다.
발신자 정보 표시기 무시(내부 통화만 해당)	<p>통화 표시 제한을 구성하고 내부 통화에 대해 수신된 모든 표시 제한을 무시하려면 “발신자 정보 표시기 무시(내부 통화만 해당)” 확인란을 선택합니다.</p> <p>팁 발신 회선 ID 표시 및 변환 패턴 수준에서 연결된 회선 ID 표시 구성과 결합하여 이 구성을 사용합니다. 또한 이러한 설정을 통해 각 통화에 대한 발신 및/또는 연결된 회선 형태(LA) 정보를 선택적으로 제공하거나 차단하도록 통화 표시 제한을 구성할 수 있습니다. 통화 표시 제한에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서 항목을 참조하십시오.</p>
DND(Do Not Disturb)	방해사절 기능을 활성화하려면 이 확인란을 선택합니다.

필드	설명
방해사절 옵션	<p>전화기에서 DND를 활성화할 때 다음과 같이 이 파라미터를 사용하여 DND 기능이 수신 통화를 처리하는 방법을 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 통화 거부 - 이 옵션은 사용자에게 수신 통화 정보를 표시하지 않도록 지정합니다. DND 수신 전화 알림(DND Incoming Call Alert) 파라미터를 구성하는 방법에 따라 전화기에서 경고음을 재생하거나 통화의 플래시 알림을 재생합니다. • 벨소리 꺼짐 - 이 옵션은 벨소리를 끄지만 디바이스에 수신 통화 정보가 표시되므로 사용자가 전화를 받을 수 있습니다. • 일반 전화 프로필 설정 사용 - 이 옵션은 이 디바이스에 [일반 전화 프로필] 창의 [DND 옵션] 설정이 사용되도록 지정합니다. <p>참고 SCCP를 실행하는 7940/7960 전화기의 경우 [벨소리 꺼짐] 옵션만 선택할 수 있습니다. 모바일 디바이스 및 듀얼 모드 전화기의 경우 [통화 거부] 옵션만 선택할 수 있습니다. 모바일 디바이스 또는 듀얼 모드 전화기에서 [DND 통화 거부]를 활성화하면, 디바이스에 아무런 통화 정보도 표시되지 않습니다.</p>
DND 수신 전화 경고	<p>이 파라미터는 [DND 벨소리 꺼짐] 또는 [통화 거부] 옵션을 활성화할 때 통화를 전화기에 표시하는 방법을 지정합니다.</p> <p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 없음 - 이 옵션은 [일반 전화 프로필] 창의 [DND 수신 통화 경고] 설정이 이 디바이스에 사용되도록 지정합니다. • 비활성화 - 이 옵션은 통화의 경고음과 플래시 알림을 비활성화하지만, [DND 벨소리 꺼짐] 옵션에 대해 수신 통화 정보가 계속 표시됩니다. [DND 통화 거부] 옵션의 경우 통화 경고가 표시되지 않고 디바이스에 정보가 전송되지 않습니다. • 경고음만 - 이 옵션을 설정하면 수신 통화에 대해 전화기에서 경고음만 재생합니다. • 깜박임만 - 이 옵션을 설정하면 수신 통화에 대해 전화기에서 플래시 경고를 표시합니다.

필드	설명
클러스터 간 Extension Mobility CSS	<p>클러스터 간 Extension Mobility 기능에 이 디바이스 프로필을 사용하려면 드롭다운 목록에서 기존 CSS(발신 검색 공간)를 선택합니다. (새 CSS를 구성하거나 기존 CSS를 수정하려면 Unified Communications Manager에서 통화 라우팅 > 제어 클래스 > 발신 검색 공간을 선택합니다.)</p> <p>기본값은 [없음]입니다.</p> <p>홈 관리자는 사용자가 해당 원격 전화기에 로그인할 때 이 CSS를 지정하는데, 이는 전화기에 할당되는 디바이스 CSS로 사용됩니다. 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서를 참조하십시오.</p>
모듈 1	<p>[확장 모듈] 필드의 [확장 모듈] 드롭다운 목록에서 전화 템플릿을 구성하여 이 디바이스 프로필에 하나 또는 두 개의 확장 모듈을 구성할 수 있습니다.</p> <p>참고 언제나 전화기 버튼 템플릿 필드 옆에 있는 [보기] 버튼 목록 링크를 선택하여 전화기 버튼 목록을 볼 수 있습니다. 별도의 대화 상자가 표시되고 해당하는 특정 확장 모듈의 전화기 버튼이 표시됩니다.</p> <p>해당 확장 모듈 또는 [없음]을 선택합니다.</p>
모듈 2	해당 확장 모듈 또는 [없음]을 선택합니다.
MLPP 도메인	<p>MLLP 우선 순위 통화에 이 사용자 디바이스 프로필이 사용될 경우 드롭다운 목록에서 [MLPP 도메인]을 선택합니다.</p> <p>참고 [MLPP 도메인 구성] 창에서 [MLPP 도메인]을 정의합니다. 액세스의 경우 시스템 > MLPP 도메인을 선택합니다.</p>

필드	설명
MLPP 표시	<p>MLPP 우선 순위 통화에 이 사용자 디바이스 프로파일 사용될 경우 디바이스 프로파일 MLPP 표시 설정을 할당합니다. 이 설정은 MLPP 우선 순위 통화를 거는 경우 우선 순위 신호음을 재생할 수 있는 디바이스에서 해당 기능을 사용할지 여부를 지정합니다.</p> <p>드롭다운 목록의 다음 옵션에서 이 디바이스 프로파일 할당할 설정을 선택합니다.</p> <ol style="list-style-type: none"> 1. 기본값 - 이 디바이스 프로파일은 연결된 디바이스의 디바이스폴에서 해당 MLPP 표시 설정을 상속합니다. 2. 끄기 - 이 디바이스에서 MLPP 우선 순위 통화 표시를 취급하거나 처리하지 않습니다. 3. 켜기 - 이 디바이스 프로파일에서 MLPP 우선 순위 통화 표시를 취급 및 처리합니다. <p>참고 [MLPP 선점]이 [강제]로 설정되어 있는 상태에서 [MLPP 표시]를 [끄기] 또는 [기본값](기본값이 [끄기]인 경우)으로 설정하는 설정 조합으로 디바이스 프로파일을 구성하지 마십시오.</p>
MLPP 선점	<p>MLPP 우선 순위 통화에 이 사용자 디바이스 프로파일 사용될 경우 디바이스 프로파일 MLPP 선점 설정을 할당합니다. 이 설정은 MLPP 우선 순위 전화를 거는 경우 진행 중인 통화를 선점할 수 있는 디바이스에서 해당 기능을 사용할지 여부를 지정합니다.</p> <p>드롭다운 목록의 다음 옵션에서 이 디바이스 프로파일 할당할 설정을 선택합니다.</p> <ol style="list-style-type: none"> 1. 기본값 - 이 디바이스 프로파일은 연결된 디바이스의 디바이스폴에서 해당 MLPP 선점 설정을 상속합니다. 2. 사용 안 함 - 우선 순위가 더 높은 통화를 완료하는 데 필요한 경우 이 디바이스는 우선 순위가 낮은 통화의 선점이 발생하는 것을 허용하지 않습니다. 3. 강제 - 우선 순위가 더 높은 통화를 완료하는 데 필요한 경우 이 디바이스는 우선 순위가 낮은 통화가 선점하도록 허용합니다. <p>참고 [MLPP 선점]이 [강제]로 설정되어 있는 상태에서 [MLPP 표시]를 [끄기] 또는 [기본값](기본값이 [끄기]인 경우)으로 설정하는 설정 조합으로 디바이스 프로파일을 구성하지 마십시오.</p>

필드	설명
로그인 사용자 ID	[로그인 사용자 ID] 드롭다운 목록에서 올바른 로그인 사용자 ID를 선택합니다. 참고 디바이스 프로필을 로그아웃 프로필로 사용하는 경우 해당 전화기와 연결할 로그인 사용자 ID를 지정합니다. 사용자가 이 사용자 디바이스 프로필에서 로그아웃하면 전화기에서 이 로그인 사용자 ID에 자동으로 로그인합니다.

사용자에 대해 **Extension Mobility** 상호 클러스터 활성화

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 사용자에 대한 설정을 수정하려면 찾기를 클릭하여 결과 목록에서 기존 사용자를 선택합니다.
- 새로 추가를 클릭하여 새 사용자를 추가합니다.

단계 3 **Extension Mobility** 창에서 클러스터 간 **Extension Mobility** 활성화 확인란을 선택합니다.

단계 4 **Extension Mobility** 창의 사용 가능한 프로파일 목록 창에서 디바이스 프로파일을 선택합니다.

단계 5 디바이스 프로파일을 제어되는 프로파일 목록 창으로 이동합니다.

단계 6 저장을 클릭합니다.

디바이스를 **Extension Mobility**에 구독

모든 디바이스에 대해 엔터프라이즈 가입을 설정하지 않은 경우 디바이스에서 **Extension Mobility**를 활성화하고 서비스에 가입합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기에서.

단계 2 사용자가 클러스터 간 **Extension Mobility**를 사용할 수 있는 전화기를 찾습니다.

단계 3 이 디바이스에 대해 내선 정보 창에서 **Extension Mobility** 활성화 확인란을 선택합니다.

단계 4 전화기 구성 창에서 관련 링크 드롭다운 목록의 서비스 가입/가입 해지 옵션을 선택합니다.

단계 5 이동을 클릭합니다.

단계 6 팝업 창이 열리면 서비스 선택 드롭다운 목록 상자에서 **Extension Mobility** 서비스를 선택합니다.

단계 7 다음을 클릭합니다.

- 단계 8 가입을 클릭합니다.
- 단계 9 팝업 창에서 저장을 클릭하고 창을 닫습니다.
- 단계 10 전화기 구성 창에서 저장을 클릭합니다.
- 단계 11 프롬프트가 표시되면 확인을 클릭합니다.

클러스터 간 **Extension Mobility**에 대한 인증서 구성

홈 및 원격 클러스터를 적절하게 구성하려면 각 클러스터에서 인증서를 동일한 SFTP 서버 및 SFTP 디렉터리로 내보내고 참여 클러스터 중 하나에서 이를 통합해야 합니다. 이 절차는 두 클러스터 사이에 신뢰가 설정되어 있는지 확인합니다.

시작하기 전에

[Configure Extension Mobility, 459 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	Bulk Provisioning Service 활성화, 470 페이지	
단계 2	벌크 인증서 관리 구성 및 인증서 내보내기, 471 페이지	Cisco Unified OS 관리에서 벌크 인증서 관리를 구성하여 홈 클러스터 및 원격 클러스터에서 인증서를 내보냅니다.
단계 3	인증서 통합, 472 페이지	모든 참여 클러스터가 인증서를 내보낸 경우 인증서를 통합합니다. 이 옵션은 둘 이상의 클러스터가 인증서를 SFTP 서버로 내보낸 경우에만 사용할 수 있습니다.
단계 4	클러스터로 인증서 가져오기, 472 페이지	홈 및 원격 (방문) 클러스터로 인증서를 다시 가져옵니다.

Bulk Provisioning Service 활성화

시작하기 전에

[Configure Extension Mobility, 459 페이지](#)

프로시저

- 단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. 도구 > 서비스 활성화.
- 단계 2 서버 드롭다운 목록에서 게시자 노드를 선택합니다.
- 단계 3 **Cisco Bulk Provisioning Service** 확인란을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 확인을 클릭합니다.

벌크 인증서 관리 구성 및 인증서 내보내기

Cisco Unified OS 관리에서 벌크 인증서 관리를 구성하여 홈 클러스터 및 원격 클러스터에서 인증서를 내보냅니다.

이 절차에서는 클러스터의 모든 노드에 대한 인증서를 포함하는 PKCS12 파일을 만듭니다.



참고

- 모든 참여 클러스터는 인증서를 동일한 SFTP 서버 및 SFTP 디렉터리로 내보내야 합니다.
- Tomcat, Tomcat-ECDSA, TFTP 또는 CAPF 인증서가 클러스터 노드에서 다시 생성될 때마다 클러스터에서 인증서를 내보내야 합니다.

프로시저

단계 1 Cisco Unified OS 관리에서 보안 > 벌크 인증서 관리를 선택합니다.

단계 2 홈 및 원격 클러스터에서 연결할 수 있는 TFTP 서버에 대한 설정을 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.

단계 3 저장을 클릭합니다.

단계 4 내보내기를 클릭합니다.

단계 5 벌크 인증서 내보내기 창에서 인증서 종류 필드에 대해 모두를 선택합니다.

단계 6 내보내기를 클릭합니다.

단계 7 단기를 클릭합니다.

참고 대량 인증서 내보내기가 수행되면 다음과 같이 인증서가 원격 클러스터에 업로드됩니다.

- CAPF 인증서가 CallManager-trust로 업로드됩니다.
- Tomcat 인증서가 Tomcat-trust로 업로드됩니다.
- CallManager 인증서가 CallManager-trust로 업로드됩니다.
- CallManager 인증서가 Phone-SAST-trust로 업로드됩니다.
- ITLRecovery 인증서가 PhoneSast-trust 및 CallManager-trust로 업로드됩니다.

위의 단계는 인증서가 자체 서명되고 다른 클러스터에 일반 트러스트가 없을 때 수행됩니다. 일반 신뢰 또는 동일한 서명자가 있는 경우 모든 인증서를 내보낼 필요는 없습니다.

인증서 통합

모든 참여 클러스터가 인증서를 내보낸 경우 인증서를 통합합니다. 이 옵션은 둘 이상의 클러스터가 인증서를 SFTP 서버로 내보낸 경우에만 사용할 수 있습니다.

이 절차에서는 SFTP 서버의 모든 PKCS12 파일을 통합하여 단일 파일을 형성합니다.



참고 통합 후 새 인증서를 내보내는 경우 다시 이 절차를 수행하여 새로 내보낸 인증서를 포함해야 합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 다음을 선택합니다보안 > 벌크 인증서 관리 > 통합 > 벌크 인증서 통합.

단계 **2** 인증서 유형 필드에서 모두를 선택합니다.

단계 **3** 통합을 클릭합니다.

참고 벌크 인증서 통합이 수행되면 다음과 같이 인증서가 원격 클러스터에 업로드됩니다.

- CAPF 인증서가 CallManager-trust로 업로드됩니다.
- Tomcat 인증서가 Tomcat-trust로 업로드됩니다.
- CallManager 인증서가 CallManager-trust로 업로드됩니다.
- CallManager 인증서가 Phone-SAST-trust로 업로드됩니다.
- ITLRecovery 인증서가 PhoneSast-trust 및 CallManager-trust로 업로드됩니다.

클러스터로 인증서 가져오기

홈 및 원격 (방문) 클러스터로 인증서를 다시 가져옵니다.



참고 업그레이드 후에도 이러한 인증서는 보존됩니다. 사용자가 인증서를 다시 가져오거나 다시 통합하지 않아도 됩니다.



주의 인증서를 가져오면 클러스터의 전화기가 자동으로 다시 시작됩니다.

프로시저

단계 1 Cisco Unified OS 관리에서 다음을 선택합니다보안 > 벌크 인증서 관리 > 가져오기 > 벌크 인증서 가져오기.

단계 2 인증서 유형 드롭다운 목록에서 모두를 선택합니다.

단계 3 가져오기를 선택합니다.

참고 벌크 인증서 가져오기가 수행되면 다음과 같이 인증서가 원격 클러스터에 업로드됩니다.

- CAPF 인증서가 CallManager-trust로 업로드됩니다.
- Tomcat 인증서가 Tomcat-trust로 업로드됩니다.
- CallManager 인증서가 CallManager-trust로 업로드됩니다.
- CallManager 인증서가 Phone-SAST-trust로 업로드됩니다.
- ITLRecovery 인증서가 PhoneSast-trust 및 CallManager-trust로 업로드됩니다.

참고 다음 유형의 인증서는 다시 시작되는 전화를 결정합니다.

- Callmanager - 인증서가 속한 노드에서 TFTP 서비스를 활성화한 경우에만 모든 전화기.
- TVS - Callmanager 그룹 구성원 자격을 기반으로 하는 일부 전화기.
- CAPF - CAPF가 활성화된 경우에만 모든 전화기.

클러스터 간 **Extension Mobility** 디바이스 및 템플릿 구성

프로시저

	명령 또는 동작	목적
단계 1	일반 디바이스 구성 만들기, 474 페이지	일반 디바이스 구성을 통해 특정 사용자와 연결할 서비스 또는 기능을 지정합니다.
단계 2	클러스터 간 Extension Mobility 템플릿 구성, 474 페이지	이 기능과 함께 일반 디바이스 구성을 연결할 클러스터 간 Extension Mobility 템플릿을 만듭니다.
단계 3	기본 템플릿 설정, 474 페이지	만든 클러스터 간 Extension Mobility 템플릿을 기본 템플릿으로 설정합니다.
단계 4	클러스터 간 Extension Mobility 디바이스 추가, 475 페이지	클러스터 간 Extension Mobility 디바이스 항목을 시스템 데이터베이스에 삽입합니다. 각 디

	명령 또는 동작	목적
		바이스는 형식 EMCC1, EMCC2 등의 고유한 이름으로 식별됩니다. 벌크 관리 도구는 마지막으로 사용된 번호를 가져와서 디바이스 번호를 할당합니다.

일반 디바이스 구성 만들기

일반 디바이스 구성을 통해 특정 사용자와 연결할 서비스 또는 기능을 지정합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 일반 디바이스 구성을 수정하려면 찾기를 클릭하고 결과 목록에서 일반 디바이스 구성을 선택합니다.
- 새 일반 디바이스 구성을 추가하려면 새로 추가를 클릭합니다.

단계 3 일반 디바이스 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

클러스터 간 Extension Mobility 템플릿 구성

이 기능과 함께 일반 디바이스 구성을 연결할 클러스터 간 Extension Mobility 템플릿을 만듭니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 벌크 관리 > **EMCC** > **EMCC** 템플릿.

단계 2 새로 추가를 클릭합니다.

단계 3 **Ping** 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

기본 템플릿 설정

만든 클러스터 간 Extension Mobility 템플릿을 기본 템플릿으로 설정합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.벌크 관리 > **EMCC** > **EMCC** 삽입/업데이트.
 - 단계 2 **EMCC** 디바이스 업데이트를 클릭합니다.
 - 단계 3 기본 **EMCC** 템플릿 드롭다운 목록에서 사용자가 구성한 클러스터 간 Extension Mobility 디바이스 템플릿을 선택합니다.
 - 단계 4 즉시 실행을 클릭합니다.
 - 단계 5 제출을 클릭합니다.
 - 단계 6 다음 작업의 성공 여부를 확인합니다.
 - a) 벌크 관리 > 작업 스케줄러를 선택합니다.
 - b) 작업 ID를 찾습니다.
-

클러스터 간 **Extension Mobility** 디바이스 추가

클러스터 간 Extension Mobility 디바이스 항목을 시스템 데이터베이스에 삽입합니다. 각 디바이스는 형식 EMCC1, EMCC2 등의 고유한 이름으로 식별됩니다. 벌크 관리 도구는 마지막으로 사용된 번호를 가져와서 디바이스 번호를 할당합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.벌크 관리 > **EMCC** > **EMCC** 삽입/업데이트.
 - 단계 2 **EMCC** 디바이스 삽입을 클릭합니다.
 - 단계 3 추가할 **EMCC** 디바이스 수 필드에 추가하는 디바이스 수를 입력합니다.
 - 단계 4 즉시 실행을 클릭하고 제출을 클릭합니다.
 - 단계 5 창을 새로 고치고 데이터베이스에 이미 존재하는 **EMCC** 디바이스 수 값에 추가한 디바이스 수가 표시되는지 확인합니다.
-

클러스터 간 **Extension Mobility**를 위한 지오로케이션 필터 구성

지오로케이션 필터를 구성하여 국가, 시/도 및 구/군/시 같이 일치하는 디바이스 위치에 대한 기준을 지정합니다. 지오로케이션은 디바이스의 위치를 식별하는 데 사용되고 필터는 지오로케이션의 어느 부분이 중요한지를 나타냅니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 지리적 위치 필터.
 - 단계 2 새로 추가를 클릭합니다.

단계 3 지오로케이션 필터 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

클러스터 간 **Extension Mobility**에 대한 기능 매개 변수 구성

지오로케이션 필터와 같이 사용자가 구성한 기능 매개 변수에 대한 값을 선택합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > **EMCC** > **EMCC** 기능 구성.

단계 2 **EMCC** 기능 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [클러스터 간 Extension Mobility에 대한 기능 매개 변수 필드, 476 페이지](#)를 참조하십시오.

단계 3 저장을 클릭합니다.

클러스터 간 **Extension Mobility**에 대한 기능 매개 변수 필드

표 36: 클러스터 간 **Extension Mobility**에 대한 기능 매개 변수 필드

EMCC 파라미터	설명
EMCC 로그인 디바이스에 대한 기본 TFTP 서버	디바이스가 원격 클러스터에서 EMCC(클러스터 간 Extension Mobility)에 로그인할 때 사용할 기본 TFTP 서버의 컴퓨터 이름 또는 IP 주소를 선택합니다.
EMCC 로그인 디바이스의 백업 TFTP 서버	디바이스가 원격 클러스터에서 EMCC에 로그인할 때 사용할 백업 TFTP 서버의 컴퓨터 이름 또는 IP 주소를 선택합니다.
만료된 EMCC 디바이스 유지 보수의 기본 간격	<p>만료된 EMCC 디바이스에 대한 시스템 점검 사이의 경과 시간(분)을 지정합니다.</p> <p>만료된 EMCC 디바이스는 원격 클러스터에서 EMCC에 로그인한 디바이스이지만, WAN 장애 또는 연결 문제로 인해 전화기가 방문 클러스터에서 로그아웃되었습니다. 연결이 복구되고 디바이스는 방문 클러스터로 다시 로그인되었습니다.</p> <p>이러한 유지 보수 작업 중 Cisco Extension Mobility 서비스는 만료된 EMCC 디바이스의 Unified Communications Manager 데이터베이스를 자동으로 확인하며 이와 같이 만료된 디바이스를 자동으로 로그아웃시킵니다.</p> <p>기본값은 1440분입니다. 유효한 값의 범위는 10분~1440분입니다.</p>

EMCC 파라미터	설명
새 원격 클러스터를 추가할 경우 모든 원격 클러스터 서비스 활성화	<p>새 클러스터를 추가할 때 새 원격 클러스터의 모든 서비스를 자동으로 활성화할지 여부를 선택합니다.</p> <p>유효 값은 [참](원격 클러스터의 모든 서비스를 자동으로 활성화) 또는 [거짓](Unified Communications Manager의 [원격 클러스터 구성] 창을 통해 원격 클러스터의 서비스를 수동으로 활성화)입니다. 원격 서비스를 활성화하기 전에 EMCC 기능을 완전히 구성할 시간을 확보하려면 서비스를 수동으로 활성화할 수 있습니다.</p> <p>기본값은 false입니다.</p>
PSTN 액세스 SIP 트렁크의 CSS	<p>EMCC 통화 처리를 위한 PSTN 액세스 SIP 트렁크에서 사용하는 CSS(발신 검색 공간)를 선택합니다.</p> <p>PSTN 액세스 SIP 트렁크는 클러스터 간 서비스 프로파일 창에서 PSTN 액세스가 구성된 SIP 트렁크입니다. 이 트렁크를 이동하는 통화는 통화를 시작한 EMCC 로그인 전화기와 같은 위치에 있는 로컬 PSTN으로만 발신할 수 있으며 해당 PSTN으로 라우팅됩니다.</p> <p>유효한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 트렁크 CSS 사용(PSTN 통화는 비상 서비스 통화를 올바르게 라우팅하는 데 유용할 수 있는 로컬 경로 그룹을 사용함) • 전화기의 원래 디바이스 CSS 사용(PSTN 통화는 원격 전화기에 구성된 발신 검색 공간, 즉, 전화기가 EMCC에 로그인되어 있지 않을 때 사용되는 CSS를 사용하여 라우팅됩니다). <p>기본값은 [트렁크 CSS 사용]입니다.</p>
EMCC 지오로케이션 필터	<p>EMCC 사용을 위해 구성된 지오로케이션 필터를 선택합니다.</p> <p>다른 클러스터에서 Extension Mobility를 통해 로그인된 전화기 및 선택된 EMCC 지오로케이션 필터와 관련된 지오로케이션의 정보를 기준으로 Cisco Unified Communications Manager가 전화기를 로밍 디바이스풀에 배치합니다.</p> <p>Cisco Unified Communications Manager는 EMCC 지오로케이션 필터가 적용된 다음 전화기 지오로케이션 정보와 가장 정확하게 일치하는 디바이스풀을 평가하여 사용할 로밍 디바이스풀을 결정합니다.</p>
EMCC 지역 최대 오디오 비트 레이트	<p>이 파라미터는 상대방과 관련된 지역과 상관없이 모든 EMCC 통화에 대한 최대 오디오 비트 레이트를 지정합니다.</p> <p>기본값은 8kbps(G.729)입니다.</p> <p>참고 참가하는 모든 EMCC 클러스터는 EMCC 지역 최대 오디오 비트 레이트에 대해 동일한 값을 지정해야 합니다.</p>

EMCC 파라미터	설명
EMCC 지역 최대 영상 통화 비트 레이트(오디오 포함)	<p>이 파라미터는 상대방과 관련된 지역의 최대 영상 통화 비트 레이트와 상관없이 모든 EMCC 영상 통화에 대한 최대 영상 통화 비트 레이트를 지정합니다.</p> <p>기본값은 384입니다. 유효한 값 범위는 0에서 8128 사이입니다.</p> <p>참고 참가하는 모든 EMCC 클러스터는 EMCC 지역 최대 영상 통화 비트 레이트에 대해 동일한 값을 지정해야 합니다.</p>
EMCC 지역 링크 손실 유형	<p>이 파라미터는 EMCC 전화기와 원격 클러스터의 디바이스 간 링크 손실 유형을 지정합니다.</p> <p>참고 EMCC 통화에서 양방향 오디오를 허용하려면 참가하는 모든 EMCC 클러스터가 동일한 EMCC 지역 링크 손실 유형을 사용해야 합니다.</p> <p>Cisco Unified Communications Manager는 구성된 [EMCC 지역 최대 오디오 비트 레이트]를 관찰하면서 선택된 옵션을 기준으로 EMCC 통화에서 최적의 오디오 코덱을 사용하려고 시도합니다.</p> <p>유효한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • Lossy—부 패킷 손실이 발생할 수 있는 링크, 예: DSL • Low Loss—적은 패킷 손실이 발생할 수 있는 링크, 예: T1 <p>이 매개 변수를 Lossy로 설정하면 Cisco Unified Communications Manager는 오디오 품질을 기준으로 EMCC 지역 최대 오디오 비트 레이트에 의해 설정된 한도 내에서 최적의 코덱을 선택합니다. 일부 패킷 손실이 발생합니다.</p> <p>이 매개 변수를 Low Loss로 설정하면 Cisco Unified Communications Manager는 오디오 품질을 기준으로 EMCC 지역 최대 오디오 비트 레이트에 의해 설정된 한도 내에서 최적의 코덱을 선택합니다. 패킷 손실이 거의 또는 전혀 발생하지 않습니다.</p> <p>Low Loss와 Lossy 옵션 오디오 코덱 기본 설정 순서의 유일한 차이는 [링크 손실 유형]이 [Low Loss]로 설정된 경우 iSAC(Internet Speech Audio Codec)보다 G.722가 우선 적용되고 [링크 손실 유형]이 [Lossy]로 설정된 경우 G.722보다 iSAC이 우선 적용된다는 점입니다.</p> <p>기본값은 Low Loss입니다.</p>

EMCC 파라미터	설명
RSVP SIP 트렁크 KeepAlive 타이머	<p>Unified Communications Manager가 EMCC RSVP SIP 트렁크에서 두 클러스터 사이에 KeepAlive 메시지 또는 확인을 송수신할 때 대기하는 시간(초)을 지정합니다.</p> <p>EMCC RSVP SIP 트렁크는 Cisco Extension Mobility Cross Cluster가 [트렁크 서비스 유형]으로 구성된 SIP 트렁크와 [클러스터 간 서비스 프로파일] 창에서 RSVP 에이전트의 SIP 트렁크로 선택된 SIP 트렁크를 지정합니다. KeepAlive 메시지 또는 확인을 수신하지 않고 이러한 두 간격이 경과할 경우 Unified Communications Manager에서 원격 클러스터에 RSVP 리소스를 릴리스합니다.</p> <p>기본값은 15초입니다. 유효한 값의 범위는 1초~600초입니다.</p>
원격 클러스터 업데이트 용 기본 서버	이 로컬 클러스터에서 Cisco Extension Mobility 서비스가 활성화된 기본 노드의 기본 서버 이름 또는 IP 주소를 선택합니다. 원격 클러스터는 이 노드에 액세스하여 이 로컬 클러스터에 대한 정보를 가져옵니다.
원격 클러스터 업데이트 용 백업 서버	이 로컬 클러스터에서 Cisco Extension Mobility 서비스가 활성화된 보조 노드의 기본 서버 이름 또는 IP 주소를 선택합니다. 기본 노드가 작동하지 않을 경우 원격 클러스터가 이 노드에 액세스하여 이 로컬 클러스터에 대한 정보를 가져옵니다.
원격 클러스터 업데이트 간격	<p>로컬 노드의 Cisco Extension Mobility 서비스가 원격 EMCC 클러스터에 대한 정보를 수집하는 간격(분)을 지정합니다. 수집된 정보에는 원격 클러스터 Unified Communications Manager 버전 및 서비스 정보 등의 상세 정보가 포함됩니다.</p> <p>기본값은 30입니다. 유효한 값 범위는 15~10,080분입니다.</p>

클러스터 간 **Extension Mobility**에 대한 클러스터 간 **SIP** 트렁크 구성

클러스터 간 PSTN 액세스 및 RSVP 에이전트 서비스에 대한 착신 또는 발신 트래픽을 처리하도록 트렁크를 구성합니다. 두 PSTN 액세스 및 RSVP 에이전트 서비스에 대해 트렁크 하나를 구성하거나 각 서비스에 대해 트렁크를 하나씩 구성할 수 있습니다. 클러스터 간 Extension Mobility를 위해 SIP 트렁크가 두 개 이상 필요하지 않습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 트렁크.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 트렁크 유형 드롭다운 목록에서 **SIP** 트렁크를 선택합니다.
- 단계 4 트렁크 서비스 유형 드롭다운 목록에서 클러스터 간 **Extension Mobility**를 선택합니다.
- 단계 5 다음을 클릭합니다.

단계 6 트렁크 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말 말을 참조하십시오.

단계 7 저장을 클릭합니다.

클러스터 간 **Extension Mobility**를 위한 클러스터 간 서비스 프로파일 구성

클러스터 간 서비스 프로파일을 구성하여 클러스터 간 **Extension Mobility**를 활성화합니다. 프로파일은 이전의 모든 구성을 수집하고 결과 보고서를 제공합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > **EMCC** > **EMCC** 클러스터 간 서비스 프로파일.

단계 2 **EMCC** 클러스터 간 서비스 프로파일 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 3 팝업 창에 오류 메시지가 표시되지 않는 경우 저장을 클릭합니다.

원격 클러스터 서비스 구성

클러스터 간 **Extension Mobility**에 대한 원격 클러스터를 구성합니다. 이 단계는 원격(방문) 클러스터와 홈 클러스터 간 연결을 완료합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > 클러스터 보기.

단계 2 찾기를 클릭하여 알려진 원격 클러스터 목록을 표시합니다.

단계 3 다음 단계 중 하나를 수행합니다.

- 구성하려는 원격 클러스터가 표시되는 경우 이 원격 클러스터 이름을 클릭하고 필드를 확인합니다.
- 구성하려는 원격 클러스터가 표시되지 않는 경우 새로 추가를 클릭하고 다음 필드를 구성합니다.
 1. 클러스터 **ID** 필드의 경우 ID가 다른 클러스터의 클러스터 ID 엔터프라이즈 매개 변수 값과 일치하는지 확인합니다.
 2. 정규화된 이름 필드에 원격 클러스터의 노드로 확인할 수 도메인 이름이나 원격 클러스터의 IP 주소를 입력합니다.
 3. 저장을 클릭합니다.

참고 클러스터 간 Extension Mobility의 경우 **TFTP** 확인란은 항상 비활성화되어 있어야 합니다.

클러스터 간 **Extension Mobility** 상호 작용

표 37: 클러스터 간 **Extension Mobility** 상호 작용

기능	상호 작용
오디오	EMCC 로그인 디바이스용 기본 최대 오디오 비트 레이트는 8kbps(G.729)입니다.
CAC(통화 허용 제어)	<ul style="list-style-type: none"> • 홈 클러스터에서는 방문 클러스터의 위치와 지역이 인식되지 않습니다. • 이 시스템은 클러스터 경계를 서로 걸쳐서 Cisco Unified Communications Manager 위치와 지역을 적용할 수 없습니다. • RSVP 에이전트 기반 CAC는 방문 클러스터의 RSVP 에이전트를 사용합니다.
착신 전환	EMCC는 착신 전환을 지원합니다.
Cisco Extension Mobility 로그인 및 로그아웃	사용자 인증은 전체 클러스터에서 수행됩니다.
방문 전화기에 대한 미디어 리소스	<p>RSVP 에이전트, TRP, MOH(대기 중 음악), MTP, 트랜스코더 및 컨퍼런스 브리지 등의 예가 있습니다.</p> <p>미디어 리소스는 방문 전화기에 로컬입니다(RSVP 에이전트 아님).</p>
방문 전화기에 대한 PSTN 액세스	<ul style="list-style-type: none"> • E911 통화가 PSTN의 로컬 게이트웨이로 라우팅됩니다. • 로컬 통화가 PSTN의 로컬 게이트웨이로 라우팅됩니다. • 로컬 통화 그룹으로 착신되는 통화가 방문 클러스터의 로컬 게이트웨이로 라우팅됩니다.
기타 통화 기능 및 서비스	제한의 예: EMCC는 인터콤 기능을 지원하지 않으므로 인터콤 구성은 구성을 고정 디바이스로 지정합니다.
보안	<ul style="list-style-type: none"> • 기본적으로 클러스터 간 보안이 제공됩니다. • 보안 및 비보안 전화 보안 프로파일을 사용하는 Cisco Unified IP Phone이 지원됩니다.

기능	상호 작용
IPv6(Internet Protocol Version 6)	Cisco Extension Mobility Cross Cluster는 IPv6을 지원합니다. IP 주소 지정 모드가 IPv6 또는 듀얼 스택(IPv4 및 IPv6)인 전화기를 사용할 수 있습니다.

클러스터 간 **Extension Mobility** 제한

표 38: 클러스터 간 **Extension Mobility** 제한

제한 사항	설명
지원되지 않는 기능	<ul style="list-style-type: none"> • EMCC는 인터콤 구성이 정적 디바이스를 필요로 하기 때문에 인터콤 기능을 지원하지 않습니다. • 위치 기반 CAC는 지원되지 않지만 RSVP 기반 CAC는 지원됩니다.
두 개 이상의 클러스터에 EMCC 디바이스 프로비저닝 불가능	EMCC가 올바르게 작동하려면 두 클러스터에 동일한 전화기(디바이스 이름)를 구성할 수 없습니다. 그렇지 않으면 중복 디바이스 오류(37)로 인해 로그인이 실패합니다. 이러한 이유로 EMCC와 함께 배포된 클러스터의 경우 EMCC 로그아웃 후 홈 클러스터에 새 디바이스가 만들어지는 것을 방지하기 위해 모든 Unified Communication Manager 노드에서 자동 등록을 비활성화해야 합니다.
EMCC 디바이스 수	<p>Cisco Unified Communications Manager는 MaxPhones 값 60,000을 지원할 수 있습니다.</p> <p>다음 계산을 사용하여 클러스터에서 지원되는 총 디바이스 수에 EMCC를 포함합니다.</p> $\text{전화기 수} + (2 \times \text{EMCC 디바이스}) = \text{MaxPhones}$ <p>참고 EMCC 로그인은 홈 클러스터에서 사용되는 라이선스 수에 영향을 주지 않습니다.</p>

제한 사항	설명
방문 디바이스 로그인 제한	<ul style="list-style-type: none"> • 최종 사용자가 EMCC로 로그인한 상태에서 홈 클러스터 관리자가 최종 사용자에게 대해 EMCC를 비활성화하는 경우, 이 최종 사용자가 자동으로 로그아웃되지 않습니다. 대신, 시스템은 이 사용자의 향후 EMCC 시도를 허용하지 않습니다. 사용자가 로그아웃할 때까지 현재 EMCC 세션이 계속됩니다. • 방문 클러스터의 전화기 구성 창에는 Extension Mobility용 [로그아웃] 버튼이 있습니다. 이 버튼은 방문 클러스터 관리자가 EMCC 전화기를 로그아웃하는 데도 사용됩니다. EMCC 전화기가 현재 방문 Cisco Unified Communications Manager에 등록되어 있지 않으므로 이 작업은 방문 클러스터의 데이터베이스 정리와 같습니다. 다른 방법으로 홈 클러스터에서 로그아웃하거나 재설정으로 인해 방문 클러스터로 돌아올 때까지 EMCC 전화기가 홈 Cisco Unified Communications Manager에 등록된 상태로 유지됩니다.
방문 디바이스 로그인 제한	<p>참가 클러스터의 Extension Mobility 서비스는 주기적인 원격 클러스터 업데이트를 수행합니다. 원격 클러스터 업데이트 간격 기능 매개 변수는 업데이트 간격을 제어합니다. 기본 간격은 30분입니다.</p> <p>클러스터A의 내선 이동 서비스가 이 업데이트에 대해 원격 클러스터(예: 클러스터B)로부터 회신을 받지 못하는 경우 클러스터A의 [원격 클러스터] 창에서 클러스터B에 대해 원격 활성화된 서비스가 False으로 설정되었음을 표시합니다.</p> <p>이 경우 방문 클러스터는 홈 클러스터로부터 응답을 받지 못하고 홈 클러스터에 대한 원격 활성화된 값을 False로 설정합니다.</p> <p>이 기간에 방문 전화기에서는 EMCC를 사용하여 로그인할 수 없습니다. 방문 전화기에서 “로그인할 수 없음” 오류 메시지를 받습니다.</p> <p>이 시점에 방문 전화기에서 EMCC로의 로그인 시도가 실패할 수 있습니다. 전화기에 “로그인할 수 없음” 오류 메시지가 표시됩니다. 이 오류는 방문 클러스터가 홈 클러스터가 서비스되지 않는 상태에서 서비스 중인 상태로 변경되었음을 아직 감지하지 못했기 때문에 발생합니다.</p> <p>원격 클러스터 상태 변경은 원격 클러스터 업데이트 간격 EMCC(Remote Cluster Update Interval EMCC) 기능 매개 변수의 값을 바탕으로, 방문 Extension Mobility 서비스에서 마지막 쿼리/업데이트를 수행한 경우에 감지됩니다.</p> <p>원격 클러스터 서비스 구성 창(고급 기능 > EMCC > EMCC 원격 클러스터)에서 지금 원격 클러스터 업데이트를 선택하여 원격 활성화 값을 참으로 설정해도 EMCC 로그인이 허용됩니다. 그렇지 않으면, 다음 번 정기 업데이트 주기가 끝난 후 방문 전화기의 EMCC 로그인이 정상으로 돌아옵니다.</p>

loginType을 사용한 다양한 클러스터 버전의 **EMCC** 로그인 결과

다음 표에서는 loginType 매개 변수가 서비스 URL에 사용될 때 서로 다른 클러스터 버전에 대한 익스텐션 모빌리티 크로스 클러스터 (EMCC) 기능의 로그인 결과를 보여 줍니다.

표 39: loginType을 사용한 다양한 클러스터 버전의 **EMCC** 로그인 결과

방문 클러스터 버전	홈 클러스터 버전	방문 클러스터 EMURL의 loginType	EMCC 로그인 결과
12.0	12.0	언급되지 않음(기본 URL)	성공
12.0	12.0	UID, SP 또는 DN	성공
12.0	11.5 이하	언급되지 않음(기본 URL)	성공
12.0	11.5 이하	UID, SP 또는 DN	실패 오류 코드로 실패 - 1 **
11.5 이하	12.0	언급되지 않음(기본 URL)	성공
11.5 이하	12.0	UID, SP 또는 DN ***	성공



참고

- * 다음은 loginType 매개 변수 옵션입니다.
 - UID — 사용자 ID 및 PIN을 사용하여 사용자 로그인
 - SP — 셀프 서비스 사용자 ID 및 PIN을 사용하여 사용자 로그인
 - DN — 기본 확장 및 PIN을 사용하여 사용자 로그인
- * 오류 코드로 실패 - 1(EMService가 EApp/EMService에서 XML을 구문 분석할 수 없는 경우)
- *** loginType은 무시되며 사용자 ID/PIN 로그인 프롬프트가 전화기에 채워집니다.

다양한 클러스터 버전을 위한 익스텐션 모빌리티 크로스 클러스터(EMCC) 및 보안 모드



참고

홈 클러스터와 방문 클러스터 버전이 둘 다 9.x 이상이며 TFTP 암호화 구성 플러그가 활성화된 경우에만 전화기 구성 파일을 암호화할 수 있습니다.

EMCC 로그인 시 방문 클러스터 버전과 홈 클러스터 버전이 둘 다 9.x 이상인 경우 전화기가 다음 표에서처럼 다양한 모드로 작동합니다.

표 40: 방문 클러스터 및 홈 클러스터가 모두 9.x 이상 버전일 때 지원되는 보안 모드

홈 클러스터 버전	홈 클러스터 모드	방문 클러스터 버전	방문 클러스터 모드	방문 전화기 모드	EMCC 상태
9.x 이상	혼합	9.x 이상	혼합	보안	보안 EMCC
9.x 이상	혼합	9.x 이상	혼합	비보안	비보안 EMCC
9.x 이상	혼합	9.x 이상	비보안	비보안	비보안 EMCC
9.x 이상	비보안	9.x 이상	혼합	보안	로그인 실패
9.x 이상	비보안	9.x 이상	비보안	비보안	비보안 EMCC

EMCC 로그인 시 방문 클러스터 버전이 8.x이고 홈 클러스터 버전이 9.x 이상이면 전화기가 다음 표에서처럼 다양한 모드로 작동합니다.

표 41: 방문 클러스터가 8.x 버전이고 홈 클러스터가 9.x 이상 버전일 때 지원되는 보안 모드

홈 클러스터 버전	홈 클러스터 모드	방문 클러스터 버전	방문 클러스터 모드	방문 전화기 모드	EMCC 상태
9.x 이상	혼합	8.x	혼합	보안	지원되지 않음
9.x 이상	혼합	8.x	혼합	비보안	비보안 EMCC
9.x 이상	혼합	8.x	비보안	비보안	비보안 EMCC
9.x 이상	비보안	8.x	혼합	보안	지원되지 않음
9.x 이상	비보안	8.x	비보안	비보안	비보안 EMCC

EMCC 로그인 시 방문 클러스터 버전이 9.x 이상이고 홈 클러스터 버전이 8.x이면 전화기가 다음 표에서처럼 다양한 모드로 작동합니다.

표 42: 방문 클러스터가 9.x 이상 버전이고 홈 클러스터가 8.x 버전일 때 지원되는 보안 모드

홈 클러스터 버전	홈 클러스터 모드	방문 클러스터 버전	방문 클러스터 모드	방문 전화기 모드	EMCC 상태
8.x	혼합	9.x 이상	혼합	보안	로그인 실패
8.x	혼합	9.x 이상	혼합	비보안	비보안 EMCC
8.x	혼합	9.x 이상	비보안	비보안	비보안 EMCC
8.x	비보안	9.x 이상	혼합	보안	로그인 실패
8.x	비보안	9.x 이상	비보안	보안	비보안 EMCC

클러스터 간 **Extension Mobility** 문제 해결

Extension Mobility 애플리케이션 오류 코드

표 43: **Extension Mobility** 애플리케이션 오류 코드

오류 코드	전화 표시	요약 설명	이유
201	다시 로그인하십시오(201).	인증 오류	사용자가 EMCC 사용자인 경우 이 클러스터 간 서비스 프로파일 창에 “EMCC”를 활성화하지 않은 경우 발생할 수 있습니다.
202	다시 로그인하십시오(202).	빈 사용자 ID 또는 PIN	사용자가 빈 사용자 ID 또는 PIN을 입력했습니다.
204	로그인할 수 없음(204)	디렉터리 서버 오류	EMApp는 IMS에서 지정된 PIN으로 인증할 수 없을 때 이 오류를 전송합니다.
205	로그인할 수 없음(205) 로그아웃할 수 없음(205)	사용자 프로파일 부재	사용자 프로파일 정보를 캐시나 데이터베이스에서 검색할 수 없을 때 발생합니다.

오류 코드	전화 표시	요약 설명	이유
207	로그인할 수 없음(207) 로그아웃할 수 없음(207)	빈 디바이스 이름	디바이스 또는 이름 태그가 요청을 때 발생합니다. 이 오류는 클러스터에서는 발생할 수 없으며 요청 플리케이션에서 전송되는 경우 발생할 수 있습니다.
208	로그인할 수 없음(208) 로그아웃할 수 없음(208)	EMService 연결 오류	방문 EApp은 방문 EService에 연결할 수 없습니다.(서비스가 중단되었거나 활성화되지 않았습니다.) 방문 EService가 홈 EService에 연결할 수 없습니다.(WAN 작동이 중단되었거나 인증서를 신뢰할 수 없습니다.)
210	로그인할 수 없음(210) 로그아웃할 수 없음(210)	초기화 실패-관리자에게 문의	EApp을 초기화하는 중에 오류(데이터베이스 연결 실패)가 발생했습니다. 데이터베이스 연결 실패로 인해 초기화가 발생할 수 있습니다.
211	로그인할 수 없음(211) 로그아웃할 수 없음(211)	EMCC가 활성화되지 않았음	PSTN이 방문 클러스터의 클러스터 서비스 프로파일 창에서 활성화되지 않았을 때 발생합니다.
212	로그인할 수 없음(212)	클러스터 ID가 잘못된	잘못된 클러스터 ID를 원격 클러스터에 전송하여 원격 클러스터 업데이트를 시도할 때 발생합니다.
213	로그인할 수 없음(213) 로그아웃할 수 없음(213)	EMCC가 지원되지 않음	디바이스는 EMCC를 지원하지 않습니다.
215	LoginType 잘못된(215)	로그인 유형이 잘못되었습니다.	loginType이 올바르지 않을 때 발생하는 값은 다음과 같습니다. <ul style="list-style-type: none"> • 셀프 서비스 사용자 ID의 경우 DN • 기본 내선 번호의 경우 DN • 사용자 ID의 경우 UID
216	DN에 여러 사용자가 있음(216)	DN에 여러 사용자가 있습니다.	EM 로그인에 사용되는 내선 번호가 여러 사용자에게 기본으로 할당될 때 발생합니다.

Extension Mobility 서비스 오류 코드

표 44: Extension Mobility 서비스 오류 코드

오류 코드	전화 표시	요약 설명	이유
0	로그인할 수 없음(0) 로그아웃할 수 없음(0)	알 수 없는 오류	알 수 없는 이유로 EMService가 실패했
1	로그인할 수 없음(1) 로그아웃할 수 없음(1)	구문 분석 오류	EMService가 EApp 또는 EMService-요청을 구문 분석할 수 없을 때. 타사 애플리케이션에서 잘못된 쿼리를 로그인 XML(E에 전송할 때 이 오류가 발생합니다. 혼문 클러스터 간의 버전 불일치로 인해 발생할 수도 있습니다.
2	로그인할 수 없음(2)	EMCC 인증 오류	사용자가 잘못된 PIN을 입력했기 때문 EMCC 사용자 인증서를 인증할 수 없
3	로그인할 수 없음(3) 로그아웃할 수 없음(3)	잘못된 애플리케이션 사용자	잘못된 애플리케이션 사용자. 이 오류 API로 인해 일반적으로 발생합니다.
4	로그인할 수 없음(4) 로그아웃할 수 없음(4)	정책 확인 오류	EMService는 알 수 없는 오류, 데이터베이스 쿼리하는 중에 발생하는 오류 또는 캐 정보를 검색하는 중에 발생하는 오류 로그인/로그아웃 요청을 확인할 수 없 이 오류를 보냅니다.
5	로그인할 수 없음(5) 로그아웃할 수 없음(5)	디바이스에 로그인할 수 없음	사용자가 전화기 구성 창에서 Extension Mobility 활성화를 선택 취소한 디바이 로그인합니다.
6	로그인할 수 없음(6) 로그아웃할 수 없음(6)	데이터베이스 오류	EMService(로그인/로그아웃 또는 디바이스 사용자 쿼리)에 의해 요청되는 쿼리 또는 프로시저를 실행하는 중에 데이터베이스 예외를 반환할 때마다 EMService에서 코드를 EApp으로 보냅니다.
8	로그인할 수 없음(8) 로그아웃할 수 없음(8)	쿼리 유형을 결정하지 못함	유효한 쿼리가 EMService로 전송되지 않습니다(DeviceUserQuery 및 UserDeviceQuery 유효한 쿼리임). 이 오류는 EM API 또는 XML 입력 때문에 발생합니다.

오류 코드	전화 표시	요약 설명	이유
9	로그인할 수 없음(9) 로그아웃할 수 없음(9)	Dir. 사용자 정보 오류	다음 두 가지 경우에 이 오류가 나타납니다. 1. IMS는 사용자를 인증하려고 시도했지만 실패하여 에러를 반환합니다. 2. 사용자에 대한 정보를 캐시나 디렉토리에서 검색할 수 없는 경우
10	로그인할 수 없음(10) 로그아웃할 수 없음(10)	앱 프록시 권한 부족	사용자는 다른 사용자 대신 로그인할 수 없습니다. 기본적으로 CCMSysUse 권한이 있습니다.
11	로그인할 수 없음(11) 로그아웃할 수 없음(11)	디바이스가 존재하지 않음	디바이스 테이블에 전화 레코드 항목이 없습니다.
12	디바이스 테이블에 전화 레코드 항목이 없음	디바이스 프로필을 찾을 수 없음	디바이스 프로파일이 원격 사용자와 연결되지 않았습니까.
18	로그인할 수 없음(18)	다른 사용자가 로그인되어 있음	다른 사용자가 전화기에 이미 로그인되어 있습니다.
19	로그아웃할 수 없음(19)	로그인한 사용자 없음	시스템이 로그인 상태가 아닌 사용자를 로그아웃하려고 시도했습니다. 타사 애플리케이션(EM API)에서 로그아웃 요청을 보냈을 때 오류가 발생합니다.
20	로그인할 수 없음(20) 로그아웃할 수 없음(20)	호텔링 플래그 오류	전화기 구성 창에서 Extension Mobility 의 선택을 취소했습니다.
21	로그인할 수 없음(21) 로그아웃할 수 없음(21)	호텔링 상태 오류	현재 사용자 상태가 로컬 캐시 또는 디렉토리에서 검색되지 않았습니다.
22	로그인할 수 없음(22)	디바이스에 로그인할 수 없음	EM이 디바이스에서 활성화되어 있지 않거나, 현재 상태에서 요청이 EM API를 통해 전송되지 않거나, 전화기에서 [서비스] 버튼을 누를 때 오류가 발생합니다.
23	로그인할 수 없음(23) 로그아웃할 수 없음(23)	사용자가 없음	원격 클러스터에 지정된 사용자 ID가 존재하지 않습니다.
25	멀티 로그인이 허용되지 않음(25)	사용자가 다른 위치에서 로그인	사용자가 현재 로컬 클러스터 또는 원격 클러스터에서 다른 전화기로 로그인되어 있습니다.
26	로그인할 수 없음(26) 로그아웃할 수 없음(26)	통화 중. 다시 하십시오.	EMService가 현재 최대 동시 요청 수를 초과하여 변수의 임계값 수준에 도달할 때 발생합니다.

오류 코드	전화 표시	요약 설명	이유
28	로그인할 수 없음(28) 로그아웃할 수 없음(28)	신뢰할 수 없는 IP 오류	IP 주소 확인 서비스 매개 변수를 True 로 설정하고 사용자가 IP 주소를 신뢰할 수 없는 IP 주소에 로그인하거나 로그아웃을 시도할 때 발생합니다. 예를 들어, 타사 애플리케이션이 컴퓨터의 EM API는 Ips 서비스 매개 변수를 신뢰할 수 있는 목록에 나타나지 않습니다.
29	로그인할 수 없음(29) 로그아웃할 수 없음(29)	ris 중지-관리자에게 문의	실시간 정보 서버 데이터 수집기(RISDC)가 만들어지거나 초기화되지 않았고 EMCC가 RISDC에 연결할 수 없습니다.
30	로그인할 수 없음(30) 로그아웃할 수 없음(30)	프록시 허용 안 함	로그인/로그아웃이 프록시를 통해 발생하면 (HTTP 헤더에 “Via”가 설정됨) 프록시 서버 서비스 매개 변수가 False 로 설정된 경우 발생합니다.
31	로그인할 수 없음(31) 로그아웃할 수 없음(31)	사용자에 대해 EMCC가 활성화되지 않음	홈 클러스터의 최종 사용자 구성 창에 클러스터 간 Extension Mobility 활성화 확인란을 선택하지 않은 경우에 발생합니다.
32	로그인할 수 없음(32) 로그아웃할 수 없음(32)	EMCC가 지원되지 않음	디바이스 모델에 EMCC 기능이 없을 때 발생합니다.
33	로그인할 수 없음(33) 로그아웃할 수 없음(33)	사용 가능한 EMCC 더미 디바이스 없음	모든 EMCC 더미 디바이스가 다른 EMCC 더미에 사용 중일 때 발생합니다.
35	로그인할 수 없음(35) 로그아웃할 수 없음(35)	홈 클러스터에 방문 클러스터 정보가 없음	홈 클러스터에 이 방문 클러스터에 대한 정보가 없을 때 발생합니다.
36	로그인할 수 없음(36) 로그아웃할 수 없음(36)	원격 클러스터 없음	관리자가 원격 클러스터를 하나도 추가하지 않은 경우에 발생합니다.
37	로그인할 수 없음(37) 로그아웃할 수 없음(37)	중복 디바이스 이름	홈 클러스터와 방문 클러스터에 동일한 디바이스 이름이 있는 경우에 발생합니다.
38	로그인할 수 없음(38) 로그아웃할 수 없음(38)	EMCC 허용 안 함	홈 클러스터에서 EMCC 로그인을 허용하지 않을 때 발생합니다(홈 클러스터에 클러스터 간 Extension Mobility 활성화가 선택되지 않음).

오류 코드	전화 표시	요약 설명	이유
39	다시 로그인하십시오(201).	구성 문제	EMCC 로그인 디바이스에 대해 기- 버 및 백업 TFTP 서버가 EMCC 기- 이지에 적절하게 설정되지 않았을 니다. 참고 내부 오류 코드입니다.
40	다시 로그인하십시오(23).	원격 호스트로부터 응답 없음	원격 호스트에서 응답이 없을 때 발- 참고 내부 오류 코드입니다.
41	PIN을 변경해야 합니다.	PIN을 변경해야 합니다.	관리자가 PIN에 대해 다음 로그인- 시 변경을 활성화할 때 발생합니다. 용자는 인증서 변경 페이지로 리디- 다. 참고 내부 오류 코드입니다.
42	로그인할 수 없음(42) 로그아웃할 수 없음(42)	잘못된 ClusterID	원격 클러스터 ID가 유효하지 않을 니다. 이 오류는 원격 클러스터 업테- 생할 수 있습니다.
43	로그인할 수 없음(43)	디바이스 보안 모드 오류	EMCC 디바이스와 연결된 디바이스- 로파일에서 [디바이스 보안 모드]가 으로 설정되어야 합니다.
44	다시 로그인하십시오(201).	구성 문제	클러스터 ID가 유효하지 않을 때 발- 참고 내부 오류 코드입니다.
45	로그인 실패(45)	원격 클러스터 버전이 지원되지 않음	방문 클러스터 버전이 9.x이고 혼합 전화기가 보안 모드이고 홈 클러스- 8.x일 때 EMCC에 로그인하는 중에 다.
46	로그인 실패(46)	원격 클러스터 보안 모드가 지원 되지 않음	방문 클러스터 보안 모드가 혼합 모- 화기가 보안 모드이고 홈 클러스터 모드일 때 EMCC에 로그인하는 중 니다.
47	DN에 여러 사용자가 있음 (47)	DN에 여러 사용자가 있습니다.	EMCC 로그인 시 로그인에 사용되- 호가 여러 사용자에게 기본으로 할- 생합니다.



34 장

클러스터 간 **Extension Mobility** 로밍



참고 클러스터 전체에서 Extension Mobility 로밍을 배포하려면 Cisco Unified Communications Manager 12.0(1)SU1의 최소 릴리스를 실행해야 합니다.

- 클러스터 간 Extension Mobility 로밍 개요, 493 페이지
- 클러스터 간 Extension Mobility 로밍에 대한 시스템 요구 사항, 494 페이지
- 클러스터 간 Extension Mobility 로밍 로그인, 494 페이지
- ILS 상호 작용, 497 페이지
- 클러스터 간 Extension Mobility 로밍 작업 흐름, 497 페이지
- 클러스터 간 Extension Mobility 상호 작용 및 제한 사항, 502 페이지
- 다른 유형의 Extension Mobility, 502 페이지
- 클러스터 간 Extension Mobility 문제 해결, 503 페이지

클러스터 간 **Extension Mobility** 로밍 개요

클러스터 간 Extension Mobility 로밍 기능을 사용하면 사용자가 여러 클러스터 간에 로밍할 수 있고 사용자의 홈 클러스터가 다운된 경우에도 전화를 걸거나 받을 수 있습니다. 이 기능은 모든 클러스터에서 Extension Mobility 사용자의 디렉터리 번호를 복제하기 위해 ILS(클러스터 간 조회 서비스)를 활용합니다.

사용자가 로밍 클러스터에 로그인하면 전화기가 디렉터리 번호를 사용하여 로밍 클러스터에 등록됩니다. 방문 클러스터의 전화기가 홈 클러스터에 등록되는 EMCC(Extension Mobility Cross Cluster)와 달리, 로밍 기능을 사용하면 사용자가 방문 중인 클러스터에서 등록을 유지할 수 있습니다.

구성 개요

이 기능을 구축하려면 다음 작업을 수행해야 합니다.

- ILS 네트워크 설정 - ILS는 클러스터 전체에서 디렉터리 번호를 동기화하는 데 사용됩니다.

ILS 구성에 대한 자세한 내용은 <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>

에서 *Cisco Unified Communications Manager*에 대한 시스템 구성 설명서의 클러스터 간 조회 서비스 구성을 참조하십시오.

- 일정한 다이얼 플랜 설정 - ILS 네트워크에서는 일정한 다이얼 플랜이 필요합니다.

다이얼 플랜을 설정하려면 <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>에서 *Cisco Unified Communications Manager*에 대한 시스템 구성 설명서의 다이얼 플랜 구성을 참조하십시오.

- 모든 클러스터에서 디바이스 프로파일 및 사용자 정보를 동기화해야 합니다.
- Extension Mobility를 구성합니다.
- Extension Mobility 사용자에게 대한 로밍 액세스를 구성합니다.
- 슈퍼 사용자 동기화 도구 - 클러스터에서 슈퍼 사용자 정보를 동기화합니다.

클러스터 간 **Extension Mobility** 로밍에 대한 시스템 요구 사항

다음은 Cisco Unified Communications Manager 시스템 요구 사항입니다.

- Cisco Unified Communications Manager 릴리스 12.0(1)SU1 이상
- Cisco Extension Mobility 서비스가 실행되고 있어야 합니다.
- 인터클러스터 Lookup 서비스 (ILS)가 실행되고 있어야 합니다.

클러스터 간 **Extension Mobility** 로밍 로그인

로그인 용어

다음 그림은 클러스터 간 Extension Mobility 로밍의 홈 클러스터와 로밍 클러스터를 보여줍니다.

그림 7: 홈 클러스터와 로밍 클러스터



홈 클러스터

홈 클러스터는 사용자 디바이스 프로파일, 다이얼 플랜 같은 사용자 구성이 있는 클러스터입니다.

로밍 클러스터

로밍 클러스터는 사용자가 홈 클러스터에서와 마찬가지로 Extension Mobility 가능 전화기에 대한 Extension Mobility 로그인을 수행할 수 있는 클러스터입니다.

수퍼유저

수퍼유저는 클러스터 간 표준 **EM** 로밍 수퍼유저 액세스 컨트롤 그룹에 연결된 사용자입니다. 이 사용자에게는 로밍 클러스터에서 Extension Mobility 로그인을 수행할 수 있는 권한이 있으며 전화를 걸거나 받을 수 있습니다.



참고

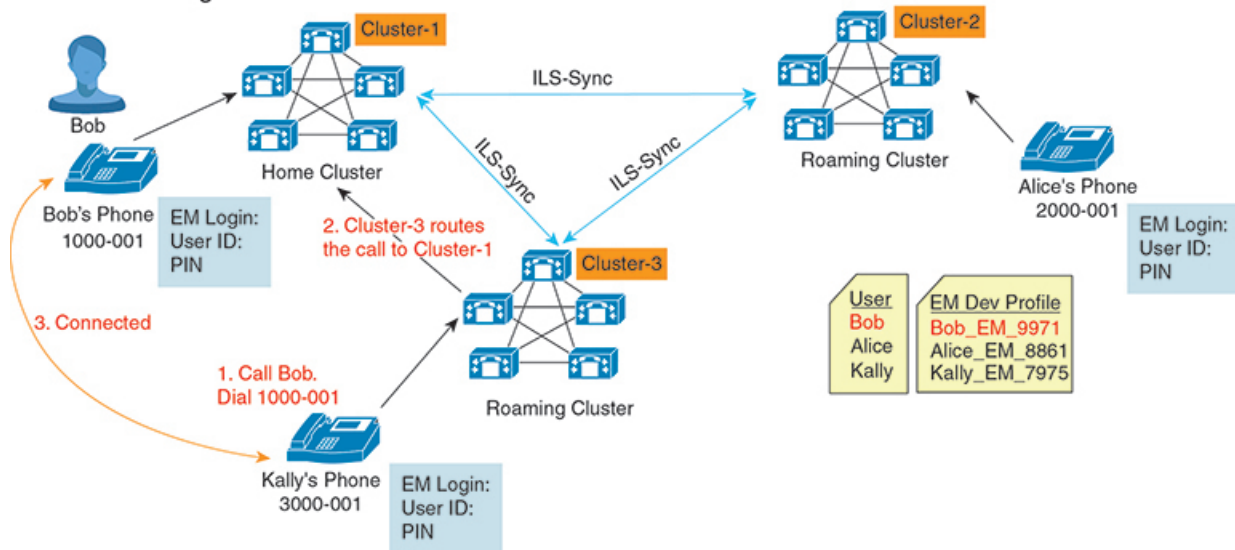
- 사용자가 로그인 중인 클러스터에 관계 없이 모든 클러스터에서 수퍼유저 정보를 공유해야 합니다.
- 클러스터 간에 수퍼유저 정보를 동기화하는 데에는 수퍼유저 동기화 도구라는 웹 기반 애플리케이션 기능이 제공됩니다. 이 동기화는 관리자가 도구에서 구성할 수 있는 예약된 동기화 시간 중에 발생합니다. <https://software.cisco.com>에서 수퍼유저 동기화 도구를 다운로드할 수 있습니다.

로그인 프로세스

Cisco Unified Communications Manager는 여러 클러스터에 걸쳐 생성된 수퍼유저에 대한 Extension Mobility 로그인을 지원합니다. 로밍 클러스터의 Extension Mobility 로그인을 사용하면 수퍼유저가 회선 표시, 서비스, 다이얼 플랜 등의 전화기 설정에 액세스할 수 있습니다. 홈 클러스터에서와 동일한 방식으로 수퍼유저는 로밍 클러스터에서 전화를 걸거나 받을 수 있습니다.

그림 8: 사용자가 홈 클러스터에 있는 경우 통화 흐름

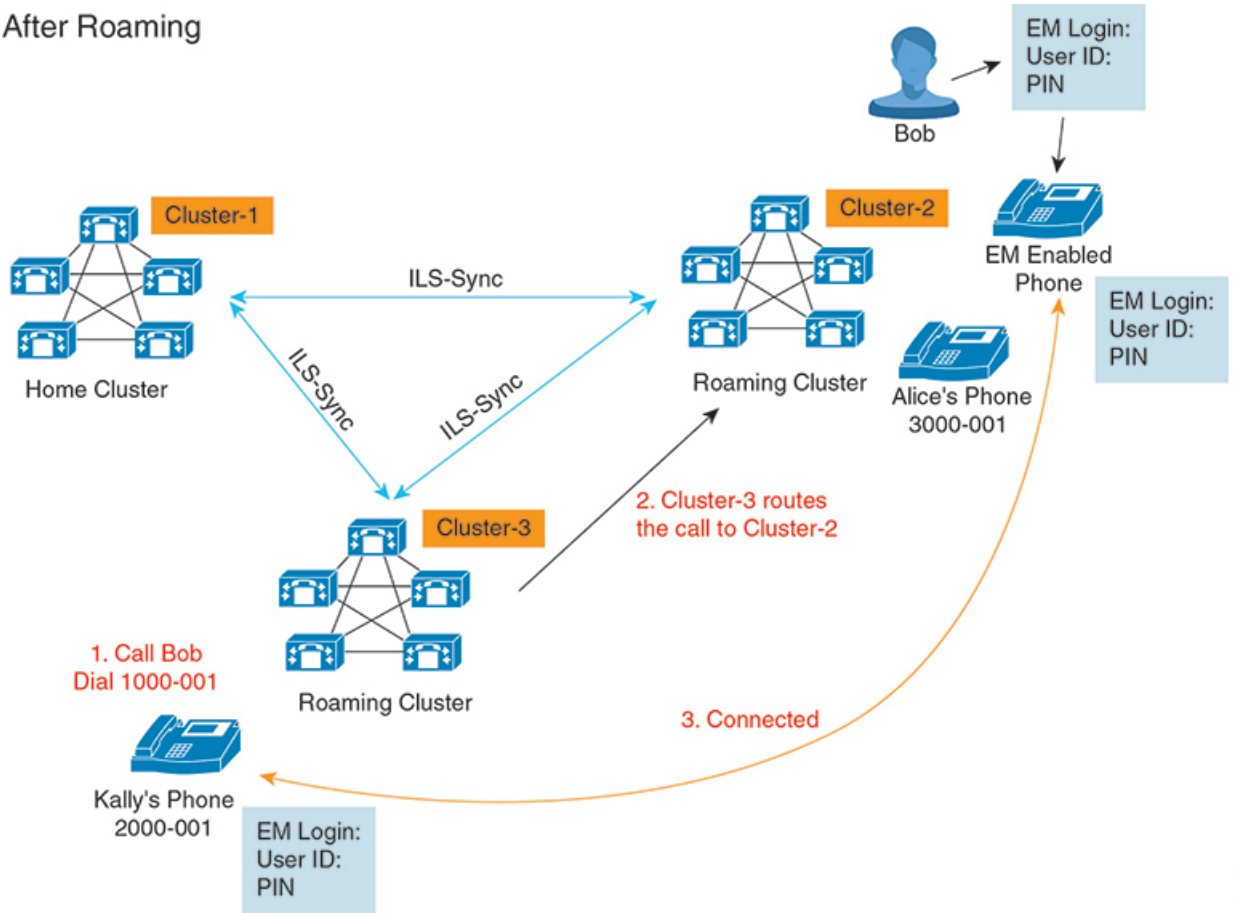
Before Roaming



앞의 그림에서는 Bob의 DN을 1000-001로 가정하고, Alice의 DN을 2000-001로 가정하고, 클러스터 1, 2 및 3에 각각 등록 된 3000-001로 Kally의 DN을 사용합니다. Kally가 Bob의 DN 1000-001에 전화를 걸면 클러스터 3이 통화를 클러스터 1과 Bob 및 Kally로 연결합니다.

그림 9: 사용자가 로밍 클러스터에 있을 때 통화 흐름

After Roaming



Bob의 홈 클러스터가 다운된 것으로 가정하고, 클러스터를 통해 로밍할 수 있는 Bob을 슈퍼유저로 구성합니다. Bob이 클러스터 2로 이동하고 Extension Mobility 로그인을 할 때, 호스팅 전화기가 Bob의 설정에 다시 등록됩니다. 로그인이 성공하면 다른 모든 클러스터는 Bob의 새 위치로 업데이트됩니다. 이제 Kally가 Bob의 DN 1000-01에 전화를 걸면 클러스터 3이 통화를 클러스터 2와 Bob 및 Kally로 연결합니다. 마찬가지로, Bob은 DN 3000-001에 전화를 걸어 Kally와 통화할 수 있습니다.



참고

- 슈퍼유저가 Extension Mobility 기능을 사용하여 다른 클러스터에 로그인하면 사용자가 홈 클러스터에서 자동으로 로그아웃됩니다. 클러스터가 다운된 경우에는 클러스터가 사용자의 이전 로그인에서 로그아웃할 때까지 기다립니다.
- 클러스터 간 Extension Mobility 로밍은 다중 로그인 동작을 지원합니다. 따라서 슈퍼유저는 동일한 클러스터 내에 있는 여러 디바이스에서 로그인할 수 있지만 클러스터 전체에서 로그인할 수는 없습니다.

ILS 상호 작용

Cisco Unified CM 관리에서는 한 쌍의 클러스터에 ILS를 구성하고 이 클러스터를 참가시켜 ILS 네트워크를 형성할 수 있습니다. ILS 네트워크를 설정한 후에는 각 클러스터 간의 연결을 구성하지 않고도 추가 클러스터를 네트워크에 참가시킬 수 있습니다.

Extension Mobility 로그인 또는 로그아웃이 발생할 때마다 ILS 동기화가 사용 가능한 정보를 다른 클러스터로 업데이트하기 시작합니다.



참고 사용자를 슈퍼유저로 구성하면 ILS의 디렉터리 번호 구성에 관계 없이 ILS 동기화가 자동으로 시작됩니다.

자세한 내용은 <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>에서 Cisco Unified Communications Manager에 대한 시스템 구성 설명서의 클러스터 간 조회 서비스 구성 장을 참조하십시오.

클러스터 간 Extension Mobility 로밍 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	Extension Mobility 기능을 지원하는 디바이스를 식별하는 보고서를 생성합니다.
단계 2	다음 하위 작업을 완료하여 Extension Mobility를 구성합니다. <ul style="list-style-type: none"> Extension Mobility 서비스 활성화, 441 페이지 Cisco Extension Mobility 전화 서비스 구성, 441 페이지 사용자에 대한 Extension Mobility 디바이스 프로파일 생성, 442 페이지 사용자에 디바이스 프로파일 연결, 443 페이지 Extension Mobility에 구독, 443 페이지 	Extension Mobility를 구성하면 원격 클러스터에서 로그인할 때 다른 전화기에서 회선 표시, 서비스 및 단축 다이얼과 같은 전화기 설정을 일시적으로 액세스할 수 있습니다. 홈 및 원격 클러스터 모두에서 이 작업 흐름을 수행하면 사용자가 홈 및 원격 클러스터에서 설정에 액세스할 수 있습니다.
단계 3	Extension Mobility 사용자에 대한 로밍 구성, 501 페이지	이 절차를 사용하여 Extension Mobility 사용자에게 동일한 로그인 자격 증명을 사용하는 동시에 ILS 네트워크의 다른 클러스터 간에 로밍할 수 있는 기능을 제공할 수 있습니다.

전화기 기능 목록 생성

구성하려는 기능을 디바이스에서 지원는지 확인하려면 전화기 기능 목록 보고서를 생성합니다.

프로시저

단계 1 Cisco Unified Reporting Administration에서 시스템 보고서를 선택합니다.

단계 2 보고서 목록에서 **Unified CM Phone** 기능 목록을 클릭합니다.

단계 3 다음 단계 중 하나를 수행합니다.

- 새 보고서 생성(막대 차트 아이콘)을 선택하고 새 보고서를 생성합니다.
- 보고서가 이미 있는 경우 **Unified CM** 전화기 기능 목록을 선택합니다.

단계 4 제품 드롭다운 목록에서 모두를 선택합니다.

단계 5 구성하려는 기능의 이름을 클릭합니다.

단계 6 제출을 클릭하여 보고서를 생성합니다.

Extension Mobility 서비스 활성화

프로시저

단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. 도구 > 서비스 활성화.

단계 2 서버 드롭다운 목록에서 필요한 노드를 선택합니다.

단계 3 다음과 같은 서비스를 활성화합니다.

- a) Cisco CallManager
- b) Cisco Tftp
- c) Cisco Extension Mobility
- d) ILS 서비스

참고 ILS 서비스를 활성화하려면 퍼블리셔 노드를 선택해야 합니다.

단계 4 저장을 클릭합니다.

단계 5 확인을 클릭합니다.

Cisco Extension Mobility 전화 서비스 구성

사용자가 나중에 가입하여 내선 기능에 액세스할 수 있는 Extension Mobility IP 전화 서비스를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화 서비스.

단계 2 새로 추가를 클릭합니다.

단계 3 서비스 이름 필드에 서비스의 이름을 입력합니다.

단계 4 서비스 URL 필드에 서비스 URL을 입력합니다.

형식은 `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#`입니다. IP 주소는 Cisco Extension Mobility가 활성화되어 실행되고 있는 Unified Communications Manager의 IP 주소입니다.

IPv4 또는 IPv6 주소일 수 있습니다.

예제:

`http://123.45.67.89:8080/emapp/EMAppServlet?device=#DEVICENAME#`

예제:

`http://[2001:0001:0001:0067:0000:0000:0000:0134]:8080/emapp/EMAppServlet?device=#DEVICENAME#`

이 형식은 사용자 ID 및 PIN을 사용하여 로그인하도록 허용합니다. Extension Mobility 서비스에 가입한 IP 전화 사용자의 경우 추가 로그인 옵션을 구성할 수 있습니다. 추가 로그인 옵션을 구성하려면 `loginType` 매개 변수를 서비스 URL에 다음 형식으로 추가합니다.

- `loginType=DN`을 사용하면 기본 내선 번호와 PIN을 사용하여 로그인할 수 있습니다.

서비스 URL 형식: `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=DN.`

- `loginType=SP`를 사용하면 셀프 서비스 사용자 ID와 PIN을 사용하여 로그인할 수 있습니다.

서비스 URL 형식: `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=SP.`

- `loginType=UID`를 사용하면 사용자 ID와 PIN을 사용하여 로그인할 수 있습니다.

서비스 URL 형식: `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=UID.`

`loginType`을 URL의 끝에 추가하지 않는 경우 표시된 기본 로그인 옵션은 사용자 ID 및 PIN입니다.

단계 5 서비스 유형 필드에서 서비스를 [서비스], [디렉터리] 또는 [메시지] 버튼 중 어떤 항목으로 설정할지 선택합니다.

단계 6 저장을 클릭합니다.

사용자에 대한 **Extension Mobility** 디바이스 프로파일 생성

Extension Mobility 디바이스 프로파일을 구성합니다. 이 프로파일은 사용자가 Extension Mobility에 로그인할 때 실제 디바이스에 매핑하는 가상 디바이스의 역할을 합니다. 물리적 디바이스는 이 프로파일의 특성에 적용됩니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 디바이스 프로파일.

단계 2 다음 작업 중 하나를 수행합니다.

- 찾기 를 클릭하여 설정을 수정하고 결과 목록에서 기존 디바이스 프로파일을 선택합니다.
- 새 디바이스 프로파일을 추가하려면 새로 추가를 클릭하고 디바이스 프로파일 유형에서 옵션을 선택합니다. 다음을 클릭합니다.
- 디바이스 프로토콜 드롭다운 목록에서 디바이스 프로토콜을 선택하고 다음을 클릭합니다.

단계 3 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

단계 5 연결 정보 섹션에서 새 **DN** 추가를 클릭합니다.

단계 6 디렉터리 번호 필드에 디렉터리 번호를 입력하고 저장을 클릭합니다.

단계 7 재설정을 클릭하고 프롬프트에 따릅니다.

사용자에 디바이스 프로파일 연결

설정을 다른 전화기에서 액세스할 수 있도록 디바이스 프로파일을 사용자와 연결합니다. 실제 디바이스를 연결하는 것과 동일한 방법으로 사용자 디바이스 프로파일을 사용자와 연결합니다.



팁 BAT(벌크 관리 도구)를 사용하여 Cisco Extension Mobility의 사용자 디바이스 프로파일을 한 번에 여러 개 추가하거나 삭제할 수 있습니다. [Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서](#)를 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 사용자에 대한 설정을 수정하려면 찾기를 클릭하고 검색 기준을 입력한 후 결과 목록에서 기존 사용자를 선택합니다.
- 새로 추가를 클릭하여 새 사용자를 추가합니다.

- 단계 3 **Extension Mobility**에서 사용자가 만든 디바이스 프로파일을 찾아 사용 가능한 프로파일을 제어되는 프로파일로 이동합니다.
- 단계 4 홈 클러스터 확인란을 선택합니다.
- 단계 5 저장을 클릭합니다.

Extension Mobility에 구독

사용자가 **Extension Mobility**에 로그인하고, 로그아웃할 수 있도록 IP 전화기 및 디바이스 프로파일을 **Extension Mobility** 서비스에 가입합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 작업 중 하나를 수행합니다.

- 디바이스 > 전화기를 선택하고 검색 조건을 지정한 후 찾기를 클릭하고 **Extension Mobility**에 사용할 전화기를 선택합니다.
- 디바이스 > 디바이스 설정 > 디바이스 프로파일을 선택하고 검색 조건을 지정하고 찾기를 클릭하고 사용자가 만든 디바이스 프로파일을 선택합니다.

단계 2 관련 링크 드롭다운 목록에서 서비스 가입/가입 해지를 선택하고 이동을 클릭합니다.

단계 3 서비스 선택 드롭다운 목록 상자에서 **Extension Mobility** 서비스를 선택합니다.

단계 4 다음을 클릭합니다.

단계 5 가입을 클릭합니다.

단계 6 저장을 클릭하고 팝업 창을 닫습니다.

Extension Mobility 사용자에게 대한 로밍 구성

이 절차를 사용하여 **Extension Mobility** 사용자에게 동일한 로그인 자격 증명을 사용하는 동시에 ILS 네트워크의 다른 클러스터 간에 로밍할 수 있는 기능을 제공할 수 있습니다. 이렇게 하려면 선택한 사용자를 클러스터 간 표준 **EM** 로밍 슈퍼유저 액세스 컨트롤 그룹에 할당해야 합니다.

시작하기 전에

클러스터 전체에서 사용자 및 로그인 정보를 복제하는 데 사용되므로 ILS 네트워크를 설정해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 사용자 관리 > 사용자 설정 > 액세스 컨트롤 그룹을 선택합니다.

단계 2 찾기를 클릭하고 클러스터 간 표준 **EM** 로밍 슈퍼유저 그룹을 선택합니다.

단계 3 그룹에 최종 사용자 추가 버튼을 클릭합니다. 사용자 찾기 및 나열 팝업 창이 표시됩니다.

단계 4 찾기를 클릭하고 로밍 기능을 제공할 사용자를 모두 선택합니다.

단계 5 선택한 항목 추가를 클릭합니다.

클러스터 간 **Extension Mobility** 상호 작용 및 제한 사항

클러스터 간 **Extension Mobility** 상호 작용

이 섹션에는 Extension Mobility Cross Cluster와 기타 Cisco Unified Communications Manager 관리 구성 요소의 상호 작용이 있습니다.

- Extension Mobility
- ILS(Inter-Cluster Lookup Service)

클러스터 간 **Extension Mobility** 상호 작용 제한 사항

이 섹션에는 Extension Mobility Cross Cluster와 기타 Cisco Unified Communications Manager 관리 구성 요소의 제한 사항이 있습니다.

- 허브 ILS가 다운된 경우 연결된 스포크는 허브가 다시 재생될 때까지 동기화되지 않습니다.

다른 유형의 **Extension Mobility**

다음 표에서는 Cisco Unified Communications Manager에서 사용할 수 있는 다양한 유형의 Extension Mobility 기능과 그 차이점을 보여줍니다.

표 45: 클러스터 간 **EM**, **EMCC** 및 **Extension Mobility** 로밍의 차이

	EM(Extension Mobility)	EMCC(Extension Mobility Cross Cluster)	클러스터 간 Extension Mobility 로밍
설명	사용자가 동일한 클러스터에 있는 다른 전화기에서 전화기 설정에 일시적으로 액세스할 수 있습니다.	사용자가 다른 클러스터에 있는 전화기에서 전화기 설정에 액세스할 수 있습니다.	사용자가 자신의 로그인 인증서를 사용하여 다른 클러스터 간에 로밍할 수 있습니다.
사용자가 다른 클러스터의 전화기에 로그인하는 경우	해당 없음	원격 클러스터 전화기가 홈 클러스터의 설정에 액세스하여 사용자의 홈 클러스터에 등록됩니다.	로밍 클러스터 전화기는 로밍 클러스터에만 등록됩니다.
클러스터 간	단일 클러스터 전용	다중 클러스터	다중 클러스터

	EM(Extension Mobility)	EMCC(Extension Mobility Cross Cluster)	클러스터 간 Extension Mobility 로밍
구성	단일 클러스터 전용	EMCC는 홈 클러스터와 사용자가 방문하는 각 클러스터에서 구성되어야 합니다.	모든 클러스터에서 Extension Mobility 로밍이 구성되어 있어야 합니다.
사용자 정보	단일 클러스터 전용	모든 클러스터에서 유지 관리되어야 합니다.	모든 클러스터에서 수퍼유저 정보가 유지 관리됩니다.

클러스터 간 Extension Mobility 문제 해결

이 섹션에는 EMap 및 EService의 오류 코드에 관한 내용이 있습니다.

인증 오류

문제 “오류 201 인증 오류”가 전화기에 표시됩니다.

해결 방법 사용자는 올바른 사용자 ID와 PIN이 입력되었는지 확인하고 시스템 관리자에게 사용자 ID 및 PIN이 올바른지 확인해야 합니다.

빈 사용자 ID 또는 PIN

문제 “오류 202 빈 사용자 ID 또는 PIN”이 전화기에 나타납니다.

해결 방법 올바른 사용자 ID 및 PIN을 입력합니다.

통화 중입니다. 다시 시도하십시오.

문제 “오류 26 통화 중. 다시 하십시오”가 전화기에 나타납니다.

해결 방법 동시 로그인 및 로그아웃 요청 수가 최대 동시 요청 서비스 매개 변수보다 큰지 확인합니다. 이 경우, 동시 요청 수를 줄입니다.



참고

동시 로그인 및 로그아웃 요청 수를 확인하려면 Cisco Unified Real-Time Monitoring Tool을 사용하여 Extension Mobility 개체의 진행 중인 요청 카운터를 봅니다. 자세한 내용은 다음 위치에서 Cisco Unified Real Time Monitoring Tool 관리 지침서를 참조하십시오. <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

데이터베이스 오류

문제 “오류 6 데이터베이스 오류”가 전화기에 표시됩니다.

해결 방법 많은 수의 요청이 있는지 여부를 확인합니다. 많은 수의 요청이 있는 경우 Extension Mobility 개체 카운터에서 진행 중인 요청 카운터가 높은 값을 표시합니다. 많은 수의 동시 요청으로 인해 요청이 거부되는 경우 조정된 요청도 높은 값을 표시합니다. 자세한 데이터베이스 로그를 수집합니다.

디바이스에 로그인할 수 없음

문제 “오류 22 디바이스에 로그인할 수 없음”이 전화기에 나타납니다.

해결 방법 전화기 구성 창에서 **Extension Mobility** 활성화 확인란을 선택했는지 확인합니다(디바이스 > 전화기).

빈 디바이스 이름

문제 “오류 207 빈 디바이스 이름”이 전화기에 나타납니다.

해결 방법 Cisco Extension Mobility에 대해 구성된 URL이 올바른지 확인합니다. 자세한 내용은 관련 항목 섹션을 참조하십시오.

관련 항목

[Cisco Extension Mobility 전화 서비스 구성](#), 441 페이지

EMService 연결 오류

문제 “오류 207 EMService 연결 오류”가 전화기에 나타납니다.

해결 방법 Cisco Unified에 Serviceability에서 도구 > 제어 센터 - 기능을 선택하여 Cisco Extension Mobility 서비스가 실행되고 있는지 확인합니다.

호스트를 찾을 수 없음

문제 “호스트를 찾을 수 없음” 오류 메시지가 전화기에 나타납니다.

해결 방법 Cisco Unified에 Serviceability에서 도구 > 제어 센터 - 네트워크 서비스를 선택하여 Cisco Tomcat 서비스가 실행되고 있는지 확인합니다.

HTTP 오류

문제 HTTP 오류 (503)가 전화기에 표시됩니다.

해결 방법

- 서비스 버튼을 누르면 이 오류가 발생하는 경우 Cisco Unified Serviceability에서 도구 > 제어 센터 - 네트워크 서비스를 선택하여 Cisco IP Phone Services 서비스가 실행 중인지 확인합니다.

- Extension Mobility 서비스를 선택하면 이 오류가 발생하는 경우 Cisco Unified Serviceability에서 도구 > 제어 센터 - 네트워크 서비스를 선택하여 Cisco Extension Mobility Application 서비스가 실행 중인지 확인합니다.

전화기 재설정

문제 사용자가 로그인 또는 로그아웃 하면 전화는 다시 시작하는 대신에 재설정합니다.

가능한 원인 로컬 변경이 재설정의 가능한 원인입니다.

해결 방법 추가 작업은 필요하지 않습니다. 로그인한 사용자 또는 프로파일과 연결된 사용자 로컬이 해당 로컬 또는 디바이스와 동일하지 않을 경우, 성공적으로 로그인한 후, 전화기가 재시작되고 재설정됩니다. 이 패턴은 전화기 구성 파일이 다시 빌드되기 때문에 발생합니다.

로그인한 후 전화 서비스를 사용할 수 없음

문제 로그인 후 사용자가 전화 서비스를 사용할 수 없습니다.

가능한 원인 이 문제는 사용자 프로파일이 전화기에 로드되었을 때 연결된 서비스가 없기 때문에 발생합니다.

해결 방법

- 사용자 프로파일에 Cisco Extension Mobility 서비스가 포함되어 있는지 확인하십시오.
- 사용자가 로그인하는 전화기의 구성을 Cisco Extension Mobility를 포함하도록 변경합니다. 전화기를 업데이트한 후 사용자가 전화 서비스에 액세스할 수 있습니다.

로그아웃한 후 전화 서비스를 사용할 수 없음

문제 사용자가 로그아웃하고 전화기가 기본 디바이스 프로파일로 전환되면 전화 서비스를 더 이상 사용할 수 없게 됩니다.

해결 방법

- 자동 디바이스 프로파일과 전화기 구성 간에 동기화 엔터프라이즈 매개 변수가 **True**로 설정되었는지합니다.
- 전화기를 Cisco Extension Mobility 서비스에 가입합니다.

사용자가 다른 위치에서 로그인

문제 “오류 25 사용자가 다른 위치에서 로그인”이 전화기에 표시됩니다.

해결 방법 사용자가 다른 전화기로 로그인했는지 여부를 확인하십시오. 멀티 로그인을 허용해야 하는 경우 멀티 로그인 동작 서비스 매개 변수가 멀티 로그인 허용으로 설정되었는지 확인합니다.

사용자 프로파일 부재

문제 “오류 205 사용자 프로파일 부재”가 전화기에 나타납니다.

해결 방법 사용자에게 디바이스 프로파일을 연결합니다.



35 장

보류 복귀

- 보류 복귀 개요, 507 페이지
- 보류 복귀 사전 요건, 508 페이지
- 보류 복귀 구성 작업 흐름, 508 페이지
- 보류 복귀 상호 작용, 511 페이지
- 보류 복귀 제한 사항, 512 페이지

보류 복귀 개요

통화를 보류했을 때 보류된 통화가 구성된 시간 제한을 초과할 경우 보류 복귀는 사용자에게 알려주는 기능입니다. 구성된 시간 제한이 만료되면 전화기에서 통화를 처리하라는 알림을 생성합니다.

다음 알림을 사용할 수 있습니다.

- 전화기 벨소리 또는 경고음을 한 번 울립니다.
- 상태 표시줄에 “보류 복귀”가 표시됩니다.
- 회선 버튼 옆에 있는 LED가 계속 깜박입니다.
- 진동하는 핸드셋 아이콘이 표시됩니다.



참고 수신되는 알림 유형은 전화기의 기능에 따라 다릅니다.

되돌려진 통화를 검색하려면 다음을 수행할 수 있습니다.

- 핸드셋을 듭니다.
- 전화기의 스피커 버튼을 누릅니다.
- 헤드셋 버튼을 누릅니다.
- 되돌려진 통화와 연결된 회선을 선택합니다.
- 재개 소프트웨어를 누릅니다.

자세한 내용은 특정 전화기 모델의 사용 설명서를 참조하십시오.

보류 복귀 사전 요건

- Cisco CallManager 서비스가 클러스터에 있는 하나 이상의 노드에서 실행 중이어야 함
- Cisco CTIManager 서비스가 클러스터에 있는 하나 이상의 노드에서 실행 중이어야 함
- Cisco Database Layer Monitor 서비스가 Cisco CallManager 서비스와 동일한 노드에서 실행 중이어야 함
- Cisco RIS Data Collector 서비스가 Cisco CallManager 서비스와 동일한 노드에서 실행 중이어야 함
- Cisco Tftp 서비스가 클러스터에 있는 하나 이상의 노드에서 실행 중이어야 함
- Cisco Unified Communications Manager 로컬 설치 관리자가 설치되어 있어야 함(영어 이외의 전화기 로컬 또는 국가별 신호음을 사용하고자 하는 경우)

보류 복귀 구성 작업 흐름

다음 단계에 따라 전화기의 보류 복귀 기능을 구성합니다. 이 절차에서는 전화기에 대한 디렉터리 번호를 구성했거나 자동 등록을 사용 중이라고 가정합니다.

시작하기 전에

- 전화기 사용자가 보류 복귀 메시지를 영어 외의 언어로 표시하려는 경우나 사용자에게 통화에 대해 국가별 신호음을 제공하려는 경우 로컬 설치 관리자를 설치했는지 확인합니다.
- [보류 복귀 사전 요건, 508 페이지](#) 검토

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	전화기 기능 목록 보고서를 실행하여 보류 복귀 기능을 지원하는 전화기를 확인합니다.
단계 2	보류 복귀를 위한 통화 포커스 우선 순위 구성, 509 페이지	전화기의 디바이스폴에 대해 통화 포커스 우선 순위 설정을 구성합니다.
단계 3	<p>다음 절차 중 하나를 수행합니다.</p> <ul style="list-style-type: none"> • 클러스터에 대한 보류 복귀 타이머 기본 값 구성, 509 페이지 • 전화기에 대한 보류 복귀 타이머 설정 구성, 510 페이지 	<p>보류 복귀 타이머 설정을 구성합니다. 클러스터 수준 서비스 매개 변수를 사용하여 타이머를 구성하거나 개별 전화 회선에서 설정을 구성할 수 있습니다.</p> <p>참고 개별 전화 회선의 설정이 클러스터 수준 서비스 매개 변수 설정보다 우선합니다.</p>

보류 복귀를 위한 통화 포커스 우선 순위 구성

관리자는 수신 통화와 되돌려진 통화의 우선 순위를 지정할 수 있습니다. 기본적으로 모든 수신 통화는 되돌려진 통화 전에 처리되지만, 통화 포커스 우선 순위를 변경하여 되돌려진 통화가 우선 처리되도록 할 수 있습니다.

시작하기 전에

[전화기 기능 목록 생성, 7 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 디바이스폴을 선택하고 전화기에 적용되는 디바이스폴을 엽니다.

단계 2 되돌려진 통화 포커스 우선 순위 필드에서 다음 설정 중 하나를 선택하고 저장을 클릭합니다.

- 기본값 - 수신 통화가 되돌려진 통화보다 우선합니다.
- 최고 - 되돌려진 통화가 수신 통화보다 우선합니다.

단계 3 저장을 클릭합니다.

단계 4 다음 단계를 수행하여 디바이스폴의 디바이스를 재설정합니다.

- a) 재설정을 클릭합니다. 디바이스 재설정 창이 표시됩니다.
- b) 디바이스 재설정 창에서 재설정을 클릭합니다.

다음에 수행할 작업

다음 절차 중 하나를 수행하여 보류 복귀 타이머 설정을 구성합니다.

- [클러스터에 대한 보류 복귀 타이머 기본값 구성, 509 페이지](#)
- [전화기에 대한 보류 복귀 타이머 설정 구성, 510 페이지](#)

클러스터에 대한 보류 복귀 타이머 기본값 구성

이 절차를 수행하여 클러스터의 모든 전화기에 대한 보류 복귀 타이머 기본 설정을 적용하는 클러스터 수준 서비스 매개 변수를 구성합니다.



참고 클러스터 수준 서비스 매개 변수를 구성하는 경우 구성이 클러스터의 모든 전화기에 대해 기본 보류 복귀 설정으로 적용됩니다. 그러나 개별 전화기 회선의 설정이 클러스터 수준 기본값을 무시할 수 있습니다.

시작하기 전에

[보류 복귀를 위한 통화 포커스 우선 순위 구성, 509 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 **CallManager** 서비스를 실행하고 있는 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 다음 클러스터 수준 서비스 매개 변수에 대한 값을 구성합니다.

- 보류 복귀 지속 시간 - 0 ~ 1200(포함) 사이의 번호를 입력하여 Cisco Unified Communications Manager가 보류 중인 상대방 전화기에 대해 복귀된 통화 알림을 발행하기 전까지의 대기 시간(초)을 지정합니다. 0을 입력하면 전화기 회선에 구성된 경우를 제외하고 Cisco Unified Communications Manager에서 복귀된 통화 알림을 발행하지 않습니다.
- 보류 복귀 간격 알림 - 0 ~ 1200(포함) 사이의 번호를 입력하여 Cisco Unified Communications Manager가 보류 중인 상대방 전화기에 주기적 미리 알림 경고를 보내는 대기 시간(초)을 지정합니다. 0을 입력하면 전화기 회선에 타이머가 구성되어 있지 않은 경우 Cisco Unified Communications Manager에서 주기적인 미리 알림 경고를 보내지 않습니다.

단계 5 저장을 클릭합니다.

전화기에 대한 보류 복귀 타이머 설정 구성

전화기 및 전화 회선에 대한 보류 복귀 타이머 설정을 구성하려면 이 절차를 수행합니다.



참고 클러스터 수준 서비스 매개 변수를 사용하여 보류 복귀 타이머 설정을 구성할 수도 있습니다. 그러나 개별 전화 회선의 설정이 클러스터 수준 서비스 매개 변수 설정보다 우선합니다.

시작하기 전에

보류 복귀 클러스터 수준 기본값을 구성하려면 [클러스터에 대한 보류 복귀 타이머 기본값 구성, 509 페이지](#)를(를) 수행합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 2 찾기를 클릭하고 보류 복귀를 구성할 전화기를 선택합니다.

단계 3 왼쪽의 연결 창에서 보류 복귀를 구성할 전화 회선을 클릭합니다.

단계 4 다음 필수 필드에 대한 값을 구성합니다.

- 보류 복귀 벨소리 지속 시간 - 0~1200(포함) 사이의 번호를 입력하여 Cisco Unified Communications Manager가 복귀된 통화 경고를 발행하기 전까지의 대기 시간(초)을 지정합니다. 0을 입력하면 Cisco Unified Communications Manager에서 이 DN으로 복귀된 통화 경고를 발행하지 않습니다. 필드를 비워두면(기본 설정) Cisco Unified Communications Manager가 보류 복귀 기간 서비스 매개 변수의 설정을 적용합니다.
- 보류 복귀 벨소리 간격 알림 - 0~1200(포함) 사이의 번호를 입력하여 Cisco Unified Communications Manager가 주기적 미리 알림 경고를 보내는 대기 시간(초)을 지정합니다. 0의 값을 입력하면 Cisco Unified Communications Manager에서 미리 알림 경고를 보내지 않습니다. 필드를 비워두면(기본 설정) Cisco Unified Communications Manager가 보류 복귀 간격 알림 서비스 매개 변수의 설정을 적용합니다.

단계 5 저장을 클릭합니다.

단계 6 다음 단계를 수행하여 전화기를 재설정합니다.

- a) 재설정을 클릭합니다. 디바이스 재설정 창이 표시됩니다.
- b) 재설정을 클릭합니다.

보류 복귀 상호 작용

표 46: 보류 복귀 기능 상호 작용

기능	상호 작용
MoH(대기 중 음악 제공 서비스)	일반 보류된 통화에 대해 MOH가 구성된 경우 회선 호에서 MOH가 지원됩니다.
통화 지정보류	보류 복귀가 호출되고 보류된 상대방이 지정보류 소프트웨어를 누를 경우 보류 중인 상대방은 계속해서 보류 복귀 경고를 수신하며 통화를 가져올 수 있습니다. 보류하는 당사자가 통화를 가져오면 MOH를 수신합니다(구성된 경우). 보류 기간이 구성된 시간 제한을 초과하기 전에 보류된 당사자가 지정보류될 경우 시스템은 해당 통화를 당겨받거나 재전송할 때까지 모든 보류 복귀 경고를 표시하지 않습니다.
MLPP	MLPP(Multilevel Precedence and Preemption) 통화가 보류 중으로 설정되고 복귀되면 MLPP 통화의 선점 상태가 손실되고 복귀된 통화가 루틴 통화로 간주됩니다. 통화가 복귀되면 시스템은 선점 벨소리를 재생하지 않습니다. 우선 순위가 높은 통화가 복귀된 통화가 되는 경우에는 시스템에서 우선 순위 신호음을 재생하지 않습니다.

기능	상호 작용
CTI 애플리케이션	<p>회선 또는 시스템에 대해 보류 복귀 기능이 활성화되면 CTI 애플리케이션에서 해당 기능에 액세스할 수 있습니다. Cisco Unified Communications Manager Assistant, 전화 교환 콘솔과 같이 Cisco에서 제공한 애플리케이션은 CTI 인터페이스를 이용한 보류 복귀 기능을 제공합니다.</p> <p>보류 복귀가 호출되면 CTI 포트는 Cisco Unified IP Phones에 표시되는 신호음 대신 이벤트 알림을 수신합니다. CTI 포트와 라우트 포인트는 이벤트 알림을 한 번만 수신하며, Cisco Unified IP Phone은 정기 간격으로 알림을 수신합니다.</p> <p>CTI 요구 사항 및 보류 복귀와의 상호 작용에 대한 자세한 내용은 다음 API 설명서를 참조하십시오.</p> <ul style="list-style-type: none"> • Cisco Unified Communications JTAPI 개발자 설명서 • Cisco Unified Communications TAPI 개발자 설명서
SIP 전화기와 상호 작용할 때 SCCP 전화기에 대한 보류 복귀 간격	SCCP 전화기는 최소 HRNI(보류 복귀 통보 간격)로 5초를 지원하지만 SIP 전화기는 최소 10초를 지원합니다. 최소 HRNI가 5초로 설정된 SCCP 전화기에서는 SIP 전화기가 포함된 통화를 처리할 때 10초의 보류 복귀 통보 벨소리 지연이 발생할 수 있습니다.
공유 회선	<p>보류 복귀를 지원하는 Cisco Unified IP Phone이 보류 복귀를 지원하지 않는 전화기 디바이스와 회선을 공유할 경우 보류 복귀 구성 설정은 지원되는 디바이스의 회선에 대해서만 표시됩니다.</p> <p>공유된 회선 디바이스에서 이 기능을 비활성화할 경우 해당 회선을 공유하는 다른 모든 디바이스에서 보류 복귀가 비활성화됩니다.</p>
벨소리 설정	전화기에 구성된 벨소리 설정이 [사용 안 함]으로 설정된 경우 전화기가 보류 복귀 기능에 대해 벨소리, 깜박임 또는 경고음을 발생하지 않습니다.

보류 복귀 제한 사항

기능	제한 사항
Cisco Extension Mobility 및 Cisco Web Dialer	Cisco Extension Mobility 및 Cisco Web Dialer 기능은 보류 복귀 기능을 지원하지 않습니다.
SCCP 전화기	<p>이 기능은 ATA 186, DPA-7610, DPA-7630과 같은 SCCP 아날로그 전화기 유형을 지원하지 않습니다.</p> <p>노드에서 SCCP를 실행하는 특정 온넷 전화 디바이스만 보류 복귀 기능을 호출할 수 있습니다.</p>
디렉터리 번호	디렉터리 번호가 보류 복귀를 지원하지 않는 전화기에 연결된 경우 디렉터리 번호 구성 창에 해당 디렉터리 번호에 대한 기능 설정이 표시되지 않습니다.

기능	제한 사항
공유 회선	<p>보류 복귀를 지원하는 Cisco Unified IP Phone이 보류 복귀를 지원하지 않는 전화기 디바이스와 회선을 공유할 경우 보류 복귀 구성 설정은 지원되는 디바이스의 회선에 대해서만 표시됩니다.</p> <p>공유된 회선 디바이스에서 이 기능을 비활성화할 경우 이 회선을 공유하는 나머지 디바이스에서 보류 복귀가 비활성화됩니다.</p>
벨소리 설정	<p>보류 복귀 벨소리는 플래시가 한 번 깜박임으로 변환되고 벨소리가 한 번 울림으로 변환되는 것을 제외하고 Cisco 통합 커뮤니케이션 매니저 관리에서 해당 사용자에게 대해 정의한 벨소리 설정(비활성화, 깜박임만, 한 번 울림, 벨울림, 경고음만)을 사용합니다.</p> <p>참고 IP 전화기 통화가 정상 보류 상태가 되면 통화 관리자로부터 벨소리 설정(전화 유휴)이 적용됩니다.</p>
되돌리기 통화의 최대 수	한 회선의 최대 복귀 통화 수는 해당 시스템의 최대 통화 수와 같습니다.
CTI 애플리케이션	<p>CTI 애플리케이션에서 이 기능을 활성화하려면, CTI 애플리케이션이 이 기능과 이 릴리스를 지원하도록 인증되었는지 확인하십시오. 그렇지 않으면, 보류 복귀 기능이 기존 CTI 애플리케이션에 영향을 미칠 수 있으므로, CTI 애플리케이션에 장애가 발생할 수 있습니다. 이 기능은 기본적으로 비활성화됩니다. CTI 요구 사항에 대한 정보는 다음 API 문서를 참조하십시오.</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager용 Cisco Unified TAPI 개발자 설명서 • Cisco Unified Communications Manager용 Cisco Unified JTAPI 개발자 설명서
Cisco Unified IP Phone	<p>이 기능을 지원하는 전화기와 연결된 DN에는 보류 복귀 설정을 구성할 수 없습니다. 보류 복귀 기능을 지원하는 Cisco Unified IP Phone만 [디렉터리 번호 구성] 창에 보류 복귀 타이머 설정을 표시합니다.</p> <p>시스템에 대해 보류 복귀가 구성된 경우 전화기가 기능을 지원해야 합니다. 그렇지 않으면 기능이 활성화되지 않습니다.</p> <p>보류 복귀에 관한 전화기 제한 사항은 보류 복귀와 Unified Communications Manager의 이 버전을 지원하는 Cisco Unified IP Phone 모델에 대한 Cisco Unified IP Phone 관리 지침서를 참조하십시오.</p>



36 장

헌트 그룹 액세스

- 헌트 그룹 개요, 515 페이지
- 헌트 그룹 사전 요건, 516 페이지
- 헌트 그룹 구성 작업 흐름, 516 페이지
- 헌트 그룹 상호 작용, 522 페이지
- 헌트 그룹 제한 사항, 522 페이지

헌트 그룹 개요

헌트 그룹은 계층 구조로 구성된 회선 그룹으로, 헌트 그룹 목록의 첫 번째 번호를 사용 중인 경우 시스템이 두 번째 번호로 전화를 겁니다. 두 번째 번호가 통화 중인 경우 시스템은 다음 번호를 다이얼하는 방식으로 전화를 겁니다.

전화기 사용자는 IP 전화기에서 헌트로그 소프트키 또는 헌트 그룹 회선 버튼을 사용하여 헌트 그룹에 로그인하거나 로그아웃할 수 있습니다. 전화기는 로그인 상태의 시각적 상태를 제공하므로 사용자가 하나 이상의 회선 그룹에 로그인되어 있는지 여부를 확인할 수 있습니다.

헌트 그룹 기능은 다음 기능을 제공합니다.

- IP 전화기의 헌트로그 소프트키를 사용하면 사용자가 전화기의 로그인 및 로그아웃을 전환할 수 있습니다.
- 헌트 그룹을 사용하면 발신자가 내선 번호 중에서 사용 가능한 회선을 자동으로 찾을 수 있습니다.
- 헌트 그룹 로그 오프 기능을 사용하면 전화기 사용자가 디렉터리 번호로 라우팅되는 수신 통화를 수신하지 못하도록 할 수 있습니다. 전화기 상태와 상관 없이 전화기는 전화기와 연결된 하나 이상의 회선 그룹으로 통화되지 않는 수신 통화에 대해 정상적으로 울립니다.



참고 DN(디렉터리 번호)은 전화기와 연결된 회선 그룹에 속합니다.

- 시스템 관리자는 헌트 그룹에 자동으로 로그인되어 있는 전화기에 사용자를 로그인하거나 로그아웃할 수 있습니다.

- 힌트로그 소프트키를 사용하면 전화기 사용자가 전화기 디렉터리 번호가 속하는 모든 회선 그룹에서 전화기를 로그아웃할 수 있습니다.
- Cisco Unified Communications Manager 릴리스 9.0 이후부터 힌트 그룹 로그오프 기능을 사용하면 모바일 디바이스를 데스크폰으로 사용할 수 있습니다. 모바일 클라이언트를 통해 힌트로그 소프트키를 사용하면 힌트 파일럿에 전송되는 통화를 더 이상 수신하지 않습니다.

힌트 그룹 사전 요건

- 전화기는 SCCP(Skinny Client Control Protocol) 또는 SIP(Session Initiation Protocol)를 실행하고 있어야 합니다.
- 전화기 벨소리 파일은 TFTP 디렉터리(/usr/local/cm/tftp)에 위치해야 합니다.

힌트 그룹 구성 작업 흐름

시작하기 전에

- [힌트 그룹 사전 요건, 516 페이지](#) 검토

프로시저

	명령 또는 동작	목적
단계 1	힌트 그룹을 위한 소프트키 템플릿 구성, 517 페이지	HLog 소프트키를 사용하여 소프트키 템플릿 구성
단계 2	<p>소프트키 템플릿을 일반 디바이스 구성에 연결, 518 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> • 소프트키 템플릿을 일반 디바이스 구성에 추가, 519 페이지 • 일반 디바이스 구성을 전화기에 연결, 519 페이지 	(선택 사항) 전화기에서 소프트키 템플릿을 사용할 수 있게 하려면 이 단계 또는 다음 단계를 완료해야 합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 이 단계를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.
단계 3	소프트키 템플릿을 전화기에 연결, 520 페이지	(선택 사항) 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하거나 일반 디바이스 구성과 함께 연결하는 대신 사용할 수 있습니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우 일반 디바이스 구성과 함께 이 절차를 사용합니다.

	명령 또는 동작	목적
단계 4	힌트 그룹을 위한 전화기 구성, 520 페이지	힌트 그룹 및 힌트 목록에서 자동으로 로그인하거나 로그아웃하도록 전화기를 구성합니다.

힌트 그룹을 위한 소프트키 템플릿 구성

전화기가 다음 통화 상태에 있을 때 HLog 소프트키가 전화기에 표시됩니다.

- 연결됨
- 온 후
- 오프 후



참고 HLog 소프트키를 구성하려면 새 소프트키 템플릿을 생성해야 합니다. 표준 소프트키 템플릿에서 HLog 소프트키를 구성할 수 없습니다.

이 절차를 사용하여 HLog 소프트키를 사용할 수 있게 합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
 - a) 새로 추가를 클릭합니다.
 - b) 기본 템플릿을 선택하고 복사를 클릭합니다.
 - c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - d) 저장을 클릭합니다.
- 단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
 - a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 필요한 기존 템플릿을 선택합니다.
- 단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.

참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.
- 단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
- 단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.

단계 7 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.

단계 8 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.

단계 9 저장을 클릭합니다.

단계 10 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

다음에 수행할 작업

다음 절차 중 하나를 수행합니다.

- [소프트키 템플릿을 일반 디바이스 구성에 추가, 519 페이지](#)
- [소프트키 템플릿을 전화기에 연결, 520 페이지](#)

소프트키 템플릿을 일반 디바이스 구성에 연결

(선택 사항) 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 [소프트키 템플릿을 전화기에 연결, 520 페이지](#)의 내용을 참조하십시오.

시작하기 전에

[현트 그룹을 위한 소프트키 템플릿 구성, 517 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	소프트키 템플릿을 일반 디바이스 구성에 추가, 519 페이지	

	명령 또는 동작	목적
단계 2	일반 디바이스 구성을 전화기에 연결, 519 페이지	

소프트키 템플릿을 일반 디바이스 구성에 추가

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성
- 단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성 하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.
 - a) 새로 추가를 클릭합니다.
 - b) 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
 - c) 저장을 클릭합니다.
- 단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.
 - a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 기존 일반 디바이스 구성을 클릭합니다.
- 단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.
- 단계 5 저장을 클릭합니다.
- 단계 6 다음 작업 중 하나를 수행합니다.
 - 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

일반 디바이스 구성을 전화기에 연결

시작하기 전에

[소프트키 템플릿을 일반 디바이스 구성에 추가, 519 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 재설정 을 클릭하여 전화기 설정을 업데이트합니다.

소프트키 템플릿을 전화기에 연결

이 절차는 선택사항입니다. 이 절차는 소프트 키 템플릿을 일반 디바이스 구성에 연결하는 대신 사용할 수 있습니다. 이 절차는 일반 디바이스 구성과 함께 작동합니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우에 사용합니다.

시작하기 전에

[헌트 그룹을 위한 소프트키 템플릿 구성, 517 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

사용자 찾기 및 나열 창이 나타납니다.

단계 2 소프트키 템플릿을 추가할 전화기를 선택합니다.

전화기 구성 창이 나타납니다.

단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.

단계 4 저장을 클릭합니다.

전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

헌트 그룹을 위한 전화기 구성

이 절차를 사용하여 헌트 그룹 및 헌트 목록에서 자동으로 로그인하거나 로그아웃하도록 전화기를 구성합니다.

시작하기 전에

전화기 디렉터리 번호가 하나 이상의 헌트 그룹에 속하는지 확인합니다.

헌트 그룹 및 헌트 목록에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 관리 지침서](#)의 내용을 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 다음 작업 중 하나를 수행합니다.

- a) 기존 전화기에 대한 필드를 수정하려면 검색 조건을 입력하고 결과 목록에서 전화기를 선택합니다. 전화기 구성 창이 나타납니다.
- b) 새 전화기를 추가하려면 새로 추가를 클릭합니다.
새 전화기 추가 창이 표시됩니다.

단계 3 전화기 구성 창에서 다음 작업 중 하나를 수행합니다.

- a) 헌트 그룹에서 전화기를 로그아웃하려면 헌트 그룹에 로그인됨 확인란을 선택 취소합니다.
- b) 전화기에서 헌트 그룹에 로그인하려면 헌트 그룹에 로그인됨 확인란이 선택되어 있는지 확인합니다.

참고 헌트 그룹에 로그인됨 확인란은 기본적으로 모든 전화기에 대해 선택되어 있습니다.

단계 4 저장을 클릭합니다.

헌트 그룹 서비스 매개 변수 구성

헌트 그룹 로그오프 알림 서비스 매개 변수는 회선 그룹으로 들어오는 통화가 현재 로그아웃된 전화기에 도착하는 경우 신호음을 켜거나 끌 수 있는 옵션을 제공합니다. 이 벨소리는 회선이 구성원인 헌트 목록에 대한 수신 통화가 있음을 로그아웃한 사용자에게 알리지만, 로그아웃 상태 때문에 해당 회선 그룹 구성원의 전화기에서 벨소리가 울리지 않습니다.

헌트 그룹 로그오프 알림 서비스 매개 변수를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개 변수를 선택합니다.

단계 2 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
서비스 매개 변수 구성 창이 표시됩니다.

단계 4 클러스터 수준 매개 변수(디바이스 - 전화기) 섹션에서 다음 헌트 그룹 로그오프 알림 서비스 매개 변수에 대한 값을 구성합니다.

회선 그룹(헌트 그룹)의 구성원이 로그아웃했을 때 Cisco IP 전화기에서 재생하는 벨소리 파일의 이름을 입력합니다. 이 서비스 매개 변수의 기본값은 [없음]입니다. 이 값은 벨소리가 없음을 나타냅니다. 최대 255자를 입력할 수 있습니다.

단계 5 저장을 클릭합니다.

창이 새로 고침되고 Cisco Unified Communications Manager에서 서비스 매개 변수를 변경 내용으로 업데이트합니다.

힌트 그룹 상호 작용

기능	상호 작용
비공유 회선 디렉터리 번호	전화기가 회선 그룹에서 로그아웃되고 전화기의 내선 번호가 공유되지 않는 경우 회선 그룹이 회선 그룹의 DN(디렉터리 번호)으로 전화를 걸지 않습니다. 회선 그룹이 일반적으로 DN에 통화를 제공하는 경우 통화 처리는 DN을 생략하고 DN이 회선 그룹에 속하지 않는 것처럼 작동합니다.
공유 회선 디렉터리 번호	<p>힌트 그룹 로그아웃 기능은 디바이스 기반이므로 사용자가 전화기를 로그아웃하면 이 기능은 로그아웃된 전화기에만 영향을 미칩니다. 공유 회선 디렉터리 번호를 포함하는 회선 그룹에 대한 통화는 다음과 같이 작동합니다.</p> <ul style="list-style-type: none"> • DN을 공유하는 모든 전화기가 로그아웃되면 DN에서 벨소리가 울리지 않습니다. • DN을 공유하는 하나 이상의 전화기가 로그인된 경우 DN에서 벨소리가 울립니다. • 로그아웃된 전화기의 신호음은 기본적으로 꺼집니다. Cisco Unified Communications Manager는 로그아웃된 힌트 그룹 구성원에게 전화가 걸려오면 다른 벨소리를 재생하도록 설정할 수 있는 시스템 매개 변수를 제공합니다.

힌트 그룹 제한 사항

제한 사항	설명
여러 회선 그룹	사용자가 힌트 로그 소프트웨어를 눌러 힌트 그룹 로그오프 기능을 활성화하면 전화기가 모든 연결된 회선 그룹에서 로그아웃됩니다. 힌트 그룹 로그오프가 디바이스 기반 기능이기 때문입니다. 전화기에 여러 회선 그룹에 속하는 DN이 있는 경우 힌트 그룹 소프트웨어를 누르면 모든 연결된 회선 그룹에서 전화기가 로그아웃됩니다.

제한 사항	설명
7940, 7960 및 타사 SIP 전화기	<ul style="list-style-type: none"> • SIP(7906, 7911, 7941, 7961,)를 실행하는 전화기가 헌트 그룹에 로그인되고 모두 착신 전환이 활성화되면 SIP를 실행하는 전화기에 통화가 표시됩니다. • SIP를 실행하는 7940 및 7960 전화기가 헌트 그룹에 로그인되고 모두 착신 전환이 활성화되면 전화기가 생략되고 회선 그룹의 다음 전화기가 올립니다. • SIP를 실행하는 7940 및 7960 전화기와 SIP를 실행하는 타사 전화기는 전화기 구성 창을 사용하여 헌트 그룹에 로그인하거나 로그아웃할 수 있지만, 소프트키가 지원되지 않습니다. • SIP를 실행하는 7940 및 7960 전화기와 SIP를 실행하는 타사 전화기는 상태 회선에서 “헌트 그룹에서 로그아웃됨”을 표시하지 않습니다. • SIP를 실행하는 7940 및 7960 전화기와 SIP를 실행하는 타사 전화기는 신호음이 구성되었는지 여부에 관계 없이 헌트 그룹 로그오프 알림음을 재생하지 않습니다.



37 장

악성 전화 식별

- 악성 전화 식별 개요, 525 페이지
- 악성 전화 식별, 525 페이지
- 악성 전화 식별 구성 작업 흐름, 526 페이지
- 악성 전화 식별 상호 작용, 533 페이지
- 악성 전화 식별 제한 사항, 535 페이지
- 악성 전화 ID 문제 해결, 535 페이지

악성 전화 식별 개요

문제가 발생하거나 위험한 통화를 추적하도록 악성 전화 식별(MCID) 기능을 구성합니다. 사용자는 Cisco Unified Communications Manager ID를 요청하여 이러한 전화를 보고할 수 있으며 네트워크에서 수신 통화의 출처를 등록할 수 있습니다.

MCID 기능을 사용하면 다음과 같은 동작이 발생합니다.

1. 사용자가 위협적인 통화를 수신하고 장난 전화를 누릅니다(또는 SCCP 게이트웨이에 연결된 POTS 전화기를 사용하는 경우 기능 코드 *39 입력).
2. Cisco Unified Communications Manager에서 사용자에게 확인 신호음과 함께, MCID 알림 수신을 확인하기 위해 디스플레이가 있는 전화기상에 텍스트 메시지를 보냅니다.
3. Cisco Unified Communications Manager에서 통화에 대한 CDR(통화 세부정보 기록)을 업데이트하여 통화가 장난 전화로 등록되었음을 표시합니다.
4. Cisco Unified Communications Manager에서 알림 및 이벤트 정보가 포함된 로컬 Syslog가 생성됩니다.
5. Cisco Unified Communications Manager에서 설비 메시지를 통해 연결된 네트워크로 MCID 호출을 보냅니다. 설비 IE(정보 요소)가 MCID 호출을 인코딩합니다.
6. 이 알림을 수신하고 나면 PSTN 또는 다른 연결된 네트워크는 법률 당국에 통화 정보를 제공하는 등의 조치를 취할 수 있습니다.

악성 전화 식별

- MCID를 지원하는 게이트웨이 및 연결:

- T1(NI2) 및 E1(ETSI) 연결을 위한 MGCP PRI 백홀 인터페이스를 사용하는 PRI 게이트웨이
- H.323 트렁크 및 게이트웨이
- MCID를 지원하는 IP 전화기

악성 전화 식별 구성 작업 흐름

시작하기 전에

- [악성 전화 식별, 525 페이지](#) 검토

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	MCID 기능을 지원하는 디바이스를 식별하는 보고서를 생성합니다.
단계 2	악성 전화 ID 서비스 매개 변수 설정, 527 페이지	Cisco Unified Communications Manager에서 MCID 표시기가 있는 CDR(통화 세부정보 기록)에 플래그를 지정할 수 있습니다.
단계 3	장난 전화 ID 알람 구성, 527 페이지	알람 정보가 시스템 로그에 표시되도록 알람을 구성합니다.
단계 4	악성 전화 식별을 위한 소프트키 템플릿 구성, 528 페이지	MCID를 사용하여 소프트키 템플릿을 구성합니다. 참고 Cisco Unified IP Phone 8900 및 9900 시리즈는 기능 버튼만 사용하여 MCID를 지원합니다.
단계 5	소프트키 템플릿을 일반 디바이스 구성에 연결, 529 페이지 에 대해 다음 하위 작업을 수행합니다. <ul style="list-style-type: none"> • 소프트키 템플릿을 일반 디바이스 구성에 추가, 530 페이지 • 일반 디바이스 구성을 전화기에 연결, 530 페이지 	(선택 사항) 전화기에서 소프트키 템플릿을 사용할 수 있게 하려면 이 단계 또는 다음 단계를 완료해야 합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 이 단계를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.
단계 6	소프트키 템플릿을 전화기에 연결, 531 페이지	(선택 사항) 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하거나 일반 디바이스 구성과 함께 연결하는 대신 사용할 수 있습니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는

	명령 또는 동작	목적
		소프트키 템플릿을 할당해야 하는 경우 일반 디바이스 구성과 함께 이 절차를 사용합니다.
단계 7	<p>악성 전화 식별 버튼 구성, 531 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> 장난 전화 ID 전화기 버튼 템플릿 구성, 531 페이지 버튼 템플릿을 전화기와 연결, 532 페이지 	전화기에 대해 관리자 및 MCID 버튼을 구성하려면 이 단계를 수행합니다.

악성 전화 ID 서비스 매개 변수 설정

Unified Communications Manager에서 MCID 표시기가 있는 CDR에 플래그를 지정할 수 있게 하려면 CDR 플래그를 활성화해야 합니다.

시작하기 전에

[장난 전화 ID 알람 구성, 527 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 서버 드롭다운 목록에서 Unified Communications Manager 서버 이름을 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
서비스 매개변수 구성 창이 표시됩니다.
- 단계 4 시스템 영역에서 **CDR** 활성화 플래그 필드를 **True**로 설정합니다.
- 단계 5 저장을 클릭합니다.
-

장난 전화 ID 알람 구성

로컬 Syslog에서 알람 이벤트 수준을 설정하고 MCID에 대한 알람을 활성화해야 합니다.

Cisco Business Edition 5000 시스템에서는 노드를 하나만 지원합니다.

시작하기 전에

[악성 전화 ID 서비스 매개 변수 설정, 527 페이지](#)

프로시저

-
- 단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다.알람 > 구성.
알람 구성 창이 표시됩니다.
- 단계 2 서버 드롭다운 목록에서 Unified Communications Manager 서버를 선택한 다음 이동을 클릭합니다.
- 단계 3 서비스 그룹 드롭다운 목록에서 **CM** 서비스를 선택합니다. 알람 구성 창에서 구성 필드가 업데이트됩니다.
- 단계 4 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- 단계 5 로컬 Syslog 아래의 알람 이벤트 수준 드롭다운 목록에서 정보를 선택합니다.
알람 구성 창에서 구성 필드가 업데이트됩니다.
- 단계 6 로컬 Syslog 아래에서 알람 활성화 확인란을 선택합니다.
- 단계 7 클러스터의 모든 노드에 대해 알람을 활성화하려면 모든 노드에 적용 확인란을 선택합니다.
- 단계 8 정보 알람을 설정하려면 업데이트를 클릭합니다.
-

악성 전화 식별을 위한 소프트키 템플릿 구성



-
- 참고 SCCP(Skinny Client Control Protocol) IP 전화기는 MCID 기능을 호출하기 위해 소프트키를 사용합니다.
-

시작하기 전에

[장난 전화 ID 알람 구성, 527 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- 새로 추가를 클릭합니다.
 - 기본 템플릿을 선택하고 복사를 클릭합니다.
 - 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - 저장을 클릭합니다.
- 단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
- 찾기를 클릭하고 검색 기준을 입력합니다.
 - 필요한 기존 템플릿을 선택합니다.
- 단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.

참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.

- 단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
- 단계 6 구성할 통화 상태 선택 필드에서 연결됨을 선택합니다.
[선택되지 않은 소프트키] 목록이 변경되어 이 통화 상태에 사용 가능한 소프트키가 표시됩니다.
- 단계 7 선택되지 않은 소프트키 드롭다운 목록에서 **MCID**(장난 전화 추적 전환)를 선택합니다.
- 단계 8 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.
- 단계 9 저장을 클릭합니다.

소프트키 템플릿을 일반 디바이스 구성에 연결

(선택 사항) 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 [소프트키 템플릿을 전화기에 연결, 531 페이지](#)의 내용을 참조하십시오.

시작하기 전에

[악성 전화 식별을 위한 소프트키 템플릿 구성, 528 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	소프트키 템플릿을 일반 디바이스 구성에 추가, 530 페이지	
단계 2	일반 디바이스 구성을 전화기에 연결, 530 페이지	

소프트키 템플릿을 일반 디바이스 구성에 추가

시작하기 전에

[악성 전화 식별을 위한 소프트키 템플릿 구성, 528 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성

단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.

- a) 새로 추가를 클릭합니다.
- b) 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
- c) 저장을 클릭합니다.

단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.

- a) 찾기를 클릭하고 검색 기준을 입력합니다.
- b) 기존 일반 디바이스 구성을 클릭합니다.

단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

단계 6 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

일반 디바이스 구성을 전화기에 연결

시작하기 전에

[소프트키 템플릿을 일반 디바이스 구성에 추가, 530 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.

단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 재설정 을 클릭하여 전화기 설정을 업데이트합니다.

소프트키 템플릿을 전화기에 연결

선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성과 연결할 수 있습니다. 이 절차는 일반 디바이스 구성과 함께 작동합니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우에 사용할 수 있습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정을 눌러 전화기 설정을 업데이트합니다.

악성 전화 식별 버튼 구성

이 섹션의 절차에서는 악성 전화 식별 버튼을 구성하는 방법에 대해 설명합니다.

시작하기 전에

[장난 전화 ID 알람 구성, 527 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	장난 전화 ID 전화기 버튼 템플릿 구성, 531 페이지 .	회선 또는 단축 다이얼 키에 악성 전화 식별 버튼 기능을 할당하려면 이 단계를 수행합니다.
단계 2	버튼 템플릿을 전화기와 연결, 532 페이지	이 단계를 수행하여 전화기에 악성 전화 식별 버튼을 구성합니다.

장난 전화 ID 전화기 버튼 템플릿 구성

시작하기 전에

[장난 전화 ID 알람 구성, 527 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.
- 단계 2 [찾기]를 클릭하여 지원 되는 전화기 템플릿 목록을 표시합니다.
- 단계 3 새 전화기 버튼 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- 전화기의 모델에 대한 기본 템플릿을 선택하고 복사를 클릭합니다.
 - 전화기 버튼 템플릿 정보 필드에 템플릿의 새 이름을 입력합니다.
 - 저장을 클릭합니다.
- 단계 4 기존 템플릿에 전화기 버튼을 추가하려는 경우 다음 단계를 수행합니다.
- 찾기를 클릭하고 검색 기준을 입력합니다.
 - 기존 템플릿을 선택합니다.
- 단계 5 회선 드롭다운 목록에서 템플릿에 추가하려는 기능을 선택합니다.
- 단계 6 저장을 클릭합니다.
- 단계 7 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다.
-

버튼 템플릿을 전화기와 연결

시작하기 전에

[장난 전화 ID 전화기 버튼 템플릿 구성, 531 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.
- 단계 3 전화기 버튼 템플릿을 추가할 전화기를 선택합니다.
- 단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.
- 단계 5 저장을 클릭합니다.
- 전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.
-

악성 전화 식별 상호 작용

표 47: 악성 전화 식별 상호 작용

기능	상호 작용
전화회의 통화	사용자가 전화회의에 연결되면 MCID 기능을 사용하여 악성 통화 플래그를 표시할 수 있습니다. Cisco Unified Communications Manager는 사용자에게 MCID 표시를 전송하고 알람을 생성하며 CDR를 업데이트합니다. 하지만, 연결된 네트워크는 전화회의에 참여 중일 수 있으므로 Cisco Unified Communications Manager는 해당 네트워크에 MCID 호출 메시지를 전송하지 않습니다.
Extension Mobility	Extension Mobility 사용자는 MCID 소프트웨어를 사용자 디바이스 프로파일의 일부로 지정할 수 있으며 전화기에 로그인되어 있으면 이 기능을 사용할 수 있습니다.
통화 세부 정보 레코드	CDR을 사용하여 악성 전화를 추적하려면 Cisco CallManager 서비스 매개변수에서 CDR 활성 플래그를 True 로 설정해야 합니다. 통화 중 MCID 기능이 사용된 경우 통화의 CDR은 [설명] 필드에 CallFlag=악성 전화 가 포함됩니다.

기능	상호 작용
알람	<p>MCID 기능에 대한 알람을 [로컬 Syslog]에 기록하려면 Cisco Unified Serviceability에서 알람을 구성해야 합니다. 로컬 Syslog 아래에서 정보 알람 이벤트 수준에 대한 알람을 활성화합니다.</p> <p>통화 중 MCID 기능이 사용되는 경우 알람의 SDL 추적 및 Cisco Unified Communications Manager 추적이 기록됩니다. Cisco Unified Serviceability를 사용하여 알람 이벤트 로그를 볼 수 있습니다. 추적에서는 다음과 같은 정보를 제공합니다.</p> <ul style="list-style-type: none"> • 날짜 및 시간 • 이벤트 유형: 정보 • Cisco Unified Communications Manager에서 악성 전화 식별 기능이 호출되었습니다. • 착신자 번호 • 착신 디바이스 이름 • 착신 표시 이름 • 발신자 번호 • 발신 디바이스 이름 • 발신 표시 이름 • 애플리케이션 ID • 클러스터 ID • 노드 ID <p>알람 및 추적에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html의 Cisco 통합 서비스 가용성 관리 가이드를 참조하십시오.</p>
Cisco ATA 186 아날로그 전화기 포트	Cisco ATA 186 아날로그 전화기 포트는 기능 코드 (*39)를 사용하여 MCID를 지원합니다.

악성 전화 식별 제한 사항

표 48: 악성 전화 식별 제한 사항

기능	제한 사항
MCID-T(악성 전화 식별 종료) 기능	Cisco Unified Communications Manager는 악성 전화 ID 시작 기능(MCID-O)만 지원합니다. Cisco Unified Communications Manager는 악성 전화 ID 종료 기능(MCID-T)을 지원하지 않습니다. Cisco Unified Communications Manager가 네트워크로부터 악성 전화 ID에 대한 알림을 받을 경우, Cisco Unified Communications Manager는 해당 알림을 무시합니다.
인터클러스터 트렁크	Cisco Unified Communications Manager가 MCID-T 기능을 지원하지 않으므로, MCID는 클러스터 간 트렁크를 통하여 작동하지 않습니다.
Cisco MGCP FXS 게이트웨이	Cisco MGCP FXS 게이트웨이는 MCID를 지원하지 않습니다. 후 플래시를 수락하고 MGCP에서 기능 코드를 수집하기 위한 메커니즘이 존재하지 않습니다.
QSIG 트렁크	MCID는 QSIG 표준이 아니므로 QSIG 트렁크를 통해 작동하지 않습니다.
Cisco VG248 아날로그 전화기 게이트웨이	Cisco VG248 아날로그 전화기 게이트웨이는 MCID를 지원하지 않습니다.
SIP 트렁크	MCID는 SIP 트렁크를 지원하지 않습니다.
지정 전환	시스템은 MCID 및 즉시 전환 기능을 함께 사용하는 것을 지원하지 않습니다.

악성 전화 ID 문제 해결

악성 전화 ID를 추적하려면 Cisco Unified Communications Manager SDL 추적 및 알람을 사용할 수 있습니다. MCID용 추적에 대한 자세한 내용은 *Cisco 통합 서비스 가용성 관리 가이드*를 참조하십시오. MCID에 대한 보고서를 생성하는 방법에 대한 자세한 내용은 *Cisco Unified CDR Analysis and Reporting* 관리 지침서를 참조하십시오.



38 장

통화 전환

- 호 전환 개요, 537 페이지
- 호 전환 구성 작업 흐름, 538 페이지
- 호 전환 상호 작용, 549 페이지
- 호 전환 제한, 550 페이지

호 전환 개요

전환 기능을 사용하면 사용자 전화기에서 다른 번호로 연결된 통화를 재전송할 수 있습니다. 호 전환 후 통화가 끊어지고 전환된 통화가 새 통화 연결로 설정됩니다.

다음은 다양한 유형의 호 전환입니다.

- 상담 전환 및 비공개 전환 - 상담 전환 시 통화로 응답하는 대상 전화기 사용자와 상담한 후 전환하는 전화기 사용자는 발신자를 다른 대상 주소로 리디렉션할 수 있습니다. 즉, 전환하는 전화기 사용자는 대상 전화기 사용자가 통화로 응답할 때까지 통화로 유지됩니다. 비공개 전환에서 전환하는 전화기 사용자는 전환 대상이 통화로 응답하기 전에 발신자를 대상 회선에 연결합니다. 대부분의 전화기는 전환에 하드 키나 소프트웨어를 사용합니다. 상담 전환 및 비공개 전환 모두 별도의 구성이 필요하지 않습니다. 두 전환 유형의 차이는 전환하는 측이 전환 버튼을 두 번 누르는 시기에 따라 달라집니다. 상담 전환의 경우 전환하는 측이 대상 응답 후 전환 버튼을 누르는 반면, 비공개 전환의 경우 대상이 응답하기 전에 전환하는 측이 전환 버튼을 누릅니다.

SCCP에서 시작된 비공개 전환의 경우 Cisco Unified Communications Manager는 전환된 사용자에게 벨소리 형태의 통화 진행 상태 표시를 제공합니다.

- 전환 온 훅 - 이 유형의 호 전환에서 사용자는 전환 소프트웨어를 누르고 통화를 전환할 번호로 전화를 건 다음 전환 소프트웨어를 다시 누르거나 단순히 온 훅으로 전환하여 전환 작업을 완료합니다. 전송 온 훅 서비스 매개 변수를 **True**로 설정해야 합니다. 이 서비스 매개 변수는 전환 작업을 시작한 후 사용자가 온 훅으로 전환될 때 호 전환이 완료되는지 여부를 결정합니다.

두 상담 전환 및 비공개 전환 모두 전송 온 훅 옵션을 사용합니다.

- 호연결 — 이 유형의 전환을 사용하면 사용자가 두 개의 설정된 통화로 참가하고(두 통화가 보류 중이거나 연결된 상태에 있을 수 있음) 전환에서 이니시에이터를 삭제할 수 있습니다. 호연결은

상담 전화를 시작하지 않고, 활성 전화를 대기 중으로 설정하지 않습니다. 사용자는 호연결 소프트웨어를 사용하여 설정된 두 개의 통화에 참가하고 이니시에이터를 제거합니다.

호 전환 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	상담 및 비공개 전환 구성, 538 페이지	호 전환 기능을 사용하면 호 전환 수신자에게 문의하지 않고 단일 통화를 새 번호로 리디렉션할 수 있습니다. 이 단계를 수행하여 호 전환을 소프트키 및/또는 버튼으로 구성합니다.
단계 2	전환 온 훅 구성, 543 페이지	(선택 사항) 호 전환 온 훅은 통화 호 전환을 완료하는 옵션입니다. 호 전환을 누르고 통화를 호 전환해야 하는 번호로 전화를 건 다음, 온 훅으로 전환하여 호 전환을 완료합니다. 이 단계를 수행하여 서비스 매개 변수를 구성합니다.
단계 3	직접 호전환 구성, 543 페이지	(선택 사항) 호 전환을 사용하면 회선에 남지 않고 두 개의 통화를 서로 전환할 수 있습니다. 이 단계를 수행하여 호연결을 소프트키 및/또는 버튼으로 구성합니다.

상담 및 비공개 전환 구성

전화기에서 소프트키 또는 버튼을 지원 있는지 여부에 따라 작업 흐름 중 하나를 완료합니다.

프로시저

	명령 또는 동작	목적
단계 1	전환을 위한 소프트키 템플릿 구성, 538 페이지	
단계 2	전환 버튼 구성, 542 페이지	

전환을 위한 소프트키 템플릿 구성

호 전환 소프트키는 통화의 참조 및 블라인드 호 전환에 사용됩니다. 호 전환 소프트키에는 다음과 같은 통화 상태가 있습니다.

- 연결됨

• 보류 중

이 절차를 사용하여 호 전환 소프트키를 사용할 수 있습니다.

프로시저

-
- 단계 1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2** 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- a) 새로 추가를 클릭합니다.
 - b) 기본 템플릿을 선택하고 복사를 클릭합니다.
 - c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - d) 저장을 클릭합니다.
- 단계 3** 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
- a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 필요한 기존 템플릿을 선택합니다.
- 단계 4** 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.
- 참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.
- 단계 5** 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
- 단계 6** 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.
- 단계 7** 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.
- 단계 8** 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.
- 단계 9** 저장을 클릭합니다.
- 단계 10** 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.
-

다음에 수행할 작업

다음 절차 중 하나를 수행합니다.

- [전환 소프트키 템플릿을 일반 디바이스 구성에 연결, 540 페이지](#)
- [호 전환 소프트키 템플릿을 전화기와 연결, 541 페이지](#)

전환 소프트키 템플릿을 일반 디바이스 구성에 연결

선택 사항. 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 [호 전환 소프트키 템플릿을 전화기와 연결, 541 페이지](#)의 내용을 참조하십시오.

시작하기 전에

[전환을 위한 소프트키 템플릿 구성, 538 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	전환 소프트키 템플릿을 일반 디바이스 구성에 추가, 540 페이지	이 단계를 수행하여 호 전환 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.
단계 2	일반 디바이스 구성을 전화기에 연결, 541 페이지	이 단계를 수행하여 호 전환 소프트키 일반 디바이스 구성을 전화기에 연결합니다.

다음에 수행할 작업

[전환 버튼 구성, 542 페이지](#)

전환 소프트키 템플릿을 일반 디바이스 구성에 추가

시작하기 전에

[전환을 위한 소프트키 템플릿 구성, 538 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성

단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.

- a) 새로 추가를 클릭합니다.
- b) 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
- c) 저장을 클릭합니다.

단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.

- a) 찾기를 클릭하고 검색 기준을 입력합니다.
- b) 기존 일반 디바이스 구성을 클릭합니다.

단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

단계 6 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

일반 디바이스 구성을 전화기에 연결

시작하기 전에

[전환 소프트키 템플릿을 일반 디바이스 구성에 추가, 540 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.

단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 재설정 을 클릭하여 전화기 설정을 업데이트합니다.

호 전환 소프트키 템플릿을 전화기와 연결

선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성과 연결할 수 있습니다. 이 절차는 일반 디바이스 구성과 함께 작동합니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우에 사용할 수 있습니다.

시작하기 전에

[전환을 위한 소프트키 템플릿 구성, 538 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정을 눌러 전화기 설정을 업데이트합니다.

전환 버튼 구성

이 섹션의 절차에서는 호 전환 버튼을 구성하는 방법에 대해 설명합니다.

프로시저

	명령 또는 동작	목적
단계 1	전환을 위한 전화기 버튼 템플릿 구성, 542 페이지	회선 또는 단축 다이얼 키에 호 전환 버튼 기능을 할당하려면 이 단계를 수행합니다.
단계 2	전환 버튼 템플릿을 전화기에 연결, 543 페이지	이 단계를 수행하여 전화기에 호 전환 버튼을 구성합니다.

전환을 위한 전화기 버튼 템플릿 구성

선택 사항. 회선 또는 단축 다이얼 키에 기능을 할당하려는 경우 이 절차를 수행합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.
- 단계 2 [찾기]를 클릭하여 지원 되는 전화기 템플릿 목록을 표시합니다.
- 단계 3 새 전화기 버튼 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
 - a) 전화기의 모델에 대한 기본 템플릿을 선택하고 복사를 클릭합니다.
 - b) 전화기 버튼 템플릿 정보 필드에 템플릿의 새 이름을 입력합니다.
 - c) 저장을 클릭합니다.
- 단계 4 기존 템플릿에 전화기 버튼을 추가하려는 경우 다음 단계를 수행합니다.
 - a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 기존 템플릿을 선택합니다.
- 단계 5 회선 드롭다운 목록에서 템플릿에 추가하려는 기능을 선택합니다.
- 단계 6 저장을 클릭합니다.

단계 7 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다.

전환 버튼 템플릿을 전화기에 연결

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.

단계 3 전화기 버튼 템플릿을 추가할 전화기를 선택합니다.

단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

전환 온 훅 구성

시작하기 전에

[상담 및 비공개 전환 구성, 538 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
서비스 매개 변수 구성 창이 표시됩니다.

단계 2 서버 드롭다운 목록 상자에서 매개 변수를 구성할 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager(활성)** 서비스를 선택합니다.

단계 4 클러스터 수준 매개 변수(디바이스 - 전화기)에서 전송 온 훅 활성화 서비스 매개 변수에 대해 **True**를 선택합니다.

단계 5 저장을 클릭합니다.

직접 호전환 구성

전화기에서 소프트키 또는 버튼을 지원하는지 여부에 따라 작업 흐름 중 하나를 완료합니다.

프로시저

	명령 또는 동작	목적
단계 1	직접 호전환을 위한 소프트키 템플릿 구성, 544 페이지	이 단계를 수행하여 직접 호전환 소프트키를 템플릿에 추가하고 일반 디바이스 구성 또는 전화기를 사용하여 소프트키를 구성합니다.
단계 2	직접 호전환 버튼 구성, 547 페이지	이 단계를 수행하여 전화기에 직접 호전환 버튼을 추가하고 구성합니다.

직접 호전환을 위한 소프트키 템플릿 구성

직접 호 전환 소프트키에는 다음과 같은 통화 상태가 있습니다.

- 연결됨
- 보류 중

이 절차를 사용하여 직접 호 전환 소프트키를 사용할 수 있게 합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- 새로 추가를 클릭합니다.
 - 기본 템플릿을 선택하고 복사를 클릭합니다.
 - 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - 저장을 클릭합니다.
- 단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
- 찾기를 클릭하고 검색 기준을 입력합니다.
 - 필요한 기존 템플릿을 선택합니다.
- 단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.
- 참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.
- 단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
- 단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.
- 단계 7 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.

단계 8 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.

단계 9 저장을 클릭합니다.

단계 10 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

다음에 수행할 작업

다음 절차 중 하나를 수행합니다.

- [직접 호전환 소프트키 템플릿을 일반 디바이스 구성에 연결, 545 페이지](#)
- [직접 호 전환 소프트키 템플릿을 전화기와 연결, 547 페이지](#)

직접 호전환 소프트키 템플릿을 일반 디바이스 구성에 연결

선택 사항. 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 다음 내용을 참조하십시오. [직접 호 전환 소프트키 템플릿을 전화기와 연결, 547 페이지](#)

시작하기 전에

[직접 호전환을 위한 소프트키 템플릿 구성, 544 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	직접 호전환 소프트키 템플릿을 일반 디바이스 구성에 추가, 546 페이지	이 단계를 수행하여 호전환 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.
단계 2	일반 디바이스 구성을 전화기에 연결, 546 페이지	이 단계를 수행하여 호전환 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

직접 호전환 소프트키 템플릿을 일반 디바이스 구성에 추가

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성
- 단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성 하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.
- a) 새로 추가를 클릭합니다.
 - b) 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
 - c) 저장을 클릭합니다.
- 단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.
- a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 기존 일반 디바이스 구성을 클릭합니다.
- 단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.
- 단계 5 저장을 클릭합니다.
- 단계 6 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.
-

일반 디바이스 구성을 전화기에 연결

시작하기 전에

[직접 호전환 소프트키 템플릿을 일반 디바이스 구성에 추가, 546 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정을 클릭하여 전화기 설정을 업데이트합니다.
-

직접 호 전환 소프트키 템플릿을 전화기와 연결

선택 사항. 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성과 연결할 수 있습니다. 이 절차는 일반 디바이스 구성과 함께 작동합니다. 일반 디바이스 구성 또는 다른 기본 소프트키 할당에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우에 사용할 수 있습니다.

시작하기 전에

[직접 호전환을 위한 소프트키 템플릿 구성, 544 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정을 눌러 전화기 설정을 업데이트합니다.
-

직접 호 전환 버튼 구성

이 섹션의 절차에서는 직접 호 전환 버튼을 구성하는 방법에 대해 설명합니다.

프로시저

	명령 또는 동작	목적
단계 1	직접 호전환을 위한 전화기 버튼 템플릿 구성, 547 페이지	회선 또는 단축 다이얼 키에 호 전환 버튼 기능을 할당하려면 이 단계를 수행합니다.
단계 2	직접 호전환 버튼 템플릿을 전화기에 연결, 548 페이지	이 단계를 수행하여 전화기에 호 전환 버튼을 추가하고 구성합니다.

직접 호전환을 위한 전화기 버튼 템플릿 구성

선택 사항. 회선 또는 단축 다이얼 키에 기능을 할당하려는 경우 이 절차를 수행합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.
- 단계 2 [찾기] 를 클릭하여 지원 되는 전화기 템플릿 목록을 표시합니다.
- 단계 3 새 전화기 버튼 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- a) 전화기의 모델에 대한 기본 템플릿을 선택하고 복사를 클릭합니다.

- b) 전화기 버튼 템플릿 정보 필드에 템플릿의 새 이름을 입력합니다.
- c) 저장을 클릭합니다.

단계 4 기존 템플릿에 전화기 버튼을 추가하려는 경우 다음 단계를 수행합니다.

- a) 찾기를 클릭하고 검색 기준을 입력합니다.
- b) 기존 템플릿을 선택합니다.

단계 5 회선 드롭다운 목록에서 템플릿에 추가하려는 기능을 선택합니다.

단계 6 저장을 클릭합니다.

단계 7 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다.

직접 호전환 버튼 템플릿을 전화기에 연결

시작하기 전에

[직접 호전환을 위한 전화기 버튼 템플릿 구성, 547 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.

단계 3 전화기 버튼 템플릿을 추가할 전화기를 선택합니다.

단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

호 전환 상호 작용

기능	상호 작용
논리적 파티션	<p>호 전환된 상대방의 역할을 하는 디바이스의 지리적 위치 식별자와 호 전환된 대상의 역할을 하는 디바이스의 지리적 위치 식별자 사이에서 논리 파티션 정책 점검이 수행됩니다.</p> <p>다음과 같은 경우에 논리적 파티션 처리가 발생합니다.</p> <ul style="list-style-type: none"> • 전화기 사용자가 호 전환 소프트키를 사용하여 통화를 호 전환하는 경우, 소프트키를 한 번 더 누르면 호 전환 기능이 호출되고 처리됩니다. • 직접 호 전환, 온 훅 호 전환, 훅 플래시 호 전환 및 CTI 애플리케이션 시작 호 전환 등 다른 호 전환 메커니즘이 통화 호 전환 기능을 호출하는 경우입니다. • 호 전환된 상대방 및 호 전환된 대상이 PSTN 참가자를 지정하는 경우 • Cisco Unified Communications Manager는 호 전환된 상대방 및 호 전환된 대상인 디바이스와 연결되는 지리적 위치 식별자 정보를 사용하여 논리적 파티션 정책 점검을 수행하는 경우 • 기본 및 보조 통화를 분할하기 전과 통화참가 전. <p>논리적 파티션은 거부된 통화를 다음과 같이 처리합니다.</p> <ul style="list-style-type: none"> • VoIP 전화기에 [외부 호 전환 제한] 메시지를 전송합니다. • 일반 호 전환 - SCCP를 실행하는 전화기의 경우 기본 통화가 보류되고 상담 통화는 활성 상태를 유지합니다. SIP를 실행하는 전화기의 경우 기본 및 상담 통화가 계속 보류되며 실패 이후 수동으로 보류해제해야 합니다. • 온 훅, 훅 플래시, 아날로그 전화기에서 시작된 호 전환 - 기본 및 보조 통화 모두 원인 코드 = 63 “서비스 또는 옵션을 사용할 수 없음”을 사용하여 지워지며 Cisco Unified Communications Manager에서 다시걸기 신호음이 재생됩니다. • [호 전환 실패 수] 성능 카운터가 증가합니다.

기능	상호 작용
MLPP(Multilevel Precedence and Preemption)	<p>스위치가 우선 수준이 동일한 두 세그먼트 사이에서 호전환을 시작할 경우 해당 세그먼트는 호전환 시 우선 수준을 유지합니다. 우선 수준이 다른 통화 세그먼트 사이에 호전환이 실시될 경우 호전환을 시작하는 스위치는 우선 수준이 더 높은 세그먼트에서 연결을 표시합니다.</p> <p>Cisco Unified Communications Manager는 호전환 작업에 포함된 통화 레그의 우선 수준을 업그레이드하여 이 요구 사항을 지원합니다. 예를 들어, 당사자 A가 [우선] 우선 수준인 당사자 B에게 전화를 겁니다. 그런 다음 당사자 B는 당사자 C에게 호전환을 시작하고 전화를 걸면서 플래시 우선 번호를 누릅니다. 호전환이 완료되면 당사자 A의 우선 수준이 [우선]에서 [플래시]로 업그레이드됩니다.</p> <p>호전환 기능은 [호전환] 소프트웨어를 지원하는 전화기에서 MLPP를 활성화할 때 자동으로 활성화됩니다.</p> <p>참고 우선 수준 업그레이드는 ICT(클러스터 간 트렁크), PRI 트렁크와 같은 트렁크 디바이스에서 작동하지 않습니다.</p>

호 전환 제한

기능	제한 사항
논리적 파티션	<p>전송된 대상 디바이스와 전송된 대상 디바이스가 모두 VoIP 전화기인 경우에는 논리적 파티셔닝 처리가 수행되지 않습니다.</p> <p>지오로케이션 또는 지오로케이션 필터가 모든 디바이스와 연결되어 있지 않은 경우에는 논리적 파티션 처리가 수행되지 않습니다.</p>
외부 호전환 제한	외부 통화 시나리오에 대한 호 전환을 제한하려면 "외부 호전환 제한" 장을 참조하십시오.
헌트 파일럿	알림이 진행 중일 때 헌트 파일럿에 대한 호전환이 시작되면 알림이 완료된 후에만 통화가 재전송됩니다.



39 장

외부 호전환 제한

- 외부 호전환 제한 사항 개요, 551 페이지
- 외부 호전환 제한 사항 작업 흐름 구성, 552 페이지
- 외부 호전환 제한 상호 작용, 556 페이지
- 외부 호전환 제한, 557 페이지

외부 호전환 제한 사항 개요

외부 호전환 제한 기능을 사용하면 게이트웨이, 트렁크 및 경로 패턴을 시스템 수준에서 온넷(내부) 또는 오프넷(외부) 디바이스로 구성할 수 있습니다. 디바이스를 오프넷으로 설정하면 외부 통화를 외부 디바이스로 호전환하는 것을 제한하여 통화료 사기를 방지할 수 있습니다.

오프넷 호전환에 대한 오프넷 차단(Block OffNet to OffNet Transfer) 서비스 매개 변수가 [참]으로 설정되어 있을 때 사용자가 오프넷 게이트웨이 또는 트렁크의 통화를 호전환하려고 하면 해당 통화를 호전환할 수 없음을 나타내는 메시지가 사용자 전화기에 표시됩니다.

이 설명서는 다음과 같은 용어를 사용합니다.

용어	설명
온 넷 디바이스	온 넷 디바이스 - 온 넷으로 구성되고 네트워크 내부에 있는 것으로 간주되는 디바이스입니다.
오프 넷 디바이스	오프 넷 디바이스 - 오프넷으로 구성되고 네트워크 외부에 있는 것으로 간주되는 디바이스입니다.
네트워크 위치	네트워크와 관련하여 온 넷 또는 오프 넷으로 간주되는 디바이스의 위치입니다.
시작 측	호전환되는 디바이스입니다. 시스템은 이 디바이스를 온넷 또는 오프넷으로 간주합니다.
종료 측	호전환된 통화를 받는 디바이스입니다. 시스템은 이 디바이스를 온넷 또는 오프넷으로 간주합니다.

용어	설명
착신 통화	온 넷 또는 오프 넷으로 분류하는 데 게이트웨이 및 트렁크 통화 분류 설정만 사용되는 통화입니다. [경로 패턴] 통화 분류 설정은 적용되지 않습니다.
발신 통화	트렁크, 게이트웨이 및 라우트 패턴의 통화 분류 설정이 고려되는 통화입니다. 라우트 패턴의 [디바이스 오버라이드 허용] 설정은 라우트 패턴 통화 분류 설정 대신에 트렁크나 게이트웨이 통화 분류 설정이 사용되는지 여부를 결정합니다.

외부 호전환 제한 사항 작업 흐름 구성

프로시저

	명령 또는 동작	목적
단계 1	외부 호전환 제한을 위한 서비스 매개 변수 구성, 552 페이지	외부 통화가 외부 디바이스 또는 번호로 호전환되지 않게 합니다.
단계 2	인터콤 통화를 구성하려면 다음 절차를 수행합니다. <ul style="list-style-type: none"> 클러스터 수준 서비스 매개 변수 구성, 554 페이지 호전환 제한을 위한 게이트웨이 구성, 554 페이지 호전환 제한을 위한 트렁크 구성, 555 페이지 	게이트웨이 구성 또는 트렁크 구성을 사용하거나 클러스터 수준의 서비스 매개 변수를 설정하여 게이트웨이 및 트렁크를 온넷(내부) 또는 오프넷(외부)으로 구성합니다.
단계 3	발신 통화 구성, 555 페이지	라우트 패턴 구성으로 호전환 기능을 구성합니다.

외부 호전환 제한을 위한 서비스 매개 변수 구성

외부 통화가 외부 디바이스 또는 번호로 호전환되지 않게 하려면 다음 단계를 수행합니다.

프로시저

단계 1 Cisco Unified CM 관리 사용자 인터페이스에서 시스템 > 서비스 매개 변수를 선택합니다.

단계 2 서비스 매개 변수 설정창 서버 드롭다운 목록에서 구성하려는 Cisco Unified CM 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager(활성)**를 선택합니다.

단계 4 오프넷 간 호전환 차단 드롭다운 목록에서 **True**를 선택합니다. 기본값은 [거짓]입니다.

단계 5 저장을 클릭합니다.

수신 통화 작업 흐름 구성

프로시저

	명령 또는 동작	목적
단계 1	(선택 사항) 클러스터 수준 서비스 매개 변수 구성, 554 페이지	Cisco Unified Communications Manager 클러스터에서 모든 게이트웨이 또는 트렁크를 오프넷(외부) 또는 온넷(내부)으로 구성합니다.
단계 2	호전환 제한을 위한 게이트웨이 구성, 554 페이지	<p>게이트웨이 구성을 사용하여 게이트웨이를 온 넷(내부) 또는 오프 넷(외부)으로 구성합니다. 클러스터 수준의 서비스 매개 변수인 오프넷 간 호전환 차단과 함께 이 기능을 사용하는 경우 이 구성에 따라 게이트웨이에서의 호전환 여부가 결정됩니다.</p> <p>다음 디바이스를 Cisco Unified Communications Manager 내부 및 외부 디바이스로 구성할 수 있습니다.</p> <ul style="list-style-type: none"> • H.323 게이트웨이 • MGCP FXO 트렁크 • MGCP T1/E1 트렁크
단계 3	호전환 제한을 위한 트렁크 구성, 555 페이지	<p>트렁크 구성을 사용하여 트렁크를 온 넷(내부) 또는 오프 넷(외부)으로 구성합니다. 클러스터 수준의 서비스 매개 변수인 오프넷 간 호전환 차단과 함께 이 기능을 사용하는 경우 이 구성에 따라 트렁크에서의 호전환 여부가 결정됩니다.</p> <p>다음 디바이스를 Cisco Unified Communications Manager 내부 및 외부 디바이스로 구성할 수 있습니다.</p> <ul style="list-style-type: none"> • 클러스터 간 트렁크 • SIP 트렁크

클러스터 수준 서비스 매개 변수 구성

Cisco Unified Communications Manager 클러스터에서 모든 게이트웨이 또는 트렁크를 오프넷(외부) 또는 온넷(내부)으로 구성하려면 다음 단계를 수행합니다.

시작하기 전에

[외부 호전환 제한을 위한 서비스 매개 변수 구성, 552 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리 사용자 인터페이스에서 시스템 > 서비스 매개 변수를 선택합니다.
 - 단계 2 서비스 매개 변수 설정창 서버 드롭다운 목록에서 구성하려는 Cisco Unified CM 서버를 선택합니다.
 - 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager(활성)**를 선택합니다.
 - 단계 4 통화 분류 드롭다운 목록에서 오프 넷 또는 온 넷(기본값은 오프 넷 지정)을 선택합니다.
-

호전환 제한을 위한 게이트웨이 구성

게이트웨이를 [오프넷], [온넷] 또는 [시스템 기본값 사용]으로 구성하려면 다음 절차를 수행합니다. 시스템은 게이트웨이를 통해 네트워크로 들어오는 통화를 각각 오프넷 또는 온넷으로 간주합니다.

시작하기 전에

[클러스터 수준 서비스 매개 변수 구성, 554 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 게이트웨이
[게이트웨이 찾기 및 나열] 창이 표시됩니다.
 - 단계 2 구성된 게이트웨이를 나열하려면 찾기를 클릭합니다.
Unified Communications Manager 표시에 구성되어 있는 게이트웨이.
 - 단계 3 오프넷 또는 온넷으로 구성할 게이트웨이를 선택합니다.
 - 단계 4 통화 분류 필드에서 오프 넷 또는 온 넷을 선택합니다. 클러스터 수준 제한에 모든 게이트웨이가 활성화된 경우 시스템 기본값을 사용하도록 각 게이트웨이를 구성합니다(통화 분류 서비스 매개 변수의 설정을 읽고 게이트웨이에 해당 설정을 사용함).
 - 단계 5 저장을 클릭합니다.
-

호전환 제한을 위한 트렁크 구성

트렁크를 [오프넷], [온넷] 또는 [시스템 기본값 사용]으로 구성하려면 다음 절차를 수행합니다. 시스템은 트렁크를 통해 네트워크로 들어오는 통화를 각각 오프넷 또는 온넷으로 간주합니다.

시작하기 전에

[호전환 제한을 위한 게이트웨이 구성, 554 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 트렁크.

[트렁크 찾기 및 나열] 창이 표시됩니다.

단계 2 구성된 트렁크를 나열하려면 찾기를 클릭합니다.

Unified Communications Manager 표시에 구성되어 있는 트렁크.

단계 3 오프넷 또는 온넷으로 구성할 트렁크를 선택합니다.

단계 4 통화 분류 드롭다운 목록에서 다음 필드 중 하나를 선택합니다.

- **오프 넷** 이 필드를 선택하면 게이트웨이를 외부 게이트웨이로 식별합니다. 통화가 오프넷으로 구성된 게이트웨이에서 수신되는 경우 시스템은 외부 벨소리를 대상 디바이스로 보냅니다.
- **온 넷** 이 필드를 선택하면 게이트웨이가 내부 게이트웨이로 식별됩니다. 통화가 온넷으로 구성된 게이트웨이에서 수신되는 경우 시스템은 내부 벨소리를 대상 디바이스로 보냅니다.
- **시스템 기본값 사용** 이 필드를 선택하면 Unified Communications Manager 클러스터 수준 서비스 매개 변수 통화 분류를 사용합니다.

참고 모든 트렁크에서 클러스터 수준 제한을 활성화한 경우 각 트렁크가 시스템 기본값을 사용하도록 구성합니다(통화 분류 서비스 매개 변수의 설정을 읽고 트렁크에 해당 설정을 사용함).

단계 5 저장을 클릭합니다.

발신 통화 구성

관리자는 통화를 온넷 또는 오프넷으로 분류하기 위해 경로 패턴 구성 창에서 통화 분류 필드를 각각 [온넷] 또는 [오프넷]으로 설정할 수 있습니다. 관리자는 경로 패턴 구성 창의 디바이스 오버라이드 허용 확인란을 선택하여 경로 패턴 설정을 무시하고 트렁크나 게이트웨이 설정을 사용할 수 있습니다.

시작하기 전에

[호전환 제한을 위한 트렁크 구성, 555 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 라우트/헌트 > 라우트 패턴을 선택하고 찾기를 클릭하여 모든 라우트 패턴을 나열합니다.
- 단계 2 구성할 라우트 패턴을 선택하거나 새로 추가를 클릭합니다.
- 단계 3 라우트 패턴 구성 창에서 다음 필드를 사용하여 라우트 패턴 구성을 사용하여 전환 기능을 구성합니다.
- a) 통화 분류 - 이 드롭다운 목록을 사용하여 이 라우트 패턴을 사용하는 통화를 [오프넷] 또는 [온넷]으로 분류합니다.
 - b) 외부 신호음 제공 - 이 확인란은 [통화 분류]가 [오프넷]으로 설정된 경우 선택됩니다.
 - c) 디바이스 오버라이드 허용 - 이 확인란을 선택할 경우 시스템에서 [라우트 패턴 구성] 창의 [통화 분류] 설정 대신 라우트 패턴과 관련된 트렁크 또는 게이트웨이의 [통화 분류] 설정을 사용합니다.
- 단계 4 저장을 클릭합니다.

외부 호전환 제한 상호 작용

기능	상호 작용
전화회의 끊기	전화회의 끊기 기능에서는 전화회의 상대방을 오프넷으로 구성할지, 아니면 온넷으로 구성할지 선택하여 기존의 애드-혹 컨퍼런스를 끊어야 할지 여부를 결정합니다. 애드-혹 컨퍼런스 끊기 서비스 매개 변수를 사용하여 [전화회의에 남은 온넷 상대방이 없는 경우] 옵션을 선택하고 기능을 구성합니다. 상대방이 사용하고 있는 디바이스 또는 경로 패턴을 확인하여 각 상대방의 온넷 상태를 판별합니다. 자세한 내용은 "애드-혹 컨퍼런스" 장에 있는 애드-혹 컨퍼런스 연결과 관련된 항목을 참조하십시오.
벌크 관리	벌크 관리에서는 게이트웨이 템플릿에 게이트웨이 구성(오프넷 또는 온넷)을 삽입합니다. 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 벌크 관리 설명서를 참조하십시오.
DNA(Dialed Number Analyzer)	게이트웨이에서 번호 분석을 수행하는 데 사용되는 경우, DNA는 게이트웨이 및 경로 패턴을 위해 구성된 통화 분류를 표시합니다. 자세한 내용은 Cisco Unified Communications Manager Dialed Number Analyzer Guide를 참조하십시오.

외부 호전환 제한

제한 사항	설명
FXS 게이트웨이	Cisco Catalyst 6000 24 포트와 같은 FXS 게이트웨이는 [게이트웨이 구성] 창에 [통화 분류] 필드가 없으므로, 시스템에서 항상 온넷으로 간주됩니다.
Cisco VG248 Gateway	시스템은 통화 분류 필드가 없는 Cisco VG248 게이트웨이를 지원하지 않습니다.
FXS 포트	Cisco Unified Communications Manager는 오프넷(외부)으로 구성할 수 없는 모든 Cisco Unified IP Phone과 FXS 포트를 온넷(내부)으로 간주합니다.



XI 부

프레즌스 및 프라이버시 기능

- 참여 , 561 페이지
- BLF 프리젠스 , 575 페이지
- 통화 표시 제한 , 591 페이지
- DND(Do Not Disturb) , 603 페이지
- 프라이버시 , 617 페이지
- 전용 회선 자동 링다운 , 623 페이지
- 보안 신호음 , 629 페이지



40 장

참여

- 참여 개요, 561 페이지
- 참여 구성 작업 흐름, 564 페이지
- 참여 상호 작용, 571 페이지
- 참여 제한 사항, 571 페이지
- 참여 문제 해결, 572 페이지

참여 개요

참여를 사용하면 사용자가 공유 회선에 있는 원격 활성 통화에 추가될 수 있습니다. 회선의 원격 활성 통화는 회선과 디렉터리 번호를 공유하는 다른 디바이스로 걸거나 다른 디바이스에서 건 활성(연결된) 통화입니다.

상대방이 통화 신호음을 구성하는 경우 기본 통화가 참여한 통화 또는 회의끼기 통화로 변경될 때 전화기에서 신호음이 재생됩니다. 또한 상대방이 다자 통화를 떠나면 다른 신호음이 재생됩니다.

전화기는 다음과 같은 전화회의 모드에서 참여를 지원합니다.

- 참여한 전화기의 내장 컨퍼런스 브리지 - 이 모드에서는 참여 소프트웨어를 사용합니다. 대부분의 Cisco Unified IP Phone에는 내장 컨퍼런스 브리지 기능이 있습니다.
- 공유 컨퍼런스 브리지 - 이 모드는 회의끼기 소프트웨어를 사용합니다.

원격 사용 중인 통화에서 참여 또는 회의끼기 소프트웨어를 누르면 사용자는 모든 상대방과의 통화에 추가되고 모든 상대방에게 참여 경고음(구성된 경우)이 울립니다. 참여에 실패하면 원래 통화가 활성 상태로 유지됩니다. 사용할 수 있는 내장 또는 공유 컨퍼런스 브리지가 없으면 참여 요청이 거부되고 참여 개시자 디바이스에 메시지가 표시됩니다. 네트워크 또는 Unified Communications Manager 오류가 발생하는 경우 참여 통화는 보존됩니다.



참고 참여 및 회의끼기 모두에 대해 소프트웨어 옵션을 표시하려면 Unified Communications Manager 사용자 인터페이스에서 공유 회선 표시를 사용하는 디바이스에 대한 프라이버시 옵션을 비활성화합니다.

참여를 지원하는 Cisco Unified IP Phone 목록을 보려면 Cisco Unified CM 보고에 로그인하고 Unified CM 전화 기능 목록 보고서를 실행합니다. 빌트-인 브리지(BIB)를 기능으로 선택해야 합니다. 자세한 내용은 [전화기 기능 목록 생성, 7 페이지](#)를 참조하십시오.

단일 버튼 참여 및 단일 버튼 회의끼기

단일 버튼 참여 및 단일 버튼 회의끼기 기능을 사용하면 사용자가 원격 활성 통화의 공유 회선 버튼을 눌러 통화에 참여할 수 있습니다. 모든 상대방에게 참여 경고음이 수신됩니다(구성된 경우). 참여에 실패하면 원래 통화가 활성 상태로 유지됩니다.

전화기는 다음 두 전화회의 모드에서 단일 버튼 참여 및 단일 버튼 회의끼기를 지원합니다.

- 참여한 전화기의 내장 컨퍼런스 브리지 - 이 모드에서는 단일 버튼 참여 기능을 사용합니다.
- 공유 컨퍼런스 브리지 - 이 모드는 단일 버튼 회의끼기 기능을 사용합니다.

원격 사용 중 통화의 공유 회선 버튼을 누르면 모든 상대방이 있는 통화의 사용자가 추가되고 모든 상대방에게 참여 경고음이 수신됩니다(구성된 경우). 참여에 실패하면 원래 통화가 활성 상태로 유지됩니다. 사용할 수 있는 내장 또는 공유 컨퍼런스 브리지가 없으면 참여 요청이 거부되고 참여 개시자 디바이스에 메시지가 표시됩니다.

내장 전화회의

참여 소프트키 또는 공유 회선 버튼을 누르면 내장 컨퍼런스 브리지(사용 가능한 경우)를 사용하여 참여 통화가 설정됩니다. 내장 컨퍼런스 브리지는 참여를 설정하는 중에 미디어 중단이나 원래 통화의 표시 변경이 발생하지 않으므로 확실히 유익합니다.

공유 전화회의

회의끼기 소프트키 또는 공유 회선 버튼을 누르면 공유 컨퍼런스 브리지(사용 가능한 경우)를 사용하여 참여 통화가 설정됩니다. 원래 통화가 분리된 후 컨퍼런스 브리지에서 참가하며 이로 인해 잠깐 동안 미디어 중단이 발생합니다. 모든 상대방의 통화 정보가 “참여”로 변경됩니다. 참여 통화가 참여 대상 디바이스를 전화회의의 컨트롤러로 사용하는 전화회의의 통화가 됩니다. 컨트롤러는 전화회의에 상대방을 더 추가하거나 제거할 수 있습니다. 통화에서 모든 상대방이 떠나는 경우에는 남아 있는 두 상대방에게 잠깐 동안의 중단이 발생한 후 포인트 간 통화로 재연결되고, 공유 전화회의의 리소스가 해제됩니다.

내장 및 공유 전화회의의 차이점

다음 표에서는 내장 컨퍼런스 브리지와 공유 전화회의를 사용하는 참여의 차이점에 대해 설명합니다.

기능	내장 전화회의를 사용하여 참여	공유 전화회의를 사용하여 참여
표준 소프트키 템플릿에 참여/회의끼기 소프트키가 포함되어 있습니다. 참고 단일 버튼 참여/회의끼기 기능을 활성화하면 소프트키가 사용되지 않습니다.	예	아니요
참여를 설정하는 동안 미디어 중단이 발생합니다.	아니요	예
사용자에게 참여 설정음이 수신됩니다(구성된 경우).	예	예
참여 이니시에이터 전화기에 텍스트가 표시됩니다.	XXX에 참여	전화회의로
대상 전화기에 텍스트가 표시됩니다.	To/From 기타	전화회의로
다른 전화기에 텍스트가 표시됩니다.	To/From 대상	전화회의로
브리지에서 이미 참여한 통화에 두 번째 참여 설정을 지원합니다.	아니요	예
개시자가 통화를 해제합니다.	원래의 두 상대방에게 미디어 중단이 발생하지 않습니다.	두 상대방만 남아 있는 경우 공유 컨퍼런스 브리지를 해제하고 나머지 상대방을 포인트 간 통화로 재연결하기 위해 미디어가 중단됩니다.
대상이 통화를 해제합니다.	개시자와 다른 상대방을 포인트 간 통화로 재연결하기 위해 미디어 중단이 발생합니다.	두 상대방만 남아 있는 경우 공유 컨퍼런스 브리지를 해제하고 나머지 상대방을 포인트 간 통화로 재연결하기 위해 미디어가 중단됩니다.
다른 상대방이 통화를 해제합니다.	세 명의 상대방 모두 해제됩니다.	두 상대방만 남아 있는 경우 공유 컨퍼런스 브리지를 해제하고 나머지 상대방을 포인트 간 통화로 재연결하기 위해 미디어가 중단됩니다.

기능	내장 전화회의를 사용하여 참여	공유 전화회의를 사용하여 참여
대상이 통화를 보류 중으로 설정하고 호전환, 통화참가 또는 통화 지정정보를 수행합니다.	개시자가 해제됩니다.	개시자와 기타 상대방이 연결된 상태를 유지합니다.

참여 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	내장 전화회의용 소프트키 템플릿 구성, 565 페이지	참여 소프트키를 소프트키 템플릿에 추가합니다. 내장 컨퍼런스 브리지에 대한 참여를 구성하는 경우 다음 절차를 수행합니다.
단계 2	공유 전화회의용 소프트키 템플릿 구성, 566 페이지	회의끼기 소프트키를 소프트키 템플릿에 추가합니다. 공유 컨퍼런스 브리지에 대한 참여를 구성하는 경우 다음 절차를 수행합니다.
단계 3	<p>소프트키 템플릿을 일반 디바이스 구성에 연결, 567 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> • 소프트키 템플릿을 일반 디바이스 구성에 추가, 568 페이지 • 일반 디바이스 구성을 전화기에 연결, 568 페이지 	(선택 사항) 전화기에서 소프트키 템플릿을 사용할 수 있게 하려면 이 단계 또는 다음 단계를 완료해야 합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 이 단계를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.
단계 4	소프트키 템플릿을 전화기에 연결, 567 페이지	(선택 사항) 이 절차를 사용하여 소프트키 템플릿을 일반 디바이스 구성에 연결하거나 일반 디바이스 구성과 함께 연결하는 대신 사용할 수 있습니다. 일반 디바이스 구성 또는 다른 기본 소프트키에서 할당을 무시하는 소프트키 템플릿을 할당해야 하는 경우 일반 디바이스 구성과 함께 이 절차를 사용합니다.
단계 5	내장 전화회의에 대한 참여 구성, 569 페이지	내장 컨퍼런스 브리지에 대한 참여를 구성합니다.
단계 6	공유 전화회의에 대한 참여 구성, 570 페이지	공유 컨퍼런스 브리지에 대한 참여를 구성합니다.
단계 7	사용자를 디바이스에 연결, 71 페이지	사용자를 디바이스와 연결합니다.

내장 전화회의용 소프트키 템플릿 구성

참여에 대한 소프트키 템플릿을 구성하고 참여 소프트웨어를 해당 템플릿에 할당합니다. 원격 연결 사용 통화 상태에서 참여 소프트웨어를 구성할 수 있습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
 - 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
 - a) 새로 추가를 클릭합니다.
 - b) 기본 템플릿을 선택하고 복사를 클릭합니다.
 - c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - d) 저장을 클릭합니다.
 - 단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
 - a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 필요한 기존 템플릿을 선택합니다.
 - 단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.
- 참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.
- 단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
 - 단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.
 - 단계 7 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.
 - 단계 8 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.
 - 단계 9 저장을 클릭합니다.
 - 단계 10 다음 작업 중 하나를 수행합니다.
 - 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 색선을 참조하십시오.

다음에 수행할 작업

다음 절차 중 하나를 수행합니다.

- 소프트키 템플릿을 일반 디바이스 구성에 추가, 568 페이지
- 일반 디바이스 구성을 전화기에 연결, 568 페이지

공유 전화회의용 소프트키 템플릿 구성

공유 전화회의에 대한 소프트키 템플릿을 구성하고 회의끼기 소프트키를 해당 템플릿에 할당합니다. 원격 사용 중 통화 상태에서 회의끼기 소프트키를 구성할 수 있습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
 - a) 새로 추가를 클릭합니다.
 - b) 기본 템플릿을 선택하고 복사를 클릭합니다.
 - c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - d) 저장을 클릭합니다.
- 단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.
 - a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 필요한 기존 템플릿을 선택합니다.
- 단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.

참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.
- 단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.
- 단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.
- 단계 7 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.
- 단계 8 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.
- 단계 9 저장을 클릭합니다.
- 단계 10 다음 작업 중 하나를 수행합니다.
 - 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

소프트키 템플릿을 전화기에 연결

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.
전화기 찾기 및 나열 창이 표시됩니다.

단계 2 소프트키 템플릿을 추가할 전화기를 찾습니다.

단계 3 다음 작업 중 하나를 수행합니다.

- 일반 디바이스 구성 드롭다운 목록에서 필요한 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.
- 소프트키 템플릿 드롭다운 목록에서 참여 또는 회의끼기 소프트키가 포함된 소프트키 템플릿을 선택합니다.

단계 4 저장을 클릭합니다.

전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

소프트키 템플릿을 일반 디바이스 구성에 연결

선택 사항. 다음 두 가지 방법으로 소프트키 템플릿을 전화기에 연결할 수 있습니다.

- 소프트키 템플릿을 전화기 구성에 추가합니다.
- 소프트키 템플릿을 일반 디바이스 구성에 추가합니다.

이 섹션의 절차에서는 소프트키 템플릿을 일반 디바이스 구성에 연결하는 방법에 대해 설명합니다. 시스템에서 일반 디바이스 구성을 사용하여 전화기에 구성 옵션을 적용하는 경우 다음 절차를 수행합니다. 이 방법은 전화기에서 사용할 수 있는 소프트키 템플릿을 만드는 데 가장 일반적으로 사용되는 방법입니다.

대체 방법을 사용하려면 [소프트키 템플릿을 전화기에 연결, 567 페이지](#)의 내용을 참조하십시오.

프로시저

단계 1 [소프트키 템플릿을 일반 디바이스 구성에 추가, 404 페이지](#)

단계 2 [일반 디바이스 구성을 전화기에 연결, 405 페이지](#)

소프트키 템플릿을 일반 디바이스 구성에 추가

시작하기 전에

필요에 따라 다음 중 하나 또는 둘 모두 수행합니다.

- [내장 전화회의용 소프트키 템플릿 구성, 565 페이지](#)
- [공유 전화회의용 소프트키 템플릿 구성, 566 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성

단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성 하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.

- a) 새로 추가를 클릭합니다.
- b) 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
- c) 저장을 클릭합니다.

단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.

- a) 찾기를 클릭하고 검색 기준을 입력합니다.
- b) 기존 일반 디바이스 구성을 클릭합니다.

단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.

단계 5 저장을 클릭합니다.

단계 6 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

일반 디바이스 구성을 전화기에 연결

시작하기 전에

필요에 따라 다음 중 하나 또는 둘 모두 수행합니다.

- [내장 전화회의용 소프트키 템플릿 구성, 565 페이지](#)
- [공유 전화회의용 소프트키 템플릿 구성, 566 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.
- 단계 3 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.
- 단계 4 저장을 클릭합니다.
- 단계 5 재설정 을 클릭하여 전화기 설정을 업데이트합니다.

다음에 수행할 작업

다음 중 하나 또는 둘 모두 수행합니다.

- [내장 전화회의에 대한 참여 구성, 569 페이지](#)
- [공유 전화회의에 대한 참여 구성, 570 페이지](#)

내장 전화회의에 대한 참여 구성

대부분의 Cisco Unified IP Phone에는 내장 컨퍼런스 브리지 기능이 포함되어 있습니다. 즉, 이러한 Cisco IP 전화기에는 참여 기능을 지원하는 작은 컨퍼런스 브리지 역할을 하는 내부 DSP가 있습니다. 전화기 자체를 포함하는 대상자를 최대 3개까지만 지원할 수 있습니다. 펌웨어 버전 11.x부터 시작하는 Cisco IP 전화기 8800 시리즈에는 BIB(빌트-인 브리지(BIB)) 기능을 데이지 체인으로 연결하는 기능이 있습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개 변수를 선택하고 빌트-인 브리지(BIB) 활성화 클러스터 수준 서비스 매개 변수를 켜기로 설정합니다.

참고	이 매개 변수를 끄기로 설정하는 경우에는 전화기 구성 창에서 빌트-인 브리지(BIB) 필드를 설정하여 각 전화기에 대한 참여를 구성합니다.
----	---
- 단계 2 대상자 입장 신호음 클러스터 수준 서비스 매개 변수를 **True**(신호음에 필요)로 설정하거나 디렉터리 번호 구성 창에서 대상자 입장 신호음 필드를 구성합니다.
- 단계 3 단일 버튼 참여/cBarge 정책을 참여로 설정합니다.

참고	이 매개 변수를 끄기로 설정하는 경우에는 전화기 구성에서 단일 버튼 참여 필드를 설정하여 각 전화기에 대한 단일 버튼 참여를 구성합니다.
----	--
- 단계 4 벨소리 울림 시 참여 허용 서비스 매개 변수를 **True**로 설정합니다.
- 단계 5 저장을 클릭합니다.

공유 전화회의에 대한 참여 구성

참여가 구성되어 있는 사용자에게 대해서는 공유 전화회의에 대한 참여(회의끼기)를 구성하지 않는 것이 좋습니다. 각 사용자별로 하나의 참여 방법만 선택하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개 변수를 선택하고 빌트-인 브리지(**BIB**) 활성화 클러스터 수준 서비스 매개 변수를 켜기로 설정합니다.

참고 이 매개 변수를 끄기로 설정하는 경우에는 전화기 구성 창에서 빌트-인 브리지(**BIB**) 필드를 설정하여 각 전화기에 대한 회의끼기를 구성합니다.

단계 2 대상자 입장 신호음 클러스터 수준 서비스 매개 변수를 **True**(신호음에 필요)로 설정하거나 디렉터리 번호 구성 창에서 대상자 입장 신호음 필드를 구성합니다.

단계 3 단일 버튼 참여/회의끼기 정책을 회의끼기로 설정합니다.

참고 이 매개 변수를 끄기로 설정하는 경우에는 전화기 구성 창에서 단일 버튼 회의끼기 필드를 설정하여 각 전화기에 대한 단일 버튼 회의끼기를 구성합니다.

단계 4 벨소리 울림 시 참여 허용 서비스 매개 변수를 **True**로 설정합니다.

단계 5 저장을 클릭합니다.

사용자를 디바이스에 연결

시작하기 전에

다음 중 하나 또는 둘 모두 수행합니다.

- [내장 전화회의에 대한 참여 구성, 569 페이지](#)
- [공유 전화회의에 대한 참여 구성, 570 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 사용자 관리 > 최종 사용자를 선택합니다.

단계 2 사용자 위치 찾기 필드에 적절한 필터를 지정한 다음, 찾기를 선택하여 사용자 목록을 검색합니다.

단계 3 목록에서 사용자를 선택합니다.
최종 사용자 구성 창이 표시됩니다.

단계 4 디바이스 정보 섹션을 찾습니다.

단계 5 디바이스 연결을 클릭합니다.
사용자 디바이스 연결 창이 나타납니다.

단계 6 CTI 원격 디바이스를 찾아 선택합니다.

단계 7 연결을 완료하려면 선택 항목/변경 사항 저장을 클릭합니다.

단계 8 관련 링크 드롭다운 목록에서 사용자로 돌아가기를 선택한 다음 이동을 클릭합니다.

최종 사용자 구성 창이 나타나고 선택한 연결 디바이스가 제어된 이바이스 창에 표시됩니다.

참여 상호 작용

기능	상호 작용
회의끼기	참여 또는 회의끼기 소프트키 중 하나를 소프트키 템플릿에 할당하는 것이 좋습니다. 각 디바이스에 이러한 소프트키 중 하나만 있게 하면 사용자의 혼동을 막고 잠재적인 성능 문제를 방지할 수 있습니다. 참고 디바이스에 참여 단일 버튼 또는 회의끼기 단일 버튼 중 하나를 활성화할 수 있습니다.
통화 지정보류	대상이 통화를 지정보류하면 참여 개시자가 해제되거나(빌트-인 브리지(BIB)를 사용할 경우) 참여 개시자 및 다른 상대방이 연결된 상태로 유지됩니다(공유 전화회의를 사용할 경우).
참가	대상이 다른 통화를 사용하여 통화에 참가하는 경우 참여 개시자가 해제되거나(빌트-인 브리지(BIB)를 사용 중인 경우) 참여 개시자와 다른 상대방이 연결된 상태로 유지됩니다(공유 전화회의를 사용 중인 경우).
PLAR(Private Line Automated Ringdown)	참여, 회의끼기 또는 단일 버튼 참여 이니시에이터는 참여 및 전용 회선 자동 링다운(PLAR)에 대해 구성된 공유 회선을 통해 통화로 참여할 수 있습니다. 참여 대상이 통화 중에 PLAR 회선에 연결된 미리 구성된 번호를 사용하는 경우 이니시에이터는 통화로 참여할 수 있습니다. Cisco Unified Communications Manager는 참여 통화를 연결하기 전에 PLAR 회선에 대해 참여 호출을 보내지 않습니다. 따라서 PLAR 대상의 상태에 관계 없이 참여가 이루어지지 않습니다. PLAR에서 참여, 회의끼기 또는 참여 단일 버튼 기능을 PLAR과 함께 작동하려면 참여, 회의끼기 또는 참여 단일 버튼을 구성해야 합니다. 또한 PLAR 대상, 특히 PLAR에 사용되는 디렉터리 번호를 구성해야 합니다.

참여 제한 사항

제한 사항	설명
추가 발신자	참여 개시자는 추가 발신자에서 전화회의를 시작할 수 없습니다.

제한 사항	설명
CTI(컴퓨터 전화 통신 인터페이스)	CTI는 TAPI 및 JTAPI 애플리케이션이 호출하는 API를 통한 참여를 지원하지 않습니다. CTI는 참여 또는 회의끼기 소프트웨어를 사용하여 IP 전화기에서 수동으로 호출하면 참여 이벤트를 생성합니다.
G.711 코덱	원래 통화에는 G.711 코덱이 필요합니다. G.711을 사용할 수 없는 경우, 회의끼기를 대신 사용하십시오.
Cisco Unified IP Phone	소프트키를 사용하는 IP 전화기에 참여 소프트웨어를 포함한 소프트웨어 템플릿을 할당할 수 있습니다. 그러나, 일부 IP 전화기는 참여 기능을 지원하지 않습니다.
암호화	Cisco Unified IP Phone 7960 및 7940에 대해 암호화를 구성할 경우, 암호화된 해당 디바이스는 암호화된 통화에 참여 중일 때 참여 요청을 수락할 수 없습니다. 통화가 암호화되어 있으면 참여 시도가 실패합니다. 전화기에서 참여가 실패했음을 나타내는 신호음이 재생됩니다.
최대 통화 수	전화회의에서 공유 회선 사용자 수가 참여를 시도하는 디바이스에 대한 최대 통화 수 설정의 구성보다 크거나 같을 경우, 전화기에 한도 초과 오류 메시지가 표시됩니다.

참여 문제 해결

사용 가능한 전화회의 브리지 없음

참여 소프트웨어를 누르면 IP 전화기에 사용 가능한 전화회의 브리지 없음 메시지가 표시됩니다.

대상 전화기에 대한 전화기 구성 창의 빌트-인 브리지(**BIB**) 필드가 제대로 설정되지 않았습니다.

문제를 해결하려면 다음 절차를 수행합니다.

1. Cisco Unified CM 관리에서 디바이스 > 전화기를 선택하고 전화기 찾기를 클릭하여 문제가 있는 전화기의 전화기 구성을 찾습니다.
2. 빌트-인 브리지(**BIB**) 필드를 켜기로 설정합니다.
3. 업데이트를 클릭합니다.
4. 전화기를 재설정합니다.

오류: 통과 제한

전화기에 오류: 초과 제한 메시지가 표시됩니다.

전화회의의 공유 회선 사용자 수는 참여하려는 디바이스의 최대 통화 수 필드에 대한 구성과 같거나 그 이상입니다.

- 서비스 매개 변수 구성 창으로 이동하여 클러스터 수준 매개 변수(기능 - 전화회의) 섹션을 찾습니다. 필요에 따라 최대 애드-혹 컨퍼런스 매개 변수 값을 늘립니다.
- 참여를 시도하는 디바이스의 공유 회선에 대한 최대 통화 수 값을 확인하고 필요에 따라 값을 늘립니다.

오류: 통과 제한



41 장

BLF 프리젠스

- BLF 프리젠스 개요, 575 페이지
- BLF 프리젠스 사전 요건, 576 페이지
- BLF 프리젠스 구성 작업 흐름, 576 페이지
- BLF 프리젠스 상호 작용, 588 페이지
- BLF 프리젠스 제한 사항, 588 페이지

BLF 프리젠스 개요

통화 상태 감시(BLF) 프레즌스 기능을 사용하면 감시자가 감시자 디바이스의 SIP(세션 시작 프로토콜) URI(통합 리소스 식별자) 또는 디렉터리 번호에서 다른 사용자의 실시간 상태를 모니터링할 수 있습니다.

감시자는 다음 옵션을 사용하여 사용자 또는 BLF 프리젠스 엔티티(프레젠테리티(presentity)라고도 함)의 상태를 모니터링할 수 있습니다.

- BLF 및 단축 다이얼 버튼
- 디렉터리 창 의 부재 중 전화, 발신 통화 또는 수신 통화 목록
- 회사 디렉터리와 같은 공유 디렉터리

통화 목록 및 디렉터리에는 기존 항목의 BLF 상태가 표시됩니다. BLF 및 단축 다이얼 버튼을 구성하는 경우 BLF 프리젠스 엔티티가 감시자 디바이스에 단축 다이얼로 표시됩니다.

BLF 프리젠스 엔티티 상태를 보기 위해 감시자는 BLF 프리젠스 요청을 Cisco Unified Communications Manager에 전송합니다. 관리자가 BLF 프리젠스 기능을 구성하고 나면 BLF 프리젠스 엔티티가 전화기에 있는지, 없는지 알 수 없는 상태인지 등을 나타내는 실시간 상태 아이콘이 감시자 디바이스에 표시됩니다.

Extension Mobility 사용자는 Extension Mobility 지원이 있는 전화기에서 BLF 프리젠스 기능을 사용할 수 있습니다.

BLF 프리젠스 그룹 권한 부여를 통해 권한 있는 감시자만 대상에 대한 BLF 프리젠스 상태에 액세스할 수 있도록 합니다. BLF 또는 단축 다이얼이 구성되면 관리자가 감시자에게 대상을 모니터링할 권한이 있는지 확인하므로 BLF 프리젠스 그룹 권한 부여가 BLF 또는 단축 다이얼에 적용되지 않습니다.

BLF 프리젠프스 사전 요건

- BLF 프리젠프스 기능을 사용하려는 경우 사용할 전화기를 구성합니다.
- BLF 프리젠프스 기능을 사용하려는 SIP 트렁크를 구성합니다.

BLF 프리젠프스 구성 작업 흐름

시작하기 전에

- [BLF 프리젠프스 사전 요건, 576 페이지](#) 검토

프로시저

	명령 또는 동작	목적
단계 1	통화 상태 감시(BLF)에 대한 클러스터 수준 엔터프라이즈 매개 변수를 구성하고 동기화합니다. BLF에 대한 클러스터 수준 엔터프라이즈 매개 변수 구성/동기화, 577 페이지 참조	동일한 클러스터의 모든 디바이스 및 서비스에 적용되는 BLF 옵션을 구성합니다. 엔터프라이즈 매개 변수 구성 변경 사항을 구성된 디바이스와 동기화하여 방해를 최소화하는 방식으로 동기화할 수 있습니다. 예를 들어 몇몇 영향을 받는 디바이스에서는 재설정 또는 재시작할 필요가 없을 수도 있습니다.
단계 2	BLF에 대한 클러스터 수준 서비스 매개 변수를 구성합니다. BLF에 대한 클러스터 수준 서비스 매개 변수 구성, 578 페이지 참조	Cisco Unified Communications Manager 관리의 선택한 서버에서 서로 다른 서비스를 구성하도록 프레즌스 서비스 매개 변수를 구성합니다.
단계 3	BLF 프리젠프스 그룹을 구성합니다. BLF 프리젠프스 그룹 구성, 579 페이지 참조	감시자가 모니터링할 수 있는 대상을 제어하도록 BLF 프리젠프스 그룹을 구성합니다.
단계 4	BLF 프리젠프스 그룹을 디바이스 및 사용자와 연결하려면 다음 하위 작업을 수행합니다. <ul style="list-style-type: none"> • BLF 프리젠프스 그룹을 전화기와 연결합니다. BLF 프리젠프스 그룹을 전화기와 연결, 581 페이지 참조 • BLF 프리젠프스 그룹을 SIP 트렁크와 연결합니다. BLF 프리젠프스 그룹을 SIP 트렁크와 연결, 582 페이지 참조 • BLF 프리젠프스 그룹을 최종 사용자와 연결합니다. BLF 프리젠프스 그룹을 최종 사용자와 연결, 583 페이지 참조 	디렉터리 번호, SIP 트렁크, SIP를 실행하는 전화기, SCCP를 실행하는 전화기, 애플리케이션 사용자(SIP 트렁크를 통해 프레즌스 요청을 보내는 애플리케이션 사용자) 또는 최종 사용자에게 BLF 프리젠프스 그룹을 적용합니다.

	명령 또는 동작	목적
	<ul style="list-style-type: none"> • BLF 프리젠스 그룹을 애플리케이션 사용자와 연결합니다. BLF 프리젠스 그룹을 애플리케이션 사용자와 연결, 583 페이지 참조 	
단계 5	외부 트렁크 및 애플리케이션에 대한 BLF 프리젠스 요청을 수락합니다. 외부 트렁크 및 애플리케이션에 대한 BLF 프리젠스 요청 수락, 584 페이지 참조	트렁크 수준 인증 외에 SIP 트렁크 애플리케이션에 대한 애플리케이션 수준 인증을 활성화합니다.
단계 6	발신 검색 공간을 구성합니다. 프레즌스 요청에 대한 발신 검색 공간 구성, 585 페이지 참조	SIP 트렁크, 전화기 또는 최종 사용자에게 SUBSCRIBE 발신 검색 공간을 적용합니다. [SUBSCRIBE 발신 검색 공간]에 따라 Cisco Unified Communications Manager가 트렁크 또는 전화기에서 보내는 프레즌스 요청의 경로를 설정하는 방법이 결정됩니다. 발신 검색 공간은 통화를 완료하려고 시도할 때 발신 디바이스에서 검색하는 파티션을 결정합니다. 프레즌스 요청에 대해 서로 다른 발신 검색 공간을 선택하지 않는 경우 SUBSCRIBE 발신 검색 공간은 기본 옵션인 없음을 선택합니다.
단계 7	BLF 및 단축 다이얼 버튼에 대한 전화기 버튼 템플릿을 구성합니다. BLF 및 단축 다이얼 버튼에 대한 전화기 버튼 템플릿 구성, 586 페이지 참조	<p>전화기 또는 사용자 디바이스 프로파일에 대해 BLF 및 단축 다이얼 버튼의 전화기 버튼 템플릿을 구성합니다.</p> <p>참고 템플릿에서 BLF 및 단축 다이얼을 지원하지 않는 경우에는 새 BLF SD 추가 링크가 할당되지 않은 연결 항목 창에 표시됩니다.</p>
단계 8	버튼 템플릿을 디바이스와 연결합니다. 버튼 템플릿을 디바이스와 연결, 587 페이지 참조	BLF 프리젠스에 대해 구성된 디바이스와 함께 버튼 템플릿을 사용합니다.
단계 9	사용자 디바이스 프로파일을 구성합니다. 사용자 디바이스 프로파일 구성, 587 페이지 참조	BLF 프리젠스에 대한 사용자 디바이스 프로파일을 구성합니다.

BLF에 대한 클러스터 수준 엔터프라이즈 매개 변수 구성/동기화

동일한 클러스터의 모든 디바이스 및 서비스에 적용되는 기본 설정에 엔터프라이즈 매개 변수를 사용합니다. 클러스터는 동일한 데이터베이스를 공유하는 Cisco Unified Communications Manager 세트로 구성됩니다. 새 Cisco Unified Communications Manager를 설치하는 경우 이 Cisco Unified Communications Manager는 엔터프라이즈 매개 변수를 사용하여 관련 디바이스 기본값의 초기값을 설정합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 엔터프라이즈 매개 변수.

단계 2 엔터프라이즈 매개 변수 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

팁 매개 변수에 대한 자세한 내용을 보려면 엔터프라이즈 매개 변수 구성 창에 표시되는 매개 변수 이름 또는 물음표를 클릭합니다.

단계 3 저장을 클릭합니다.

단계 4 (선택 사항) 구성 적용을 클릭하여 클러스터 수준 매개 변수를 동기화합니다.

구성 정보 적용 대화 상자가 표시됩니다.

단계 5 확인을 클릭합니다.

BLF에 대한 클러스터 수준 서비스 매개 변수 구성

서비스 매개 변수 구성 창에서 BLF에 사용할 수 있는 서비스를 하나 이상 구성할 수 있습니다.

시작하기 전에

[BLF에 대한 클러스터 수준 엔터프라이즈 매개 변수 구성/동기화, 577 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 매개 변수를 구성할 서버를 선택합니다.

단계 3 서비스 매개 변수 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

팁 서비스 매개 변수에 대한 자세한 내용을 보려면 서비스 매개 변수 구성 창에 표시되는 매개 변수 이름 또는 물음표를 클릭합니다.

단계 4 저장을 클릭합니다.

참고 기본 프레즌스 그룹 간 가입(Default Inter-Presence Group Subscription) 매개 변수는 BLF 및 단축 다이얼에 적용되지 않습니다.

BLF 프리젠프스 그룹 구성

BLF 프리젠프스 그룹을 사용하여 감시자가 모니터링할 수 있는 대상을 제어할 수 있습니다. BLF 프리젠프스 그룹을 구성하려면 Cisco 통합 커뮤니케이션 매니저 관리에서 그룹을 생성하고 하나 이상의 대상 및 감시자를 같은 그룹에 할당합니다.

새 BLF 프리젠프스 그룹을 추가할 때 Unified Communications Manager는 기본 클러스터 필드를 초기 권한 필드로 사용하여 새 그룹에 대한 모든 그룹 관계를 정의합니다. 다른 권한을 적용하려면 변경하려는 각 권한에 대한 새 그룹 및 기존 그룹 사이에 새 권한을 구성합니다.



참고 시스템에서는 같은 BLF 프리젠프스 그룹 내의 BLF 프리젠프스 요청을 항상 허용합니다.

프레즌스 엔티티의 상태를 보려면 감시자는 Unified Communications Manager로 프레즌스 요청을 보냅니다. 감시자는 다음과 같은 요구 사항을 사용하여 권한을 부여 받아야 시스템에서 프레즌스 엔티티에 대한 상태 요청을 시작할 수 있습니다.

- 감시자 BLF 프리젠프스 그룹은 클러스터 내부이든 클러스터 외부이든 프레즌스 엔티티 프레즌스 그룹에 대한 상태를 얻을 수 있도록 인증을 받아야 합니다.
- Unified CM은 외부 프레즌스 서버 또는 애플리케이션의 BLF 프리젠프스 요청을 수락할 수 있도록 인증을 받아야 합니다.

시작하기 전에

[BLF에 대한 클러스터 수준 서비스 매개 변수 구성, 578 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > **BLF** 프리젠프스 그룹.

단계 2 **BLF** 프리젠프스 그룹 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [BLF에 대한 BLF 프리젠프스 그룹 필드, 580 페이지](#)의 내용을 참조하십시오.

참고 Cisco CallManager 서비스에 기본 프레즌스 간 그룹 구독 서비스 매개 변수를 사용합니다. 이는 BLF 프리젠프스 그룹에 대한 클러스터 수준 권한 매개 변수를 설정하여 구독을 허용하거나 구독을 거부합니다. 이 필드를 통해 관리자는 클러스터에 대한 기본 필드를 사용하여 시스템 기본값을 설정하고 BLF 프리젠프스 그룹 관계를 구성할 수 있습니다.

단계 3 저장을 클릭합니다.

참고 BLF 프리젠프스 그룹에 대해 구성된 권한은 **BLF** 프리젠프스 그룹 관계 창에 표시됩니다. 그룹 간 관계에 대해 시스템 기본 권한 필드를 사용하는 권한은 표시되지 않습니다.

다음에 수행할 작업

다음 하위 작업을 수행하여 BLF 프리젠스 그룹을 디바이스 및 사용자와 연결합니다.

- [BLF 프리젠스 그룹을 전화기와 연결, 581 페이지](#)
- [BLF 프리젠스 그룹을 SIP 트렁크와 연결, 582 페이지](#)
- [BLF 프리젠스 그룹을 최종 사용자와 연결, 583 페이지](#)
- [BLF 프리젠스 그룹을 애플리케이션 사용자와 연결, 583 페이지](#)

BLF에 대한 BLF 프리젠스 그룹 필드

프레즌스 인증은 BLF 프리젠스 그룹에 적용됩니다. 다음 표에서는 BLF 프리젠스 그룹 구성 필드에 대해 설명합니다.

필드	설명
이름	구성할 BLF 프리젠스 그룹의 이름을 입력합니다. (예: Executive_Group).
설명	구성 중인 BLF 프리젠스 그룹에 대한 설명을 입력합니다.
기타 프레즌스 그룹에 대한 관계 수정	하나 이상의 BLF 프리젠스 그룹을 선택하여 지정된 그룹에 대한 권한 필드를 선택된 그룹으로 구성합니다.
가입 권한	<p>선택된 BLF 프리젠스 그룹의 경우 드롭다운 목록에서 다음 옵션의 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 시스템 기본값 사용 - 권한 필드를 기본 프레즌스 그룹 간 가입(Default Inter-Presence Group Subscription) 클러스터 수준 서비스 매개 변수 필드(가입 허용 또는 가입 허용 안 함)로 구성합니다. • 가입 허용 - 지정된 그룹의 구성원이 선택된 그룹의 구성원에 대한 실시간 상태를 보도록 허용합니다. • 가입 허용 안 함 - 지정된 그룹의 구성원이 선택된 그룹의 구성원에 대한 실시간 상태를 보지 못하도록 차단합니다. <p>구성하는 권한은 저장을 클릭하면 [BLF 프리젠스 그룹 관계] 창에 표시됩니다. 시스템 기본 권한 필드를 사용하는 모든 그룹이 나타나는 것은 아닙니다.</p>

디바이스 및 사용자와의 BLF 존재 그룹 연결

다음 절차를 수행하여 전화기, SIP 트렁크, SIP를 실행하는 전화기, SCCP를 실행하는 전화기, 애플리케이션 사용자(SIP 트렁크를 통해 프레즌스 요청을 보내는 애플리케이션 사용자) 및 최종 사용자에게 BLF 프리젠스 그룹을 적용합니다.



참고 시스템에서는 동일한 BLF 프리젠스 그룹 내 구성원 간의 프레즌스 요청을 허용합니다.

BLF 프리젠스 그룹을 전화기와 연결

전화기와 트렁크에 프레즌스 요청을 보내고 받을 수 있는 권한이 있을 때 전화기와 트렁크에 BLF 프리젠스를 사용할 수 있습니다.

Cisco Unified Communications Manager는 Cisco Unified Communications Manager 사용자를 위해 BLF 프리젠스 요청을 처리하며, 이는 클러스터 안에서든 밖에서든 무관합니다. 전화기를 통해 BLF 프리젠스 요청을 보내는 Cisco Unified Communications Manager 감시자의 경우, Cisco Unified Communications Manager는 전화기와 BLF 프리젠스가 같은 곳에 배치되어 있으면 BLF 프리젠스 상태로 응답합니다.

시작하기 전에

[BLF 프리젠스 그룹 구성, 579 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기 > 새로 추가를 선택합니다.

새 전화기 추가 창이 표시됩니다.

단계 2 전화기 유형드롭다운 목록에서 BLF 프리젠스 그룹을 연결할 전화기 유형을 선택합니다.

단계 3 다음을 클릭합니다.

단계 4 전화기 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.

참고 **SUBSCRIBE** 발신 검색 공간 드롭다운 목록에서 전화기의 프레즌스 요청에 사용할 **SUBSCRIBE** 발신 검색 공간을 선택합니다. Cisco Unified Communications Manager 관리에서 구성하는 발신 검색 공간이 모두 **SUBSCRIBE** 발신 검색 공간 드롭다운 목록에 나타납니다. 드롭다운 목록에서 최종 사용자에 대한 다른 발신 검색 공간을 선택하지 않으면 이 필드의 값은 기본값 없음을 적용합니다. **SUBSCRIBE** 발신 검색 공간을 특별히 이 용도에 맞게 구성하려면 모든 발신 검색 공간과 마찬가지로 발신 검색 공간을 구성해야 합니다.

단계 5 저장을 클릭합니다.

다음에 수행할 작업

다음 하위 작업을 수행하여 BLF 프리젠스 그룹을 디바이스 및 사용자와 연결합니다.

- [BLF 프리젠스 그룹을 SIP 트렁크와 연결, 582 페이지](#)
- [BLF 프리젠스 그룹을 최종 사용자와 연결, 583 페이지](#)
- [BLF 프리젠스 그룹을 애플리케이션 사용자와 연결, 583 페이지](#)

BLF 프리젼스 그룹을 SIP 트렁크와 연결

SIP 트렁크에 대해 다이제스트 인증이 구성되지 않으면 수신 가입을 수락하도록 트렁크를 구성할 수 있지만 애플리케이션 수준 인증을 시작할 수 없고 Unified CM이 그룹 권한 부여를 수행하기 전에 모든 수신 요청을 수락합니다. 애플리케이션 수준 인증에 다이제스트 인증이 사용되면 Unified CM에서도 BLF 프리젼스 요청을 전송 중인 애플리케이션의 자격 증명을 인증합니다.

클러스터 외부에 있는 디바이스에 대한 BLF 프리젼스 요청이 있는 경우 Unified Communications Manager는 SIP 트렁크를 통해 외부 디바이스를 쿼리합니다. 감시자에게 외부 디바이스를 모니터링할 권한이 있는 경우, SIP 트렁크는 BLF 프리젼스 요청을 외부 디바이스에 보내며 BLF 프리젼스 상태를 감시자에게 반환합니다.



팁 SIP 트렁크의 수신 프레즌스 요청에 BLF 프리젼스 그룹 권한 부여를 사용하려면 External_Presence_Serv_Group1 같이 트렁크에 대한 프레즌스 그룹을 구성한 다음 클러스터 내의 다른 그룹에 대해 적절한 권한을 구성합니다.

SIP 트렁크 프레즌스 요청에 대한 두 가지 수준의 권한 부여를 모두 구성하는 경우, 애플리케이션에 대한 수신 요청에서 BLF 프리젼스 그룹이 식별되지 않을 때에만 SIP 트렁크에 대한 BLF 프리젼스 그룹이 사용됩니다.

시작하기 전에

[BLF 프리젼스 그룹 구성, 579 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 트렁크, 새로 추가를 클릭합니다.

단계 2 트렁크 유형 드롭다운 목록에서 BLF 프리젼스 그룹을 연결할 전화기 유형을 선택합니다.

디바이스 프로토콜 드롭다운 목록에 있는 값이 자동으로 채워집니다.

단계 3 다음을 클릭합니다.

단계 4 트렁크 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.

참고 Unified CM 시스템이 SIP 트렁크로부터 수신되는 BLF 프리젼스 요청을 수락하도록 권한을 부여하려면 [SIP 트렁크 보안 프로파일 구성] 창의 [프레즌스 가입 수락] 확인란을 선택합니다. SIP 트렁크의 수신 프레즌스 요청을 차단하려면 확인란의 선택을 취소합니다. SIP 트렁크 BLF 프리젼스 요청을 허용하면 Unified CM이 트렁크에 연결하는 SIP 사용자 에이전트(SIP 프록시 서버 또는 외부 BLF 프리젼스 서버)의 요청을 수락합니다. SIP 트렁크의 BLF 프리젼스 요청을 수락하도록 Unified CM을 구성하는 경우 다이제스트 인증을 옵션으로 고려하십시오.

단계 5 저장을 클릭합니다.

다음에 수행할 작업

다음 하위 작업을 수행하여 BLF 프리젠스 그룹을 디바이스 및 사용자와 연결합니다.

- [BLF 프리젠스 그룹을 전화기와 연결, 581 페이지](#)
- [BLF 프리젠스 그룹을 최종 사용자와 연결, 583 페이지](#)
- [BLF 프리젠스 그룹을 애플리케이션 사용자와 연결, 583 페이지](#)

BLF 프리젠스 그룹을 최종 사용자와 연결

관리자는 BLF 프리젠스 그룹을 최종 사용자와 연결하여 사용자 디렉터리 및 통화 목록을 구성하고 Extension Mobility 설정을 구성합니다.

시작하기 전에

[BLF 프리젠스 그룹 구성, 579 페이지](#)

프로시저

-
- 단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 최종 사용자를 선택하고 새로 추가를 클릭합니다. 최종 사용자 구성 창이 표시됩니다.
- 단계 **2** 최종 사용자 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.
- 단계 **3** 저장을 클릭합니다.
-

다음에 수행할 작업

다음 하위 작업을 수행하여 BLF 프리젠스 그룹을 디바이스 및 사용자와 연결합니다.

- [BLF 프리젠스 그룹을 전화기와 연결, 581 페이지](#)
- [BLF 프리젠스 그룹을 SIP 트렁크와 연결, 582 페이지](#)
- [BLF 프리젠스 그룹을 애플리케이션 사용자와 연결, 583 페이지](#)

BLF 프리젠스 그룹을 애플리케이션 사용자와 연결

관리자는 BLF 프리젠스 그룹을 외부 애플리케이션에 대한 애플리케이션 사용자와 연결합니다. 이러한 외부 애플리케이션은 SIP 트렁크 또는 SIP 트렁크에 연결된 프록시 서버의 홈에 BLF 프리젠스 요청을 보냅니다. 예를 들어 웹 다이얼, 미팅 장소, 전화회의 서버 및 프레즌스 서버가 있습니다.

시작하기 전에

[BLF 프리젠스 그룹 구성, 579 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택하고 새로 추가를 클릭합니다. 애플리케이션 사용자 구성 화면이 나타납니다.
- 단계 2 애플리케이션 사용자 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.
- 단계 3 저장을 클릭합니다.
-

다음에 수행할 작업

다음 하위 작업을 수행하여 BLF 프리젠프스 그룹을 디바이스 및 사용자와 연결합니다.

- [BLF 프리젠프스 그룹을 전화기와 연결, 581 페이지](#)
- [BLF 프리젠프스 그룹을 SIP 트렁크와 연결, 582 페이지](#)
- [BLF 프리젠프스 그룹을 최종 사용자와 연결, 583 페이지](#)

외부 트렁크 및 애플리케이션에 대한 BLF 프리젠프스 요청 수락

클러스터 외부의 BLF 프리젠프스 요청을 허용하려면 외부 트렁크 또는 애플리케이션의 BLF 프리젠프스 요청을 수락하도록 시스템을 구성합니다. 클러스터 외부의 트렁크 및 애플리케이션에 BLF 프리젠프스 그룹을 할당하여 BLF 프리젠프스 그룹 권한 부여를 호출할 수 있습니다.

시작하기 전에

다음 하위 작업을 수행하여 BLF 프리젠프스 그룹을 디바이스 및 사용자와 연결합니다.

- [BLF 프리젠프스 그룹을 전화기와 연결, 581 페이지](#)
- [BLF 프리젠프스 그룹을 SIP 트렁크와 연결, 582 페이지](#)
- [BLF 프리젠프스 그룹을 최종 사용자와 연결, 583 페이지](#)
- [BLF 프리젠프스 그룹을 애플리케이션 사용자와 연결, 583 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 트렁크, 새로 추가를 클릭합니다. 트렁크 구성 창이 나타납니다.
- 단계 2 SIP 트렁크에서 BLF 프리젠프스 요청을 허용하려면, **SIP** 트렁크 보안 프로파일 구성 창에서 프레즌스 가입 수락 확인란을 선택합니다.
- 단계 3 트렁크 수준 권한 부여와 더불어 SIP 트렁크 애플리케이션에 대한 애플리케이션 수준 권한 부여를 활성화하려면 **SIP** 트렁크 보안 프로파일 구성 창에서 다음 확인란을 선택합니다.

- 다이제스트 인증 활성화
- 애플리케이션 수준 권한 부여 활성화

참고 다이제스트 인증 활성화를 선택하지 않는 경우 애플리케이션 수준 권한 부여 활성화를 선택할 수 없습니다.

단계 4 트렁크에 프로파일을 적용합니다. 재설정을 클릭하여 트렁크 변경 사항을 적용합니다.

참고 애플리케이션 수준 권한 부여 활성화를 선택한 경우 애플리케이션의 애플리케이션 사용자 구성 창에서 프레즌스 가입 수락을 선택합니다.

프레즌스 요청에 대한 발신 검색 공간 구성

[SUBSCRIBE 발신 검색 공간] 옵션을 사용하면 통화 처리 [BLF 프리젠프를 위한 발신 검색 공간] 요청과 별도로 발신 검색 공간을 적용할 수 있습니다. 프레즌스 요청에 대해 다른 발신 검색 공간을 선택합니다. 그렇지 않는 경우 SUBSCRIBE 발신 검색 공간은 없음 기본 옵션을 선택합니다. 최종 사용자와 연관된 SUBSCRIBE 발신 검색 공간은 Extension Mobility 통화에 사용됩니다.

SIP 트렁크, 전화기 또는 최종 사용자에게 SUBSCRIBE 발신 검색 공간을 적용할 수 있습니다. 최종 사용자와 연관된 SUBSCRIBE 발신 검색 공간은 Extension Mobility 통화에 사용됩니다.

시작하기 전에

[외부 트렁크 및 애플리케이션에 대한 BLF 프리젠프스 요청 수락, 584 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 발신 검색 공간.
- 단계 2 발신 검색 공간 구성 창이 표시되면 **SUBSCRIBE** 발신 검색 공간 드롭다운 목록에서 발신 검색 공간을 선택합니다.
- 단계 3 새로 추가를 클릭합니다.
- 단계 4 이름 필드에 이름을 입력합니다.
- 단계 5 (선택 사항) 설명 필드에 발신 검색 공간을 식별하기 위한 설명을 입력합니다.
- 단계 6 사용 가능한 파티션 목록에서 하나 이상의 파티션을 선택하고 화살표 키를 클릭합니다. 선택한 파티션이 선택한 파티션 목록에 표시됩니다.
- 단계 7 (선택 사항) 선택한 파티션 목록에서 파티션을 추가하거나 제거하려면 목록 상자 옆의 화살표 키를 클릭합니다.
- 단계 8 저장을 클릭합니다.

Cisco 통합 커뮤니케이션 매니저 관리에서 구성하는 발신 검색 공간은 모두 트렁크 구성 또는 전화기 구성 창의 **SUBSCRIBE** 발신 검색 공간 드롭다운 목록에 표시됩니다.

BLF 및 단축 다이얼 버튼에 대한 전화기 버튼 템플릿 구성

전화기 또는 사용자 디바이스 프로파일에 대해 BLF 및 단축 다이얼 버튼을 구성할 수 있습니다. 전화기나 디바이스 프로파일에 템플릿을 적용하고 전화기 또는 디바이스 프로파일 구성을 저장하면 Cisco Unified Communications Administration에서 새 BLF SD 추가 링크가 연결 정보 창에 표시됩니다.



참고 템플릿에서 BLF 및 단축 다이얼을 지원하지 않는 경우에는 새 BLF SD 추가 링크가 할당되지 않은 연결 항목 창에 표시됩니다.

관리자는 SIP URI에 대해 BLF 및 단축 다이얼 버튼을 추가하거나 변경하도록 결정할 때 감시자가 해당 대상을 모니터링할 권한이 있는지 확인합니다. 시스템에서 SIP 트렁크를 사용하여 SIP URI BLF 대상에 연결하면 SIP 트렁크와 연결된 BLF 프리젠스 그룹이 적용됩니다.



참고 BLF 및 단축 다이얼에 대해서는 BLF 프리젠스 그룹 또는 기본 프레즌스 그룹 간 가입(Default Inter-Presence Group Subscription) 매개 변수를 구성할 필요가 없습니다.

시작하기 전에

[프레즌스 요청에 대한 발신 검색 공간 구성, 585 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.

단계 2 새로 추가 단추를 클릭합니다.

전화기 버튼 템플릿 구성 창이 나타납니다.

단계 3 버튼 템플릿 이름 필드에 템플릿의 이름을 입력합니다.

단계 4 전화기 버튼 템플릿 드롭다운 목록에서 전화기 버튼 템플릿을 선택합니다.

단계 5 선택한 버튼 템플릿의 레이아웃을 기반으로 새 버튼 템플릿을 만들려면 복사를 클릭합니다.

단계 6 저장을 클릭합니다.

버튼 템플릿을 디바이스와 연결

전화기 또는 사용자 디바이스 프로파일에 대해 BLF 및 단축 다이얼 버튼을 구성합니다. BLF 값은 클러스터에 있을 필요가 없습니다. 전화기에 표시되는 통화 상태 감시(BLF) 상태 아이콘에 대해서는 사용 중인 전화기를 지원하는 Cisco Unified IP Phone 설명서를 참조하십시오. 전화기가 BLF 프리젼스를 지원하는지 확인하려면 사용 중인 전화기 및 이 Unified Communications Manager 버전을 지원하는 Cisco Unified IP Phone 설명서를 참조하십시오.

시작하기 전에

[BLF 및 단축 다이얼 버튼에 대한 전화기 버튼 템플릿 구성, 586 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 디바이스 프로파일.
 - 단계 2 검색 매개 변수를 입력하여 구성된 전화기 버튼 템플릿을 찾고 찾기를 클릭합니다.
모든 검색 기준과 일치하는 레코드가 표시됩니다.
 - 단계 3 레코드 중 하나를 클릭합니다.
디바이스 프로파일 구성 창이 나타납니다.
 - 단계 4 전화기 버튼 템플릿 목록에서 전화기 버튼 템플릿을 선택합니다.
 - 단계 5 (선택 사항) 구성된 디바이스의 값을 수정합니다.
 - 단계 6 저장을 클릭합니다.
-

사용자 디바이스 프로파일 구성

자세한 내용은 [BLF 프리젼스 상호 작용, 588 페이지](#)의 “Extension Mobility를 통한 BLF 프리젼스” 섹션을 참조하십시오.

시작하기 전에

[버튼 템플릿을 디바이스와 연결, 587 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > '디바이스 프로파일'을 선택합니다.
 - 단계 2 새로 추가를 클릭합니다.
디바이스 프로파일 구성 창이 나타납니다.
 - 단계 3 디바이스 프로파일 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.

참고 전화기 또는 디바이스 프로필에 적용한 전화기 버튼 템플릿이 BLF 및 단축 다이얼을 지원하지 않는 경우 링크는 연결 정보 창에 나타나지 않고 할당되지 않은 연결 항목 창에 나타납니다.

단계 4 저장을 클릭합니다.

BLF 프리젼스 상호 작용

기능	상호 작용
H.323 전화기 디바이스가 프레즌스 엔터티로 사용되는 경우 H.323 전화기의 DN이 있는 프레즌스 BLF	H.323 전화기가 [링인] 상태인 경우 BLF 상태는 [통화 중]으로 보고됩니다. SCCP 또는 SIP를 실행 중이고 RING IN 상태에 있는 전화기의 프레즌스 엔터티의 경우 BLF 상태는 유휴로 보고됩니다.
H.323 전화기 디바이스가 프레즌스 엔터티로 사용되는 경우 H.323 전화기의 DN이 있는 프레즌스 BLF	어떤 이유(예: 전화기에서 이더넷 케이블이 분리됨)로든 H.323 전화기가 Cisco Unified Communications Manager에 연결되지 않은 경우 BLF 상태는 항상 [유휴]로 보고됩니다. SCCP 또는 SIP를 실행 중이나 Cisco Unified Communications Manager에 연결되지 않은 전화기 프레즌스 엔터티의 경우 BLF 상태는 [알 수 없음]으로 보고됩니다.
Extension Mobility를 통한 BLF 프리젼스	Cisco Unified Communications Manager 관리의 사용자 디바이스 프로파일에서 BLF 및 단축 다이얼 버튼을 구성하면 Cisco Extension Mobility를 지원하는 전화기는 디바이스에 로그인한 후 BLF 및 단축 다이얼 버튼에 BLF 프리젼스 상태를 표시합니다. Extension Mobility 사용자가 로그아웃하면 Cisco Extension Mobility를 지원하는 전화기의 BLF 및 단축 다이얼 버튼에는 구성된 로그아웃 프로파일에 대한 BLF 프리젼스 상태가 표시됩니다.

BLF 프리젼스 제한 사항

제한 사항	설명
SIP 프레즌스	Cisco 통합 커뮤니케이션 매니저 Assistant는 SIP 프레즌스를 지원하지 않습니다.
BLF 프리젼스 요청	Cisco 통합 커뮤니케이션 매니저 관리는 헌트 파일럿에 연결된 디렉터리 번호에 대한 BLF 프리젼스 요청을 거부합니다.

제한 사항	설명
통화 목록 기능의 BLF	통화 목록 기능의 BLF는 Cisco Unified IP Phone 7940 및 Cisco Unified IP Phone 7960에서 지원되지 않습니다.
BLF 및 단축 다이얼	<p>관리자는 감시자가 BLF 및 단축 다이얼을 구성할 때 대상을 모니터링할 권한이 있는지 확인합니다. BLF 프리젠프스 그룹 인증은 BLF 및 바로 호출에 적용되지 않습니다.</p> <p>참고 SIP를 실행하는 전화기의 경우 통화 목록에 표시되는 BLF 및 단축 다이얼로 구성된 디렉터리 번호 또는 SIP URI에도 BLF 프리젠프스 그룹 권한 부여가 적용되지 않습니다.</p> <p>서로 다른 파티션에 동일한 내선 번호가 있는 중복 DN이 있는 경우, 디바이스에 할당된 SUBSCRIBE CSS 내에 구성된 파티션의 순서에 따라 프레즌스 알림이 선택됩니다.</p> <p>예를 들어, 전화기에 두 개의 BLF 단축 다이얼이 구성되어 있습니다.</p> <ul style="list-style-type: none"> • "내부" 파티션의 내선 번호 1234 • "외부" 파티션의 내선 번호 1234 <p>SUBSCRIBE CSS 내에서 첫 번째로 나열되는 파티션은 가입된 디바이스에 BLF 프리젠프스를 제공할 것입니다.</p>
BLF 프리젠프스 권한 부여	여러 회선을 사용하는 Cisco Unified IP Phone의 경우 전화기에서는 BLF 프리젠프스 인증을 확인하기 위해 부재 중 전화 및 발신 통화에 대해 회선 디렉터리 번호와 연결된 캐시된 정보를 사용합니다. 이 통화 정보가 제공되지 않는 경우 전화기에서는 BLF 프리젠프스 인증을 위한 가입자로 기본 회선을 사용합니다. 여러 회선을 사용하는 Cisco Unified IP Phone에 있는 BLF 및 단축 다이얼 버튼의 경우 전화기에서는 사용 가능한 첫 번째 회선을 가입자로 사용합니다.
Cisco Unified IP Phone	사용자가 SIP를 실행하는 Cisco Unified IP Phone 7960 및 7940에 사용하도록 구성된 디렉터리 번호를 모니터링하는 경우 프레즌스 엔터티가 오프 혹은 일 때(그러나 통화가 연결된 상태는 아님) 감시자 디바이스에 '통화 중이 아님'에 해당하는 상태 아이콘이 표시됩니다. 이러한 전화기는 오프 혹은 상태를 감지하지 않습니다. 기타 모든 전화기 유형의 경우 프레즌스 엔터티의 오프 혹은 상태에 대해 감시자 디바이스에 '통화 중'에 해당하는 상태 아이콘이 표시됩니다.
SIP 트렁크	BLF 프리젠프스 요청 및 응답은 SIP 트렁크 또는 SIP 트렁크와 연결된 경로로 전송되어야 합니다. 시스템에서는 MGCP 및 H323 트렁크 디바이스로 라우팅되는 BLF 프리젠프스 요청을 거부합니다.

제한 사항	설명
SIP를 실행하는 BLF 프리젠프스 지원 전화기	SIP를 실행 중인 BLF 프리젠프스 지원 전화기의 경우 디렉터리 번호 또는 SIP URI를 BLF 및 단축 다이얼을 구성할 수 있습니다. SCCP를 실행 중인 BLF 프리젠프스 지원 전화기의 경우 디렉터리 번호만 BLF 및 단축 다이얼 버튼으로 구성할 수 있습니다.
SIP를 실행하는 전화기	SIP를 실행하는 전화기의 경우 통화 목록에 표시되는 BLF 및 단축 다이얼로 구성된 디렉터리 번호 또는 SIP URI에도 BLF 프리젠프스 그룹 권한 부여가 적용되지 않습니다.



42 장

통화 표시 제한

- [통화 표시 제한 개요, 591 페이지](#)
- [통화 표시 제한 구성 작업 흐름, 591 페이지](#)
- [통화 표시 제한 상호 작용, 601 페이지](#)
- [통화 표시 제한 기능 제한 사항, 602 페이지](#)

통화 표시 제한 개요

Cisco Unified Communications Manager는 통화 및 연결된 사용자 모두에 대한 번호 및 이름 정보의 표시를 허용하고 제한하는 융통성 있는 구성 옵션을 제공합니다. 연결된 번호와 이름을 서로 독립적으로 제한할 수 있습니다.

SIP 트렁크 수준 또는 통화별 기준으로 연결된 번호 및 이름 제한을 구성할 수 있습니다. SIP 트렁크 수준 구성은 통화별 구성을 재정의합니다.

예를 들어 호텔 환경에서는 객실과 안내 데스크 간에 이루어진 통화에 대한 표시 정보는 보아야 할 수 있지만 객실 간 통화의 경우 어느 전화기에서도 통화 정보를 표시하지 않아야 합니다.

통화 표시 제한 구성 작업 흐름

시작하기 전에

- [통화 표시 제한 상호 작용, 601 페이지](#) 검토

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	통화 표시 제한 기능을 지원하는 엔드포인트를 식별하는 보고서를 생성합니다.
단계 2	통화 표시 제한을 위한 파티션 구성, 592 페이지	연결성 특성이 비슷한 디렉터리 번호(DN) 및 라우트 패턴의 논리적 그룹을 만들기 위해 파

	명령 또는 동작	목적
		티션을 구성합니다. 예를 들어 호텔 환경에서는 방 간에 전화를 걸 파티션을 구성하고 PSTN(공중 전화 교환망)으로 전화를 걸기 위한 파티션을 구성할 수 있습니다.
단계 3	통화 표시 제한 기능에 대한 발신 검색 공간 구성, 594 페이지.	발신 검색 공간을 구성하여 발신 디바이스에서 통화를 완료하려고 할 때 검색할 수 있는 파티션을 식별합니다. 객실, 안내 데스크, 다른 호텔 내선, PSTN 및 객실 지정 보류 범위(통화 지정 보류용)에 대한 발신 검색 공간을 만듭니다.
단계 4	연결된 번호 표시 제한에 대한 서비스 매개 변수 구성, 594 페이지.	연결된 회선 ID를 전화 건 번호에만 표시하도록 서비스 매개 변수를 구성합니다.
단계 5	변환 패턴 구성, 595 페이지.	다른 표시 제한 수준으로 변환 패턴을 구성합니다.
단계 6	전화기에 통화 표시 제한 구성, 597 페이지	통화 표시 제한 기능에 사용하려는 파티션 및 발신 검색 공간과 엔드포인트를 연결합니다.
단계 7	통화 표시 제한 기능을 위한 PSTN 게이트웨이 구성, 598 페이지	통화 표시 제한 기능에 사용하려는 파티션 및 발신 검색 공간과 PSTN 게이트웨이를 연결합니다.
단계 8	(선택 사항) SIP 트렁크에서 통화 표시 제한 구성, 599 페이지	이 절차를 사용하여 SIP 트렁크 수준에서 연결된 번호 및 이름 제한을 구성합니다. SIP 트렁크 수준 구성은 통화별 구성을 재정의합니다.

통화 표시 제한을 위한 파티션 구성

연결성 특성이 비슷한 디렉터리 번호(DN) 및 라우트 패턴의 논리적 그룹을 만들기 위해 파티션을 구성합니다. 파티션은 조직, 위치 및 통화 유형에 따라 라우트 플랜을 논리적 하위 집합으로 나눔으로써 콜 라우팅을 지원합니다. 여러 파티션을 구성할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 파티션.

단계 2 새로 추가를 클릭하여 새 파티션을 생성합니다.

단계 3 파티션 이름, 설명 필드에 경로 플랜에 고유한 파티션 이름을 입력합니다.

파티션 이름에는 영숫자 문자는 물론 공백, 하이픈(-) 및 밑줄(_)을 사용할 수 있습니다. 파티션 이름에 대한 지침은 온라인 도움말을 참조하십시오.

단계 4 파티션 이름 뒤에 쉼표(,)를 입력하고 동일한 줄에 파티션 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\), 꺾쇠괄호(<>) 또는 대괄호([])는 사용할 수 없습니다.

설명을 입력하지 않으면 Cisco Unified Communications Manager에서 자동으로 이 필드에 파티션 이름을 입력합니다.

단계 5 여러 파티션을 생성하려면 각 파티션 항목마다 한 행을 사용합니다.

단계 6 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.

시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성 상태로 유지됩니다.

단계 7 구성할 다음 라디오 버튼 중 하나를 선택하고 시간대를 구성합니다.

- 시작 디바이스—이 라디오 버튼을 선택하면 시스템은 발신 디바이스의 표준 시간대를 시간 일정과 비교하여 파티션을 수신 통화를 받는 데 사용할 수 있는지 여부를 확인합니다.
- 특정 표준 시간대—이 라디오 버튼을 선택한 후에 드롭다운 목록에서 표준 시간대를 선택합니다. 시스템은 선택한 표준 시간대를 시간 일정과 비교하여 수신 통화를 받는 데 파티션을 사용할 수 있는지 여부를 확인합니다.

단계 8 저장을 클릭합니다.

파티션 이름 지침

발신 검색 공간의 파티션 목록에서 최대 문자 수는 1024자로 제한됩니다. 즉, CSS의 최대 파티션 수는 파티션 이름의 길이에 따라 달라집니다. 다음 표를 사용하여 파티션 이름이 고정 길이인 경우 발신 검색 공간에 추가할 수 있는 최대 파티션 수를 결정합니다.

표 49: 파티션 이름 지침

파티션 이름 길이	최대 파티션 수
2자	340
3자	256
4자	204
5자	172
...	...
10자	92
15자	64

통화 표시 제한 기능에 대한 발신 검색 공간 구성

발신 검색 공간을 구성하여 발신 디바이스에서 통화를 완료하려고 할 때 검색할 수 있는 파티션을 식별합니다. 객실, 안내 데스크, 다른 호텔 내선, PSTN 및 객실 지정 보류 범위(통화 지정 보류용)에 대한 발신 검색 공간을 만듭니다.

시작하기 전에

[통화 표시 제한을 위한 파티션 구성, 592 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 발신 검색 공간.

단계 2 새로 추가를 클릭합니다.

단계 3 이름 필드에 이름을 입력합니다.

각 발신 검색 공간 이름은 시스템에 고유해야 합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.

단계 4 설명 필드에 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.

단계 5 사용 가능한 파티션 드롭다운 목록에서 다음 단계 중 하나를 수행합니다.

- 단일 파티션의 경우 해당 파티션을 선택합니다.
- 여러 파티션의 경우 컨트롤(**CTRL**) 키를 누른 상태에서 해당 파티션을 선택합니다.

단계 6 상자 사이에서 아래쪽 화살표를 선택하여 선택한 파티션 필드로 파티션을 이동합니다.

단계 7 (선택 사항) 선택한 파티션 상자 오른쪽의 화살표 키를 사용하여 선택한 파티션의 우선 순위를 변경합니다.

단계 8 저장을 클릭합니다.

연결된 번호 표시 제한에 대한 서비스 매개 변수 구성

연결된 번호 표시 제한은 연결된 회선 ID 표시를 전화를 건 번호로만 제한합니다. 이 옵션은 전화기 사용자에게 의미 없는 연결된 번호 표시 문제뿐 아니라 고객 프라이버시 문제도 해결합니다.

시작하기 전에

[통화 표시 제한 기능에 대한 발신 검색 공간 구성, 594 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.
- 단계 2 Cisco CallManager 서비스가 실행되는 서버를 선택한 다음 Cisco CallManager 서비스를 선택합니다.
- 단계 3 원래 전화 건 번호 항상 표시 서비스 매개 변수를 **True**로 설정하여 이 기능을 활성화합니다.
- 기본값은 **false**입니다.
- 단계 4 (선택 사항) 변환될 때 원래 전화 건 번호에 대한 이름 표시 서비스 매개 변수를 설정합니다.
- 기본 필드에는 변환 전에 원래 전화 건 번호의 경고 이름이 표시됩니다. 변환 후 전화 건 번호의 경고 이름을 표시하도록 이 매개 변수를 변경할 수 있습니다. 원래 번호 항상 표시 서비스 매개 변수를 **False**로 설정한 경우 이 매개 변수를 적용할 수 없습니다.
- 단계 5 저장을 클릭합니다.
-

변환 패턴 구성

Unified Communications Manager에서는 통화를 전송하기 전에 변환 패턴을 사용하여 전화 건 번호를 조작할 수 있습니다. 시스템에서 전화 건 번호를 사용하지 않는 경우가 있습니다. 또는 PSTN(Public Switched Telephone Network)에서 전화 건 번호를 인식하지 못할 수 있습니다. 통화 표시 제한 기능의 경우 통화가 실제 디바이스로 확장되기 전에 다양한 변환 패턴을 통해 통화가 전송됩니다.

시작하기 전에

[연결된 번호 표시 제한에 대한 서비스 매개 변수 구성, 594 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 변환 패턴.
- 단계 2 변환 패턴 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [통화 표시 제한 기능에 대한 변환 패턴 필드, 596 페이지](#)를 참조하십시오.
- 단계 3 저장을 클릭합니다.
-

통화 표시 제한 기능에 대한 변환 패턴 필드

필드	설명
변환 패턴	<p>숫자와 와일드 카드를 포함하여 변환 패턴을 입력합니다. 공백은 사용하지 마십시오. 예를 들어 NANP의 일반적인 로컬 액세스를 위해서는 9.@를 입력하고, 일반적인 개인 네트워크 번호 지정 플랜을 위해서는 8XXX를 입력합니다.</p> <p>올바른 문자에는 대문자 A, B, C, D와 국제 이스케이프 문자 +를 나타내는 \+가 포함됩니다.</p>
설명	변환 패턴에 대한 설명을 입력합니다. 설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&) 또는 꺾쇠괄호(<>)는 사용할 수 없습니다.
파티션	드롭다운 목록에서 이 변환 패턴과 연결할 파티션을 선택합니다.
발신 검색 공간	드롭다운 목록에서 이 변환 패턴과 연결할 발신 검색 공간을 선택합니다.
발신 회선 ID 표시	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 기본값—발신 회선 ID의 표시를 변경하지 않을 경우 이 옵션을 선택합니다. 허용됨—발신자의 전화 번호를 표시하려면 이 옵션을 선택합니다. 제한됨—Cisco Unified Communications Manager가 발신자 전화 번호를 표시하는 것을 차단하려면 이 옵션을 선택합니다.
발신 이름 표시	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 기본값—발신 이름의 표시를 변경하지 않을 경우 이 옵션을 선택합니다. 허용됨—발신자의 이름을 표시하려면 이 옵션을 선택합니다. 제한됨—Cisco Unified Communications Manager가 발신 이름을 표시하는 것을 차단하려면 이 옵션을 선택합니다.

필드	설명
연결된 회선 ID 표시	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 기본값—연결된 회선 ID의 표시를 변경하지 않을 경우 이 옵션을 선택합니다. 허용됨—연결된 상대의 전화 번호를 표시하려면 이 옵션을 선택합니다. 제한됨—Cisco Unified Communications Manager가 연결된 상대의 전화 번호를 표시하는 것을 차단하려면 이 옵션을 선택합니다.
연결된 이름 표시	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 기본값—연결된 상대 이름의 표시를 변경하지 않을 경우 이 옵션을 선택합니다. 허용됨—연결된 상대의 이름을 표시하려면 이 옵션을 선택합니다. 제한됨—Cisco Unified Communications Manager가 연결된 상대의 이름을 표시하는 것을 차단하려면 이 옵션을 선택합니다.

전화기에 통화 표시 제한 구성

통화 표시 제한 기능에 사용되는 파티션 및 발신 검색 공간과 전화기를 연결하려면 이 절차를 사용합니다.

시작하기 전에

[변환 패턴 구성, 595 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 전화기에 대한 필드를 수정하려면 검색 조건을 입력하고 결과 목록에서 전화기를 선택합니다. 전화기 구성 창이 나타납니다.
- 새 전화기를 추가하려면 새로 추가를 클릭합니다.
새 전화기 추가 창이 표시됩니다.

단계 3 발신 검색 공간 드롭다운 목록에서 시스템이 전화를 건 번호의 경로를 확인할 때 사용하려는 발신 검색 공간을 선택합니다.

단계 4 내부 통화에 대한 모든 표시 제한을 무시하려면 발신자 정보 표시기 무시(내부 통화만 해당) 확인란을 선택합니다.

- 단계 5 저장을 클릭합니다.
데이터베이스에 전화기가 추가됩니다.
- 단계 6 추가된 전화기를 디렉터리 번호에 연결하려면 디바이스 > 전화기를 선택하고 추가한 전화기를 검색할 검색 매개 변수를 입력합니다.
- 단계 7 전화기 찾기 및 나열 창에서 전화기 이름을 클릭합니다.
전화기 구성 창이 나타납니다.
- 단계 8 연결 창에서 디렉터리 번호를 추가하거나 수정할 전화기 이름을 클릭합니다.
디렉터리 번호 구성 창이 나타납니다.
- 단계 9 디렉터리 번호 구성 창의 디렉터리 번호 텍스트 상자에서 디렉터리 번호의 값을 추가 또는 수정하고 경로 파티션 드롭다운 목록에서 값을 선택합니다.
- 단계 10 저장을 클릭합니다.

전화기 구성 예

전화기 A(Room-1)에 파티션 P_Room 및 디바이스/회선 발신 검색 공간 CSS_FromRoom을 구성합니다.

{ P_Phones, CSS_FromRoom } : 221/Room-1

전화기 B(Room-2)에 파티션 P_Room 및 디바이스/회선 발신 검색 공간 CSS_FromRoom을 구성합니다.

{ P_Phones, CSS_FromRoom } : 222/Room-2

전화기 C(Front Desk-1)를 파티션 P_FrontDesk 및 디바이스/회선 발신 검색 공간으로 구성

CSS_FromFrontDesk 및 발신자 정보 표시기 무시 확인란 활성화됨

{ P_FrontDesk, CSS_FromFrontDesk, IgnorePresentationIndicators set } : 100/Reception

전화기 D(Front Desk-2)를 파티션 P_FrontDesk 및 디바이스/회선 발신 검색 공간으로 구성

CSS_FromFrontDesk 및 발신자 정보 표시기 무시 확인란 활성화됨

{ P_FrontDesk, CSS_FromFrontDesk, IgnorePresentationIndicators set } : 200/Reception

전화기 E(Club)에 파티션 P_Club 및 발신 검색 공간 CSS_FromClub을 구성합니다.

{ P_Club, CSS_FromClub } : 300/Club

통화 표시 제한 기능을 위한 PSTN 게이트웨이 구성

통화 표시 제한 기능에 사용하려는 파티션 및 발신 검색 공간과 PSTN 게이트웨이를 연결합니다.

시작하기 전에

[전화기에 통화 표시 제한 구성, 597 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.
- 단계 2 검색 조건을 입력하고 결과 목록에서 PSTN 게이트웨이를 선택합니다.
게이트웨이 구성 창이 나타납니다.
- 단계 3 발신 검색 공간 드롭다운 목록에서 시스템이 PSTN에서 수신 통화의 경로 지정 방법을 확인할 때 사용하려는 발신 검색 공간을 선택합니다.
- 단계 4 저장 및 재설정을 클릭하여 구성 변경 사항을 적용합니다.
- 단계 5 (선택 사항) 사용 가능한 트렁크 또는 게이트웨이를 연결하려면 Cisco Unified Communications Manager 관리에서 **SIP** 경로 패턴을 선택하고 **SIP** 트렁크/경로 목록 드롭다운 목록에서 SIP 트렁크 또는 경로 목록을 선택합니다.

게이트웨이 구성 예

PSTN 게이트웨이에 경로 패턴 P_PSTN 및 발신 검색 공간 CSS_FromPSTN을 구성합니다.

```
{CSS_FromPSTN}, RoutePattern {P_PSTN}
```

SIP 트렁크에서 통화 표시 제한 구성

SIP 트렁크 수준에서 연결된 번호 및 이름 제한을 구성할 수 있습니다. SIP 트렁크 수준 구성은 통화별 구성을 재정의합니다.

시작하기 전에

(선택 사항) [통화 표시 제한 기능을 위한 PSTN 게이트웨이 구성, 598 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 트렁크.
트렁크 찾기 및 나열 창이 나타납니다.
- 단계 2 검색 기준을 입력하고 찾기를 클릭합니다.
- 단계 3 업데이트하려는 트렁크의 이름을 선택합니다.
- 단계 4 **SIP** 트렁크 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 [통화 표시 제한을 위한 SIP 트렁크 필드, 600 페이지](#)를 참조하십시오.
- 단계 5 저장을 클릭합니다.

통화 표시 제한을 위한 SIP 트렁크 필드

표 50: 착신 전화

필드	설명
발신 회선 ID 표시	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 기본값—발신 회선 ID의 표시를 변경하지 않을 경우 이 옵션을 선택합니다. 허용됨—발신자의 전화 번호를 표시하려면 이 옵션을 선택합니다. 제한됨—Cisco Unified Communications Manager가 발신자 전화 번호를 표시하는 것을 차단하려면 이 옵션을 선택합니다.
발신 이름 표시	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 기본값—발신 이름의 표시를 변경하지 않을 경우 이 옵션을 선택합니다. 허용됨—발신자의 이름을 표시하려면 이 옵션을 선택합니다. 제한됨—Cisco Unified Communications Manager가 발신 이름을 표시하는 것을 차단하려면 이 옵션을 선택합니다.
발신 검색 공간	드롭다운 목록에서 이 변환 패턴과 연결할 발신 검색 공간을 선택합니다.

표 51: 발신 전화

필드	설명
연결된 회선 ID 표시	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 기본값—연결된 회선 ID의 표시를 변경하지 않을 경우 이 옵션을 선택합니다. 허용됨—연결된 상대의 전화 번호를 표시하려면 이 옵션을 선택합니다. 제한됨—Cisco Unified Communications Manager가 연결된 상대의 전화 번호를 표시하는 것을 차단하려면 이 옵션을 선택합니다.

필드	설명
연결된 이름 표시	<p>드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 기본값—연결된 상대 이름의 표시를 변경하지 않을 경우 이 옵션을 선택합니다. • 허용됨—연결된 상대의 이름을 표시하려면 이 옵션을 선택합니다. • 제한됨—Cisco Unified Communications Manager가 연결된 상대의 이름을 표시하는 것을 차단하려면 이 옵션을 선택합니다.

통화 표시 제한 상호 작용

이 섹션에서는 통화 표시 제한 기능이 Cisco Unified Communications Manager 애플리케이션 및 통화 처리 기능과 상호 작용하는 방식을 설명합니다.

기능	상호 작용
통화 지정보류	<p>통화 표시 제한 기능을 통화 지정보류와 함께 사용할 경우 통화 표시 제한 기능을 유지하려면 개별 통화 지정보류 번호에 관련 변환 패턴을 구성해야 합니다. 단일 변환 패턴을 구성하여 통화 지정보류 번호 범위를 처리할 수 없습니다.</p> <p>예를 들어 다음 시나리오를 참고하십시오.</p> <ol style="list-style-type: none"> 1. 시스템 관리자가 77x 대의 통화 지정보류 범위를 만들고 P_ParkRange 라는 파티션에 배치합니다. (전화기의 발신 검색 공간[CSS_FromRoom]에 P_ParkRange 파티션을 포함하면 객실 전화기에서 다른 객실의 전화기에 P_ParkRange 파티션이 표시되는 것을 볼 수 있습니다.) 2. 관리자는 각 통화 지정보류 디렉터리 번호에 별도의 변환 패턴을 구성하고 표시 필드를 [제한됨]으로 구성합니다. (이 시나리오에서 관리자는 770, 771, 772...779의 변환 패턴을 만듭니다.) <p>참고 통화 표시 제한 기능을 올바르게 작동하려면 관리자가 특정 번호대(예: 77x 또는 77[0-9])에 단일 변환 패턴을 구성하는 것이 아니라 별도의 변환 패턴을 구성해야 합니다.</p> <ol style="list-style-type: none"> 3. 객실-1에서 객실-2에 전화를 겁니다. 4. 객실 2가 응답하고 객실 1이 통화를 지정보류합니다. 5. 객실 1이 다시 통화를 가져오면 객실 2는 객실 1 통화 정보 표시를 볼 수 없습니다. <p>통화 대기 개요 참조</p>

기능	상호 작용
전화회의 목록	통화 표시 제한을 사용하면 전화회의 참가자 목록에 대한 표시 정보를 제한할 수 있습니다. 애드-혹 컨퍼런스 개요 참조
전화회의 및 음성 메일	통화 표시 제한을 전화회의, 음성 메일 등의 기능과 함께 사용할 경우 전화기에 표시되는 통화 정보에 해당 상태가 반영됩니다. 예를 들어, 전화회의 기능을 호출할 경우 통화 정보에 전화회의 연결이 표시됩니다. 메시지 버튼을 선택하여 음성 메일에 액세스할 경우 통화 정보에 음성 메일 연결이 표시됩니다.
Extension Mobility	Extension Mobility와 통화 표시 제한 기능을 함께 사용하려면 Cisco Unified Communications Manager 관리의 전화기 구성 창과 Cisco Unified Communications Manager 관리의 디바이스 프로파일 구성 창에서 발신자 정보 표시기 무시(내부 통화만) 매개 변수를 모두 활성화하십시오. Extension Mobility와 통화 표시 제한 기능을 모두 활성화할 경우 통화 정보의 표시 또는 제한은 디바이스에 로그인된 사용자와 연결된 회선 프로파일에 따라 달라집니다. 사용자 디바이스 프로파일(사용자와 연결됨)에 입력된 구성에 의해 (Extension Mobility가 활성화된 전화기의) 전화기 구성에 입력된 구성이 무시됩니다.
착신 전환	연결 번호 표시 제한은 시스템의 모든 발신 통화에 적용됩니다. True 로 설정하면 이 필드가 기존의 Cisco Unified Communications Manager 애플리케이션, 기능 및 통화 처리와 상호 작용합니다. 이 값은 시스템 내부 또는 외부의 모든 착신 통화에 적용됩니다. 통화가 모두 착신 전환 또는 통화 중 착신 전환 대상으로 라우팅되거나 착신 전환 또는 CTI 애플리케이션을 통해 재전송되는 경우 연결된 번호 표시가 업데이트되어 수정된 번호나 재전송된 번호가 표시됩니다.

통화 표시 제한 기능 제한 사항

변환 패턴 — 변환 패턴에서 중복 항목은 허용되지 않습니다.



43 장

DND(Do Not Disturb)

- 방해 사절 개요, 603 페이지
- 방해 사절 구성 작업 흐름, 604 페이지
- 방해 사절 상호 작용 및 제한 사항, 612 페이지
- 방해 사절 문제 해결, 615 페이지

방해 사절 개요

DND(방해 사절)는 다음과 같은 옵션을 제공합니다.

- 통화 거부 - 이 옵션은 수신 통화가 거부되었음을 지정합니다. DND 수신 전화 알림(DND Incoming Call Alert) 매개 변수를 구성하는 방법에 따라 전화기에서 경고음을 재생하거나 통화의 플래시 알림을 재생합니다.
- 벨소리 꺼짐 - 이 옵션은 벨소리를 끄지만 디바이스에 수신 통화 정보가 표시되므로 사용자가 전화를 받을 수 있습니다.

DND가 활성화되면, 일반 우선 순위를 지닌 새 수신 통화는 모두 해당 디바이스의 DND 설정을 인식하게 됩니다. CER(Cisco Emergency Responder) 통화나 MLPP(Multi-Level Precedence & Preemption) 통화 같이 우선 순위가 높은 통화는 디바이스에 수신되어 벨이 울립니다. 또한 DND를 활성화하는 경우 자동 응답 기능은 비활성화됩니다.

사용자는 다음과 같은 방법으로 전화기에서 방해 사절을 활성화할 수 있습니다.

- 소프트키
- 기능 버튼
- Cisco 통합 커뮤니케이션 자가 관리 포털



참고

Cisco Unified Communications Manager에서 전화기별 기준으로 기능을 활성화 또는 비활성화할 수 있습니다.

전화기 동작

방해 사절을 활성화할 경우 Cisco Unified IP Phone에 “방해사절 활성화 상태” 메시지가 표시됩니다. 일부 Cisco Unified IP Phone에는 DND 상태 아이콘이 표시됩니다. 개별 전화기 모델에서 방해 사절을 사용하는 방법에 대한 자세한 내용은 해당 전화기 모델의 사용자 설명서를 참조하십시오.

DND를 활성화하더라도 Cisco Unified Communications Manager 관리의 착신 통화 경고 설정에 지정된 대로 계속 전화기에서 수신 통화 알림을 받을 수 있지만, 우선 순위가 높은 통화(예: Cisco Emergency Responder 및 MLPP 통화)를 제외하고 전화기 벨은 울리지 않습니다. 또한 전화기 벨이 울리는 동안 DND를 활성화한 경우 전화기의 벨울림이 멈춥니다.

상태 알림

SIP 및 Cisco SCCP(Skinny Call Control Protocol) 디바이스에서 모두 방해 사절 기능이 지원됩니다.

SIP 전화기는 SIP PUBLISH 방법을 사용하여 Cisco Unified Communications Manager에 DND 상태 변경을 신호합니다. Cisco Unified Communications Manager는 Remote-cc REFER 요청을 사용하여 SIP 전화기에 DND 상태 변경 신호를 전송합니다.

SCCP 전화기는 SCCP 메시징을 사용하여 Cisco Unified Communications Manager에 DND 상태 변경을 신호합니다.

방해 사절 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	Cisco Unified Reporting에서 전화기 기능 목록 보고서를 실행하여 방해 사절을 지원하는 전화기를 확인합니다. 참고 SIP를 실행하는 Cisco Unified IP Phone 7940 및 7960에는 자체 구현된 방해사절 기능이 사용되며, 이 기능은 이전 버전과 호환됩니다. 방해사절 기능은 SIP 프로파일에서 구성합니다.
단계 2	통화 상태 감시(BLF) 상태 구성, 605 페이지	통화 상태 감시(BLF) 상태 서비스 매개 변수를 구성합니다.
단계 3	일반 전화 프로파일에 방해 사절 구성, 606 페이지	(선택 사항) 일반 전화 프로파일에 대해 방해 사절을 구성합니다. 프로파일을 사용하여 네트워크의 전화기 그룹에 방해 사절 설정을 적용할 수 있습니다.
단계 4	전화기에 방해 사절 설정 적용, 606 페이지.	전화기에 방해 사절 설정을 적용합니다.

	명령 또는 동작	목적
단계 5	<p>전화기에서 소프트키 또는 기능 버튼을 사용하는지 여부에 따라 다음 작업 중 하나를 수행합니다.</p> <ul style="list-style-type: none"> • 방해 사절 기능 버튼 구성, 607 페이지 • 방해 사절 소프트키 구성, 609 페이지 	전화기에 방해 사절 기능 버튼 또는 소프트키를 추가합니다.

통화 상태 감시(BLF) 상태 구성

BLF 상태가 **DND**를 나타냄 서비스 매개 변수를 설정하여 BLF 상태가 방해 사절을 나타내는 방식을 구성할 수 있습니다. BLF 상태를 설정하려면 다음을 수행합니다.

시작하기 전에



- 참고
- **DND**에 대한 통화 중 램프 필드(BLF) 프레즌스 상태는 공유 회선 DN에 대해 등록된 모든 장치가 **DND**로 설정된 경우에만 작동합니다.
 - 동일한 DN에서 iOS용 Jabber 또는 Android용 Jabber를 사용하는 경우 등록되지 않고 방금 구성된 때도 등록된 것으로 간주됩니다.

[전화기 기능 목록 생성, 7 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개 변수를 선택합니다.

단계 2 구성할 서버의 **Cisco CallManager** 서비스를 선택합니다.

단계 3 클러스터 수준 매개 변수(시스템 - 현재) 창에서 **BLF** 상태 표시 **DND**를 제공합니다 서비스 매개 변수에 대해 다음 값 중 하나를 지정합니다.

- **True** -디바이스에서 방해 사절 상태가 활성화되면 디바이스 또는 회선 표시에 대한 BLF 상태 표시기에 방해 사절 상태가 반영됩니다.
- **False** -디바이스에서 방해 사절 상태가 활성화되면 디바이스 또는 회선 표시에 대한 BLF 상태 표시기에 실제 디바이스 상태가 반영 됩니다.

다음에 수행할 작업

다음 절차 중 하나를 수행합니다.

[일반 전화 프로파일에 방해 사절 구성, 606 페이지](#)

[전화기에 방해 사절 설정 적용, 606 페이지](#)

일반 전화 프로파일에 방해 사절 구성

일반 전화 프로파일을 사용하여 방해 사절 설정을 구성한 다음 해당 설정을 해당 프로파일을 사용하는 네트워크의 전화기 그룹에 적용할 수 있습니다.

시작하기 전에

[통화 상태 감시\(BLF\) 상태 구성, 605 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 일반 전화 프로파일을 선택합니다.

단계 2 **DND** 옵션 드롭다운 목록에서 방해 사절 기능을 사용하여 수신 통화를 처리하는 방법을 선택합니다.

- **통화 거부** - 사용자에게 수신 통화 정보를 표시하지 않습니다. DND 수신 전화 알림(DND Incoming Call Alert) 파라미터를 구성하는 방법에 따라 전화기에서 경고음을 재생하거나 통화의 플래시 알림을 재생합니다.
- **벨소리 꺼짐** - 이 옵션은 벨소리를 끄지만 디바이스에 수신 통화 정보가 표시되므로 사용자가 전화를 받을 수 있습니다.

참고 휴대폰 및 듀얼 모드 전화기의 경우 통화 거부 옵션만 선택할 수 있습니다.

단계 3 수신 통화 경고 드롭다운 목록에서 방해 사절이 설정되어 있는 동안 수신 통화의 전화 사용자에게 알리는 방법을 선택합니다.

- **비활성화** - 통화에 대한 경고음과 플래시 알림이 비활성화됩니다. DND 벨소리 꺼짐 옵션을 구성한 경우에는 수신 통화 정보가 계속 표시됩니다. 그러나 DND 통화 거부 옵션의 경우 통화 경고가 표시되지 않고 디바이스에 정보가 전송되지 않습니다.
- **플래시만** — 전화가 걸려오면 전화기가 깜박입니다.
- **경고음만** - 전화가 걸려오면 플래시 알림이 표시됩니다.

단계 4 저장을 클릭합니다.

전화기에 방해 사절 설정 적용

이 절차는 Cisco Unified IP Phone에 방해 사절 설정을 적용하는 방법에 대해 설명합니다. Cisco Unified CM 관리의 전화기 구성 창을 통해 DND 설정을 적용하거나, 일반 전화 프로파일에 DND 설정을 적용한 다음 해당 프로파일을 전화기에 적용할 수 있습니다.

시작하기 전에

일반 전화 프로파일을 사용하는 경우에는 [일반 전화 프로파일에 방해 사절 구성, 606 페이지](#)를 완료합니다.

그렇지 않으면, 완료합니다. [통화 상태 감시\(BLF\) 상태 구성, 605 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 2 찾기를 클릭하고 방해 사절을 구성할 전화기를 선택합니다.

단계 3 일반 전화 프로파일에서 방해 사절 설정을 적용하려면 일반 전화 프로파일 드롭다운 목록에서 방해 사절로 구성된 프로파일을 선택합니다.

단계 4 전화기에서 방해사절을 활성화하려면 방해 사절 확인란을 선택합니다.

단계 5 **DND** 옵션 드롭다운 목록의 다음 옵션 중에서 DND 기능을 사용하여 수신 통화를 처리하는 방법을 지정합니다.

- 통화 거부 - 사용자에게 수신 통화 정보를 표시하지 않습니다. 구성에 따라 전화기는 경고음을 재생하거나 플래시 알림을 표시합니다.
- 벨소리 꺼짐 - 수신 통화 정보는 사용자가 전화를 받을 수 있지만 벨소리가 꺼지도록 디바이스에 제공됩니다.
- 일반 프로파일 설정 사용 - 이 디바이스에 대해 지정된 일반 전화 프로파일에 대한 방해 사절 설정입니다.

참고 SCCP를 실행하는 7940/7960 전화기의 경우 [벨소리 꺼짐] 옵션만 선택할 수 있습니다. 모바일 디바이스 및 듀얼 모드 전화기의 경우 [통화 거부] 옵션만 선택할 수 있습니다. 모바일 디바이스 또는 듀얼 모드 전화기에서 [DND 통화 거부]를 활성화하면, 디바이스에 아무런 통화 정보도 표시되지 않습니다.

단계 6 **DND** 수신 통화 알림 드롭다운 목록에서 DND가 켜져 있을 때 전화기에서 수신 통화를 표시하는 방법을 다음 옵션 중에서 지정합니다.

- 없음 - 일반 전화 프로파일의 DND 수신 통화 알림 설정이 이 디바이스에 사용됩니다.
- 비활성화 - DND 벨소리가 꺼지는 경우 신호음과 플래시 알림이 모두 비활성화되지만 수신 통화 정보는 계속 표시됩니다. 통화 거부의 경우 경고음 및 플래시 알림이 비활성화되고 수신 통화 정보가 디바이스에 전달되지 않습니다.
- 경고음만 - 수신 전화의 경우 전화기에서 신호음만 울립니다.
- 플래시만 - 수신 전화의 경우 전화기에 플래시 알림이 표시됩니다.

단계 7 저장을 클릭합니다.

다음에 수행할 작업

다음 절차 중 하나를 완료합니다.

[방해 사절 기능 버튼 구성, 607 페이지](#)

[방해 사절 소프트키 구성, 609 페이지](#)

방해 사절 기능 버튼 구성

다음 단계에 따라 Cisco Unified IP Phone에 방해 사절 기능 버튼을 추가합니다.

프로시저

	명령 또는 동작	목적
단계 1	방해 사절에 대한 전화기 버튼 템플릿 구성, 608 페이지	방해 사절 버튼이 포함된 전화기 버튼 템플릿을 만듭니다.
단계 2	버튼 템플릿을 전화기와 연결, 277 페이지	방해 사절 버튼 템플릿을 전화기에 연결합니다.

방해 사절에 대한 전화기 버튼 템플릿 구성

이 절차에 따라 방해 사절 버튼을 포함하는 전화기 버튼 템플릿을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.

단계 2 [찾기]를 클릭하여 지원 되는 전화기 템플릿 목록을 표시합니다.

단계 3 새 전화기 버튼 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.

- 전화기의 모델에 대한 기본 템플릿을 선택하고 복사를 클릭합니다.
- 전화기 버튼 템플릿 정보 필드에 템플릿의 새 이름을 입력합니다.
- 저장을 클릭합니다.

단계 4 기존 템플릿에 전화기 버튼을 추가하려는 경우 다음 단계를 수행합니다.

- 찾기를 클릭하고 검색 기준을 입력합니다.
- 기존 템플릿을 선택합니다.

단계 5 회선 드롭다운 목록에서 템플릿에 추가하려는 기능을 선택합니다.

단계 6 저장을 클릭합니다.

단계 7 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다.

버튼 템플릿을 전화기와 연결

시작하기 전에

[방해 사절에 대한 전화기 버튼 템플릿 구성, 608 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.
- 단계 3 전화기 버튼 템플릿을 추가할 전화기를 선택합니다.
- 단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.
- 단계 5 저장을 클릭합니다.
- 전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

방해 사절 소프트키 구성

(선택 사항) 전화기에서 소프트키를 사용하는 경우 다음 작업 흐름의 작업을 수행하여 전화기에 방해 사절 소프트키를 추가합니다.

프로시저

	명령 또는 동작	목적
단계 1	방해 사절에 대한 소프트키 템플릿 구성, 609 페이지	방해 사절 소프트키를 포함하는 소프트키 템플릿을 만듭니다.
단계 2	다음 절차를 수행합니다. <ul style="list-style-type: none"> • 소프트키 템플릿을 일반 디바이스 구성에 연결, 610 페이지 • 소프트키 템플릿을 전화기에 연결, 612 페이지 	소프트키를 일반 디바이스 구성에 연결한 다음 해당 구성을 전화기 그룹에 연결하거나, 소프트키 템플릿을 전화기에 직접 연결할 수 있습니다.

방해 사절에 대한 소프트키 템플릿 구성

이 단계를 수행하여 방해 사절 소프트키를 포함하는 소프트키 템플릿을 구성합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 소프트키 템플릿.
- 단계 2 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
- 새로 추가를 클릭합니다.
 - 기본 템플릿을 선택하고 복사를 클릭합니다.
 - 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
 - 저장을 클릭합니다.

단계 3 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.

- a) 찾기를 클릭하고 검색 기준을 입력합니다.
- b) 필요한 기존 템플릿을 선택합니다.

단계 4 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.

참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.

단계 5 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.

단계 6 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.

단계 7 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.

단계 8 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.

단계 9 저장을 클릭합니다.

단계 10 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

다음에 수행할 작업

다음 절차 중 하나를 수행하여 소프트키 템플릿을 전화기에 추가합니다.

[소프트키 템플릿을 일반 디바이스 구성에 연결, 610 페이지](#)

[소프트키 템플릿을 전화기에 연결, 612 페이지](#)

소프트키 템플릿을 일반 디바이스 구성에 연결

DND(방해 사절) 소프트키 소프트 템플릿을 일반 디바이스 설정에 연결하면 해당 공통 디바이스 설정을 사용하는 Cisco Unified IP Phone 그룹에 DND 소프트키를 추가할 수 있습니다.

시작하기 전에

[방해 사절에 대한 소프트키 템플릿 구성, 609 페이지](#)

프로시저

	명령 또는 동작	목적
단계 1	소프트키 템플릿을 일반 디바이스 구성에 추가, 611 페이지	DND 소프트키 템플릿을 일반 디바이스 설정에 연결
단계 2	일반 디바이스 구성을 전화기에 연결, 611 페이지	일반 디바이스 설정을 전화기에 연결하여 DND 소프트키를 전화기에 추가합니다.

소프트키 템플릿을 일반 디바이스 구성에 추가

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성
- 단계 2 다음 단계를 수행하여 새 일반 디바이스 구성을 생성 하고 소프트키 템플릿을 해당 구성에 연결합니다. 그렇지 않으면 다음 단계를 진행합니다.
- 새로 추가를 클릭합니다.
 - 이름 필드에 일반 디바이스 구성의 이름을 입력합니다.
 - 저장을 클릭합니다.
- 단계 3 기존 일반 디바이스 구성에 소프트키 템플릿을 추가하려면 다음 절차를 수행합니다.
- 찾기를 클릭하고 검색 기준을 입력합니다.
 - 기존 일반 디바이스 구성을 클릭합니다.
- 단계 4 소프트키 템플릿 필드의 드롭다운 목록에서 사용하려는 소프트키가 포함된 소프트키 템플릿을 선택합니다.
- 단계 5 저장을 클릭합니다.
- 단계 6 다음 작업 중 하나를 수행합니다.
- 이미 디바이스와 연결되어 있는 일반 디바이스 구성을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
 - 새 일반 디바이스 구성을 만든 경우 구성을 디바이스와 연결한 다음 다시 시작합니다.

일반 디바이스 구성을 전화기에 연결

시작하기 전에

[소프트키 템플릿을 일반 디바이스 구성에 연결, 610 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 **2** 찾기를 클릭하고 전화기 디바이스를 선택하여 소프트키 템플릿을 추가합니다.

단계 **3** 일반 디바이스 구성 드롭다운 목록에서 새 소프트키 템플릿이 포함된 일반 디바이스 구성을 선택합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** 재설정을 클릭하여 전화기 설정을 업데이트합니다.

소프트키 템플릿을 전화기에 연결

방해 사절 소프트키를 사용하여 소프트키 템플릿을 구성하고 해당 소프트키 템플릿을 전화기에 연결 하려는 경우 이 절차를 수행합니다.

시작하기 전에

[방해 사절에 대한 소프트키 템플릿 구성, 609 페이지](#)

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 **2** 찾기를 클릭하고 전화기를 선택하여 소프트키 템플릿을 추가합니다.

단계 **3** 소프트키 템플릿 드롭다운 목록에서 새 소프트키가 포함된 템플릿을 선택합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** 재설정을 눌러 전화기 설정을 업데이트합니다.

방해 사절 상호 작용 및 제한 사항

이 섹션에는 방해사절 상호 작용 및 제한 사항에 관한 내용이 있습니다.

상호 작용

다음 표에서는 DND(방해 사절) 기능을 사용한 기능 상호 작용에 대해 설명합니다. 별도로 언급하지 않는 한 상호 작용은 DND 벨소리 꺼짐 및 DND 통화 거부 옵션 모두에 적용됩니다.

기능	방해 사절과의 상호 작용
모든 통화 착신 전환	Cisco Unified IP Phone에서는 DND(방해사절) 기능이 활성화됨을 나타내는 메시지가 사용자에게 새 음성 메시지가 있음을 나타내는 메시지보다 우선합니다. 하지만, 모두 착신 전환 기능이 활성화됨을 나타내는 메시지는 방해사절보다 우선 순위가 높습니다.

기능	방해 사절과의 상호 작용
지정보류 복귀	<p>로컬로 지정보류된 통화의 경우 지정보류 복귀가 DND를 무시합니다. 전화기 A에서 DND가 켜져 있고 통화가 지정보류되어 있는 경우 전화기 A에 대해 지정보류 복귀가 발생하여 전화기 A의 벨소리가 울립니다.</p> <p>원격으로 지정보류된 통화의 경우 DND가 지정보류 복귀를 무시합니다.</p> <ul style="list-style-type: none"> • 전화기 A가 DND 벨소리 꺼짐을 활성화하고 전화기 A-prime이 통화를 지정보류할 때 전화기 A-prime과 회선을 공유하는 경우 전화기 A에서 지정보류를 복귀하면 DND 설정을 따르고 벨이 울리지 않습니다. • 전화기 A가 DND 통화 거부를 활성화하면 지정보류 복귀가 전화기 A에 표시되지 않습니다.
당겨받기	<p>로컬로 발신된 당겨받기 요청의 경우 당겨받기가 DND를 무시합니다. DND가 켜져 있는 전화기 A가 당겨받기를 시작하면 당겨받기 통화가 정상적으로 제공되고 전화기 A에 벨소리가 울립니다.</p> <p>원격으로 발신된 당겨받기 요청의 경우 DND가 다음과 같이 당겨받기를 무시합니다.</p> <ul style="list-style-type: none"> • 전화기 A가 DND 벨소리 꺼짐 모드에 있고 전화기 A-prime과 회선을 공유하면 전화기 A-prime이 당겨받기를 시작할 때 전화기 A에 대한 당겨받기 통화에서 DND 설정이 적용되고 전화기 A에서 벨소리가 울리지 않습니다. • 전화기 A가 DND 통화 거부 모드에 있으면 당겨받기 통화가 전화기 A에 제공되지 않습니다.
보류 복귀와 인터콤	보류 복귀와 인터콤 기능은 DND를 무시하므로 통화가 정상적으로 표시됩니다.
MLPP 및 CER	MLPP(Multilevel Precedence and Preemption)(SCCP를 실행하는 전화기) 및 Cisco Emergency Responder 통화가 DND를 무시합니다. 일반적으로 MLPP(Multilevel Precedence and Preemption) 및 Cisco Emergency Responder 통화가 정상적으로 표시되고 전화기가 울립니다.
콜백	<p>개시 측에서는 콜백이 DND를 덮어씁니다. 활성 디바이스가 DND 모드인 경우 사용자에게 콜백 알림(오디오 및 비디오)이 표시됩니다.</p> <p>종료 측에서는 DND가 다음과 같이 콜백을 덮어씁니다.</p> <ul style="list-style-type: none"> • 종료 측이 [DND 벨소리 꺼짐]인 경우 종료 측이 오프 훅으로 전환했다 온 훅으로 전환한 이후 [콜백 사용 가능] 화면이 전송됩니다. • 종료 측이 [DND 통화 거부]이고 사용 가능한 경우 활성 디바이스가 동일한 클러스터에 있으면 활성 디바이스에 <DirectoryNumber>를 사용할 수 있지만 DND-R에 있음이라는 새 화면이 전송됩니다. 콜백 사용 가능 알림은 종료 측에서 [DND 통화 거부]를 비활성화한 다음에만 전송됩니다.

기능	방해 사절과의 상호 작용
당겨받기 알림	[DND 벨소리 꺼짐] 옵션의 경우 시각적 알림만 디바이스에 제공됩니다. [DND 통화 거부] 옵션의 경우 알림이 디바이스에 제공되지 않습니다.
헌트 목록	헌트 목록에 있는 디바이스에서 [DND 벨소리 끄기]가 활성화된 경우 여전히 해당 사용자에게 통화가 표시됩니다. 하지만 [방해사절 수신전화 경고] 설정이 여전히 적용됩니다. 헌트 목록에 있는 디바이스에서 [DND 통화 거부]가 활성화된 경우 해당 헌트 목록으로 걸려온 통화가 모두 다음 구성원으로 이동하고 이 디바이스로 전송되지 않습니다.
Extension Mobility	Extension Mobility의 경우 디바이스 프로파일 설정에 DND 수신 통화 경고 및 DND 상태가 포함됩니다. 사용자가 로그인하고 DND를 활성화하는 경우 DND 수신 통화 경고 및 DND 상태 설정이 저장되며 이러한 설정은 사용자가 다시 로그인할 때 사용됩니다. 참고 Extension Mobility에 로그인된 사용자가 DND 수신 통화 경고나 DND 상태 설정을 수정하는 경우 이 작업은 실제 디바이스 설정에는 적용되지 않습니다.

제한 사항

사용하는 전화기 또는 디바이스 유형에 따라, DND 사용에 몇 가지 제한 사항이 적용됩니다.

- SCCP를 실행하는 다음 전화기 모델과 디바이스는 DND 벨소리 꺼짐만 지원합니다.
 - Cisco Unified IP Phone 7940
 - Cisco Unified IP Phone 7960
 - Cisco IP Communicator



참고 SIP를 실행하는 Cisco Unified IP Phones 7940 및 7960은 자체 구현된 방해사절 기능을 사용하며, 이 기능은 이전 버전과 호환됩니다.

- 다음 전화기 모델과 디바이스는 DND 통화 거부 옵션만 지원합니다.
 - 모바일 디바이스(듀얼 모드)
 - 원격 대상 프로파일
 - Cisco Unified Mobile Communicator

방해 사절 문제 해결

이 섹션에서는 Cisco Unified IP Phone(SCCP 및 SIP)에 대한 문제 해결 정보를 제공합니다.

SIP 전화기의 경우 문제 해결을 위해 다음 정보를 사용하십시오.

- debugs: sip-dnd, sip-messages, dnd-settings
- show: config, dnd-settings
- 스니퍼 추적

SCCP 전화기의 경우 문제 해결을 위해 다음 정보를 사용하십시오.

- debug: jvm all info
- 스니퍼 추적

오류 문제 해결

다음 표에서는 방해 사절을 사용하여 오류 문제를 해결하는 방법을 설명합니다.

문제점	작업
[DND] 소프트키가 표시되지 않음 또는 DND 기능 버튼이 표시되지 않음	<ul style="list-style-type: none"> • 이 전화기의 소프트키 또는 버튼 템플릿에 DND가 포함되어 있는지 확인합니다. • 스니퍼 추적을 캡처하여 전화기에 올바른 소프트키 또는 버튼 템플릿을 가져오는지 확인합니다. • 전화기 펌웨어가 버전 8.3(1) 이상인지 확인합니다.
BLF 바로 호출에 DND 상태가 표시되지 않음	<ul style="list-style-type: none"> • BLF DND가 엔터프라이즈 매개 변수에서 활성화됨으로 설정되어 있는지 확인합니다. • 스니퍼 추적을 캡처하여 전화기에 올바른 알림 메시지를 가져오는지 확인합니다. • 전화기 펌웨어가 버전 8.3(1) 이상인지 확인합니다.
DND 변경 사항은 모니터링 장치에 반영되지 않습니다.	<ul style="list-style-type: none"> • BOT/TCT 장치가 DND 상태가 OFF로 설정된 공유 회선 장치인지 확인합니다. 상태가 켜짐으로 설정되어 있으면 다른 공유 회선의 DND 상태에 대한 변경 사항이 반영되지 않습니다. • 사용자가 모니터링할 회선에서 DND 상태의 변경 사항을 반영하려면 BOT/TCT 장치의 DND 상태가 끄기로 설정되어 있는지 확인하십시오.



44 장

프라이버시

- 프라이버시 개요, 617 페이지
- 프라이버시 구성 작업 흐름, 618 페이지
- 프라이버시 제한 사항, 621 페이지

프라이버시 개요

프라이버시 기능을 사용하면 동일한 회선(DN)을 공유하는 전화기를 사용하는 사용자가 통화 상태를 보고 통화에 참여할 수 있는 기능을 활성화하거나 비활성화할 수 있습니다. 각 전화기나 모든 전화기에 대해 프라이버시를 활성화하거나 비활성화할 수 있습니다. 기본적으로 클러스터의 모든 전화기에 대해 프라이버시가 활성화됩니다.

프라이버시가 구성된 디바이스가 Cisco Unified Communications Manager에 등록되면 프라이버시가 구성된 전화기의 기능 버튼에 레이블이 지정되고 아이콘을 통해 상태가 표시됩니다. 버튼에 램프가 있으면 켜집니다.

전화기에서 수신 통화를 받으면 사용자는 [프라이버시] 기능 버튼을 눌러 통화를 개인으로 만들 수 있습니다(따라서 공유 회선에 통화 정보가 표시되지 않음). 프라이버시 기능 버튼은 켜기와 끄기 사이에서 전환됩니다.

Cisco Unified IP Phone에서 프라이버시를 지원 있는지 확인하려면 전화기 모델에 대한 사용자 설명서를 참조하십시오.

보류 중 프라이버시

보류 중 프라이버시를 사용하면 동일한 회선(DN)을 공유하는 사용자가 통화 상태를 보고 보류 중인 통화를 검색할 수 있는 기능을 활성화하거나 비활성화할 수 있습니다.

특정 전화기 또는 모든 전화기에 대해 보류 중 프라이버시를 활성화하거나 비활성화할 수 있습니다. 보류 중 통화를 활성화한 경우 모든 개인 통화에서 보류 중 통화가 자동으로 활성화됩니다. 기본적으로 클러스터의 모든 전화기에 대해 보류 중 프라이버시가 비활성화됩니다.

보류 중 프라이버시를 활성화하려면 사용자는 개인 통화 중에 보류 소프트키나 보류 버튼을 누릅니다. 통화로 돌아가려면 사용자는 보류해제 소프트키를 누릅니다. 통화를 보류 중으로 설정하는 전화

기에는 보류 전화에 대한 상태 표시기가 표시됩니다. 공유 회선에는 개인 및 보류 통화의 상태 표시기가 표시됩니다.

프라이버시 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성, 7 페이지	프라이버시 기능을 지원하는 디바이스를 식별하는 보고서를 생성합니다.
단계 2	프라이버시 클러스터 전체 활성화, 618 페이지	기본적으로 클러스터의 모든 전화기에 대해 프라이버시를 활성화합니다.
단계 3	디바이스에 대한 프라이버시 활성화, 619 페이지	특정 디바이스에 대한 프라이버시를 활성화합니다.
단계 4	프라이버시 전화기 버튼 템플릿 구성, 619 페이지	디바이스에 대한 프라이버시 전화기 버튼 템플릿을 구성합니다.
단계 5	프라이버시 전화기 버튼 템플릿을 전화기와 연결, 620 페이지	전화기 버튼 템플릿을 사용자와 연결합니다.
단계 6	공유 회선 표시 구성, 620 페이지	공유 회선 표시를 구성합니다.
단계 7	(선택 사항) 프라이버시 보류 중 구성, 621 페이지	프라이버시 보류 중 구성

프라이버시 클러스터 전체 활성화

전체 클러스터에 대해 기본적으로 프라이버시를 활성화하려면 다음 단계를 수행합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.
서비스 매개 변수 구성 창이 표시됩니다.
- 단계 2 서버 드롭다운 목록에서 **Cisco CallManager** 서비스를 실행하고 있는 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- 단계 4 프라이버시 설정드롭다운 목록에서 **True**를 선택합니다.
- 단계 5 저장을 클릭합니다.

디바이스에 대한 프라이버시 활성화

시작하기 전에

전화기 모델에서 프라이버시를 지원하는지 확인합니다. 자세한 내용은 [전화기 기능 목록 생성, 7 페이지](#)의 내용을 참조하십시오.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
 - 단계 2 검색 기준을 지정하고 찾기를 클릭합니다.
전화기 검색 결과가 나타납니다.
 - 단계 3 전화기를 선택합니다.
 - 단계 4 프라이버시 드롭다운 목록에서 기본값을 선택합니다.
 - 단계 5 저장을 클릭합니다.
-

프라이버시 전화기 버튼 템플릿 구성

시작하기 전에

[디바이스에 대한 프라이버시 활성화, 619 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 전화기 버튼 템플릿.
 - 단계 2 [찾기] 를 클릭하여 지원 되는 전화기 템플릿 목록을 표시합니다.
 - 단계 3 새 전화기 버튼 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.
 - a) 전화기의 모델에 대한 기본 템플릿을 선택하고 복사를 클릭합니다.
 - b) 전화기 버튼 템플릿 정보 필드에 템플릿의 새 이름을 입력합니다.
 - c) 저장을 클릭합니다.
 - 단계 4 기존 템플릿에 전화기 버튼을 추가하려는 경우 다음 단계를 수행합니다.
 - a) 찾기를 클릭하고 검색 기준을 입력합니다.
 - b) 기존 템플릿을 선택합니다.
 - 단계 5 회선 드롭다운 목록에서 템플릿에 추가하려는 기능을 선택합니다.
 - 단계 6 저장을 클릭합니다.
 - 단계 7 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다.

프라이버시 전화기 버튼 템플릿을 전화기와 연결

시작하기 전에

[프라이버시 전화기 버튼 템플릿 구성, 619 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
- 단계 2 찾기를 클릭하여 구성된 전화기 목록을 표시합니다.
- 단계 3 전화기 버튼 템플릿을 추가할 전화기를 선택합니다.
- 단계 4 전화기 버튼 템플릿 드롭다운 목록에서 새 기능 버튼을 포함하는 새 전화기 버튼 템플릿을 선택합니다.
- 단계 5 저장을 클릭합니다.
전화기 설정을 업데이트하려면 재설정을 누르라는 메시지가 포함된 대화 상자가 표시됩니다.

공유 회선 표시 구성

시작하기 전에

[프라이버시 전화기 버튼 템플릿을 전화기와 연결, 620 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기
사용자 찾기 및 나열 창이 나타납니다.
- 단계 2 특정 전화기를 찾으려면 검색 조건을 입력하고 찾기를 클릭합니다.
검색 조건과 일치하는 전화기 목록이 표시됩니다.
- 단계 3 공유 회선 형태를 구성하려는 전화기를 선택합니다.
전화기 구성 창이 표시됩니다.
- 단계 4 전화기 구성 창 왼쪽에 있는 연결 정보 영역에서 새 **DN** 링크 추가를 클릭합니다.
디렉터리 번호 구성 창이 나타납니다.
- 단계 5 디렉터리 번호를 입력하고 디렉터리 번호가 속하는 라우트 파티션을 선택합니다.

단계 6 디렉터리 번호 구성 창에서 나머지 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 7 공유 회선 형태를 만들 모든 전화기에 대해 단계 3, 620 페이지부터 단계 6, 621 페이지까지 반복합니다.

참고 공유 회선 형태에 포함되는 모든 전화기에 동일한 디렉터리 번호 및 라우트 파티션을 할당해야 합니다.

프라이버시 보류 중 구성

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

서비스 매개 변수 구성 창이 표시됩니다.

단계 2 서버 드롭다운 목록에서 Cisco CallManager 서비스를 실행하고 있는 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 보류 중인 통화에 프라이버시 설정 적용 서비스 매개 변수를 **True**로 설정합니다.

단계 5 저장을 클릭합니다.

프라이버시 제한 사항

제한 사항	설명
CTI	<ul style="list-style-type: none"> CTI는 TAPI 및 JTAPI 애플리케이션이 호출하는 API를 통한 프라이버시를 지원하지 않습니다. 프라이버시 기능 버튼을 사용하여 IP 전화기에서 프라이버시를 활성화거나 비활성화하면 CTI가 이벤트를 생성합니다. CTI는 TAPI/JTAPI 애플리케이션이 호출하는 API를 통한 보류 중 프라이버시를 지원하지 않습니다. CTI는 프라이버시 지원 통화가 보류될 때, 그리고 보류 중 프라이버시 기능 버튼을 사용하여 IP 전화기에서 프라이버시가 활성화되거나 비활성화될 때 이벤트를 생성합니다.



45 장

전용 회선 자동 링다운

- 전용 회선 자동 링다운 개요, 623 페이지
- SCCP 전화기에 대한 전용 회선 자동 링다운 구성 작업 흐름, 623 페이지
- SIP 전화기에 대한 전용 회선 자동 링다운 구성 작업 흐름, 626 페이지
- 전용 회선 자동 링다운 문제 해결, 627 페이지

전용 회선 자동 링다운 개요

PLAR(Private Line Automatic Ringdown) 기능은 사용자가 오프 hook 상태가 되는 경우(또는 [전화걸기] 소프트키 또는 회선 키를 누른 경우) 전화기에서 미리 구성된 번호로 즉시 전화를 겁니다. 전화기 사용자는 PLAR용으로 구성된 전화 회선에서는 다른 번호로 전화를 걸 수 없습니다.

PLAR는 끼어들기, 회의끼기 또는 참여 단일 버튼 같은 기능과 함께 작동합니다. PLAR를 특정 기능과 함께 사용할 경우 기능 설명서에 설명된 기능을 구성해야 하며, 특히 PLAR에 사용될 디렉터리 번호에 해당하는 PLAR 대상도 구성해야 합니다.

SCCP 전화기에 대한 전용 회선 자동 링다운 구성 작업 흐름

SCCP 전화기에서 PLAR(Private Line Automatic Ringdown)을 구성하려면 다음 작업을 수행합니다.

프로시저

	명령 또는 동작	목적
단계 1	파티션 생성, 624 페이지	PLAR 대상에 대한 파티션을 만듭니다. 이 파티션에 할당할 수 있는 유일한 디렉터리 번호는 PLAR 대상입니다.
단계 2	발신 검색 공간에 파티션 할당, 624 페이지	고유한 CSS에 파티션을 할당하고 PLAR 대상 디바이스를 포함하는 CSS를 할당합니다.
단계 3	전용 회선 자동 링다운 대상에 파티션 할당, 625 페이지	널 파티션 및 CSS를 PLAR 대상 디렉터리 번호에 할당합니다.

	명령 또는 동작	목적
단계 4	전화기에서 전용 회선 자동 링다운에 대한 변환 패턴 구성, 625 페이지	널 변환 패턴을 생성하여 PLAR 대상 디렉터리 번호에 할당합니다.

파티션 생성

전용 회선 자동 링다운(PLAR) 대상에 대한 새 파티션을 만듭니다. 이 기능을 사용하려면 PLAR에 대해 구성 하는 널 변환 패턴만 파티션에 할당할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 파티션.

단계 2 새로 추가를 클릭합니다.

단계 3 이름 필드에 쉼표로 구분된 파티션 이름과 설명을 입력합니다.

단계 4 저장을 클릭합니다.

발신 검색 공간에 파티션 할당

SCCP 전화기의 PLAR(Private Line Automatic Ringdown)의 경우 두 개의 CSS(발신 검색 공간)를 구성해야 합니다.

- 첫 번째 CSS에는 대상 전화기로 라우팅하는 파티션 뿐만 아니라 null 변환 패턴에 대한 새 파티션이 포함되어야 합니다.
- 두 번째 CSS에는 null 변환 패턴에 대한 새 파티션만 포함되어야 합니다.

시작하기 전에

[파티션 생성, 624 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 제어 > 제어 클래스 > 발신 검색 공간.

단계 2 찾기를 클릭하고 PLAR 대상 디바이스에 대한 발신 검색 공간을 선택합니다.

단계 3 화살표를 사용하여 null 변환 패턴에 대해 생성한 새 파티션 및 대상 디바이스로 라우팅하는 파티션을 모두 선택한 파티션 목록 상자로 이동합니다.

단계 4 저장을 클릭합니다.

단계 5 새로 추가를 클릭합니다.

단계 6 발신 검색 공간에 대한 이름 및 설명을 입력합니다.

단계 7 화살표를 사용하여 새 파티션을 선택한 파티션 목록 상자로 이동합니다.

단계 8 저장을 클릭합니다.

전용 회선 자동 링다운 대상에 파티션 할당

SCCP 전화기에서 PLAR(Private Line Automatic Ringdown)을 구성하는 경우 PLAR 대상으로 사용할 디렉터리 번호에 널 파티션을 할당합니다.



참고 각 PLAR 대상 디렉터리 번호에는 고유한 파티션이 있어야 합니다. PLAR 대상에 대해 생성한 널 파티션에는 다른 디렉터리 번호를 추가하지 마십시오.

시작하기 전에

[발신 검색 공간에 파티션 할당, 624 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 디렉터리 번호를 선택합니다.

단계 2 찾기를 클릭하고 PLAR 대상으로 사용할 디렉터리 번호를 선택합니다.

단계 3 경로 파티션 필드에서 PLAR 대상에 대해 생성한 파티션을 선택합니다.

단계 4 발신 검색 공간 드롭다운 목록에서 널 파티션과 대상 디바이스를 모두 포함하는 CSS를 선택합니다.

단계 5 저장을 클릭합니다.

전화기에서 전용 회선 자동 링다운에 대한 변환 패턴 구성

전화기에서 PLAR(Private Line Automatic Ringdown)을 구성하려면 널 변환 패턴을 구성하고 해당 변환 패턴에 PLAR 대상 번호를 할당합니다.

시작하기 전에

[전용 회선 자동 링다운 대상에 파티션 할당, 625 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 변환 패턴을 선택합니다.

단계 2 새로 추가를 클릭하여 새 변환 패턴을 만듭니다.

단계 3 변환 패턴 필드는 비워 둡니다.

단계 4 파티션 드롭다운 목록에서 널 변환 패턴에 대해 생성한 새 파티션을 선택합니다.

단계 5 발신 검색 공간 드롭다운 목록에서 새 파티션과 PLAR 대상 디바이스에 대한 파티션이 모두 포함된 발신 검색 공간을 선택합니다.

단계 6 착신자 변환 마스크 필드에 PLAR 대상 디렉터리 번호를 입력합니다.

단계 7 저장을 클릭합니다.

SIP 전화기에 대한 전용 회선 자동 링다운 구성 작업 흐름

이러한 작업을 수행하여 SIP 전화기에 대한 PLAR(Private Line Automatic Ringdown)을 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	전용 회선 자동 링다운에 대한 SIP 다이얼 규칙 생성, 626 페이지	PLAR에 대한 SIP 다이얼 규칙을 생성합니다.
단계 2	SIP 전화기에 전용 회선 자동 링다운 다이얼 규칙 할당, 627 페이지	전화기에 PLAR 다이얼 규칙을 할당합니다.

전용 회선 자동 링다운에 대한 SIP 다이얼 규칙 생성

SIP 전화기에서 PLAR(Private Line Automatic Ringdown)을 구성하려면 PLAR 대상 번호에 대한 SIP 다이얼 규칙을 구성해야 합니다.

시작하기 전에

[파티션 생성, 624 페이지](#)

[발신 검색 공간에 파티션 할당, 624 페이지](#)

[전용 회선 자동 링다운 대상에 파티션 할당, 625 페이지](#)

[전화기에서 전용 회선 자동 링다운에 대한 변환 패턴 구성, 625 페이지](#)

프로시저

단계 1 Unified CM 관리에서 통화 라우팅 > 제어 클래스 > **SIP** 다이얼 규칙을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 다이얼 패턴 드롭다운 목록에서 **7940_7960_OTHER**를 선택합니다.

단계 4 다음을 클릭합니다.

단계 5 다이얼 규칙의 이름과 설명을 입력합니다.

단계 6 다음을 클릭합니다.

단계 7 패턴 필드에 PLAR 대상 번호와 일치하는 패턴을 입력하고 **PLAR** 추가를 클릭합니다.

단계 8 저장을 클릭합니다.

SIP 전화기에 전용 회선 자동 링다운 다이얼 규칙 할당

전화기에 PLAR 사용 SIP 다이얼 규칙을 할당하여 SIP 전화기에 PLAR(Private Line Automatic Ringdown)을 구성할 수 있습니다.

시작하기 전에

[전용 회선 자동 링다운에 대한 SIP 다이얼 규칙 생성, 626 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 2 찾기를 클릭하고 PLAR을 구성할 전화기를 선택합니다.

단계 3 **SIP** 다이얼 규칙 드롭다운 목록에서 PLAR에 대해 생성한 다이얼 규칙을 선택합니다.

단계 4 저장을 클릭합니다.

전용 회선 자동 링다운 문제 해결

SCCP 전화기에서 전용 회선 자동 링다운 문제 해결

문제점	해결 방법
전화기가 오프 후 상태가 되고 사용자가 빠른 통화 중(다시 걸기) 신호음을 듣습니다.	PLAR 변환 패턴에 할당되는 CSS에 PLAR 대상의 파티션이 포함되어 있는지 확인합니다.
전화기가 오프 후 상태가 되고 다이얼톤을 받습니다.	전화기에 할당된 CSS에 null PLAR 변환 패턴의 파티션이 포함되어 있는지 확인합니다.

SIP 전화기에서 전용 회선 자동 링다운 문제 해결

문제점	해결 방법
전화기가 오프 hook 상태가 되고 사용자가 빠른 통화중(다시 걸기) 신호음을 듣습니다.	SIP 전화기의 CSS가 PLAR 대상에 연결할 수 있는지 확인합니다.
전화기가 오프 hook 상태가 되고 다이얼톤을 받습니다.	SIP 다이얼 규칙이 생성되고 전화기에 할당되었는지 확인합니다.



46 장

보안 신호음

- 보안 신호음 개요, 629 페이지
- 보안 신호음 사전 요건, 630 페이지
- 보안 신호음 구성 작업 흐름, 630 페이지
- 보안 신호음 상호 작용, 633 페이지
- 보안 신호음 제한 사항, 633 페이지

보안 신호음 개요

보안 신호음 기능은 통화가 암호화될 때 보안 표시 신호음을 재생하도록 전화기를 구성할 수 있습니다. 이 신호음은 통화가 보호되고 기밀 정보가 교환될 수 있음을 나타냅니다. 2초 신호음은 3개의 긴 경고음으로 구성됩니다. 통화가 보호된 경우에는 착신자가 응답하는 즉시 신호음이 보호된 전화기에서 재생되기 시작합니다.

통화가 보호되지 않으면 시스템은 보호된 전화기에서 6개의 짧은 경고음을 표시하는 비보안 표시음을 재생합니다.



참고 보호된 전화기의 발신자만 보안 및 비보안 표시음을 들을 수 있습니다. 보호되지 않는 전화기의 발신자는 이러한 신호음을 들을 수 없습니다.

보안 및 비보안 표시 신호음이 지원되는 통화 유형은 다음과 같습니다.

- 클러스터 내와 IP 연결 사이의 통화
- 클러스터 간 보호된 통화
- 보호된 MGCP E1 PRI 게이트웨이를 통한 TDM(IP-to-Time-Division-Multiplexing) 통화

영상 통화의 경우 시스템은 보호된 디바이스에서 보안 및 비보안 표시 신호음을 재생합니다.



참고 영상 통화의 경우, 사용자는 먼저 통화의 오디오 부분에 대한 보안 표시음을 듣고 전체 비보안 미디어에 대한 비보안 표시음을 들을 수 있습니다.

Cisco Unified IP Phone에 표시되는 잠금 아이콘은 미디어가 암호화되어 있음을 나타내지만 전화기가 보호된 디바이스로 구성되었음을 나타내지는 않습니다. 그러나 보호된 통화가 발생하려면 잠금 아이콘이 있어야 합니다.

보호된 디바이스 게이트웨이

Cisco Unified Communications Manager에서 지원되는 Cisco Unified IP Phone 및 MGCP E1 PRI 게이트웨이만 보호된 디바이스로 구성할 수 있습니다.

Cisco Unified Communications Manager는 시스템이 보호된 통화 상태를 결정하는 경우 보안 및 비보안 표시 신호음을 재생하도록 MGCP Cisco IOS 게이트웨이를 보낼 수도 있습니다.

보호되는 디바이스는 다음 기능을 제공합니다.

- SCCP 또는 SIP를 실행 중인 전화기를 보호된 디바이스로 구성할 수 있습니다.
- 보호되는 디바이스는 암호화되었거나 암호화되지 않은 비보호 디바이스를 호출할 수 있습니다. 이러한 경우에는 통화는 비보호로 지정되며 시스템에서 통화 시 전화기에 비보안 표시 신호음을 재생합니다.
- 보호된 전화기가 다른 보호된 전화기에 전화를 걸 때 미디어가 암호화되지 않으면 시스템에서 통화의 전화기에 비보안 표시 신호음을 재생합니다.

보안 신호음 사전 요건

- SRTP 암호화에 대한 MGCP 게이트웨이를 구성해야 합니다. 다음 명령을 사용하여 게이트웨이를 구성합니다. **mgcp package-capability srtp-package**.
- MGCP 게이트웨이는 고급 IP 서비스 또는 고급 엔터프라이즈 서비스 이미지(예: c3745-adventerprisek9-mz.124-6.T.bin)를 지정해야 합니다.

보안 신호음 구성 작업 흐름

시작하기 전에

- [보안 신호음 사전 요건](#), 630 페이지 검토

프로시저

	명령 또는 동작	목적
단계 1	전화기 기능 목록 생성 , 7 페이지	보안 신호음 기능을 지원하는 디바이스를 식별하는 보고서를 생성합니다.
단계 2	전화기를 보호된 디바이스로 구성 , 631 페이지	전화기를 보호된 디바이스로 구성합니다.
단계 3	보안 신호음에 대한 디렉터리 번호 구성 , 632 페이지	보호된 디바이스에 대한 여러 통화 및 통화 대기 설정을 구성합니다.

	명령 또는 동작	목적
단계 4	보안 신호음 서비스 매개 변수 구성, 632 페이지	서비스 매개 변수를 구성합니다.
단계 5	(선택 사항) MGCP E1 PRI 게이트웨이 구성, 632 페이지	이 구성을 사용하면 시스템에서 MGCP 게이트웨이에 연결하는 보호된 PBX 전화기와 Cisco Unified IP Phone 엔드포인트 간에 통화의 보호된 상태를 전달할 수 있습니다.

전화기를 보호된 디바이스로 구성

시작하기 전에

[전화기 기능 목록 생성, 7 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

단계 2 보안 신호음 매개 변수를 설정할 전화기를 클릭합니다.
전화기 구성 창이 표시됩니다.

단계 3 창의 디바이스 정보 부분에 있는 소프트키 템플릿 드롭다운 목록에서 표준 보호 전화기를 선택합니다.

참고 보호된 전화기에 대한 보조 서비스 소프트키가 없는 새 소프트키 템플릿을 사용해야 합니다.

단계 4 회선 간 통화 참가 옵션을 끄기로 설정합니다.

단계 5 보호된 디바이스 확인란을 선택합니다.

단계 6 디바이스 보안 프로파일 드롭다운 목록(창의 프로토콜 관련 정보 부분)에서 전화기 보안 프로파일 구성 창(시스템 > 보안 프로파일 > 전화기 보안 프로파일)에 이미 구성되어 있는 보안 전화기 프로파일을 선택합니다.

단계 7 저장을 클릭합니다.

다음에 수행할 작업

다음 절차 중 하나를 수행합니다.

- [보안 신호음에 대한 디렉터리 번호 구성, 632 페이지](#)
- [MGCP E1 PRI 게이트웨이 구성, 632 페이지](#)

보안 신호음에 대한 디렉터리 번호 구성

시작하기 전에

[전화기를 보호된 디바이스로 구성, 631 페이지](#)

프로시저

-
- 단계 1 전화기 구성 창에서 연결 섹션을 찾습니다.
 - 단계 2 새 **DN** 추가를 선택합니다.
디렉터리 번호 구성 창이 표시됩니다.
 - 단계 3 디렉터리 번호 필드에 디렉터리 번호를 지정합니다.
 - 단계 4 디렉터리 번호 구성 창의 디바이스 [디바이스 이름]에 있는 다중 통화/통화 대기 설정 영역에서 최대 통화 수 및 통화 중 트리거 옵션을 1로 설정합니다.
 - 단계 5 디렉터리 번호 구성 창에서 나머지 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
 - 단계 6 저장을 클릭합니다.
-

보안 신호음 서비스 매개 변수 구성

프로시저

-
- 단계 1 Cisco Unified Communications Manager Administration에서 시스템 > 서비스 매개 변수를 선택합니다.
 - 단계 2 서버 드롭다운 목록에서 서버를 선택합니다.
 - 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
 - 단계 4 클러스터 수준 매개 변수(기능 - 보안 신호음) 영역에서 보안/비보안 통화 상태를 표시하는 신호음 재생 옵션을 **True**로 설정합니다.
 - 단계 5 저장을 클릭합니다.
-

MGCP E1 PRI 게이트웨이 구성

MGCP 게이트웨이에 연결되는 보호된 PBX 전화기와 Cisco Unified IP Phone 엔드포인트 간에 통화의 보호된 상태를 전달하도록 하려면 다음 단계를 수행하십시오.

시작하기 전에

[전화기를 보호된 디바이스로 구성, 631 페이지](#)

프로시저

- 단계 1 Cisco Unified Communications Manager 관리에서 디바이스 > 게이트웨이를 선택합니다.
- 단계 2 적절한 검색 기준을 지정하고 찾기를 클릭합니다.
- 단계 3 MGCP 게이트웨이를 선택합니다.
게이트웨이 구성 창이 나타납니다.
- 단계 4 전역 **ISDN** 스위치 유형을 유로로 설정합니다.
- 단계 5 게이트웨이 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 6 저장을 클릭합니다.
- 단계 7 창에서 하위 유닛 0 오른쪽에 나타나는 엔드포인트 아이콘을 클릭합니다. 보호된 설비 **IE** 활성화 확인란이 나타납니다. 이 확인란을 선택합니다.

보안 신호음 상호 작용

기능	상호 작용
호 전환, 전화회의 및 통화 대기	사용자가 보호된 전화기에서 이러한 기능을 호출하면 시스템에서 보안 또는 비보안 표시 신호음을 재생하여 통화의 업데이트된 상태를 나타냅니다.
보류/재시작 및 모두 착신 전환	이러한 기능은 보호된 통화에서 지원됩니다.

보안 신호음 제한 사항

제한 사항	설명
Cisco Extension Mobility 및 회선 간 참가 서비스	Cisco Extension Mobility 및 회선 간 참가 서비스는 보호된 전화기에서 비활성화됩니다.
공유 회선 구성	공유 회선 구성은 보호된 전화기에서 사용할 수 없습니다.
암호화되지 않은 미디어	Cisco Unified IP Phone과 MGCP E1 PRI 게이트웨이 사이에 있는 미디어가 암호화되지 않으면 통화가 끊어집니다.



XII 부

사용자 정의 기능

- 브랜딩 사용자 지정 , 637 페이지
- 클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC), 645 페이지
- 사용자 지정 전화기 벨소리 및 배경, 653 페이지
- 대기 중 음악 , 663 페이지
- 셀프 서비스 포털 , 683 페이지
- 비상 통화 처리기 , 687 페이지
- RedSky로 비상 통화 처리, 701 페이지
- 엔터프라이즈 그룹 , 707 페이지



47 장

브랜딩 사용자 지정

- [브랜드 개요, 637 페이지](#)
- [브랜드 필수 조건, 637 페이지](#)
- [브랜딩 작업 흐름, 638 페이지](#)
- [브랜딩 파일 요구 사항, 640 페이지](#)

브랜드 개요

브랜딩 기능을 사용하여 Cisco Unified Communications Manager에 맞게 사용자 정의된 브랜딩을 업로드할 수 있습니다. 브랜딩은 Cisco Unified CM 관리 로그인 및 구성 창에 적용됩니다. 수정할 수 있는 항목에는 다음이 포함됩니다.

- 회사 로고
- 배경색
- 테두리 색상
- 글꼴 색

셀프 서비스 포털에 로고 추가

브랜딩 기능을 사용하면 회사 로고를 Unified Communications 자가 관리 포털 로그인 페이지와 사용자 인터페이스 헤더에 추가할 수 있습니다. branding_logo.png 파일을 branding.zip 파일에 포함하고 zip 파일을 Cisco Unified Communications Manager에 업로드해야 합니다. Cisco Unified Communications Manager에서 브랜딩을 활성화한 후에는 로고가 셀프 서비스 포털에 표시됩니다.

셀프 서비스 포털에 대한 배경색 또는 글꼴을 사용자 정의하는 옵션은 없습니다.

브랜드 필수 조건

지정한 폴더 구조와 파일을 포함하는 branding.zip 파일을 생성해야 합니다. 자세한 내용은 [브랜딩 파일 요구 사항, 640 페이지](#)를 참조하십시오.

브랜딩 작업 흐름

이러한 작업을 완료하여 Cisco Unified Communications Manager 및 Unified Communications 자가 관리 포털에 브랜딩을 적용합니다.

시작하기 전에

- [브랜드 필수 조건, 637 페이지](#) 검토

프로시저

	명령 또는 동작	목적
단계 1	다음 절차 중 하나를 사용하여 브랜딩 설정을 구성합니다. <ul style="list-style-type: none"> • 브랜딩 활성화, 638 페이지 • 브랜딩 비활성화, 639 페이지 	Cisco Unified Communications Manager 클러스터에 브랜딩을 적용합니다.
단계 2	Tomcat 서비스 다시 시작, 640 페이지	새 브랜딩 설정을 위해 Cisco Tomcat 서비스를 다시 시작하여 Unified Communications 자가 관리 포털에서 당겨 받을 수 있도록 해야 합니다.

브랜딩 활성화

이 절차를 사용하여 Unified Communications Manager에 대해 브랜딩 사용자 정의를 활성화합니다. SAML SSO(Single Sign-on)에 대해 시스템을 활성화한 경우에는 브랜딩 업데이트가 표시됩니다.



참고 브랜딩을 활성화하려면 권한 수준 4 액세스 권한이 있는 기본 관리자 계정을 사용해야 합니다. 이는 설치 중에 생성되는 기본 관리자 계정입니다.



참고 브랜드를 활성화하거나 비활성화하려면 GUI와 CLI 중 하나만 사용해야 합니다. 예를 들어, GUI 인터페이스를 사용하여 브랜딩을 활성화하는 경우 GUI 인터페이스 자체를 사용하여 브랜딩을 비활성화해야 합니다. 그렇지 않으면 제대로 작동하지 않습니다.

시작하기 전에

branding.zip 파일을 준비하고 Unified Communications Manager에서 액세스할 수 있는 위치에 저장합니다.

프로시저

단계 1 Cisco Unified OS 관리에 로그인합니다.

단계 2 소프트웨어 업그레이드 > 브랜딩을 선택합니다.

단계 3 원격 서버로 이동하고 branding.zip 파일을 선택합니다.

단계 4 파일 업로드를 클릭합니다.

단계 5 브랜딩 활성화를 클릭합니다.

참고 **utils branding enable** CLI 명령을 실행하여 브랜딩을 활성화할 수도 있습니다.

단계 6 브라우저를 새로 고치십시오.

단계 7 모든 Cisco Unified Communications Manager 클러스터 노드에서 이 절차를 반복합니다.

회사 로고를 셀프 서비스 포털 사용자 인터페이스에 추가하려면 [Tomcat 서비스 다시 시작, 640 페이지](#)의 내용을 참조하십시오.

브랜딩 비활성화

이 절차를 사용하여 Cisco Unified Communications Manager 클러스터에서 브랜딩을 비활성화합니다. 셀프 서비스 포털에서 회사 로고를 제거하려는 경우에는 브랜딩을 비활성화해야 합니다.



참고 브랜딩을 비활성화하려면 권한 수준 4 액세스 권한이 있는 기본 관리자 계정을 사용해야 합니다. 이는 설치 중에 생성되는 기본 관리자 계정입니다.



참고 브랜드를 활성화하거나 비활성화하려면 GUI와 CLI 중 하나만 사용해야 합니다. 예를 들어, GUI 인터페이스를 사용하여 브랜딩을 활성화하는 경우 GUI 인터페이스 자체를 사용하여 브랜딩을 비활성화해야 합니다. 그렇지 않으면 제대로 작동하지 않습니다.

프로시저

단계 1 Cisco Unified OS 관리에 로그인합니다.

단계 2 소프트웨어 업그레이드 > 브랜딩을 선택합니다.

단계 3 브랜딩 비활성화를 클릭합니다.

참고 **utils branding disable** CLI 명령을 실행하여 브랜딩을 비활성화할 수도 있습니다.

단계 4 브라우저를 새로 고치십시오.

단계 5 모든 Cisco Unified Communications Manager 클러스터 노드에서 이 절차를 반복합니다.

셀프 서비스 포털 사용자 인터페이스에서 회사 로고를 제거하려면 [Tomcat 서비스 다시 시작, 640 페이지](#)의 내용을 참조하십시오.

Tomcat 서비스 다시 시작

셀프 서비스 포털에 반영되도록 브랜딩 업데이트를 위해 Cisco Tomcat 서비스를 다시 시작해야 합니다.

시작하기 전에

다음 작업을 완료해야 합니다.

- 셀프 서비스 포털에 로고를 추가하려면 먼저 Cisco Unified Communications Manager에서 브랜딩을 활성화해야 합니다. branding.zip 업로드 파일은 회사 로고를 포함하는 44x25 픽셀 branding_logo.png 파일을 포함해야 합니다. 자세한 내용은 [브랜딩 활성화, 638 페이지](#)의 내용을 참조하십시오.
- 셀프 서비스 포털에서 로고를 제거하려면 Cisco Unified Communications Manager에서 브랜딩을 비활성화해야 합니다. 자세한 내용은 [브랜딩 비활성화, 639 페이지](#)의 내용을 참조하십시오.

프로시저

단계 1 명령줄 인터페이스에 로그인합니다.

단계 2 **utils service restart Cisco Tomcat** CLI 명령을 실행합니다.

단계 3 모든 Cisco Unified Communications Manager 클러스터 노드에서 이 절차를 반복합니다.

다음에 수행할 작업

서비스가 다시 시작되면 브라우저를 새로 고쳐 셀프 서비스 포털의 변경 사항을 확인합니다.

브랜딩 파일 요구 사항

사용자 지정 브랜딩을 시스템에 적용하기 전에 지정된 사양에 따라 branding.zip 파일을 만듭니다. 원격 서버에서 브랜딩 폴더를 만들고 지정된 내용으로 폴더를 채웁니다. 모든 이미지 파일과 하위 폴더를 추가했으면 전체 폴더를 압축하여 파일을 branding.zip으로 저장합니다.

헤더에 대해 단일 이미지를 사용할지 아니면 여섯 개의 이미지 조합을 사용하여 헤더에 대해 단계별 효과를 만들지 여부에 따라 폴더 구조에는 두 가지 옵션이 있습니다.

표 52: 폴더 구조 옵션

브랜딩 옵션	폴더 구조
단일 헤더 옵션	<p>헤더 배경(설명선 항목 3)에 대해 단일 이미지를 원하는 경우 브랜딩 폴더에 다음 하위 폴더 및 이미지 파일이 있어야 합니다.</p> <pre> Branding (folder) ccmadmin (folder) BrandingProperties.properties (properties file) brandingHeader.gif (2048*1 pixel image) ciscoLogo12pxMargin.gif (44*44 pixel image) branding_logo.png (44*25 pixel image) </pre>
단계별 헤더 옵션	<p>헤더 배경의 단계별 이미지를 만들려면 단계별 효과를 만들기 위해 6 개의 별도 이미지 파일이 필요합니다. 브랜딩 폴더에는 이러한 하위 폴더 및 파일이 있어야 합니다.</p> <pre> Branding(folder) ccmadmin (folder) BrandingProperties.properties (file) brandingHeaderBegLTR.gif (652*1 pixel image) brandingHeaderBegRTR.gif (652*1 pixel image) brandingHeaderEndLTR.gif (652*1 pixel image) brandingHeaderEndRTR.gif (652*1 pixel image) brandingHeaderMidLTR.gif (652*1 pixel image) brandingHeaderMidRTR.gif (652*1 pixel image) ciscoLogo12pxMargin.gif (44*44 pixel image) branding_logo.png (44*25 pixel image) </pre>

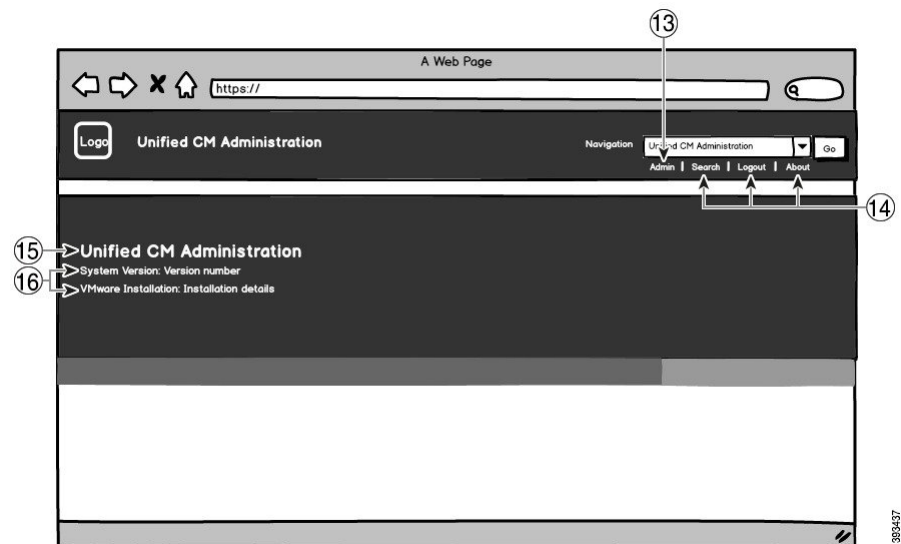
사용자 인터페이스 브랜딩 옵션

다음 이미지는 Cisco Unified CM 관리 사용자 인터페이스의 사용자 정의 옵션을 표시합니다.

그림 10: Unified CM 관리 로그인 화면의 브랜딩 옵션



그림 11: Unified CM 관리 로그인됨 화면의 브랜딩 옵션



다음 표는 콜아웃 옵션에 대해 설명합니다.

표 53: 사용자 인터페이스 브랜딩 옵션: 로그인 화면

항목	설명	브랜딩 편집
1	회사 로고	<p>Cisco Unified Communications Manager에 로고를 추가하려면 회사 로고를 다음 파일 이름의 44x44 픽셀 이미지로 저장합니다.</p> <p>ciscoLogo12pxMargin.gif (44*44 픽셀)</p> <p>참고 셀프 서비스 포털의 헤더 및 로그인 화면에 로고를 추가하려는 경우에도 로고를 44x25 픽셀 branding_logo.png 파일로 저장해야 합니다.</p>
2	Unified CM 관리 헤더 글꼴 색	heading.heading.color
3	헤더 배경	<p>단일 이미지 또는 6개의 이미지 조합을 사용하여 단계별 효과를 만들 수 있습니다.</p> <p>단일 이미지 옵션 - 헤더 배경을 단일 이미지로 저장합니다.</p> <ul style="list-style-type: none"> • brandingHeader.gif(2048*1 픽셀) <p>단계별 배경 옵션: - 헤더 배경을 동일한 효과를 위해 6개의 이미지로 저장합니다.</p> <ul style="list-style-type: none"> • brandingHeaderBegLTR.gif(652*1 픽셀) • brandingHeaderBegRTR.gif(652*1 픽셀) • brandingHeaderEndLTR.gif(652*1 픽셀) • brandingHeaderEndRTR.gif(652*1 픽셀) • brandingHeaderMidLTR.gif(652*1 픽셀) • brandingHeaderMidRTR.gif(652*1 픽셀)
4	탐색 텍스트	header.navigation.color
5	이동 버튼	<p>header.go.font.color</p> <p>header.go.background.color</p> <p>header.go.border.color</p>
6	사용자 이름 텍스트	splash.username.color
7	암호 텍스트	splash.password.color

항목	설명	브랜딩 편집
8	로그인 버튼	splash.login.text.color splash.login.back.ground.color
9	재설정 버튼	splash.reset.text.color splash.reset.back.ground.color
10	아래 배경색 - 오른쪽	splash.hex.code.3
11	아래 배경색 - 왼쪽	splash.hex.code.2
12	배너	splash.hex.code.1

표 54: 사용자 인터페이스 브랜딩 옵션: 로그인됨 화면

항목	설명	브랜딩 편집
13	사용자 텍스트(예: 'admin')	header.admin.color
14	검색, 정보 및 로그인 텍스트	header.hover.link.color
15	Unified CM 관리 텍스트 머리글	splash.header.color
16	시스템 버전 및 VMware 설치 텍스트	splash.reset.text.color splash.version.color

브랜딩 속성 편집 예

브랜딩 속성은 속성 파일에 16진 코드를 추가하여 편집할 수 있습니다 (BrandingProperties.properties). 특성 파일은 HTML 기반 16진 코드를 사용합니다. 예를 들어 탐색 텍스트 항목(콜아웃 항목 4번)의 색상을 빨간색으로 변경하려면 속성 파일에 다음 코드를 추가합니다.

```
header.navigation.color="#FF0000"
```

이 코드에서 header.navigation.color는 편집하려는 브랜딩 속성이고 "#FF0000"은 새 설정(빨간색)입니다.



48 장

클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC)

- 클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 개요, 645 페이지
- 클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 사전 요건, 645 페이지
- 클라이언트 매터 코드 및 강제 인증 코드 구성 작업 흐름, 646 페이지
- 클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 상호 작용, 649 페이지
- 클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 제한 사항, 650 페이지

클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 개요

CMC(Client Matter Code) 및 FAC(Forced Authorization Code)를 사용하여 통화 액세스 및 계정을 효과적으로 관리할 수 있습니다. CMC는 클라이언트에 대한 통화 계정 관리 및 청구를 지원하고, FAC는 특정 사용자가 걸 수 있는 통화 유형을 규제합니다.

CMC의 경우 사용자가 코드를 입력해야 합니다. 이러한 조치는 해당 통화가 특정 클라이언트 문제와 관련되어 있음을 나타냅니다. 통화 회계 및 청구 목적으로 고객, 학생 또는 기타 사용자에게 클라이언트 매터 코드를 할당할 수 있습니다. FAC의 경우 통화가 완료되기 전에 사용자가 특정 액세스 레벨로 할당된 유효한 인증 코드를 입력해야 합니다.

클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 사전 요건

- SCCP 및 SIP를 실행 중인 Cisco Unified IP Phone에서는 CMC 및 FAC를 지원합니다.
- CMC 및 FAC 신호음은 SCCP 또는 SIP를 실행하는 Cisco Unified IP Phone, TAPI/JTAPI 포트 및 MGCP FXS 포트에서만 재생됩니다.

클라이언트 매터 코드 및 강제 인증 코드 구성 작업 흐름

CMC 및 FAC를 개별적으로 구현하거나 함께 구현할 수 있습니다. 예를 들어 특정 클래스의 전화(예: 장거리 통화)를 걸고 이 통화 클래스를 특정 클라이언트에 할당할 수 있는 권한을 사용자에게 부여할 수 있습니다. CMC 및 FAC 신호음은 사용자에게 동일하게 재생됩니다. 따라서 두 코드를 모두 구성하는 경우 첫 번째 신호음 이후에 FAC를 입력하고 두 번째 신호음 이후에 CMC를 입력하도록 사용자에게 지침이 제공됩니다.

시작하기 전에

- 클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 사전 요건, 645 페이지 검토

프로시저

	명령 또는 동작	목적
단계 1	클라이언트 매터 코드 구성, 646 페이지에 대해 다음 하위 작업을 수행합니다. <ul style="list-style-type: none"> 클라이언트 매터 코드(Client Matter Code) 추가, 647 페이지 클라이언트 매터 코드 활성화, 647 페이지 	사용할 CMC 목록을 결정한 후 이러한 코드를 데이터베이스에 추가하고 라우트 패턴에서 CMC 기능을 활성화합니다.
단계 2	강제 인증 코드 구성, 648 페이지에 대해 다음 하위 작업을 수행합니다. <ul style="list-style-type: none"> 강제 인증 코드(FAC) 추가, 648 페이지 강제 인증 코드 활성화, 648 페이지 	사용할 FAC 목록과 인증 수준을 결정한 후 이러한 코드를 데이터베이스에 추가하고 라우트 패턴에서 FAC 기능을 활성화합니다.

클라이언트 매터 코드 구성

프로시저

	명령 또는 동작	목적
단계 1	클라이언트 매터 코드(Client Matter Code) 추가, 647 페이지	사용하려는 고유한 클라이언트 매터 코드를 결정하고 시스템에 추가합니다. CMC의 수는 시스템을 시작하는 데 필요한 시간에 직접적인 영향을 주므로, CMC의 수를 최대 60,000으로 제한합니다. 최대 CMC를 최대 개수보다 많이 구성하는 경우에는 상당한 지연이 예상됩니다.
단계 2	클라이언트 매터 코드 활성화, 647 페이지	경로 패턴을 통해 클라이언트 매터 코드를 활성화합니다.

클라이언트 매터 코드(Client Matter Code) 추가

사용하려는 고유한 클라이언트 매터 코드를 결정하고 시스템에 추가합니다. CMC의 수는 시스템을 시작하는 데 필요한 시간에 직접적인 영향을 주므로, CMC의 수를 최대 60,000으로 제한합니다. 최대 CMC를 최대 개수보다 많이 구성하는 경우에는 상당한 지연이 예상됩니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 클라이언트 매터 코드.
 - 단계 2 새로 추가를 클릭합니다.
 - 단계 3 클라이언트 매터 코드 필드에 전화를 걸 때 사용자가 입력하는 고유 코드를 16자 이하로 입력합니다.
 - 단계 4 클라이언트 매터 코드를 식별하려는 경우 설명 필드에 클라이언트 이름을 입력합니다.
 - 단계 5 저장을 클릭합니다.
-

클라이언트 매터 코드 활성화

경로 패턴을 통해 클라이언트 매터 코드를 활성화합니다.

시작하기 전에

[클라이언트 매터 코드\(Client Matter Code\) 추가, 647 페이지](#)

프로시저

-
- 단계 1 Cisco 통합 CM 관리에서 콜 라우팅 > 라우트/힌트 > 라우트 패턴을 선택합니다.
 - 단계 2 다음 작업 중 하나를 수행합니다.
 - 기존 라우트 패턴을 업데이트하려면 검색 조건을 입력하고 찾기를 클릭한 다음 결과 목록에서 라우트 패턴을 선택합니다.
 - 새 라우트 패턴을 만들려면 새로 추가를 클릭합니다.
 - 단계 3 라우트 패턴 구성 창에서 클라이언트 매터 코드 요구 확인란을 선택합니다.
 - 단계 4 저장을 클릭합니다.
-

강제 인증 코드 구성

프로시저

	명령 또는 동작	목적
단계 1	강제 인증 코드(FAC) 추가, 648 페이지	사용하려는 고유한 강제 인증 코드를 결정하고 이를 시스템에 추가합니다.
단계 2	강제 인증 코드 활성화, 648 페이지	라우트 패턴을 통해 강제 인증 코드를 활성화합니다.

강제 인증 코드(FAC) 추가

이 절차를 사용하여 사용하려는 고유한 강제 인증 코드를 결정하고 이를 시스템에 추가합니다. 통화를 성공적으로 경로 지정하려면 사용자 인증 수준이 통화에 대한 라우트 패턴에 지정된 인증 수준보다 높거나 같아야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 강제 인증 코드를 선택합니다.

단계 2 인증 코드 이름 필드에 50자 이하의 고유한 이름을 입력합니다.

이 이름은 특정 사용자나 사용자 그룹에 인증 코드를 연결합니다.

단계 3 인증 코드 필드에 16자리 이하의 고유한 인증 코드를 입력합니다.

사용자는 FAC 지원 라우트 패턴을 통해 호출할 때 이 코드를 입력합니다.

단계 4 인증 레벨 필드에 0 - 255 범위의 세 자리 인증 레벨을 입력합니다.

단계 5 저장을 클릭합니다.

강제 인증 코드 활성화

경로 패턴을 통해 강제 인증 코드를 사용하도록 설정합니다.

프로시저

단계 1 Cisco 통합 CM 관리에서 콜 라우팅 > 라우트/헌트 > 라우트 패턴을 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 찾기를 클릭한 다음 결과 목록에서 경로 패턴을 선택하여 기존의 경로 패턴을 업데이트합니다.
- 새로 추가를 클릭하여 새 라우트 패턴을 생성합니다.

단계 3 경로 패턴 구성 창에서 강제 인증 코드 필요 확인란을 선택합니다.

단계 4 인증 레벨 필드에 0에서 255 사이의 인증 레벨 값을 입력합니다.

통화를 라우팅하려면 사용자의 FAC 레벨이 구성된 레벨과 같거나 구성된 레벨보다 높아야 합니다.

단계 5 저장을 클릭합니다.

클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 상호 작용

표 55: 클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 상호 작용

기능	상호 작용
CDR Analysis and Reporting(CAR)	CAR(CDR Analysis and Reporting)을 사용하면 클라이언트 매터 코드(CMC), 강제 인증 코드 (FAC) 및 인증 수준에 대한 통화 세부 정보를 제공하는 보고서를 실행할 수 있습니다.
CTI JTAPI 및 TAPI 애플리케이션	<p>대부분의 경우 시스템은 CTI, JTAPI 또는 TAPI 애플리케이션에 사용자가 통화 중에 코드를 입력해야 한다는 사실을 알려줄 수 있습니다. 사용자가 전화를 걸거나 애드-후 컨퍼런스를 생성하거나 CMC 또는 FAC 사용 라우트 패턴을 통해 상담 호전환을 수행하는 경우 사용자가 신호음을 수신하고 나면 코드를 입력해야 합니다.</p> <p>사용자가 CMC 또는 FAC 사용 라우트 패턴을 통해 통화를 재전송하거나 블라인드 호전환하는 경우 사용자는 신호음을 받지 못하므로 애플리케이션에서 Cisco Unified Communications Manager로 코드를 보내야 합니다. 시스템에서 적절한 코드를 수신하면 통화가 의도된 상대방에게 연결됩니다. 시스템에서 적절한 코드를 수신하지 못하면 Cisco Unified Communications Manager가 누락된 코드를 나타내는 오류를 애플리케이션으로 보냅니다.</p>

기능	상호 작용
Cisco Web Dialer	<p>Web Dialer는 다음과 같은 방법으로 CMC 및 FAC를 지원합니다.</p> <ul style="list-style-type: none"> • 사용자는 WD HTML 페이지 또는 SOAP 요청의 다이얼 텍스트 상자에 대상 번호를 입력한 다음 전화기에 CMC 또는 FAC를 수동으로 입력할 수 있습니다. • 사용자는 WD HTML 페이지 또는 SOAP 요청의 다이얼 텍스트 상자에 FAC 또는 CMC를 사용하여 대상 번호를 입력할 수 있습니다. <p>예를 들어, 대상 번호가 5555이고 FAC가 111이고 CMC가 222인 경우, 사용자는 5555111#(FAC), 5555222#(CMC) 또는 5555111222#(CMC 및 FAC)을 다이얼하여 전화를 걸 수 있습니다.</p> <p>참고</p> <ul style="list-style-type: none"> • WebDialer는 대상 번호에 대한 유효성 검사를 처리하지 않습니다. 전화기에서 필수 확인을 처리합니다. • 사용자가 코드를 제공하지 않거나 잘못된 코드를 제공하는 경우 통화는 실패합니다. • 사용자가 특수 문자를 포함하는 DN을 사용하여 WebApp에서 전화를 거는 경우 특수 문자를 제거한 후 통화가 성공적으로 수행됩니다. 동일한 규칙이 SOAP UI에서 작동하지 않습니다.
단축 다이얼 URI	<p>단축 다이얼을 사용하여 FAC, CMC, 전화 걸기 일시 중지 또는 추가 숫자(예: 사용자 내선 번호, 회의 액세스 코드 또는 음성 메일 암호)가 필요한 대상에 도달할 수 있습니다. 구성된 단축 다이얼을 누르면 전화기에서 대상 번호와의 통화를 설정하고 전화 걸기 일시 중지를 삽입하여 지정된 FAC, CMC 및 추가 숫자를 전송합니다.</p>

클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 제한 사항

표 56: 클라이언트 매터 코드(Client Matter Code) 및 강제 인증 코드(FAC) 제한 사항

제한 사항	설명
아날로그 게이트웨이	이러한 게이트웨이에서는 신호음을 재생할 수 없으므로 H.323 아날로그 게이트웨이는 CMC 또는 FAC를 지원하지 않습니다.

제한 사항	설명
통화 착신 전환	<p>CMC 또는 FAC 사용 경로 패턴으로 착신 전환되는 통화는 실패하게 되는데, 코드를 입력하는 사용자가 없기 때문입니다. 사용자가 착신전환 소프트웨어를 누르고 경로 패턴에서 CMC 또는 FAC가 활성화되어 1있는 번호를 입력하면 착신 전환이 실패합니다.</p> <p>통화 처리 중단을 최소화하려면 착신 전환을 구성하기 전에 번호를 테스트하십시오. 이를 위해서는 착신 전환 번호로 전화를 겁니다. 코드를 입력하라는 메시지가 표시되면 해당 번호에 대해 착신 전환을 구성하지 마십시오. 착신 전환된 통화가 의도된 대상에 연결되지 않는 데 따른 불만 건수를 최소화하려면 사용자에게 이 방법을 안내해 주십시오.</p>
Cisco Unified Mobility	CMC 또는 FAC를 필요로 하는 경로 패턴이 발견되고 발신자가 Cisco Unified Mobility로 구성되지 않은 경우, SIP 트렁크, H.323 또는 MGCP 게이트웨이에서 시작되는 통화가 실패합니다.
DvO(Dial via Office) 콜백 번호	Cisco Mobility의 CMC 및 FAC 기능은 DvO(Dial via Office) 콜백 번호로 대체 번호를 지원하지 않습니다. DVO 콜백 번호는 이동성 ID 창에 등록된 숫자여야 합니다.
페일오버 통화	CMC 및 FAC는 페일오버 통화에서 작동하지 않습니다.
청각 장애가 있는 사용자	청각 장애가 있는 사용자는 전화 번호로 전화를 건 후에 1~2초간 기다렸다가 인증 코드 또는 클라이언트 매터 코드를 입력해야 합니다.
지역화	<p>Cisco에서는 CMC 또는 FAC를 지역화하지 않습니다. CMC 및 FAC 기능에서는 Cisco Unified Communications Manager에서 지원되는 모든 로캘에 대해 동일한 기본 신호음을 사용합니다.</p> <p>참고 Cisco Mobility의 경우 CMC 및 FAC가 지역화되었습니다.</p>
중복 송신	Cisco Unified Communications Manager는 사용자에게 코드를 요구하는 메시지를 표시하는 시점을 결정할 수 없으므로 CMC 및 FAC 기능에서는 중복 송신을 지원하지 않습니다. 라우트 패턴 구성 창에서 강제 인증 코드 필요 또는 클라이언트 매터 코드 필요 확인란을 선택하면 중복 송신 허용 확인란이 자동으로 선택 취소되거나 선택됩니다.
바로 호출 버튼	단축 다이얼 버튼에는 FAC 또는 CMC를 구성할 수 없습니다. 시스템에서 코드를 입력하라는 메시지가 표시되면 코드를 입력해야 합니다.



49 장

사용자 지정 전화기 벨소리 및 배경

- 사용자 지정 전화기 벨소리 개요, 653 페이지
- 사용자 지정 전화기 벨소리 사전 요건, 653 페이지
- 사용자 지정 전화기 벨소리 구성 작업 흐름, 654 페이지
- 사용자 정의 배경, 656 페이지
- 사용자 지정 배경 구성 작업 흐름, 657 페이지

사용자 지정 전화기 벨소리 개요

사용자 지정 전화기 벨소리를 사용하여 사용자 지정된 전화기 벨소리를 생성하고 사용자 지정 파일을 Cisco Unified IP Phone에서 액세스할 수 있는 TFTP 서버 Cisco Unified Communications Manager에 업로드할 수 있습니다.

Cisco Unified IP Phone에는 하드웨어에서 구현되는 기본 벨소리 유형, 즉 Chirp1 및 Chirp2가 제공됩니다. 또한 Cisco Unified Communications Manager는 다음 파일을 전화기에 업로드하는 기능을 제공합니다.

PCM 파일

Cisco Unified Communications Manager는 소프트웨어에서 PCM(Pulse Code Modulation) 오디오 파일로 구현되는 전화기 벨소리 기본 세트를 제공합니다. 각 PCM 파일은 단일 벨소리 유형을 지정합니다.

Ringlist.xml 파일

Ringlist.xml 파일은 전화기에 사용할 수 있는 벨소리 옵션 목록을 설명합니다.

사용자 지정 벨소리 및 콜백 신호음 등과 같은 사용자 지정된 PCM 오디오 파일을 Cisco Unified Communications Manager의 TFTP 디렉터리에 업로드할 수 있습니다.

사용자 지정 전화기 벨소리 사전 요건

다음 사전 요건은 사용자 정의 전화기 벨소리에 적용됩니다.

- 사용자 정의 전화기 벨소리를 업로드하려면 Cisco TFTP 서비스가 실행되고 있어야 합니다.

- 업로드하려는 PCM 파일은 Cisco Unified IP Phone과 호환되려면 파일 요구 사항 집합을 충족해야 합니다. 자세한 내용은 [PCM 파일 형식 요구 사항, 655 페이지](#) 항목을 검토하십시오.
- Ringlist.xml 파일은 일련의 서식 지정 지침을 충족해야 합니다. 자세한 내용은 [Ringlist.xml 파일 형식 요구 사항, 656 페이지](#) 항목을 검토하십시오.

사용자 지정 전화기 벨소리 구성 작업 흐름

시작하기 전에

- [사용자 지정 전화기 벨소리 사전 요건, 653 페이지](#) 검토

프로시저

	명령 또는 동작	목적
단계 1	업로드를 위한 사용자 지정 전화기 벨소리 준비, 654 페이지	사용자 정의된 PCM 및 Ringlist.xml 파일을 생성합니다.
단계 2	TFTP 서버에 사용자 지정 전화기 벨소리 업로드, 655 페이지	사용자 정의 파일을 Cisco Unified Communications Manager TFTP 서버에 업로드합니다.
단계 3	TFTP 서비스 다시 시작, 655 페이지	업로드가 완료되면 Cisco TFTP 서비스를 다시 시작합니다.

업로드를 위한 사용자 지정 전화기 벨소리 준비

프로시저

-
- 단계 1 `file get tftp <tftp path>` CLI 명령을 사용하여 수정하려는 PCM 파일 외에 기존 Ringlist.xml 파일을 다운로드합니다.
- 단계 2 업로드하려는 각 벨소리 유형에 대한 PCM 파일을 생성합니다. Cisco Unified Communications Manager와의 PCM 파일 호환성에 대한 지침은 [PCM 파일 형식 요구 사항, 655 페이지](#)의 내용을 참조하십시오.
- 단계 3 ASCII 편집기를 사용하여 새 전화기 벨소리로 Ringlist.xml 파일을 업데이트합니다. Ringlist.xml 파일 형식 요구 사항에 대한 자세한 내용은 [Ringlist.xml 파일 형식 요구 사항, 656 페이지](#)의 내용을 참조하십시오.
-

TFTP 서버에 사용자 지정 전화기 벨소리 업로드

시작하기 전에

[업로드를 위한 사용자 지정 전화기 벨소리 준비, 654 페이지](#)

프로시저

단계 1 Cisco Unified OS 관리에서 소프트웨어 업그레이드 > **TFTP** > 파일 관리를 선택합니다.

단계 2 파일 업로드를 클릭합니다.

단계 3 찾아보기를 클릭하고 Ringlist.xml 파일 및 업로드할 PCM 파일을 선택합니다.

단계 4 파일 업로드를 클릭합니다.

TFTP 서비스 다시 시작

시작하기 전에

[TFTP 서버에 사용자 지정 전화기 벨소리 업로드, 655 페이지](#)

프로시저

단계 1 Cisco Unified Serviceability에 로그인하고 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 2 서버 그룹다운 목록에서 Cisco TFTP 서비스가 실행 중인 서버를 선택합니다.

단계 3 **Cisco TFTP** 서비스에 해당하는 무선 단추를 클릭합니다.

단계 4 재시작을 클릭합니다.

PCM 파일 형식 요구 사항

Cisco Unified IP Phone에서 제대로 재생되려면 전화기 벨소리용 PCM 파일이 요구 사항을 충족해야 합니다. PCM 파일을 생성하거나 수정할 때 다음 파일 형식 요구 사항을 지원하는 모든 표준 오디오 편집 패키지를 사용할 수 있습니다.

- 원시 PCM
- 초당 8000개 샘플
- 샘플당 8비트
- mu-law 압축
- 최대 벨소리 크기 = 16080개 샘플
- 벨소리 샘플 수를 240개 단위로 균일하게 나누어야 함

- 벨소리는 부호 변화점에서 시작하고 끝납니다.

Ringlist.xml 파일 형식 요구 사항

Ringlist.xml 파일은 전화기 벨소리 유형 목록이 포함된 XML 객체를 정의합니다. 각 벨소리 유형에는 해당 벨소리 유형에 사용되는 PCM 파일에 대한 포인터와 해당 벨소리에 대해 Cisco Unified IP Phone의 [벨소리 유형] 메뉴에 표시되는 텍스트가 포함됩니다.

CiscoIPPhoneRinglist XML 객체는 다음의 간단한 태그 설정을 사용하여 정보를 기술합니다.

```
<CiscoIPPhoneRinglist>    <Ring>
    <DisplayName/>
    <FileName/>
</Ring>
</CiscoIPPhoneRinglist>
```

다음 특성이 정의 이름에 적용됩니다.

- **DisplayName**은 Cisco Unified IP Phone의 [벨소리 유형] 메뉴에 표시될, 연결된 PCM 파일의 사용자 정의 벨소리의 이름을 정의합니다.
- **FileName**은 사용자 정의 벨소리를 DisplayName과 연결하기 위한 PCM 파일의 이름을 지정합니다.



팁 DisplayName 및 FileName 필드는 25자를 초과해서는 안 됩니다.

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

```
<CiscoIPPhoneRinglist>    <Ring>
    <DisplayName>Analog Synth 1</DisplayName>
    <FileName>Analog1.raw</FileName>
</Ring>
<Ring>
    <DisplayName>Analog Synth 2</DisplayName>
    <FileName>Analog2.raw</FileName>
</Ring>
</CiscoIPPhoneRinglist>
```



팁 각 전화기 벨소리 유형별로 필요한 DisplayName과 FileName을 포함해야 합니다. Ringlist.xml 파일에는 최대 50개의 벨소리 유형이 포함될 수 있습니다.

사용자 정의 배경

TFTP 서버를 사용하여 새 사용자 정의 배경 이미지를 네트워크의 전화기로 업로드할 수도 있습니다. 전화기 사용자는 전화기 배경으로 업로드하는 이미지를 선택할 수 있습니다. 전화기 사용자가 이미지 분류에서 선택할 수 있도록 시스템을 구성하거나 모든 전화기에 대해 특정 배경 이미지를 할당할 수 있습니다.

전화기 사용자가 전화기 배경을 사용자 정의할 수 있게 하려면 새 이미지를 업로드할 때마다 다음 작업을 준비하고 TFTP 서버에 업로드해야 합니다.

- 전체 크기 배경 이미지 — 전화기 모델에 대한 이미지 크기(픽셀) 및 색상 유형 등 이미지 사양에 대한 전화기 설명서를 참조하십시오.
- 썸네일 이미지 - 전화기 사용자가 자신의 배경 이미지를 선택할 수 있게 하려는 경우에만 필요합니다. 썸네일 이미지 사양에 대한 자세한 내용은 전화기 설명서를 참조하십시오.
- 편집된 List.xml 파일 - 이 파일에는 전화기 사용자가 선택할 수 있는 배경 이미지 목록이 포함되어 있습니다. 새 이미지를 이 파일에 추가해야 합니다.

모든 전화기에 특정 이미지를 할당하려면 기본 배경 이미지만 업로드해야 합니다. 또한 사용자가 할당하는 이미지를 사용하도록 전화기에 지시하려면 일반 전화 프로파일을 업데이트 해야 합니다.

사용자 지정 배경 구성 작업 흐름

구축의 전화기에 대한 사용자 정의 배경 이미지를 구성하고 업로드하려면 이러한 작업을 완료합니다. 전화기 사용자가 이미지 분류 중에서 선택할 수 있도록 시스템을 구성하거나 모든 전화기에 표시되는 특정 배경 이미지를 할당할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	전화기 배경 이미지 만들기, 658 페이지	<p>전체 크기 배경 이미지와 해당 썸네일 이미지 (필요한 경우)를 생성합니다. 파일 유형, 이미지 크기(픽셀) 및 색상 유형을 포함하여 이미지 사양에 대한 자세한 내용은 전화기 설명서를 참조하십시오.</p> <p>참고 특정 배경 이미지를 할당하는 경우에는 썸네일이 필요하지 않습니다.</p>
단계 2	List.xml 파일 편집, 658 페이지	<p>해당 TFTP 디렉터리에서 새 이미지를 사용하여 List.xml 파일을 업데이트합니다. 이는 전화기 사용자가 전화기 배경 옵션 목록에 새 이미지를 표시하기 위해 필요합니다.</p> <p>참고 이 절차는 사용자에게 자신의 배경을 선택할 수 있는 옵션을 제공하는 경우에만 필요합니다. 특정 배경 이미지를 할당하는 경우에는 이 파일을 편집할 필요가 없습니다.</p>

	명령 또는 동작	목적
단계 3	TFTP 서버에 배경 업로드, 659 페이지	파일을 TFTP 서버에 업로드합니다.
단계 4	TFTP 서버 다시 시작, 660 페이지	이미지를 전화기로 푸시하기 위해 Cisco TFTP 서비스를 다시 시작합니다.
단계 5	전화기 사용자에게 전화기 배경 할당, 660 페이지	(선택 사항) 기본적으로 Cisco Unified Communications Manager는 전화기 사용자에게 자신의 전화기 배경 이미지를 선택할 수 있는 옵션을 제공합니다. 그러나 일반 전화 프로파일을 사용하여 이 일반 전화 프로파일을 사용하는 모든 전화기의 특정 배경 이미지를 할당할 수 있습니다.

전화기 배경 이미지 만들기

배경 이미지 사양 및 썸네일 이미지 사양에 대한 자세한 내용은 전화기 설명서를 참조하십시오. 여기에는 이미지 크기(픽셀), 파일 유형 및 해당 전화기 모델에 대한 적절한 대상 TFTP 디렉터리(TFTP 디렉터리는 이미지 사양을 기반으로 함)가 포함됩니다.

- 사용자가 업로드하는 이미지를 사용하거나 사용하지 않도록 하는 옵션을 사용하려면 특정 전화기 모델에 대한 사양에 따라 전체 크기 이미지와 썸네일 이미지를 모두 준비해야 합니다.
- 이미지를 특정 전화기에 할당하려는 경우에는 전체 크기 이미지만 필요합니다.

다음에 수행할 작업

전화기 사용자가 자신의 배경 이미지를 선택할 수 있게하려면 [List.xml 파일 편집, 658 페이지](#).

특정 배경 이미지를 할당하려는 경우에는 List.xml 파일을 업데이트할 필요가 없습니다. 다음 페이지의 절차를 수행합니다. [TFTP 서버에 배경 업로드, 659 페이지](#)

List.xml 파일 편집

전화기 사용자가 자신의 배경 이미지를 선택할 수 있게 하려면 이 절차를 사용하여 기존 List.xml 파일에 업로드하는 새 배경 이미지를 추가합니다. 각 TFTP 이미지 디렉터리에는 해당 TFTP 디렉터리를 사용하는 전화기에서 사용되는 List.xml 파일이 포함되어 있습니다. 이 파일은 각 배경 옵션에 대한 특정 배경 및 축소판 이미지를 가리키며, 50개의 배경 이미지를 포함할 수 있습니다. 이미지는 전화기에 표시되는 순서대로 나열됩니다. 각 이미지에 대해 이 파일에는 다음 두 속성이 포함된 <ImageItem> 요소가 포함되어 있습니다.

- 이미지: 전화기의 배경 이미지 메뉴에 나타날 썸네일 이미지를 포함하는 전화기의 위치를 지정하는 URI(Uniform Resource Identifier).
- URL: 전화기가 전체 크기 이미지를 가져올 위치를 지정하는 URI.

예:

다음 예(Cisco Unified IP Phone 7971G-GE 및 7970G)는 두 개의 이미지를 정의하는 List.xml 파일을 보여줍니다. 각 이미지에 대해 필수 이미지와 URL 특성을 포함해야 합니다. HTTP URL 지원이 제공되지 않으므로 예에 나타난 TFTP URI는 전체 크기 및 썸네일 이미지에 연결하는 데 지원되는 유일한 방법입니다.

```
<CiscoIPPhoneImageList>
  <ImageItem Image="TFTP:Desktops/320x212x12/TN-Fountain.png"
    URL="TFTP:Desktops/320x212x12/Fountain.png"/>
  <ImageItem Image="TFTP:Desktops/320x212x12/TN-FullMoon.png"
    URL="TFTP:Desktops/320x212x12/FullMoon.png"/>
</CiscoIPPhoneImageList>
```

프로시저

단계 1 CLI(Command Line Interface)에 로그인합니다.

단계 2 `file get tftp <filename>` CLI 명령을 실행합니다. 여기서 <filename>은 적절한 TFTP 디렉토리에 대한 List.xml 파일의 파일 및 파일 경로를 나타냅니다.

참고 각 이미지 디렉토리에 고유한 파일이 있는 경우 해당 TFTP 디렉토리에서 List.xml 파일을 다운로드해야 합니다. 디렉터리가 이미지 사양에 기반을 둔 것이므로 해당 전화기 모델의 해당 TFTP 디렉토리에 대한 자세한 내용은 전화기 설명서를 참조하십시오.

단계 3 추가하려는 각 새 배경 옵션에 대해 새 <ImageItem> 요소로 xml 파일을 편집합니다.

TFTP 서버에 배경 업로드

이 절차를 사용하여 새 전화기 백그라운드 파일을 TFTP 서버에 업로드합니다.

- 전화기 사용자가 자신의 배경 이미지를 선택할 수 있게하려면 전체 크기의 배경 이미지, 썸네일 이미지 및 업데이트된 List.xml 파일을 업로드해야 합니다.
- 특정 배경 이미지를 할당하는 경우에는 전체 크기 배경 이미지만 업로드해야 합니다.

프로시저

단계 1 Cisco Unified OS 관리에서 소프트웨어 업그레이드 > **TFTP** 파일 관리를 선택합니다.

단계 2 파일 업로드를 클릭하고 다음을 수행합니다.

- a) 파일 선택을 클릭하여 업로드할 이미지로 이동한 다음 해당 이미지를 선택합니다.
- b) 디렉터리 필드에 해당 전화기 모델에 해당하는 TFTP 디렉토리를 입력합니다. TFTP 디렉토리는 이미지 크기 및 색상 유형에 해당합니다. 이미지 사양에 대한 자세한 내용은 전화기 설명서를 참조하십시오.

- c) **Upload File**(파일 업로드)을 클릭합니다.
- d) 이 단계를 반복하여 썸네일 이미지와 `list.xml` 파일을 모두 업로드합니다. 이러한 파일은 기본 배경 이미지와 동일한 TFTP 디렉터리에 로드되어야 합니다.

단계 3 단계를 클릭합니다.

TFTP 서버 다시 시작

TFTP 디렉터리에 사용자 정의 파일을 업로드한 후 Cisco TFTP 서버를 다시 시작하여 파일을 전화기로 푸시합니다.

프로시저

단계 1 Cisco Unified Serviceability에 로그인하고 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 2 서버 드롭다운 목록에서 Cisco TFTP 서비스가 실행 중인 서버를 선택합니다.

단계 3 **Cisco TFTP** 서비스에 해당하는 무선 단추를 클릭합니다.

단계 4 재시작을 클릭합니다.

전화기 사용자에게 전화기 배경 할당

기본적으로 Cisco Unified Communications Manager에서는 전화기 사용자가 자신의 전화 배경 이미지를 사용자 정의할 수 있습니다. 그러나 일반 전화 프로파일 설정을 사용하여 이 일반 전화 프로파일을 사용하는 모든 전화기의 특정 배경 이미지를 할당할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 일반 전화 프로파일을 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 전화기에서 사용하는 일반 전화 프로파일을 선택합니다.
- 새로 추가를 클릭하여 새 일반 전화 프로파일을 생성합니다.

단계 3 사용자가 배경 이미지를 선택할 수 있도록 하려면 전화기 배경 이미지 설정에 최종 사용자 액세스 활성화 확인란이 선택되어 있는지 확인합니다(기본 설정임).

단계 4 이 프로파일을 사용하는 전화기의 특정 배경 이미지를 할당하려면 다음을 수행합니다.

- 전화 배경 이미지 설정에 최종 사용자 액세스 활성화 확인란을 선택 취소합니다.
- [배경 이미지 텍스트 상자에서 할당할 이미지 파일의 파일 이름을 입력합니다. 이 텍스트 상자에 해당하는 엔터프라이즈 설정 무시 확인란을 선택합니다.

- 단계 5 일반 전화 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.
- 단계 6 저장을 클릭합니다.
특정 배경 이미지를 할당한 경우 이 일반 전화 프로파일을 사용하는 모든 전화기가 지정하는 이미지를 사용합니다.

다음에 수행할 작업

새 일반 전화 프로파일을 만든 경우 이 프로파일을 사용하도록 전화기를 다시 구성합니다. Cisco Unified Communications Manager에서 전화기를 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "엔드포인트 디바이스 구성" 섹션을 참조하십시오.



팁 할당할 전화기 수가 많은 경우 벌크 관리 도구를 사용하여 단일 작업에서 많은 수의 전화기에 일반 전화 프로파일을 할당합니다. 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.



참고 구성을 완료한 후 전화기를 재설정합니다.



50 장

대기 중 음악

- 대기 중 음악 개요, 663 페이지
- 외부 멀티캐스트 MOH와 유니캐스트 MOH의 상호 연동, 667 페이지
- 대기 중 음악 사전 요건, 669 페이지
- 대기 중 음악 구성 작업 흐름, 669 페이지
- 유니캐스트 및 멀티캐스트 오디오 소스, 676 페이지
- 대기 중 음악 상호 작용, 678 페이지
- 대기 중 음악 제한 사항, 680 페이지
- 대기 중 음악 문제 해결, 682 페이지

대기 중 음악 개요

통합 MOH(대기 중 음악) 기능을 통해 사용자는 스트리밍 소스에서 음악과 함께 온넷 및 오프넷 사용자를 대기 상태로 전환할 수 있습니다. 사용자가 보류시킨 온넷 또는 오프넷 디바이스는 이 소스를 통해 음악을 사용할 수 있습니다. 온넷 디바이스에는 IVR(대화형 음성 응답) 또는 통화 분배자가 보류, 상담 보류, 지정 보류한 스테이션 디바이스와 애플리케이션이 있습니다. 오프넷 사용자는 MGCP(Media Gateway Control Protocol)/SCCP(Skinny Call Control Protocol) 게이트웨이, Cisco IOS H.323 게이트웨이, Cisco IOS Media Gateway Control Protocol 게이트웨이를 통해 연결된 사용자입니다. 또한 이 시스템은 Cisco IOS H.323 또는 MGCP의 FXS(Foreign Exchange Station) 포트를 통해 Cisco IP 네트워크에 연결하는 Cisco IP POTS 전화기와 Cisco MGCP 또는 SCCP 게이트웨이를 위한 대기 중 음악 기능을 제공합니다.

Cisco Unified Communications Manager를 시작하여 미디어 리소스 관리자를 만듭니다. MoH 서버는 MoH 리소스로 미디어 리소스 관리자에 등록됩니다. MOH 서버는 대기 중 음악 오디오 소스를 제공하고 대기 중 음악 오디오 소스를 여러 스트림에 연결하는 소프트웨어 애플리케이션입니다.

엔드 디바이스 또는 기능이 통화를 보류시키면 Cisco Unified Communications Manager가 보류된 디바이스를 음악 리소스에 연결합니다. 보류된 디바이스가 검색되면 MoH 리소스에서 연결을 해제하고 정상 작업을 재개합니다.

발신자별 대기 중 음악

SIP 트렁크를 통해 전화기가 수신하는 SIP 통화에 대해 Cisco Unified Communications Manager에서는 다양한 MOH 오디오 소스를 사용할 수 있습니다.

Cisco Unified Customer Voice Portal(CVP) 고객지원 센터 솔루션과 같은 외부 애플리케이션은 공중 전화 교환망(PSTN)에서 걸려오는 전화를 받을 때 발신자 ID, 전화 건 번호 또는 IVR 상호 작용에 따라 가장 적절한 MOH 오디오 소스를 결정합니다.

자세한 내용은 Cisco Unified Customer Voice Portal 설명서(<http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html>)를 참조하십시오.

IP 음성 미디어 스트리밍 애플리케이션 및 확장된 MOH 오디오 소스의 용량 증가

Cisco IP Voice Media Streaming 애플리케이션은 Cisco Unified Communications Manager 설치 시 자동으로 설치됩니다. MOH(대기 중 음악) 기능을 활성화하려면 이 애플리케이션을 활성화합니다.

이 릴리스부터는 고유 및 동시 MOH 오디오 소스를 지원하는 Cisco Unified Communications Manager의 용량이며 MOH 서버에서 대기 중 음악 서비스를 실행 하는 동안에는 51에서 501로 증가합니다. MOH 오디오 소스는 숫자 51에 남아 있는 고정 MOH 오디오 소스를 사용하여 1 ~ 501로 번호가 지정됩니다.

고정 MOH 디바이스는 USB MOH 디바이스를 통해 연결되는 오디오 소스를 사용할 수 없습니다. Cisco Unified Communications Manager가 VMware에서 실행 중인 경우 USB를 지원하지 않기 때문입니다. VMware에서는 고정 MOH USB 디바이스 사용이 지원되지 않습니다. 그러나 Cisco SRST(Survivable remote site Remote Site Telephony) 멀티캐스트 MOH를 활용하는 구축에서 사용할 외부 사운드 디바이스를 프로비저닝합니다.

각 MOH 오디오 소스를 초기 인사말 및/또는 해당 음악을 듣는 발신자에게 주기적으로 재생되는 사용자 정의 알림을 사용하도록 구성할 수 있습니다. Cisco Unified Communications Manager는 하나 또는 여러 MOH 오디오 소스에서 사용할 수 있는 500개의 사용자 지정 알림을 제공합니다. 이러한 알림은 클러스터 내의 Cisco Unified Communications Manager 서버 간에는 배포되지 않습니다. 이러한 사용자 정의 알림 파일은 MOH 및 알림 서비스를 제공하는 각 서버에 업로드해야 합니다. 각 서버에 MOH 오디오 소스에 대한 각 사용자 정의 음악 파일을 업로드해야 합니다.

미디어 디바이스와 서비스의 성능 영향

Cisco IP Voice Media Streaming 애플리케이션은 알림 디바이스-음성 송출기(ANN), 소프트웨어 컨퍼런스 브리지, MOH(대기 중 음악 제공 서비스) 및 소프트웨어 미디어 종료 지점과 같은 4개의 미디어 디바이스에 대한 서비스로 실행됩니다. 통화 처리를 사용하여 Cisco Unified Communications Manager 서버에서 이 서비스를 활성화합니다. 이 서비스를 활성화할 때 통화 처리에 미치는 영향을 피하기 위해 이러한 미디어 디바이스를 제한된 용량에 맞게 구성해야 합니다. 미디어 디바이스에 대한 기본 설정은 이 공동 상주 작업을 기반으로 정의됩니다. 다른 설정을 늘리기 위해 하나 이상의 미디어 디바이스 사용을 줄여 이러한 설정을 조정할 수 있습니다.

예를 들어 소프트웨어 미디어 종료 지점 디바이스를 사용하지 않는 경우 SW MTP에 대한 실행 플래그 설정을 **False**로 선택하고 시스템 > 서비스 매개 변수 > **Cisco IP Voice media Streaming** 앱 서비스 > **MTP** 매개 변수를 선택하고 **MTP** 통화 수 설정을 미디어 리소스 > **MOH** 서버 > 최대 반이중 스트림 구성에 추가할 수 있습니다. 통화 트래픽에 따라 기본 설정을 수정할 수 있습니다. 그러나 CPU, 메모리 및 IO 대기에 대한 서버 성능 활동을 모니터링합니다. 7500 사용자 OVA 구성을 사용하는 것과 같은 용량이 더 큰 클러스터의 경우 통화 수에 대한 기본 미디어 디바이스 설정을 25%까지 늘릴 수 있습니다.

미디어 디바이스(예: 대기 중 음악)를 많이 사용해야 하는 설치의 경우 또는 높은 통화 볼륨이 더 많은 수의 미디어 연결을 필요로 하는 경우 통화 처리가 활성화되지 않은 하나 이상의 Cisco Unified Communications Manager 서버에서 Cisco IP Voice media Streaming 애플리케이션 서비스를 활성화합니다. 이 서비스를 활성화하면 미디어 디바이스 사용이 통화 처리와 같은 다른 서비스에 미치는 영향을 제한합니다. 그런 다음 미디어 디바이스에 대한 최대 통화 수에 대한 구성 설정을 증가시킬 수 있습니다.

Cisco Unified Communications Manager 서비스를 사용하여 Cisco IP Voice Media Streaming 애플리케이션을 공존으로 활성화하면 통화 처리 성능에 영향을 줄 수 있습니다. 기본 설정에서 대기 중 음악 또는 음성 송출기에 대한 용량 설정을 늘리려면 Cisco Unified Communications Manager를 활성화하지 않고 서버에서 Cisco IP Voice Media Streaming 애플리케이션을 활성화하는 것이 좋습니다.

활성 발신자가 보류 중이거나 멀티캐스트 MOH 오디오 스트림이 구성된 경우에는 CPU 성능이 MOH의 영향을 받습니다.

표 57: 일반 성능 결과

구성 참고 사항	CPU 성능
전용 MOH 서버, 1000 보류된 통화, 인사말 및 정기 알림을 사용하는 500 MOH 소스	25-45%(7500 사용자 OVA 구성)
전용 MOH 서버 및 음성 송출기 서버가 포함된 기본 통화 대기, 1000 대기 통화, 인사말 및 정기 알림을 사용하는 500 MOH 소스 음성 송출기는 동시에 인사말 알림을 300까지 재생할 수 있습니다.	25-45%(7500 사용자 OVA 구성)
전용 MOH 서버, 500 보류된 통화, 인사말 및 정기 알림을 사용하는 500 MOH 소스	15-35%(7500 사용자 OVA 구성)

표 58: 추론 권장 사항

구성	권장 한도
Cisco IP Voice Media Streaming 애플리케이션을 Cisco Unified Communications Manager와 함께 사용할 때 2500 OVA(중간 통화 처리).	MOH: 500 보류된 발신자, 100 MOH 소스 및 48~64 음성 송출기 발신자.
Cisco IP Voice Media Streaming 애플리케이션이 전용 서버일 때 2500 OVA.	MOH: 750 보류된 발신자, 250 MOH 소스 및 250 음성 송출기 발신자.

구성	권장 한도
Cisco IP Voice Media Streaming 애플리케이션을 Cisco Unified Communications Manager와 함께 사용할 때 7500/10K OVA(중간 통화 처리).	MOH: 500 보류된 발신자, 250 MOH 소스 및 128 음성 송출기 발신자.
Cisco IP Voice Media Streaming 애플리케이션이 전용 서버일 때 7500/10K OVA.	MOH: 1000 보류된 발신자, 500 MOH 소스 및 300-700 음성 송출기 발신자(1 MOH 코덱 사용). 참고 2개의 MOH 코덱에 대한 음성 송출기를 300으로 줄입니다.



참고 이러한 권장 사항은 MOH/ANN 디바이스에만 해당됩니다. 이러한 디바이스를 MTP(소프트웨어 미디어 종료 지점) 및 CFB(통화 시 착신 전환) 디바이스와 결합하는 경우 스트림을 제공하기 위한 제한을 줄이십시오.

용량 수립 계획에 대한 구성 제한

Cisco IP 음성 스트리밍 애플리케이션 및 셀프 프로비저닝 IVR 서비스는 미디어 커널 드라이버를 사용하여 RTP(실시간 전송 프로토콜) 스트림을 만들고 제어합니다. 이 미디어 커널 드라이버에는 6000 스트림 용량이 있습니다. 이러한 스트림을 사용하여 미디어 디바이스와 IVR에서 리소스 예약을 수행할 수 있습니다.

이러한 예약은 다음 용량 계산을 기반으로 합니다.

미디어 디바이스	용량
알림 디바이스	(통화 수 서비스 매개 변수) * 3 여기서 3은 엔드포인트에 대한 총 수신(RX) 및 전송(TX) 통화를 나타내고 .wav 파일에 대해 1을 나타냅니다.
소프트웨어 컨퍼런스 브리지	(통화 수 서비스 매개 변수) * 2 여기서 2는 RX 및 TX 엔드포인트의 총 스트림을 나타냅니다.
소프트웨어 미디어 터미네이션 포인트	(통화 수 서비스 매개 변수) * 2 여기서 2는 RX 및 TX 엔드포인트의 총 스트림을 나타냅니다.

미디어 디바이스	용량
대기 중 음악	$((\text{최대 반이중 스트림 수}) * 3) + (501 * 2 * [\text{활성화된 MOH 코덱 수}])$ 여기서: <ul style="list-style-type: none"> • (최대 반이중 스트림 수)는 MOH 디바이스 구성 관리 웹 페이지의 구성 설정입니다. • 3은 RX, TX 및 인사말 알림 .wav 파일의 총 스트림 수를 나타냅니다. • 501은 최대 MOH(대기 중 음악) 소스 수를 나타냅니다. • 2는 음악 .wav 스트림과 가능한 멀티캐스트 TX 스트림을 나타냅니다. • [활성화된 MOH 코덱 수]는 Cisco IP 음성 스트리밍 애플리케이션 서비스 매개 변수에서 활성화된 MOH 코덱 수를 기반으로 합니다.
셀프 프로비저닝 IVR 서비스	$(500 * 2)$ 여기서 500은 발신자를 나타내고, 2는 RX 및 TX 스트림에서 총 스트림 수를 나타냅니다.

따라서 MOH가 최대 1000건의 발신자를 지원하도록 하려면 다음 방정식을 사용합니다. 활성화된 코덱 1개가 있는 드라이버 스트림의 경우 $1000 * 3 + 501 * 2 * 1 = 4002$ 및 활성화된 코덱이 2개인 경우 $1000 * 3 + 501 * 2 * 2 = 5004$. 나머지 디바이스를 줄이고, 전체 예약을 6000으로 제한하도록 셀프 프로비저닝 IVR 서비스를 비활성화합니다. 이를 통해 MOH 디바이스에서 이렇게 예약할 수 있습니다. 또한 Cisco IP 음성 스트리밍 애플리케이션을 사용하는 동일한 서버에서 셀프 프로비저닝 IVR 서비스를 활성화하지 않아도 됩니다.

미디어 디바이스의 구성 설정이 미디어 디바이스 드라이버의 용량을 초과하는 경우 디바이스 드라이버에 등록하는 미디어 디바이스에서 필수 스트림 리소스를 예약할 수 있습니다. 나중에 등록하는 미디어 디바이스는 요청된 스트림 리소스보다 적은 수로 제한됩니다. 나중에 등록된 미디어 디바이스는 일부 알람 메시지를 기록하고 제한된 미디어 디바이스의 통화 수를 자동으로 축소합니다.



참고 용량이 6000 스트림인 미디어 커널 드라이버는 여러 개의 동시 미디어 디바이스 연결을 지원하지 않을 수 있습니다.

외부 멀티캐스트 MOH와 유니캐스트 MOH의 상호 연동

이 릴리스부터는 Cisco SRST(Survivable Remote Site Telephony) 라우터를 오디오 소스로 구성할 수 있습니다. 이 라우터는 멀티캐스트 수신 가능 디바이스에 멀티캐스트 MOH 오디오를 제공합니다. 이 접근 방식에서 디바이스는 Cisco Unified Communications Manager 멀티캐스트 MOH 오디오를 전송하는 것처럼 작동합니다. 그러나 유니캐스트 수신만을 사용할 수 있는 디바이스는 외부 MOH 소스(예:

Cisco Unified SRST 라우터)가 전송하는 MOH 오디오를 들을 수 없습니다. 유니캐스트 수신기 가능한 디바이스의 예로는 PSTN(공중 전화 교환망) 전화기, SBC(세션 보더 컨트롤러) 및 SIP(세션 시작 프로토콜) 트렁크가 될 수 있습니다.

이 Cisco Unified Communications Manager 릴리스에서는 외부 오디오 소스에서 멀티캐스트 MOH 오디오를 수신하고 유니캐스트 MOH 오디오로 전송하도록 이 기능이 향상되었습니다. Cisco Unified Communications Manager는 이 기능을 사용하여 멀티캐스트 MOH 오디오를 유니캐스트 MOH 음성으로 재생할 수 있는 디바이스에 대한 유니캐스트 MOH로 재생합니다. 외부 MOH 오디오 소스의 예는 멀티캐스트 MOH 오디오를 전송할 수 있는 Cisco Unified SRST 라우터나 소프트웨어가 될 수 있습니다.

관리자가 대기 중 음악 오디오 소스 구성 창 Cisco Unified CM 관리에서 이 기능에 대한 필드를 구성합니다.



참고

- 이 기능은 멀티캐스트 수신 가능 디바이스에 대한 외부 오디오 소스를 사용하여 멀티캐스트 MOH 오디오를 재생하는 기존 기능에 영향을 미치지 않습니다.
- 유니캐스트 미디어 연결의 경우 외부 멀티캐스트 소스를 사용하여 MOH 오디오 소스를 구성해도 Cisco Unified Communications Manager MOH 서버는 초기 알림과 정기 알림을 재생합니다.

코덱 관련 인바운드 오디오 스트림에 대한 구성 팁

Cisco Unified SRST 라우터와 같은 외부 멀티캐스트 오디오 소스를 MOH 서버에 구성하여 필요한 오디오 피드를 스트리밍합니다.

Cisco Unified SRST 라우터와 같은 외부 멀티캐스트 오디오 소스를 구성하려면 **MOH** 오디오 소스 구성 창에서 소스 **IPv4** 멀티캐스트 주소 및 소스 포트 번호 필드를 구성합니다.

- Cisco Unified Communications Manager는 **MOH** 오디오 소스 구성 창에서 구성한 외부 멀티캐스트 IP 주소 및 포트의 멀티캐스트 G.711 mu-law 스트림을 수신 대기합니다. MOH 서버는 G.711 mu-law 또는 a-law 또는 L16 256K 광대역 MOH 코덱 사이에서 트랜스코딩이 가능합니다. 외부 멀티캐스트 RTP 스트림은 G.711 mu-law 또는 a-law 또는 L16 256K 광대역 MOH 코덱의 소스로 MOH를 위한 G.711 mu-law 코덱을 사용합니다. G.711 a-law 및 광대역 통화의 경우, Cisco Unified Communications Manager MOH 서버는 인바운드 G.711 mu-law 스트림을 디바이스에 전송하기 전에 아웃바운드 G.711 a-law 또는 광대역 스트림으로 트랜스코딩합니다.
- Cisco Unified Communications Manager는 **MOH** 오디오 소스 구성 창에 구성된 4개의 포트 값으로 추가된 외부 멀티캐스트 IP 및 포트에서 멀티캐스트 G.729 스트림을 수신 대기합니다. 예를 들어 239.1.1.1:16384로 MOH 오디오 소스를 구성하는 경우 Cisco Unified Communications Manager는 239.1.1.1:16384의 G.711 mu-law 스트림과 239.1.1.1:16388의 G.729 스트림(4로 추가된 포트 값)을 수신 대기합니다. MOH 서버는 729 코덱에 대해 트랜스코딩할 수 없습니다. MOH G.729 코덱을 사용하는 발신자는 G.729 또는 G.729a 코덱을 사용하는 외부 멀티캐스트 RTP 스트림이 필요합니다.

대기 중 음악 사전 요건

- 멀티캐스트를 구성하기 전에 MOH 서버 및 오디오 소스를 구성해야 합니다. 고정 오디오 소스를 사용하려면 멀티캐스트를 구성하기 전에 이를 구성합니다.
- 유니캐스트 또는 멀티캐스트 대기 중 음악을 사용할지 여부를 결정해야 합니다.
- 구축되고 구성된 하드웨어의 용량을 계획하고 네트워크의 예상 통화량을 지원할 수 있는지 확인하는 것이 중요합니다. MOH 리소스의 하드웨어 용량을 파악하고 이 용량과 관련된 멀티캐스트 및 유니캐스트 MOH의 의미를 고려해야 합니다. 네트워크 통화량이 이러한 제한을 초과하지 않도록 하십시오. MOH 세션이 이러한 제한에 도달하면 추가 로드로 인해 MOH 품질이 저하되거나 MOH 작동이 끊기거나 MOH 기능이 손실될 수 있습니다.
- 멀티캐스트 MOH를 사용하는 경우와 멀티캐스트 MOH 스트림을 수신하는 디바이스가 동일한 IP 네트워크에 없는 경우 IP 네트워크에서 멀티캐스트 라우팅을 사용하도록 설정해야 합니다. 잘못 전송된 멀티캐스트 패킷으로 인한 네트워크 포트의 잠재적인 플러딩을 방지하려면(특히 WAN 링크에서) 멀티캐스트 라우팅을 사용하도록 설정할 때 주의하십시오. 멀티캐스트 MOH 패킷이 필요하지 않고 최대 홉 수 매개변수를 사용하는 인터페이스에서는 멀티캐스트를 사용하지 않도록 설정합니다.
- 서버 용량을 포함하여 대기 중 음악 구축 계획에 대한 자세한 내용은 *Cisco Collaboration System* 솔루션 참조 네트워크 설계의 대기 중 음악 용량 항목을 참조하십시오.

대기 중 음악 구성 작업 흐름

이 작업을 완료하여 시스템에 MOH(대기 중 음악)를 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	Cisco IP Voice Media Streaming 활성화, 670 페이지	Cisco IP Voice Media Streaming Service Application 서비스를 활성화하여 대기 중 음악을 활성화합니다.
단계 2	대기 중 음악 서버 구성, 670 페이지	MOH 서버에 대한 기본 서버 설정을 구성합니다.
단계 3	대기 중 음악용 오디오 파일 업로드, 671 페이지	(선택 사항) 자신의 오디오 파일을 업로드하여 MOH 오디오 스트림으로 사용할 수 있게 합니다.
단계 4	대기 중 음악 오디오 소스 구성, 672 페이지	대기 중 음악 오디오 스트림을 구성합니다. 업로드한 오디오 파일을 MOH 오디오 스트림에 연결할 수도 있습니다.

	명령 또는 동작	목적
단계 5	고정 대기 중 음악 오디오 소스 구성, 673 페이지	고정 대기 중 음악 오디오 소스를 구성합니다. 시스템은 단일 고정 MOH 오디오 소스(스트림 51)를 지원합니다.
단계 6	미디어 리소스 그룹에 MOH 추가, 673 페이지	대기 중 음악 서비스를 미디어 리소스 그룹에 할당합니다. 그룹은 통화 중 엔드포인트에서 사용할 수 있는 미디어 리소스를 컴파일합니다.
단계 7	미디어 리소스 그룹 목록 구성, 674 페이지	우선 순위가 지정된 미디어 리소스 그룹 목록에 미디어 리소스 그룹을 할당합니다.
단계 8	디바이스 풀에 미디어 리소스 추가, 674 페이지	디바이스 또는 디바이스풀에 미디어 리소스 그룹 목록을 할당하여 엔드포인트에서 음악을 대기 중으로 설정할 수 있습니다.
단계 9	MOH 서비스 매개 변수 구성, 675 페이지	(선택 사항) 기본 코덱 및 기본 오디오 스트림 등과 같이 보류 중인 통화에 대한 선택적 대기 중 음악 매개 변수를 구성합니다.

Cisco IP Voice Media Streaming 활성화

대기 중 음악을 사용하려면 **Cisco IP** 음성 스트리밍 애플리케이션 서비스를 활성화해야 합니다.



참고 설치 과정에서 Unified Communications Manager는 기본 대기 중 음악 오디오 소스를 설치하고 구성합니다. 대기 중 음악 기능은 기본 오디오 소스를 사용하여 진행할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 도구 > 서비스 활성화.

단계 2 서버 드롭다운 목록에서 서버를 선택합니다.

단계 3 CM 서비스에서 **Cisco IP** 음성 미디어 스트리밍 앱 서비스가 활성화인지 확인합니다. 서비스가 비활성화된 경우 서비스를 선택하고 저장을 클릭합니다.

대기 중 음악 서버 구성

시작하기 전에

MOH(대기 중 음악) 서버를 한 개 이상 사용할 수 있는지 확인합니다.



참고 Cisco Unified Communications Manager MOH 서버는 **Cisco IP Voice Media Streaming Application** 서비스가 활성화될 때 자동으로 추가됩니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.미디어 리소스 > 대기 중 음악 서버.

단계 2 찾기를 클릭하고 업데이트할 대기 중 음악 서버를 선택합니다.

단계 3 호스트 서버를 선택합니다.

단계 4 설명과 함께 대기 중 음악 서버 이름을 입력합니다.

단계 5 이 서버에 사용할 디바이스폴을 선택합니다.

단계 6 다음 필드를 구성하여 서버 용량을 구성합니다.

- 최대 하프 듀플렉스 스트림—해당 시점에 이 대기 중 음악 서버에서 스트림되는 유니캐스트 대기 중 음악에 있을 수 있는 최대 디바이스 수가 결정됩니다. 다음 수식을 사용하여 최대값을 계산할 수 있습니다.

참고 $(\text{서버 및 구축 용량}) - ([\text{멀티캐스트 MOH 소스 수}] * [\text{활성화된 MOH 코덱 수}])$

- 최대 멀티캐스트 연결—주어진 시간에 두 멀티캐스트 MOH에 배치할 수 있는 디바이스 수보다 크거나 같은 값으로 설정해야 합니다.

단계 7 (선택 사항) 멀티캐스팅을 활성화하려면 이 **MOH** 서버에서 멀티캐스트 오디오 소스 활성화 확인란을 선택하고 멀티캐스트 IP 주소 범위를 구성합니다.

단계 8 대기 중 음악 서버 구성 창에서 추가 필드를 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 9 저장을 클릭합니다.

대기 중 음악용 오디오 파일 업로드

대기 중 음악 오디오 스트림에서 사용할 수 있는 사용자 정의된 오디오 파일을 업로드하려는 경우 이 절차를 사용합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.미디어 리소스 > **MOH** 오디오 파일 관리.

단계 2 파일 업로드를 클릭합니다.

단계 3 파일 선택을 클릭하고 업로드할 파일을 탐색합니다. 파일을 선택한 후 열기를 클릭합니다.

단계 4 업로드를 클릭합니다.

업로드 결과 창에 업로드 결과가 표시됩니다. 업로드 절차는 파일을 업로드하고 오디오 변환을 수행하여 MOH를 위한 코덱별 오디오 파일을 생성합니다. 원본 파일의 크기에 따라 완료되는 데 몇 분이 소요될 수 있습니다.

단계 5 단기를 클릭하여 업로드 결과 창을 닫습니다.

단계 6 추가 오디오 파일을 업로드하려면 이 절차를 반복합니다.

참고 오디오 소스 파일을 가져오면 Unified Communications Manager가 파일을 처리하여 음악 대기 서버에서 사용할 수 있는 올바른 형식으로 변환합니다. 다음은 유효한 입력 오디오 소스 파일의 예입니다.

- 16비트 PCM .wav 파일
- 스테레오 또는 모노
- 샘플 레이트 48kHz, 44.1kHz, 32kHz, 16kHz, 8kHz

참고 MOH 오디오 소스 파일은 클러스터의 다른 MoH 서버로 자동으로 전파되지 않습니다. 오디오 소스 파일을 각 MOH 서버 또는 클러스터의 각 서버에 별도로 업로드해야 합니다.

대기 중 음악 오디오 소스 구성

이 절차를 사용하여 대기 중 음악 오디오 소스를 구성합니다. 오디오 스트림을 구성하고 업로드된 파일을 오디오 스트림에 연결할 수 있습니다. 오디오 스트림을 500개까지 구성할 수 있습니다.



참고 새 버전의 오디오 소스 파일을 사용할 수 있는 경우 업데이트 절차를 수행하여 새 버전을 사용하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 미디어 리소스 > 대기 중 음악 오디오 소스를 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 오디오 스트림을 선택합니다.
- 새로 추가를 클릭하여 새 스트림을 구성합니다.

단계 3 MOH 오디오 스트림 번호에서 오디오 스트림을 선택합니다.

단계 4 MOH 오디오 소스 이름 필드에 고유한 이름을 입력합니다.

단계 5 (선택 사항) 이 파일을 다중 캐스팅하도록 허용하려면 다중 캐스팅 허용 확인란을 선택합니다.

단계 6 오디오 소스를 구성합니다.

- **MOH WAV** 파일 소스 라디오 버튼을 선택하고 **MOH** 오디오 소스 파일에서 할당할 파일을 선택합니다.
- 외부 멀티캐스트 소스 재브로드캐스트 라디오 버튼을 선택하고 멀티캐스트 소스 IP 주소 세부 정보를 입력합니다.

단계 7 보류 및 힌트 파일럿 통화에 대한 알림 설정 섹션에서 이 오디오 소스에 사용할 알림을 할당합니다.

단계 8 대기 중 음악 오디오 소스 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 9 저장을 클릭합니다.

고정 대기 중 음악 오디오 소스 구성

클러스터당 하나의 고정 오디오 소스(소스 51)를 정의할 수 있습니다. 각 MOH 서버에 클러스터별로 구성되는 고정 오디오 소스를 설정해야 합니다. 고정 오디오 소스는 로컬 컴퓨터의 오디오 드라이버를 사용하는 고정 디바이스에서 공급됩니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.미디어 리소스 > 고정 **MOH** 오디오 소스.
- 단계 2 (선택 사항) 이 오디오 소스를 멀티캐스트하도록 허용하려면 멀티캐스트 허용 확인란을 선택합니다.
- 단계 3 고정 오디오 소스를 활성화하려면 활성화 확인란을 선택합니다. 이 확인란을 선택하면 이름이 필요합니다.
- 단계 4 보류 및 힌트 파일럿 통화에 대한 알림 설정 영역에서 이 오디오 소스에 대한 알림을 구성합니다.
- 단계 5 고정 **MOH** 오디오 소스 구성 창에서 필드를 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.
- 단계 6 저장을 클릭합니다.

미디어 리소스 그룹에 **MOH** 추가

미디어 리소스 그룹은 논리적으로 그룹화한 미디어 리소스입니다. 필요에 따라 미디어 리소스 그룹을 지리적 위치나 사이트와 연결할 수 있습니다. 또한 미디어 리소스 그룹을 형성하여 서버 사용이나 유니캐스트 또는 멀티캐스트 서비스 유형을 제어할 수도 있습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.미디어 리소스 > 미디어 리소스 그룹.
- 단계 2 다음 중 하나를 수행합니다.
- 찾기를 클릭하고 기존 그룹을 선택합니다.

- 새로 추가를 클릭하여 새 그룹을 만듭니다.

단계 3 이름과 설명을 입력합니다.

단계 4 사용 가능한 미디어 리소스 목록에서 대기 중 음악 리소스를 선택하고 아래쪽 화살표를 사용하여 선택한 미디어 리소스에 리소스를 추가합니다. 이 그룹에 할당할 다른 미디어 리소스에 대해 이 단계를 반복합니다.

단계 5 (선택 사항) 대기 중 음악 멀티캐스트를 허용하려면 **MOH** 오디오에 멀티캐스트 사용 확인란을 선택합니다.

단계 6 저장을 클릭합니다.

미디어 리소스 그룹 목록 구성

미디어 리소스 그룹 목록에는 우선 순위가 지정된 미디어 리소스 그룹이 나열됩니다. 애플리케이션은 미디어 리소스 그룹 목록에 정의된 우선 순위 순서에 따라 사용 가능한 그룹 중에서 필요한 미디어 리소스를 선택할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 미디어 리소스 > 미디어 리소스 그룹 목록.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 미디어 리소스 그룹 목록을 선택합니다.
- 새로 추가를 클릭하여 새 미디어 리소스 그룹 목록을 만듭니다.

단계 3 목록에 대한 이름을 입력합니다.

단계 4 사용 가능한 미디어 리소스 그룹 목록에서 이 목록에 추가할 그룹을 선택하고 아래쪽 화살표를 사용하여 선택한 미디어 리소스 그룹으로 이동합니다.

단계 5 선택한 미디어 리소스 그룹 목록에서 목록의 오른쪽에 있는 위쪽 및 아래쪽 화살표를 사용하여 우선 순위 그룹의 순서를 편집합니다.

단계 6 저장을 클릭합니다.

디바이스 풀에 미디어 리소스 추가

MOH 리소스를 포함하는 미디어 리소스 그룹 목록을 디바이스 또는 디바이스풀에 할당하여 디바이스에서 MOH를 사용하도록 할 수 있습니다.



참고 통화 중인 디바이스는 전화기 구성 창에서 디바이스에 할당된 미디어 리소스 그룹 목록을 사용합니다. 할당된 것이 없으면 통화에서 사용 되는 디바이스풀에 대한 미디어 리소스 그룹 목록이 사용됩니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 중 하나를 수행합니다.

- 시스템 > 디바이스폴을 선택합니다.
- 장치 > 전화기를 선택합니다.

단계 2 찾기를 클릭하고 기존 전화기 또는 기존 디바이스폴을 선택합니다.

단계 3 미디어 리소스 그룹 목록 드롭다운 목록에서 대기 중 음악 리소스를 포함하는 미디어 리소스 그룹 목록을 선택합니다.

단계 4 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

MOH 서비스 매개 변수 구성

MOH(대기 중 음악)에 대해 옵션 서비스 매개 변수를 구성 하려면 이 절차를 사용합니다. 대부분의 구축의 경우 기본 설정만으로도 충분합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개 변수를 선택합니다.

단계 2 서버 드롭다운 목록에서 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco IP** 음성 미디어 스트리밍을 선택합니다.

단계 4 클러스터 수준 매개 변수(모든 서버에 적용되는 매개 변수) 영역에서 옵션 MOH 서비스 매개 변수를 구성합니다.

단계 5 저장을 클릭합니다.

단계 6 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 7 선택적 MOH 매개 변수를 구성합니다. 예를 들어 클러스터 수준 매개 변수(서비스)에서 보류에 대한 기본 오디오 소스를 할당할 수 있습니다.

단계 8 저장을 클릭합니다.

참고 모든 매개 변수는 클러스터 전체 그룹에 있는 매개 변수를 제외한 현재 서버에만 적용됩니다.

대기 중 음악 오디오 파일 보기

시스템에 저장된 기존 대기 중 음악 오디오 파일을 봅니다.

프로시저

단계 1 Cisco Unified CM 관리에서 미디어 리소스 > **MOH** 오디오 파일 관리를 선택합니다.

대기 중 음악 오디오 파일 관리 창이 나타납니다.

단계 2 각 레코드에 대한 다음 정보를 봅니다.

- 확인란 - 오디오 파일을 삭제할 수 있는 경우 파일 이름 열 앞에 확인란이 표시됩니다.
 - 파일 이름 - 이 열에는 오디오 파일 이름이 표시됩니다.
 - 길이 - 이 열에는 오디오 파일 길이(분 및 초)가 표시됩니다.
 - 파일 상태 - 이 열에는 오디오 파일의 다음 상태 중 하나가 표시됩니다.
 - 변환 완료 - 이 상태는 파일이 성공적으로 업로드되었고 대기 중 음악 오디오 소스의 오디오 파일로 사용할 수 있으면 나타납니다.
 - 사용 중 - 이 상태는 이 오디오 파일을 MOH 오디오 소스 파일로 사용하는 대기 중 음악 오디오 소스를 추가하면 나타납니다.
- 참고 사용 중 상태의 파일은 삭제할 수 없습니다.

유니캐스트 및 멀티캐스트 오디오 소스

유니캐스트 대기 중 음악은 시스템 기본 옵션입니다. 그러나 필요한 경우 멀티캐스트를 구성해야 합니다. 멀티캐스트 및 유니캐스트 구성 모두 보류 상대방에 동일한 오디오 소스 동작을 제공합니다. 각 오디오 소스가 한 번 사용되며 스트림이 내부적으로 분할되어 보류 상대방에게 전송됩니다. 이 경우 멀티캐스트와 유니캐스트 간의 유일한 차이점은 데이터가 네트워크를 통해 전송되는 방법입니다.

표 59: 유니캐스트 및 멀티캐스트 오디오 소스 간의 차이점

유니캐스트 오디오 소스	멀티캐스트 오디오 소스
MOH 서버에서 MOH 오디오 스트림을 요청하는 엔드포인트로 직접 전송되는 스트림으로 구성됩니다.	MOH 서버에서 멀티캐스트 그룹 IP 주소로 전송되는 스트림으로 구성됩니다. MOH 오디오 스트림을 요청하는 엔드포인트는 필요에 따라 멀티캐스트 MOH에 참가할 수 있습니다.
멀티캐스트 MOH 스트림은 서버와 엔드포인트 디바이스 간의 포인트-투-포인트, 단방향 오디오 RTP 스트림입니다.	멀티캐스트 MOH 스트림은 MOH 서버와 멀티캐스트 그룹 IP 주소 간 일대다 지점 간 단방향 오디오 RTP 스트림입니다.

유니캐스트 오디오 소스	멀티캐스트 오디오 소스
유니캐스트 MOH는 각 사용자나 연결에 대해 별도의 소스 스트림을 사용합니다. 엔드포인트 디바이스가 사용자 또는 네트워크 이벤트를 통해 보류되면 MOH 스트림 수가 증가합니다.	여러 사용자가 동일한 오디오 소스 스트림을 사용하여 MOH를 제공할 수 있습니다.
유니캐스트 보류 상대방에게 재생될 초기(인사말) 알림을 사용하여 MOH 오디오 소스를 구성할 수도 있습니다. 유니캐스트 MOH 사용자에게는 이 알림이 처음부터 들리고,	멀티캐스트 사용자에게는 이 알림이 들리지 않습니다.
추가 MOH 스트림은 네트워크 처리량 및 대역폭에 부정적인 영향을 줄 수 있습니다.	멀티캐스트 MOH는 시스템 리소스 및 대역폭을 절약합니다.
멀티캐스트가 활성화되지 않았거나 디바이스에서 멀티캐스트가 불가능한 네트워크에서 매우 유용합니다.	네트워크가 멀티캐스트에 대해 활성화되지 않았거나 엔드포인트 디바이스가 멀티캐스트를 처리할 수 없는 상황에서 문제가 될 수 있습니다.
관리 디바이스만 포함됩니다.	디바이스, IP 주소 및 포트 관리를 포함합니다.
대기 중 음악 서버를 정의하는 것은 필요하지 않습니다.	관리자는 멀티캐스팅을 허용하도록 오디오 소스를 하나 이상 정의해야 합니다. 멀티캐스트용 대기 중 음악 서버를 정의하려면 먼저 멀티캐스팅을 허용하도록 서버를 정의해야 합니다.
MOH 오디오 소스, MOH 서버 또는 미디어 리소스 그룹 목록을 구성하지 않고 작동합니다.	미디어 리소스 그룹과 미디어 리소스 그룹 목록이 모두 멀티캐스트 대기 중 음악 서버를 포함하도록 정의된 경우에만 작동합니다. 미디어 리소스 그룹의 경우 멀티캐스트용으로 설정된 대기 중 음악 서버를 포함해야 합니다. 이러한 서버에는 (MOH) [멀티캐스트] 라는 레이블이 지정되어 있습니다. 또한 멀티캐스트의 미디어 리소스 그룹을 정의할 때 MOH 오디오에 멀티캐스트 사용 확인란을 선택합니다.



참고 SIP에 대한 멀티캐스트 MOH 방향 특성 서비스 매개 변수에서는 Cisco Unified Communications Manager가 멀티캐스트 MOH(대기 중 음악) INVITE 메시지에서 SDP(Session Description Protocol)의 방향 특성을 **sendOnly**로 설정하는지 **recvOnly**로 설정하는지를 지정합니다.

구축에서 Cisco Unified IP Phone 7940 및 7960에 대해 릴리스 8.4 이하를 사용하거나, SIP 전화기에서 릴리스 8.1(x) 이하를 Cisco Unified IP Phone 7906, 7911, 7941 및 7961 이전 버전을 사용하는 경우 이 매개 변수를 **sendOnly**로 설정합니다. 그 외의 경우에는 이 매개 변수를 기본값인 **recvOnly**로 둡니다.

대기 중 음악 상호 작용

기능	상호 작용
H.323 클러스터 간 트렁크를 통한 멀티캐스트 MoH(대기 중 음악)	<p>H.323 인터클러스터 트렁크를 통한 멀티캐스트 MOH 기능을 사용하면 멀티캐스트 MOH를 H.323 인터클러스터 트렁크(ICT)에서 작동할 수 있습니다. 통화가 클러스터 간 트렁크를 통해 연결되고 상대방의 한 명이 보류 키를 누르면 MoH가 클러스터 간 트렁크를 통해 스트리밍됩니다. 멀티캐스트 MOH가 켜지고 보류한 상대방과 트렁크가 멀티캐스트 MoH 서버를 사용하도록 구성되면 MOH가 멀티캐스트를 통해 스트리밍됩니다. 이 트렁크에서 보류되는 통화 수와 관계에서 트렁크를 통해 하나의 멀티캐스트 MoH 스트림만 트렁크를 통해 스트리밍됩니다.</p> <p>이 기능에 대한 추가 사항:</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager 간의 중간 상자가 TCS(터미널 기능 세트) 및 OLC 메시지로 새 필드를 전달하지 않으면 이 기능이 작동하지 않습니다. • 이 기능은 필드업 멀티캐스트 MOH에 대한 추가 구성이 필요하지 않으며, 단일 전송기 멀티캐스트를 지원하는 Cisco Unified Communications Manager 간에만 적용됩니다. • 이 기능은 기본적으로 켜져 있지만 H.245 OLC 메시지의 멀티캐스트 MOH 전송 서비스 매개 변수를 False로 설정하여 해제할 수 있습니다. 이 값을 설정하면 기능에서 발생할 수 있는 상호 운용성 문제를 해결할 수 있습니다.
MoH(대기 중 음악) 장애 조치 및 폴백	<p>MOH 서버는 소프트웨어 컨퍼런스 브리지 및 MTP(Media Termination Point)를 통해 구현된 Cisco Unified Communications Manager 목록 및 장애 조치를 지원합니다. 장애 조치 시 시스템에서는 백업 Cisco Unified Communications Manager에 대한 연결을 유지합니다(사용할 수 있는 경우).</p> <p>활성 대기 중 음악 세션 중에 대기 중 음악 서버에 장애가 발생하면 보류된 당사자는 이 지점의 음악을 듣습니다. 그러나 이 상황은 일반 통화 기능에는 영향을 미치지 않습니다.</p>

기능	상호 작용
통화 지정보류 및 통화 전환 보류	<p>대기 중 음악을 사용하여 사용자는 스트리밍 소스에서 제공하는 음악으로 통화를 보류할 수 있습니다. 대기 중 음악을 사용하면 다음 두 가지 유형의 보류가 가능합니다.</p> <ul style="list-style-type: none"> • 사용자 보류 - 사용자가 [보류] 버튼 또는 [보류] 소프트키를 누르면 시스템에서 이 보류 유형을 호출합니다. • 네트워크 보류 - 사용자가 호전환, 전화회의 또는 통화 지정보류 기능을 활성화하면 이 보류 유형이 발생하고 보류가 자동으로 호출됩니다. 이 보류 유형은 통화 전환 보류에 적용됩니다. 통화 전환 보류는 호전환 기능이기 때문입니다. 그러나 통화 전환 보류에서는 오디오 소스에 대해 Cisco Call Manager 서비스 매개 변수인 기본 네트워크 보류 MOH 오디오 소스를 사용합니다.
익스텐션 모빌리티 크로스 클러스터(EMCC)-객원 전화에 대한 미디어 리소스	<p>RSVP 에이전트, TRP, MOH(대기 중 음악), MTP, 트랜스코더 및 컨퍼런스 브리지 등의 예가 있습니다.</p> <p>미디어 리소스는 방문 전화기에 로컬입니다(RSVP 에이전트 아님).</p>
보류 복귀	Cisco Unified Communications Manager는 일반 보류 통화에 대해 MOH가 구성된 경우 되돌린 통화에서 MOH를 지원합니다.
미디어 리소스 선택	보류 상대방이 Cisco Unified Communications Manager에서 대기 중 음악 리소스를 할당하는 데 사용하는 미디어 리소스 그룹 목록을 결정합니다.
SRTP를 사용한 보안 대기 중 음악	<p>Cisco Unified Communications Manager는 SRTP(Secure Real Time Protocol)를 지원하기 위해 Cisco IP 음성 스트리밍 애플리케이션 서비스를 개선합니다. 따라서 보안을 위해 Cisco Unified Communications Manager 클러스터 또는 시스템을 활성화하면 MOH 서버가 Cisco Unified Communications Manager를 SRTP 가능 디바이스로 등록합니다. 수신 디바이스도 SRTP 가능한 경우 음악 미디어가 수신 디바이스에 스트리밍되기 전에 암호화됩니다.</p> <p>다음을 확인 하십시오.</p> <ul style="list-style-type: none"> • 클러스터 보안은 혼합 모드여야 함 - <code>utils ctl set-cluster mixed-mode</code> CLI 명령을 실행합니다. • 경로의 SIP 트렁크가 SRTP를 지원함 - 트렁크 구성 창에서 SRTP 허용 확인란을 선택해야 SRTP가 트렁크에서 작동할 수 있습니다. • 디바이스 지원 SRTP - 엔드포인트에서 사용하는 전화기 보안 프로파일에서 디바이스 보안 모드를 암호화해야 합니다.

대기 중 음악 제한 사항

제한 사항	설명
멀티캐스트 대기 중 음악 지원	컴퓨터 텔레포니 통합(CTI) 및 미디어 터미네이션 포인트(MTP) 디바이스는 멀티캐스트 대기 중 음악 기능을 지원하지 않습니다. CTI 디바이스의 미디어 리소스 그룹 목록에서 멀티캐스트 MoH 디바이스로 CTI 또는 MTP 디바이스를 구성하는 경우 통화 제어 문제가 발생할 수 있습니다. CTI 및 MTP 디바이스는 멀티캐스트 미디어 스트리밍을 지원하지 않습니다.
인터넷 프로토콜 (IP)	멀티캐스트 대기 중 음악은 IPv4만 지원합니다. MoH(대기 중 음악)의 구성 요소인 Cisco IP Voice Media Streaming Application은 유니캐스트 MoH에 IPv4 및 IPv6 오디오 미디어 연결을 모두 지원합니다. 멀티캐스트 MoH에서는 IPv4만 지원합니다. IP 주소 지정 모드가 IPv6 전용인 디바이스는 멀티캐스트를 지원할 수 없습니다.
고정 디바이스 오디오 소스 배포	Cisco Unified Communications Manager는 미디어 리소스 그룹에 포함된 전체 MoH 서버에서 고정 디바이스(하드웨어) 오디오 소스 분배를 지원하지 않습니다.
허용되지 않는 오디오 품질 (G-729a 코덱 포함)	G.729a 코덱은 음성용으로 설계되었으므로 대기 중 음악에서 음악에 사용하면 적절한 오디오 품질을 제공할 수 있습니다.
Cisco Unified Communications Manager 시스템 지원	Cisco Unified Communications Manager 클러스터 또는 시스템은 Cisco UCS(Unified Computing System) 서버 또는 다른 Cisco 승인 타사 서버 구성에서 가상화된 배포만 지원합니다. 외부 소스에서 MoH를 제공하는 노드의 경우 대기 중 음악 기능을 외부 소스(USB 오디오 동글)에서 사용할 수 없습니다.
멀티캐스트 지원	멀티캐스트를 지원하는 리소스가 존재하는 경우 관리자가 MoH 서버를 유니캐스트 또는 멀티캐스트로 지정할 수 있습니다.
발신자별 MOH 지원	QSIG 터널링 사용 SIP 트렁크를 통해 통화를 수신하거나 호전환하면 발신자별 MOH가 지원되지 않습니다.
MP3 형식 지원	대기 중 음악 기능은 MP3 형식을 지원하지 않습니다.
H.323과 SIP 프로토콜 간의 상호 운용성	멀티캐스트 MoH는 H.323 프로토콜과 SIP 프로토콜 간의 상호 운용성을 지원하지 않습니다.
SRTP 지원	멀티캐스트 대기 중 음악 오디오 스트림은 암호화되지 않으며, SRTP를 지원하지 않습니다.
멀티캐스트 스트림	MTP에서는 멀티캐스트 미디어 스트림을 지원하지 않습니다.

제한 사항	설명
멀티캐스트 대기 중 음악 RTP 스트림 암호화	Cisco Unified Communications Manager에서는 멀티캐스트 대기 중 음악 RTP 스트림의 암호화를 지원하지 않습니다. 보안 MoH 오디오가 필요한 경우 멀티캐스트 오디오 소스를 구성하지 않아야 합니다.
고정 대기 중 음악 디바이스	고정 대기 중 음악 디바이스는 USB를 통해 연결되는 오디오 소스를 지원할 수 없습니다. Cisco Unified Communications Manager가 VMware에서 실행 중인 경우 USB를 지원하지 않기 때문입니다. 그러나 VMware에서는 내부 대기 중 음악을 지원합니다.
MOH 서버 실패	Cisco Unified Communications Manager는 활성 대기 중 음악 세션 중에 MoH 서버가 실패할 때 동작을 수행하지 않습니다.
멀티캐스트 MOH	멀티캐스트 MOH를 사용하는 사이트의 통화 레그에서 MTP 리소스가 호출되면 Cisco Unified Communications Manager 멀티캐스트 MOH 대신 유니캐스트 MOH로 대체됩니다.
프로비저닝	사용자 및 네트워크 MOH 오디오 소스 ID를 프로비저닝하지 않거나 두 값 중 하나 또는 모두 잘못된 경우 SIP 헤더의 발신자별 MOH 정보가 무시됩니다. 통화에 대기음이 복귀되고 잘못된 MOH 오디오 소스 경고가 표시됩니다.
헤더 값	<ul style="list-style-type: none"> 헤더에 사용자와 네트워크 MOH 오디오 소스 ID가 모두 표시되면 잘못된 값이 기본값(0)으로 대체됩니다. 두 값이 모두 0이거나 유일한 값이 0인 경우 수신 INVITE의 헤더가 무시됩니다.
MOH 오디오 소스 식별자	<ul style="list-style-type: none"> SIP 헤더에 MOH 오디오 소스 ID가 하나만 제공하는 경우(MOH 오디오 소스 ID 값의 앞이나 뒤에 쉼표가 표시되는 경우 포함) 사용자 및 네트워크 MOH에 모두 동일한 MOH ID가 사용됩니다. SIP 트렁크에서 SIP 헤더의 사용자 및 네트워크 MOH 오디오 소스 ID를 둘 다 채우므로 통화 제어에서 항상 두 값을 모두 수신합니다. 쉼표로 구분된 MOH 오디오 소스 ID 값이 헤더에 세 개 이상 있는 경우에는 처음 두 값이 사용됩니다. 그 다음 값은 무시됩니다.
일관된 발신자별 MOH 구성을 위한 관리자	관리자는 Cisco Unified Communications Manager 클러스터가 여러 개 포함되는 경우 발신자별 MOH 구성을 일관적으로 유지 관리해야 합니다.
수신되는 원래 발신자	콜 센터로 수신되는 원래 발신자는 전체 통화 과정 동안 변경할 수 없습니다.
MOH 정보	대기 중 음악 정보는 SIP 트렁크 간에만 공유됩니다.

대기 중 음악 문제 해결

대기 중 음악이 전화기에서 재생되지 않음

전화기 사용자가 대기 중 음악을 들을 수 없습니다.

- G.729a 코덱은 음악의 경우 MOH와 함께 사용되며, 이는 적합한 오디오 품질을 제공하지 않을 수 있습니다.
- 멀티캐스트 MoH를 사용하는 사이트의 통화 레그에서 MTP 리소스가 호출됩니다.
- 멀티캐스트 MoH를 사용 중인 사이트의 통화 레그에서 MTP 리소스가 호출되는 경우 발신자는 대기 중 음악을 수신하지 않고 아무 소리도 수신하지 않습니다. 이 시나리오를 방지하려면 멀티캐스트 MoH 대신 유니캐스트 MoH나 대기 중 신호음을 구성합니다.



51 장

셀프 서비스 포털

- 셀프 서비스 포털 개요, 683 페이지
- 셀프 서비스 포털 작업 흐름, 684 페이지
- 셀프 서비스 포털 상호 작용 및 제한 사항, 685 페이지

셀프 서비스 포털 개요

Cisco 통합 커뮤니케이션 자가 관리 포털에서 사용자는 전화기 기능 및 설정을 사용자 정의할 수 있습니다. 관리자는 포털에 대한 액세스를 제어할 수 있습니다. 최종 사용자가 포털에 액세스하려면 먼저 사용자를 기본 표준 **CCM** 일반 사용자 액세스 컨트롤 그룹 또는 표준 **CCM** 일반 사용자 역할이 할당된 모든 액세스 컨트롤 그룹에 추가해야 합니다. 또한 사용자에게 포털에 액세스할 수 있는 사용자 ID, 암호 및 URL이 필요합니다. 사용자는 다음 URL을 통해 포털에 액세스할 수 있습니다.

http(s)://<server_name>:<port_number>/ucmuser/

여기서:

- **<server_name>**은 Unified Communications Manager IP 주소, 호스트 이름 또는 FQDN(Fully Qualified Domain Name)를 나타냅니다.
- **<port_number>**는 연결할 포트를 나타냅니다. 포트는 선택 사항이지만 방화벽 상황에 유용합니다.
- **ucmuser**는 셀프 케어를 가리키는 필수 하위 경로입니다.

선택적으로, Cisco Unified Communications Manager 내에서 엔터프라이즈 매개 변수를 구성하여 최종 사용자가 구성할 수 있는 전화 설정을 지정할 수도 있습니다. 예를 들어 착신 전환 표시 엔터프라이즈 매개 변수는 사용자가 포털을 통해 착신 전환을 구성할 수 있는지 여부를 결정합니다.

셀프 서비스 포털 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	셀프 서비스 포털에 사용자 액세스 권한 부여, 684 페이지	포털에 액세스하려면 최종 사용자가 표준 CCM 최종 사용자 액세스 컨트롤 그룹 또는 표준 CCM 최종 사용자 역할 할당이 있는 그룹에 할당되어야 합니다.
단계 2	셀프 서비스 포털 옵션 구성, 684 페이지	포털에 액세스하는 사용자가 사용할 수 있는 구성 옵션을 제어 하기 위해 엔터프라이즈 매개 변수를 구성합니다.

셀프 서비스 포털에 사용자 액세스 권한 부여

포털에 액세스하려면 최종 사용자가 표준 **CCM** 최종 사용자 액세스 컨트롤 그룹 또는 표준 **CCM** 최종 사용자 역할 할당이 있는 그룹에 할당되어야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 자체 관리 액세스를 제공할 사용자를 검색합니다.

단계 3 최종 사용자 섹션에서 사용자가 암호와 PIN을 구성했는지 확인합니다.

일반적으로 이러한 인증서는 새 사용자가 추가될 때 입력됩니다.

단계 4 권한 정보 섹션에서 액세스 컨트롤 그룹에 추가를 클릭합니다.

단계 5 찾기를 클릭하고 표준 **CCM** 최종 사용자 그룹 또는 표준 **CCM** 최종 사용자 역할을 포함하는 사용자 정의 그룹을 선택합니다.

참고 액세스 컨트롤 그룹 및 액세스 컨트롤 그룹에 대한 역할 할당을 편집하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 관리 지침서의 "사용자 액세스 관리" 장을 참조하십시오.

단계 6 저장을 선택합니다.

셀프 서비스 포털 옵션 구성

이 절차를 사용하여 포털에 액세스하는 사용자가 사용할 수 있는 구성 옵션을 제어하기 위해 셀프 서비스 포털 엔터프라이즈 매개 변수를 구성합니다.

시작하기 전에

[셀프 서비스 포털에 사용자 액세스 권한 부여, 684 페이지](#)

프로시저

단계 1 Cisco Unified Communications Manager 관리에서 시스템 > 엔터프라이즈 매개변수를 선택합니다.

단계 2 셀프 서비스 포털 매개 변수 아래의 드롭다운 목록에서 사용 가능한 서버 중 하나를 선택하여 셀프 서비스 포털 기본 서버를 설정합니다.

이 매개 변수는 내장된 셀프 케어 옵션 페이지를 표시하는 데 사용되는 Cisco Unified CM 서버 Jabber를 결정합니다. 없음을 선택하면 Jabber가 게시자에 대해 기본값으로 설정됩니다.

단계 3 나머지 셀프 서비스 포털 매개 변수를 구성하여 포털에 대한 기능을 활성화하거나 비활성화합니다. 필드에 대한 도움말은 엔터프라이즈 매개 변수 도움말을 참조하십시오.

단계 4 저장을 선택합니다.

셀프 서비스 포털 상호 작용 및 제한 사항

다음 표에서는 셀프 서비스 포털의 기능 상호 작용 및 제한 사항을 중점적으로 설명합니다.

기능	상호 작용 및 제한 사항
활성화 코드를 통해 디바이스 온보딩	<p>사용자가 셀프 서비스 포털을 통해 전화기를 활성화할 수 있으면 활성화할 준비가 된 전화기 표시 엔터프라이즈 매개 변수가 True(기본 설정)로 설정되어 있어야 합니다.</p> <p>이 기능을 통해 사용자는 셀프 서비스 포털에 로그인하여 활성화 코드를 얻을 수 있습니다. 전화기의 비디오 카메라를 사용하여 바코드를 스캔하거나 전화기에 수동으로 코드를 입력하여 전화기를 활성화하고 등록할 수 있습니다.</p> <p>활성화 코드에 대한 자세한 내용은 <i>Cisco Unified Communications Manager</i>에 대한 시스템 구성 설명서의 "활성화 코드를 통해 디바이스 온보딩" 장을 참조하십시오.</p>
인증된 사용자 https 요청	<p>인증된 사용자가 <code>https://{CUCM_address}/ucmuser/hostAlive/{host}</code>에 대한 요청을 하면 다음과 같은 상황이 발생합니다.</p> <ul style="list-style-type: none"> • <code>http: {host}/</code>를 얻는 데 성공하거나 요청에서 {host}를 ping할 수 있는 경우 Cisco Unified Communications Manager는 "true"라는 문자열을 반환합니다. • 요청이 실패하는 경우 Cisco Unified Communications Manager는 "false"라는 문자열을 반환합니다.

기능	상호 작용 및 제한 사항
Extension Mobility를 위한 최대 로그인	<p>최종 사용자가 셀프 서비스 포털 내에서 이 설정을 구성할 수 있으면 관리자가 연결된 Cisco Unified CM 관리의 사용자 프로파일에서 최종 사용자가 내선 이동을 최대 로그인 시간을 설정하도록 허용 옵션을 선택해야 합니다.</p> <p>사용자 프로파일 내에서 이 옵션을 선택하는 경우 프로파일을 사용하는 모든 사용자에게 대해 셀프 서비스 포털 설정이 Cisco Unified Communications Manager에서 클러스터 내 최대 로그인 시간과 클러스터 간 최대 로그인 시간 서비스 매개 변수에 대한 관리자 구성 값을 무시합니다.</p>



52 장

비상 통화 처리기

- 비상 통화 처리기 개요, 687 페이지
- 비상 통화 처리기 사전 요건, 688 페이지
- 비상 통화 처리기 작업 흐름, 688 페이지
- 상호 작용, 695 페이지
- 비상 통화 처리기 문제 해결, 697 페이지

비상 통화 처리기 개요

비상 통화 처리기는 현지 법령 및 규정을 따르면서 전화 통신 네트워크에서 비상 통화를 관리하는 데 도움이 됩니다.

비상 통화가 걸려오면 다음 요건이 충족되어야 합니다.

- 발신자 위치에 따라 비상 통화를 로컬 PSAP(Public-Safety Answering Point)로 라우팅해야 합니다.
- 발신자 위치 정보가 비상 오퍼레이터 터미널에 표시되어야 합니다. ALI(자동 위치 정보) 데이터베이스에서 위치 정보를 얻을 수 있습니다.

발신자 위치는 ELIN(Emergency Location Identification Number)에 따라 결정됩니다. ELIN은 비상 통화가 끊기거나 PSAP에서 발신자를 다시 연결해야 하는 경우 PSAP에서 전화를 걸어 비상 발신자를 다시 연결할 수 있는 DID(Direct Inward Dial) 번호입니다. 이 번호와 연결된 위치 정보에 따라 비상 통화가 PSAP로 라우팅됩니다.

사무실 시스템과 같은 다중 회선 전화기 시스템의 경우 ELIN 그룹에 전화기를 그룹화하여 ELIN을 두 개 이상의 전화기와 연결할 수 있습니다. 비상 통화 처리기의 ELIN 그룹은 위치를 식별합니다. 이 ELIN 그룹의 ELIN을 ALI 데이터베이스에 있는 위치로 매핑해야 합니다.

각 위치에서 동시 비상 통화를 지원하는 데 필요한 만큼의 ELIN을 생성해야 합니다. 예를 들어 다섯 통 동시 통화를 지원하려면 ELIN 그룹에 ELIN이 다섯 개 있어야 합니다.



참고 비상 통화 처리기는 클러스터당 최대 100개의 ELIN을 지원합니다.

ELIN이 동일한 위치에서의 다음 긴급 통화에서 사용될 때까지 기존 발신자의 ELIN 매핑이 활성화되었는지 확인합니다. ELIN 매핑이 사용되지 않는 경우 DN이 최대 3시간만 활성화됩니다.

다음과 같은 전화기 유형에서 ELIN 그룹을 사용할 수 있습니다.

- SIP 및 SCCP IP 전화기
- CTI 포트
- MGCP 및 SCCP 아날로그 전화기
- H.323 전화기

비상 통화 처리기 사전 요건

예

네트워크에 비상 통화 처리기를 구축하기 전에 ALI 제출 프로세스를 테스트하는 것이 좋습니다. 서비스 공급업체의 도움을 받아 PSAP가 ALI 데이터를 사용하여 네트워크로 콜백하는 것을 테스트해 볼 수 있습니다.

로컬 PSAP에서 ELIN 번호를 예약합니다. 법령 및 규정이 서로 다른 위치와 회사마다 다를 수 있으므로, 이 기능을 구축하기 전에 보안 및 법률 요구 사항을 조사하십시오.

비상 통화 처리기 작업 흐름

시작하기 전에

- [비상 통화 처리기 사전 요건, 688 페이지](#) 검토

프로시저

	명령 또는 동작	목적
단계 1	비상 통화 처리기 사용, 689 페이지	Cisco Unified Communications Manager에서 비상 통화 처리기 기능을 활성화합니다. 비상 통화 처리기는 필수 비상 통화 기능을 제공하며 정적 구성으로 전화기 위치가 할당된 제한된 수의 위치를 지원합니다. 다수의 특정 위치 또는 동적 위치 할당 등과 같은 고급 비상 통화

	명령 또는 동작	목적
		기능이 필요한 경우에는 Cisco Emergency Responder 사용을 고려해 보십시오.
단계 2	비상 위치 그룹 구성, 690 페이지	특정 사이트나 위치에 비상 위치(ELIN) 그룹을 구성합니다.
단계 3	비상 위치 그룹에 디바이스폴 추가, 691 페이지	비상 위치(ELIN) 그룹을 사용하도록 디바이스폴을 구성합니다.
단계 4	(선택 사항) 비상 위치 그룹에 디바이스 추가, 691 페이지	<p>특정 비상 위치(ELIN) 그룹을 사용하도록 특정 디바이스폴을 구성합니다. 이 디바이스에 연결되는 디바이스폴 ELIN 그룹을 사용하려는 경우에는 이 섹션을 무시할 수 있습니다.</p> <p>참고 디바이스 수준에서 설정한 구성은 디바이스폴 수준에서 설정한 모든 구성을 덮어씁니다.</p>
단계 5	경로 패턴 및 변환 패턴 활성화, 692 페이지	<p>경로 패턴 또는 변환 패턴에 비상 위치(ELIN) 서비스를 활성화합니다.</p> <p>주의 비상 호출 처리기에서 설정된 ELIN을 변환할 수 있으므로 게이트웨이 또는 트렁크에서는 발신자 변환 마스크가 설정되지 않습니다.</p> <p>참고 경로 패턴 또는 변환 패턴 둘 중 하나를 반드시 활성화해야 하지만 둘 다 활성화할 수는 없습니다.</p>
단계 6	<p>(선택사항) 다음 절차에 따라 ELIN 그룹 정보 및 전화기에서 벌크 관리 작업을 수행합니다.</p> <ul style="list-style-type: none"> • 비상 위치(ELIN) 그룹 정보 가져오기, 693 페이지 • 비상 위치(ELIN) 그룹 정보 내보내기, 694 페이지 • 새 비상 위치(ELIN) 그룹으로 전화기 업데이트, 694 페이지 	이 섹션에서는 ELIN 그룹 정보를 업데이트하고 새 ELIN 그룹에 전화기를 추가할 수 있는 벌크 관리 작업에 대한 정보를 제공합니다. 벌크 관리에 대한 내용은 <i>Cisco Unified Communications Manager</i> 벌크 관리 지침서, 릴리스 11.0(1)을 참조하십시오.

비상 통화 처리기 사용

Cisco Unified Communications Manager에서 비상 통화 처리기 기능을 활성화합니다. 비상 통화 처리기는 필수 비상 통화 기능을 제공하며 정적 구성으로 전화기 위치가 할당된 제한된 수의 위치를 지원

합니다. 다수의 특정 위치 또는 동적 위치 할당 등과 같은 고급 비상 통화 기능이 필요한 경우에는 Cisco Emergency Responder 사용을 고려해 보십시오.



참고 Cisco Emergency Responder와 같은 외부 비상 통화 솔루션을 사용 중인 경우에는 이 기능을 활성화하지 마십시오.

이 기능을 활성화하려면 외부 비상 통화 솔루션을 비활성화해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 비상 통화 처리기 > 비상 위치 구성.

단계 2 비상 위치 구성 창에서 다음을 수행합니다.

- 비상 통화 처리기 기능을 활성화하려면 비상 위치(**ELIN**) 지원 활성화 확인란을 선택합니다. 기본 설정은 비활성화입니다. 이 기능을 활성화하면 [관련된 설정] 분할창에 이 기능과 관련된 설정이 나타납니다. 이 설정을 구성해야 기능이 작동됩니다. 관련된 설정 구성 방법에 대한 자세한 내용은 아래 설명된 작업을 참조하십시오.
- 비상 통화 처리기 기능을 비활성화하려면 비상 위치(**ELIN**) 지원 활성화 확인란을 선택 취소합니다.

참고 이 기능을 비활성화하면 구성된 모든 관련 설정이 제거됩니다. 구성된 모든 설정을 보려면 [관련된 설정] 분할창을 참조하십시오.

참고 500대 이상의 디바이스가 ELIN 그룹에 연결되어 있는 상태에서 이 기능을 비활성화하려는 경우 연결된 디바이스가 500대 미만이 될 때까지 연결을 수동으로 삭제해야 이 기능을 비활성화할 수 있습니다.

단계 3 저장을 클릭합니다.

비상 위치 그룹 구성

특정 사이트나 위치에 비상 위치(ELIN) 그룹을 구성합니다.

시작하기 전에

[비상 통화 처리기 사용, 689 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 비상 통화 처리기 > **ELIN**(비상 위치) 그룹.
- 단계 2 **ELIN**(비상 위치) 그룹 구성 창에서 이름 필드에 그룹의 이름을 입력합니다.
- 단계 3 번호 필드에서 PSAP(Public Safety Answering Point)에 등록된 DID 번호 풀을 입력합니다.
- 단계 4 저장을 클릭합니다.

비상 위치 그룹에 디바이스폴 추가

비상 위치(ELIN) 그룹을 사용하도록 디바이스폴을 구성합니다.

시작하기 전에

[비상 위치 그룹 구성, 690 페이지](#)

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 디바이스폴.
- 단계 2 디바이스폴 찾기 및 나열 창에서 기존 디바이스폴을 추가하는 경우 찾기를 클릭하고 목록에서 디바이스폴을 선택합니다. 새 디바이스폴을 추가하는 경우 새로 추가를 클릭합니다.
- 단계 3 디바이스폴 구성 창의 **ELIN**(비상 위치) 그룹 드롭다운 목록에서 디바이스폴을 추가할 ELIN 그룹을 선택합니다. 새 디바이스폴을 추가하는 경우 다른 모든 필수 필드를 채웁니다.
- 단계 4 저장을 클릭합니다.

비상 위치 그룹에 디바이스 추가

특정 비상 위치(ELIN) 그룹을 사용하도록 특정 디바이스폴을 구성합니다. 이 디바이스에 연결되는 디바이스폴 ELIN 그룹을 사용하려는 경우에는 이 섹션을 무시할 수 있습니다.



참고 디바이스 수준에서 설정한 구성은 디바이스폴 수준에서 설정한 모든 구성을 덮어씁니다.



참고 ELIN 그룹에 추가되는 디바이스는 해당 디바이스가 있는 특정 위치를 나타내는 ELIN 그룹에 추가되어야 합니다.

시작하기 전에

[비상 위치 그룹에 디바이스폴 추가, 691 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기

참고 IP 전화기가 아닌 전화기 유형을 사용하는 경우 해당 유형의 전화기에 대한 관련 구성 페이지로 이동합니다.

단계 2 전화기 찾기 및 나열 창에서 기존 디바이스를 추가하는 경우 찾기를 클릭하고 목록에서 구성하려는 디바이스를 선택합니다. 새 디바이스를 추가하는 경우 새로 추가를 클릭합니다.

단계 3 새 전화기를 추가하는 경우 전화기 유형 드롭다운 목록에서 추가할 전화기의 유형을 선택하고 다음을 클릭합니다.

단계 4 전화기 구성 창의 **ELIN(비상 위치)** 그룹 드롭다운 목록에서 디바이스를 추가할 ELIN 그룹을 선택합니다. 새 디바이스를 추가하는 경우 다른 모든 필수 필드를 채웁니다.

단계 5 저장을 클릭합니다.

경로 패턴 및 변환 패턴 활성화

경로 패턴 또는 변환 패턴에 비상 위치(ELIN) 서비스를 활성화합니다.



참고 경로 패턴 또는 변환 패턴 둘 중 하나를 반드시 활성화해야 하지만 둘 다 활성화할 수는 없습니다.

시작하기 전에

[비상 위치 그룹에 디바이스 추가, 691 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 중 하나를 선택합니다.

- 라우트 패턴을 활성화하려면 통화 라우팅 > 경로/힌트 > 라우트 패턴을 선택합니다.
- 변환 패턴을 활성화하려면 통화 라우팅 > 변환 패턴을 선택합니다.

단계 2 라우트 패턴 찾기 및 나열 또는 변환 패턴 찾기 및 나열 창에서 찾기를 클릭하고 목록에서 라우트 패턴 또는 변환 패턴을 선택합니다.

단계 3 라우트 패턴 구성 또는 변환 패턴 구성 창에서 비상 서비스 번호임 확인란을 선택합니다.

참고 비상 통화 처리기를 사용 중이고 Cisco Emergency Responder와 같은 다른 외부 비상 통화 솔루션을 사용하지 않는 경우에만 이 확인란을 선택합니다.

단계 4 저장을 클릭합니다.

비상 위치 그룹 및 전화기의 벌크 관리

• 비상 위치 그룹 및 전화기의 벌크 관리 작업 흐름, 693 페이지

비상 위치 그룹 및 전화기의 벌크 관리 작업 흐름

이 섹션에서는 ELIN 그룹 정보를 업데이트하고 새 ELIN 그룹에 전화기를 추가할 수 있는 벌크 관리 작업에 대한 정보를 제공합니다. 벌크 관리에 대한 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 지침서, 릴리스 11.0(1)을 참조하십시오.



참고 이러한 절차를 수행하기 전에 비상 통화 처리기 기능을 활성화했는지 확인하십시오. [비상 통화 처리기 사용, 689 페이지](#) 참조

프로시저

	명령 또는 동작	목적
단계 1	비상 위치(ELIN) 그룹 정보 가져오기, 693 페이지	벌크 관리 도구를 사용하여 ELIN(비상 위치) 그룹 정보를 가져옵니다.
단계 2	비상 위치(ELIN) 그룹 정보 내보내기, 694 페이지	벌크 관리 도구를 사용하여 ELIN(비상 위치) 그룹 정보를 내보냅니다.
단계 3	새 비상 위치(ELIN) 그룹으로 전화기 업데이트, 694 페이지	여러 전화기를 찾아서 나열하고 새 ELIN(비상 위치) 그룹을 사용하여 해당 전화기를 구성합니다.

비상 위치(ELIN) 그룹 정보 가져오기

벌크 관리 도구를 사용하여 ELIN(비상 위치) 그룹 정보를 가져옵니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 벌크 관리 > 가져오기/내보내기 > 가져오기.
- 단계 2 파일 이름 드롭다운 목록에서 가져올 .tar 파일의 이름을 선택하고 다음을 클릭합니다.
- 단계 3 가져오기 구성 섹션에 .tar 파일의 모든 구성 요소가 나열됩니다. 가져올 옵션의 ELIN 그룹 관련 확인란을 선택합니다.
- 단계 4 해당 라디오 버튼을 클릭하여 작업을 즉시 실행하거나 나중에 실행합니다.

단계 5 선택한 데이터 가져오기 작업을 만들려면 제출을 클릭합니다. 상태 섹션의 메시지를 통해 작업이 성공적으로 제출되었는지 확인할 수 있습니다.

단계 6 이 작업을 예약하거나 활성화하려면 벌크 관리 주 메뉴의 작업 스케줄러 옵션을 사용합니다.

비상 위치(ELIN) 그룹 정보 내보내기

벌크 관리 도구를 사용하여 ELIN(비상 위치) 그룹 정보를 내보냅니다.

시작하기 전에

[비상 위치\(ELIN\) 그룹 정보 가져오기, 693 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 벌크 관리 > 가져오기/내보내기 > 내보내기.

단계 2 데이터 내보내기 창에서, 작업 정보 창에 있는 **Tar** 파일 이름 필드에 확장자 없이 .tar 파일 이름을 입력합니다. BPS는 이 파일 이름을 사용하여 구성 세부 정보를 내보냅니다.

참고 동시에 내보낸 모든 파일은 번들로 묶이며(.tar) 서버에서 다운로드할 수 있습니다.

단계 3 비상 위치(ELIN) 그룹 정보를 내보내려면 내보낼 항목 선택 창에서 **Elin** 그룹 확인란을 선택합니다.

단계 4 (선택 사항) 다음 단계를 수행합니다.

- ELIN 그룹이 구성된 디바이스폴을 내보내려면 디바이스폴 확인란을 선택합니다.
- ELIN 그룹이 구성된 전화기를 내보내려면 전화기 확인란을 선택합니다.

단계 5 작업 설명 필드에 작업에 대해 무시할 설명을 입력합니다. 기본 설명은 [구성 내보내기]입니다.

단계 6 해당 라디오 버튼을 클릭하여 작업을 즉시 실행하거나 나중에 실행할 수 있습니다.

단계 7 선택한 데이터 내보내기 작업을 만들려면 제출을 클릭합니다. 상태 창의 메시지를 통해 작업이 성공적으로 제출되었는지 확인할 수 있습니다.

단계 8 이 작업을 예약하거나 활성화하려면 벌크 관리 주 메뉴의 작업 스케줄러 옵션을 사용합니다.

새 비상 위치(ELIN) 그룹으로 전화기 업데이트

여러 전화기를 찾아서 나열하고 새 ELIN(비상 위치) 그룹을 사용하여 해당 전화기를 구성합니다.

시작하기 전에

[비상 위치\(ELIN\) 그룹 정보 내보내기, 694 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 벌크 관리 > 전화기 > 전화기 업데이트 > 쿼리를 선택합니다.

단계 2 업데이트할 전화기 찾기 및 나열 창에서 검색에 사용할 매개 변수를 설정하고 찾기를 클릭합니다.

참고 모든 전화기를 업데이트하려면 찾기를 클릭하고 쿼리를 지정하지 않습니다.

단계 3 업데이트할 전화기 찾기 및 나열 창에 선택한 전화기의 세부 정보가 표시됩니다. 다음을 클릭합니다.

단계 4 전화기 업데이트 창에서 비상 위치(ELIN) 그룹 확인란을 선택하고 드롭다운 목록 상자에서 새 ELIN 그룹을 선택합니다.

단계 5 제출을 클릭합니다.

상호 작용

기능	상호 작용
방해 사절 통화 거부	<p>PSAP 콜백에서 발신한 통화는 대상 디바이스의 DND(방해 사절) 구성을 덮어씁니다.</p> <p>DND 통화 거부가 활성화된 경우 변환 패턴을 사용하여 비상 번호를 다이얼하면 ELIN이 이 아웃바운드 비상 통화에 연결됩니다. 통화가 끊어진 상태에서 PSAP 콜백을 사용하여 ELIN을 콜백 하면 통화가 전화기의 DND 설정에 관계 없이 전화기로 라우팅됩니다.</p>
모든 통화 착신 전환	<p>PSAP 콜백에서 발신한 통화는 대상 디바이스의 통화 착신 전환(CFA) 설정을 덮어씁니다.</p> <p>전화기에 CFA가 활성화되어 있고 변환 패턴을 사용하는 비상 번호를 다이얼하면 ELIN이 이 아웃바운드 비상 통화에 연결됩니다. 통화가 끊어진 상태에서 PSAP 콜백을 사용하여 ELIN을 콜백 하면 통화가 전화기의 CFA 설정에 관계 없이 전화기로 라우팅됩니다.</p>
단일 전화번호 연결	<p>PSAP 콜백에서는 SNR(단일 번호 연락) 구성을 무시합니다.</p> <p>전화기가 휴대폰 번호를 가리키는 원격 대상으로 SNR을 활성화한 경우 변환 패턴을 사용하여 비상 번호를 다이얼하는 경우 ELIN이 이 아웃바운드 비상 통화에 연결됩니다. 통화가 끊어진 상태에서 PSAP 콜백을 사용하여 ELIN 번호를 콜백하는 경우 통화가 원격 대상이 아니라 전화기로 라우팅됩니다.</p>

기능	상호 작용
Extension Mobility	<p>PSAP 콜백 통화는 EM(Extension Mobility) 상태를 고려합니다.</p> <p>EM 프로파일 자격 증명으로 로그인하고 변환 패턴을 사용하여 비상 번호로 다이얼하는 경우 ELIN이 이 아웃바운드 비상 통화에 연결됩니다. 통화 연결이 끊기고 사용자가 여전히 로그인되어 있는 ELIN이 PSAP 콜백을 사용하여 콜백되는 경우 통화는 통화를 시작한 디바이스로 라우팅됩니다.</p> <p>참고 이 디바이스는 사용자가 여전히 로그인되어 있는 디바이스입니다.</p>
	<p>PSAP 콜백을 수행하기 전에 사용자가 로그아웃하면 PSAP 콜백이 실패합니다.</p> <p>사용자가 EM 프로파일 자격 증명을 사용하여 로그인할 때 변환 패턴을 사용하여 비상 번호를 다이얼하면 ELIN이 이 아웃바운드 비상 통화에 연결됩니다. 통화 연결이 끊기고 PSAP 콜백을 사용하여 콜백되는 경우, 사용자가 로그아웃한 후에는 통화가 통화를 시작한 디바이스로 라우팅되지 않으며 실패하게 됩니다.</p>
	<p>다른 디바이스에 로그인한 사용자와 함께 PSAP 콜백</p> <p>사용자가 전화기 A에서 EM 프로파일 인증서를 사용하여 로그인하고 변환 패턴을 사용하여 비상 번호로 다이얼하면, ELIN이 이 아웃바운드 비상 통화에 연결됩니다. 통화의 연결이 끊어지면 사용자는 전화기 A에서 로그아웃해야 합니다. 그런 다음 사용자가 다른 전화기에 로그인하고, 동일한 프로파일을 사용하고, ELIN이 PSAP 콜백을 사용하여 콜백한 경우, 통화가 일반 우선 순위를 사용하는 전화기 B로 라우팅됩니다. CFA 설정이 무시되고 DND 설정이 무시되지 않습니다.</p>
	<p>여러 로그인이 포함된 PSAP 콜백 통화.</p> <p>사용자가 전화기 A에서 EM 프로파일 인증서를 사용하여 로그인하고 변환 패턴을 사용하여 비상 번호로 다이얼하면, ELIN 번호가 이 아웃바운드 비상 통화에 연결됩니다. 통화 연결이 끊기고 사용자가 전화기 A에 로그인되어 있는 동안에도 동일한 프로파일을 사용하여 다른 전화기인 전화기 B에 로그인하고, PSAP 콜백을 사용하여 ELIN을 다시 호출하면 통화가 발신된 디바이스에만 통화가 전송됩니다.</p>
디바이스 모빌리티	<p>로밍 디바이스는 발신 비상 통화에 대해 로밍 디바이스폴의 ELIN 그룹을 사용합니다.</p> <p>로밍 디바이스폴과 연결되도록 홈 위치에서 활성화된 디바이스 모빌리티를 사용하여 디바이스 모빌리티를 로밍 위치(IP 서브넷의 변경)로 이동합니다. 변환 패턴을 사용하여 비상 번호를 다이얼하는 경우 ELIN이 이 아웃바운드 비상 통화에 연결됩니다. ELIN은 로밍 디바이스폴과 연결된 ELIN 그룹에 속합니다.</p>

기능	상호 작용
공유 회선	<p>다른 디바이스에서 회선을 공유하는 경우에는 비상 통화를 한 디바이스에만 PSAP 콜백이 올립니다.</p> <p>전화기 A와 전화기 B가 DN(디렉터리 번호)을 공유합니다. 변환 패턴을 사용하여 비상 번호를 다이얼하는 경우 ELIN이 이 아웃바운드 비상 통화에 연결됩니다. 통화 연결이 끊어지고 PSAP 콜백을 사용하여 ELIN이 콜백되면 통화가 발신된 디바이스인 전화기 A로 라우팅됩니다.</p>

비상 통화 처리기 문제 해결

비상 통화 처리기 문제 해결 시나리오 정보

이 섹션에서는 다음 영역에서 일부 비상 통화 처리기 문제 해결 시나리오에 대한 정보를 제공합니다.

- 구성 시나리오
- 발신 통화 시나리오
- 수신 통화 시나리오

Configuration Scenarios

비상 통화에 통화 중 신호가 들리고 라우팅되지 않음

문제:

비상 통화에 통화 중 신호가 들리고 라우팅되지 않습니다.

해결 방법:

비상 통화에 전화를 거는 사용자가 다시 걸기 신호음을 실행 중인 경우 다음 확인을 수행합니다.

- 비상 통화에 대한 변환 또는 라우트 패턴이 사용되었는지 확인합니다. 이 경우 CSS에서 디바이스 또는 전화기를 확인해야 할 수 있습니다.
- 비상 통화의 변환 또는 라우트 패턴에 대해 긴급 서비스 번호 확인란을 선택했는지, 게이트웨이에 올바르게 라우팅하는 지 확인합니다.

비상 통화에 전화를 거는 사용자가 올바른 게이트웨이 또는 PSAP(공개 서비스 응답 지점)에 도달하지 않는 경우 전화기 또는 디바이스의 설정 또는 디바이스풀 설정이 올바른 비상 위치(ELIN) 그룹으로 구성되어 있는지 확인합니다.

다시 걸기 신호음을 실행 중인 외부에서 비상 위치 번호로 전화가 걸림

문제:

다시 걸기 신호음을 실행 중인 동안 외부에서 비상 위치 번호(ELIN)로 전화가 걸립니다.

원인:

이 경우 ELIN은 발신자의 위치를 식별하는 데 사용되는 DID로 설정되었습니다. 이는 모든 전화기 또는 다른 용도로 사용되지 않아야 합니다.

해결 방법:

ELIN 구성 정보를 확인하고, DID로 설정된 ELIN을 설정 해제하십시오.

Outgoing Calls Scenarios

발신 비상 통화에 발신자가 비상 위치 번호로 포함되어 있지 않음

문제:

발신 비상 통화에는 발신자가 비상 위치(ELIN) 번호로 포함되지 않습니다.

원인:

이 ELIN에 대한 변환 패턴 또는 라우트 패턴이 올바르게 구성되지 않았습니다.

해결 방법:

이 ELIN에 대한 변환 패턴 또는 라우트 패턴 설정이 올바르게 구성되었는지 확인하고 관련 변환 패턴 또는 라우트 패턴 구성 페이지에서 비상 서비스 번호임 확인란이 선택되어 있는지 확인합니다.

발신 비상 통화에 수정된 비상 위치 번호가 포함

문제:

발신 비상 통화에는 수정된 비상 위치(ELIN) 번호가 포함됩니다.

원인:

발신 트렁크 또는 라우트 목록에는 ELIN에 필요하지 않은 추가 변환이 포함되어 있습니다.

해결 방법:

통화에 적용된 변환을 확인하고, 발신 트렁크 또는 라우트 목록에 ELIN에 대한 필수 변환만 있는지 확인합니다.

Incoming Calls Scenarios

수신 PSAP 콜백 통화 실패

문제:

수신 PSAP 콜백 통화가 실패합니다.

원인:

원래 비상 통화를 수행한 디바이스가 올바르게 등록되지 않았습니다.

해결 방법:

원래 비상 통화를 만든 디바이스가 등록되었는지, Extension Mobility가 관련되었는지 여부를 확인합니다.

수신 **PSAP** 콜백 통화가 예상대로 라우팅되지 않음

문제:

수신 **PSAP** 콜백 통화가 예상대로 라우팅되지 않습니다.

원인:

비상 위치(ELIN) 번호가 원래 전화 건 상대방의 번호와 일치하지 않습니다.

해결 방법:

ELIN이 원래 전화 건 상대방에게 성공적으로 역방향 매핑하려면 이 두 숫자가 일치해야 합니다. 수신 게이트웨이 또는 트렁크에서 구성된 유효 숫자가 이미 변환된 경우 마지막 변환된 착신자에서 ELIN 번호와 일치하는지 확인합니다.

수신 **PSAP** 콜백 통화가 예상대로 라우팅되지 않음



53 장

RedSky로 비상 통화 처리

- RedSky로 비상 통화 처리 개요, 701 페이지
- 비상 통화 처리 구성 작업 흐름, 702 페이지

RedSky로 비상 통화 처리 개요



중요 이 기능은 릴리스 12.5(1)SU6 및 14SU2부터 적용할 수 있습니다.

Unified Communications Manager와 통합된 RedSky 솔루션을 통해 고객은 캠퍼스 내든 원격이든 모든 직원에 대해 9-1-1 비상 통화를 수행할 수 있는 활성 위치를 확보하고 긴급 구조대원에게 통화를 보낼 수 있습니다.

엔드포인트에는 HTTP HELD(Enabled Location Delivery) 요청에 대한 응답으로 RedSky 서버로부터 받은 URI 위치가 저장됩니다. Webex에서 비상 번호 9-1-1을 누르면 Unified Communications Manager는 이전에 저장된 위치 URI를 INVITE 메시지의 지오로케이션 헤더로 가져오고 호출된 장치의 위치에 해당하는 지오로케이션 헤더로 위치 URI를 포함하는 송신 INVITE를 사용하여 RedSky 서버로 호출을 라우팅합니다. RedSky 서버가 오른쪽 ELIN으로 교체되고 비상 전송을 위해 공공 안전 응답 지점(PSAP)으로 호출을 보냅니다. E911 Anywhere는 SMS 텍스트, 이메일 및 보안 데스크 화면 알람을 포함한 통화 알람을 동시에 전송합니다.

Cisco Emergency Responder는 사용자가 E911 규정을 준수할 수 있도록 기업 전체로 이동하는 모든 장치의 디스패치 가능한 위치를 자동으로 찾아 추적합니다. Emergency Responder는 스위치 포트 또는 액세스 포인트 또는 IP 서브넷을 통해 Cisco IP 전화기를 추적하거나 수동으로 구성합니다. Emergency Responder는 전화기 상태(온프레미스, 오프프레미스, 위치 없음)를 유지하고 모든 자동 위치 정보(ALI) 또는 ELIN 정보를 RedSky에 전달합니다. 전화기 사용자는 Unified CM을 사용하여 비상 통화를 RedSky 및 지정된 비상 공급자에게 라우팅합니다.

오프프레미스 전화기의 경우 사용자의 현재 위치가 이전에 정의되지 않은 경우 사용자는 Emergency Responder 오프프레미스 사용자 웹 페이지로 이동하여 새 위치를 만듭니다. 새 위치가 정의되고 주소가 확인된 후에는 오프프레미스 전화기에서 걸려오는 비상 통화가 RedSky를 통해 완료됩니다.



참고 직원이 조직 사이트의 온프레미스에서 작업하는 경우 통화 시스템 관리자가 사용자의 위치를 정의하는 것이 좋습니다.

비상 통화 처리 구성 작업 흐름

관리자는 다음 작업을 사용하여 9-1-1 비상 통화를 위한 동적 위치를 확보하고 비상 대응자에게 통화를 전환할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	RedSky 서버 구성	RedSky 서버로 호출을 라우팅하기 위한 SIP 트렁크를 만듭니다.
단계 2	서비스 프로파일 구성	최종 사용자의 서비스 프로파일 세부 정보를 비상 통화에 추가합니다.
단계 3	서비스 프로파일 할당	생성된 서비스 프로파일을 Webex 클라이언트 최종 사용자에게 할당합니다.
단계 4	통화 라우팅에 대한 SIP 경로 패턴 설정	도메인 이름으로 SIP 경로 패턴을 만들고 이전에 생성된 SIP 트렁크와 동일하게 연결합니다.

RedSky 서버 구성

이 절차를 사용하여 RedSky 서버로 호출을 라우팅하기 위한 SIP 트렁크를 만듭니다.



참고 7, 8 및 9단계는 온-프레미스 통합 중에만 필요합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 트렁크 유형 드롭다운 목록에서 **SIP** 트렁크를 선택합니다.
- 단계 4 프로토콜 유형 드롭다운 목록에서 구축과 일치하는 SIP 트렁크 유형을 선택하고 다음을 클릭합니다.
- 단계 5 **SIP** 정보 영역에서 SIP 트렁크에 연결할 서버 또는 엔드 포인트의 RedSky 서버 IPv4 주소, 정규화된 도메인 이름 또는 DNS SRV 레코드를 대상 주소 텍스트 상자에 입력합니다.

- 단계 6 **SIP** 트렁크 보안 프로파일 드롭다운에서 보안 프로파일을 할당합니다. 이 옵션을 선택하지 않는 경우, SIP 트렁크 보안 프로파일 비보안 프로파일이 할당됩니다.
- 단계 7 (선택 사항) **SIP** 프로파일 드롭다운 목록에서 **Ping** 옵션이 활성화된 **RedSky SIP** 프로파일을 할당합니다.
- 단계 8 (선택 사항) 정규화 스크립트 영역의 정규화 스크립트 드롭다운에서 **redsky-alternate-id-interop**를 선택합니다.
- 단계 9 (선택 사항) 매개 변수 이름 및 매개 변수 값에는 해당 정보를 입력합니다.
- 매개 변수 이름에는 다음과 같은 입력이 지원됩니다.

- **RedSky-CustomerID** - 이 필드는 필수 필드입니다. 이는 RedSky 관리 페이지의 HELD ID입니다. 이는 발신자에 대한 고객 계정을 식별하는 데 사용됩니다.
- 대체 콜백 번호 - 이 필드는 선택 사항입니다. 이 필드는 응급 전화에 대한 옵션 콜백 번호를 삽입합니다. 콜백에 대한 DID(Direct Inward Dial) 번호가 없는 발신자에게 사용해야 합니다.
- 내선 길이 - 이 필드는 선택 사항입니다. 이 매개 변수는 E.164 이외의 번호 지정 규칙을 사용하는 고객에게 사용됩니다. 이 매개 변수는 비 E.164를 RedSky E911 사용자 ID 헤더에 입력합니다.
- 상담사 내선 번호 - 이 필드는 선택 사항입니다. 이 매개 변수는 선행 숫자를 기준으로 상담사 내선 번호를 식별합니다. 이 매개 변수를 채우면 상담사 발신자가 RedSky E911 사용자 ID 헤더에 들어갑니다.

단계 10 저장을 클릭합니다.

서비스 프로파일 구성

이 절차를 사용하여 최종 사용자의 서비스 프로파일 세부 정보를 비상 통화에 추가할 수 있습니다.

시작하기 전에

- Ping 옵션이 활성화된 SIP 프로파일과 RedSky 서버를 사용하여 SIP 트렁크를 생성해야 합니다. 필수 도메인 이름(RedSky)을 사용하여 SIP 경로 패턴을 생성해야 하며 이전에 만든 트렁크와 연결됩니다.
- 서비스 프로파일은 소유자 사용자 ID를 지정한 경우에만 지정한 장치에 적용됩니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 사용자 관리 > 사용자 설정 > 서비스 프로파일을 선택합니다.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 선택한 서비스 프로파일 구성에 대한 이름 및 설명을 입력합니다.

참고 이 프로파일의 일부가 되려는 각 UC 서비스의 경우, 해당 서비스에 대한 기본, 보조 및 3차 연결을 할당합니다. 서비스 프로파일 구성 창의 필드는 사용자가 구성하는 UC 서비스에 따라 달라집니다.

단계 4 비상 통화 프로파일 섹션에서 다음을 수행합니다.

- 엔드포인트에 대한 구성 매개 변수와 소프트웨어 클라이언트가 위치를 업데이트하고 비상 통화 서비스 공급자에 비상 통화를 보낼 수 있도록 하려면 비상 통화 활성화를 선택합니다.
- 계정이 생성될 때 비상 통화 서비스 공급자가 제공한 회사 ID 및 암호를 입력하고 조직 ID 및 비밀번호 필드에 서비스가 활성화됩니다. 예를 들어, RedSky에서 제공하는 32자의 영숫자 문자열입니다.
- 비밀 필드에서 비상 통화 서비스 공급자 인증 서비스에 필요한 암호를 입력합니다. 예를 들어, RedSky에서 제공하는 16자의 영숫자 문자열입니다.
- 위치 URL 필드에 장치가 위치를 요청하고 설정하는 데 사용하는 URL을 입력합니다.
- 긴급 서비스 번호를 입력합니다. 기본적으로 911, 933은 각 번호를 구분하는 쉼표와 함께 입력됩니다.

참고 Webex 클라이언트에서 비상 번호로 구성된 비상 패턴으로 전화를 걸면 이는 SIP 트렁크에 구성된 RedSky 서버에 지오로케이션 헤더를 사용하여 라우팅됩니다.

단계 5 서비스 프로파일 구성 창에서 나머지 필드를 완료합니다. 자세한 필드 설명은 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

서비스 프로파일 할당

이 절차를 사용하여 생성된 서비스 프로파일을 Webex 클라이언트 최종 사용자에게 할당합니다. Webex가 Unified CM에 등록되지 않은 경우 최종 사용자는 활성 상태가 되지 않으며 비상 통화를 RedSky에 라우팅하지 않습니다.

최종 사용자에게 서비스 프로파일을 적용하여 서비스 프로파일의 UC 서비스 구성 설정을 해당 최종 사용자에게 할당할 수 있습니다. 조직의 다른 사용자 그룹에 대해 다른 서비스 프로파일을 구성하여 각 사용자 그룹이 해당 작업에 대해 구성된 적절한 서비스를 갖도록 할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 사용자 관리 > 최종 사용자를 선택합니다.

단계 2 찾기 및 나열 창에서 다음 작업 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 사용자를 구성합니다.
- 사용자 위치 찾기 필드에 필터를 지정한 다음, 찾기를 선택하여 사용자 목록을 검색합니다.

참고 디바이스를 사용자와 연결하는 방법에 대한 자세한 내용은 [Cisco Emergency Responder 관리 지침서](#)의 최종 사용자에게 디바이스 연결 섹션을 참조하십시오.

- 단계 3 서비스 설정 섹션의 UC 서비스 프로파일 드롭다운 목록에서 RedSky 서비스 프로파일을 선택합니다.
- 단계 4 최종 사용자 구성 창에서 나머지 필드를 완료합니다. 자세한 필드 설명은 온라인 도움말을 참조하십시오.
- 단계 5 저장을 클릭합니다.

통화 라우팅에 대한 SIP 경로 패턴 설정

이 절차를 사용하여 도메인 이름으로 SIP 경로 패턴을 만들고 이전에 생성된 SIP 트렁크와 동일하게 연결합니다.

비상 공급자에 라우팅된 모든 비상 통화는 경로 패턴과 일치해야 합니다. 경로 패턴은 RedSky 서버에 연결할 수 있는 경로 그룹, 경로 목록 및 SIP 트렁크 또는 PRI 게이트웨이로 통화를 전송합니다.

PRI - RedSky는 고객에게 계정 특정 액세스 번호를 제공합니다. 이 경우 번호는 고객 ID이고 발신자는 사용자 참조입니다. 이는 기존 RP/RG/RL/GW 중복을 따릅니다. 발신자 번호는 RedSky 사용자의 ID와 일치해야 합니다.

SIP 트렁크를 사용하여 RedSky 서버에 연결하는 것이 좋습니다. 전용 인스턴스의 경우 이 방법이 기본 방법입니다. Unified Communications Manager 온프레미스의 온프레미스 배포 환경을 보유한 고객의 경우 RedSky 서버에 도달하는 데 사용할 경로 패턴을 만들기 전에 SIP 트렁크, 경로 그룹 및 경로 목록을 구성해야 합니다.

SIP 트렁크를 사용하는 경우, 관리자는 사전 정의된 LUA 스크립트를 사용하여 고객을 올바르게 식별해야 합니다. Unified CM 배포의 경우 스크립트를 업로드하고 SIP 트렁크에 적용해야 합니다. LUA 스크립트를 사용하면 하나의 매개 변수(RedskyOrgID)만 사용할 수 있습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 통화 라우팅 > SIP 라우트 패턴을 선택합니다.
- 단계 2 새로 추가를 클릭하여 RedSky 경로 패턴을 추가합니다.
- 단계 3 패턴 사용 드롭다운에서 도메인 라우팅을 선택합니다.
- 단계 4 IPv4 또는 IPv6 주소를 구축하는지 여부에 따라 IPv4 패턴 또는 IPv6 패턴 필드에 경로 문자열을 입력합니다.
- 단계 5 SIP 트렁크/경로 목록* 드롭다운에서 RedSky SIP 트렁크를 선택합니다.
- 단계 6 (선택 사항) 편집 링크를 클릭하여 트렁크 구성 세부 정보를 보거나 변경합니다.
- 단계 7 SIP 라우트 패턴 구성 창에서 나머지 필드를 완료합니다. 자세한 필드 설명은 온라인 도움말을 참조하십시오.
- 단계 8 저장을 클릭합니다.



54 장

엔터프라이즈 그룹

- 엔터프라이즈 그룹 개요, 707 페이지
- 엔터프라이즈 그룹 필수 조건, 708 페이지
- 엔터프라이즈 그룹 구성 작업 흐름, 709 페이지
- 엔터프라이즈 그룹 구축 모델 (Active Directory), 713 페이지
- 엔터프라이즈 그룹 제한 사항, 715 페이지

엔터프라이즈 그룹 개요

엔터프라이즈 그룹이 구성되면 Cisco Unified Communications Manager는 데이터베이스를 외부 LDAP 디렉터리와 동기화할 때 사용자 그룹을 포함합니다. Cisco Unified CM 관리에서 사용자 그룹 창에서 동기화된 그룹을 볼 수 있습니다.

관리자는 이 기능을 사용하여 다음을 수행할 수 있습니다.

- 기능의 의견 세트(예: 영업 및 회계 팀)와 유사한 특성을 가진 사용자를 프로비전합니다.
- 특정 그룹의 모든 사용자를 대상으로 한 메시지를 보냅니다.
- 특정 그룹의 모든 구성원에 대해 동일한 액세스 구성

또한 이 기능은 Cisco Jabber 사용자가 공통된 특징을 공유하는 사용자의 연락처 목록을 신속하게 구축하는 데 도움이 됩니다. Cisco Jabber 사용자는 외부 LDAP 디렉터리에서 사용자 그룹을 검색한 다음 연락처 목록에 추가할 수 있습니다. 예를 들어, Jabber 사용자는 외부 LDAP 디렉터리를 검색하고 영업 그룹을 연락처 목록에 추가하여 모든 영업 팀원을 연락처 목록에 추가할 수 있습니다. 그룹이 외부 디렉터리에서 업데이트되면 사용자의 연락처 목록이 자동으로 업데이트됩니다.

엔터프라이즈 그룹은 외부 LDAP 디렉터리처럼 Windows의 Microsoft Active Directory에서 지원됩니다.



참고 관리자가 엔터프라이즈 그룹 기능을 비활성화하면 Cisco Jabber 사용자가 엔터프라이즈 그룹을 검색하거나 연락처 목록에 이미 추가한 그룹을 볼 수 없습니다. 관리자가 기능을 비활성화할 때 사용자가 이미 로그인되어 있으면 사용자가 로그아웃할 때까지 해당 그룹이 표시됩니다. 사용자가 다시 로그인하면 해당 그룹이 표시되지 않습니다.

보안 그룹

보안 그룹은 엔터프라이즈 그룹의 하위 기능입니다. Cisco Jabber 사용자는 보안 그룹을 검색하고 연락처 목록에 추가할 수도 있습니다. 이 기능을 설정하려면 관리자는 사용자 정의 LDAP 필터를 구성하고 구성된 LDAP 디렉터리 동기화에 적용해야 합니다. 보안 그룹은 Microsoft Active Directory에서만 지원됩니다.

허용되는 최대 항목 수

엔터프라이즈 그룹을 구성할 때 그룹을 처리하는 연락처 목록 최대 값을 구성해야 합니다

- 연락처 목록에 허용되는 최대 항목 수는 연락처 목록에 있는 항목 수와 연락처 목록에 이미 추가된 그룹의 항목 수를 합한 개수입니다.
- 연락처 목록의 최대 항목 수 = (연락처 목록의 항목 수) + (그룹의 항목 수)
- 엔터프라이즈 그룹 기능이 활성화되면 연락처 목록의 항목 수가 허용되는 최대 항목 수보다 작은 경우 Cisco Jabber 사용자가 연락처 목록에 그룹을 추가할 수 있습니다. 이 기능이 비활성화되어 있을 때 허용되는 최대 항목 수를 초과하면 기능이 활성화될 때까지 사용자가 제한되지 않습니다. 기능이 활성화된 후에도 사용자가 계속 로그인되어 있으면 오류 메시지가 표시되지 않습니다. 사용자가 로그아웃했다가 다시 로그인하면 초과된 항목을 지우라는 오류 메시지가 표시됩니다.

엔터프라이즈 그룹 필수 조건

이 기능은 아래 조건으로 구성된 LDAP 디렉터리 동기화 일정이 이미 있다고 가정합니다. LDAP 디렉터리 동기화를 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "LDAP 디렉터리에서 사용자 가져오기" 장을 참조하십시오.

- Cisco DirSync 서비스를 활성화해야 합니다.
- LDAP 디렉터리 동기화는 사용자와 그룹을 모두 포함해야 합니다.
- **LDAP** 디렉터리 동기화 일정으로 구성된 대로 일반 LDAP 디렉터리 동기화를 예약해야 합니다.

지원되는 LDAP 디렉터리

Microsoft Active Directory만 엔터프라이즈 그룹에서 지원됩니다.

엔터프라이즈 그룹 구성 작업 흐름

엔터프라이즈 그룹 기능을 구성하려면 다음 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 1	LDAP 디렉터리에서 그룹 동기화 확인, 709 페이지	LDAP 디렉터리 동기화에 사용자와 그룹이 모두 포함되어 있는지 확인하십시오.
단계 2	엔터프라이즈 그룹 활성화, 709 페이지	Cisco Jabber는 Microsoft Active Directory에서 엔터프라이즈 그룹을 검색하여 연락처 목록에 추가할 수 있습니다.
단계 3	보안 그룹 활성화, 710 페이지	(선택 사항) Cisco Jabber 사용자가 연락처 목록을 검색하여 보안 그룹을 해당 연락처 목록에 추가할 수 있게하려면 이 작업 흐름을 완료하십시오.
단계 4	사용자 그룹 보기, 712 페이지	(선택 사항) Cisco Unified Communications Manager 데이터베이스와 동기화되는 엔터프라이즈 그룹 및 보안 그룹을 봅니다.

LDAP 디렉터리에서 그룹 동기화 확인

이 절차를 사용하여 LDAP 디렉터리 동기화에 사용자 및 그룹이 포함되어 있는지 확인합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 서버 > **LDAP** > **LDAP 디렉터리**
- 단계 2 찾기를 클릭하고 엔터프라이즈 그룹을 동기화하는 LDAP 디렉터를 선택합니다.
- 단계 3 동기화 필드에 사용자 및 그룹이 선택되었는지 확인합니다.
- 단계 4 LDAP 디렉터리 구성 창의 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.
- 단계 5 저장을 클릭합니다.

엔터프라이즈 그룹 활성화

LDAP 디렉터리 동기화에 엔터프라이즈 그룹을 포함하도록 시스템을 구성합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.
- 단계 2 사용자 관리 파라미터 아래에서 **Cisco IM and Presence**에 대한 디렉토리 그룹 작업 파라미터를 활성화됨으로 설정합니다.
- 단계 3 프레즌스 정보를 사용할 수 있는 최대 엔터프라이즈 그룹 크기 파라미터에 대한 값을 입력합니다. 허용되는 범위는 1 ~ 200 사용자이며 기본값은 100 사용자입니다.
- 단계 4 엔터프라이즈 그룹의 동기화 모드 드롭다운 목록에서 정기적으로 수행할 LDAP 동기화(없음, 차등 동기화, 전체 동기화)를 구성합니다.
- 참고 이러한 필드 구성에 대한 추가 지원은 엔터프라이즈 매개 변수 도움말을 참조하십시오.
- 단계 5 저장을 클릭합니다.

보안 그룹 활성화

Cisco Jabber 사용자가 해당 연락처 목록에 보안 그룹을 추가할 수 있도록하려면 이러한 옵션 작업을 완료하여 보안 그룹을 LDAP 디렉토리 동기화에 포함합니다.



참고 보안 그룹 동기화는 Microsoft Active Directory에서만 지원됩니다.



참고 초기 동기화가 이미 발생한 경우 Cisco 통합 커뮤니케이션 매니저의 기존 LDAP 디렉토리 구성에 새 구성을 추가할 수 없습니다.

프로시저

	명령 또는 동작	목적
단계 1	보안 그룹 필터 생성, 711 페이지	디렉토리 그룹 및 보안 그룹을 모두 필터링하는 LDAP 필터를 생성합니다.
단계 2	LDAP 디렉토리에서 보안 그룹 동기화, 711 페이지	새 LDAP 필터를 LDAP 디렉토리 동기화에 추가합니다.
단계 3	보안 그룹에 대한 Cisco Jabber 구성, 712 페이지	기존 서비스 프로필을 업데이트하여 연결된 Cisco Jabber 사용자에게 보안 그룹을 검색하고 추가하도록 해당 서비스 프로필 액세스 권한을 부여합니다.

보안 그룹 필터 생성

보안 그룹을 필터링하는 LDAP 필터를 생성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > **LDAP** > **LDAP** 필터.

단계 2 새로 추가를 클릭합니다.

단계 3 고유한 필터 이름을 입력합니다. 예를 들어 syncSecurityGroups 합입다.

단계 4 필터: (&(objectClass=group)(CN=*))를 입력합니다.

단계 5 저장을 클릭합니다.

LDAP 디렉토리에서 보안 그룹 동기화

LDAP 디렉토리 동기화에 보안 그룹 필터를 추가하고 동기화를 완료합니다.



참고 초기 LDAP 동기화가 이미 발생한 경우 Cisco 통합 커뮤니케이션 매니저의 기존 LDAP 디렉토리 구성에 새 구성을 추가할 수 없습니다.



참고 새 LDAP 디렉토리 동기화를 설정하는 방법에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서의 "최종 사용자 구성" 부분을 참조하십시오.

시작하기 전에

[보안 그룹 필터 생성, 711 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉토리를 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 LDAP 디렉토리를 만듭니다.
- 찾기를 클릭하고 보안 그룹을 동기화할 LDAP 디렉토리를 선택합니다.

단계 3 그룹에 대한 **LDAP** 사용자 정의 필터 드롭다운 목록에서 사용자가 생성한 보안 그룹 필터를 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 **LDAP** 디렉토리 구성 창의 나머지 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 6 지금 전체 동기화 수행을 클릭하여 즉시 동기화합니다. 그렇지 않으면 다음 예약된 LDAP 동기화가 발생할 때 보안 그룹이 동기화됩니다.

보안 그룹에 대한 Cisco Jabber 구성

해당 서비스 프로필에 연결된 Cisco Jabber 사용자가 LDAP 디렉토리의 보안 그룹을 해당 연락처 목록에 추가할 수 있도록 기존 서비스 프로필을 업데이트합니다.



참고 새 서비스 프로필을 설정하고 Cisco Jabber 사용자에게 할당하는 방법에 대한 자세한 내용은 *Cisco* 통합 커뮤니케이션 매니저 시스템 구성 설명서의 "서비스 프로필 구성" 장을 참조하십시오.

시작하기 전에

[LDAP 디렉토리에서 보안 그룹 동기화, 711 페이지](#)

프로시저

단계 1 서비스 프로필 구성 창의 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 2 찾기를 클릭하고 Jabber 사용자가 사용하는 서비스 프로필을 선택합니다.

단계 3 디렉토리 프로필 아래에서 **Jabber**에서 보안 그룹 검색 및 추가 허용 확인란을 선택합니다.

단계 4 저장을 클릭합니다.

이 서비스 프로필에 연결된 Cisco Jabber 사용자는 이제 보안 그룹을 검색하고 추가할 수 있습니다.

단계 5 Cisco Jabber 사용자가 사용하는 모든 서비스 프로필에 대해 이 절차를 반복합니다.

사용자 그룹 보기

다음 단계에 따라 Cisco 통합 커뮤니케이션 매니저 데이터베이스와 동기화되는 엔터프라이즈 그룹 및 보안 그룹을 확인할 수 있습니다.

프로시저

단계 1 [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 사용자 그룹을 선택합니다. 사용자 그룹 찾기 및 나열 창이 표시됩니다.

단계 2 검색 기준을 입력하고 찾기를 클릭합니다. 검색 기준과 일치하는 사용자 그룹 목록이 표시됩니다.

- 단계 3 사용자 그룹에 속하는 사용자의 목록을 보려면 해당 사용자 그룹을 클릭합니다.
사용자 그룹 구성 창이 나타납니다.
- 단계 4 검색 기준을 입력하고 찾기를 클릭합니다.
검색 기준과 일치하는 사용자 목록이 표시됩니다.
- 목록에서 사용자를 클릭하면 최종 사용자 구성 창이 표시됩니다.

엔터프라이즈 그룹 구축 모델 (Active Directory)

엔터프라이즈 그룹 기능은 Active Directory에 대해 두 가지 구축 옵션을 제공합니다.

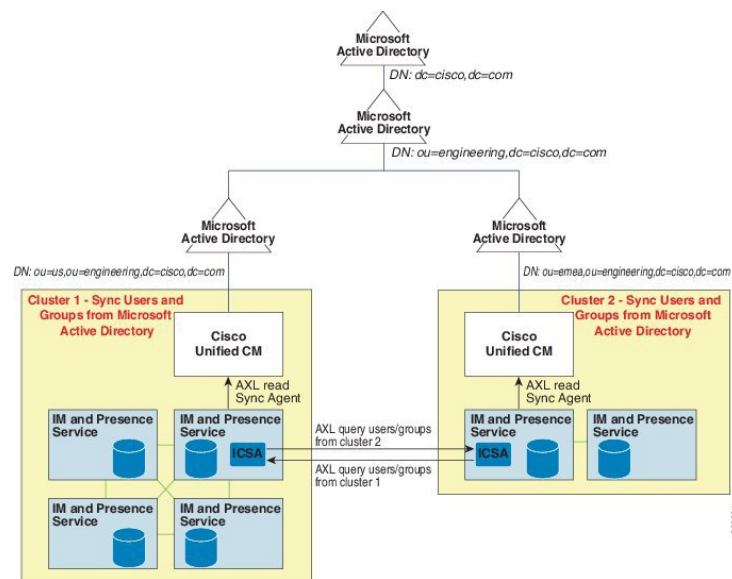


- 중요 Cisco 클러스터 간 동기화 에이전트 서비스를 통해 데이터를 동기화하기 전에 클러스터 1과 클러스터 2에 고유한 UserGroup, UserGroupMember 및 UserGroupWatcherList 레코드 집합이 있는지 확인하십시오. 두 클러스터에 모두 고유한 레코드 세트가 있는 경우, 두 클러스터 모두 동기화 후 모든 레코드의 수퍼 세트를 갖게 됩니다.

엔터프라이즈 그룹 구축 모델 1

이 구축 모델에서 클러스터 1과 클러스터 2는 Microsoft Active Directory의 사용자 및 그룹의 서로 다른 하위 집합을 동기화합니다. Cisco 클러스터 간 동기화 에이전트 서비스는 클러스터 2의 데이터를 클러스터 1로 복제하여 사용자 및 그룹의 전체 데이터베이스를 구축합니다.

그림 12: 엔터프라이즈 그룹 구축 모델 1



엔터프라이즈 그룹 구축 모델 2

이 구축 모델에서 클러스터 1은 Microsoft Active Directory의 모든 사용자 및 그룹을 동기화합니다. 클러스터 2는 Microsoft Active Directory의 사용자만 동기화합니다. Cisco 클러스터 간 동기화 에이전트 서비스는 클러스터 1의 그룹 정보를 클러스터 2로 복제합니다.

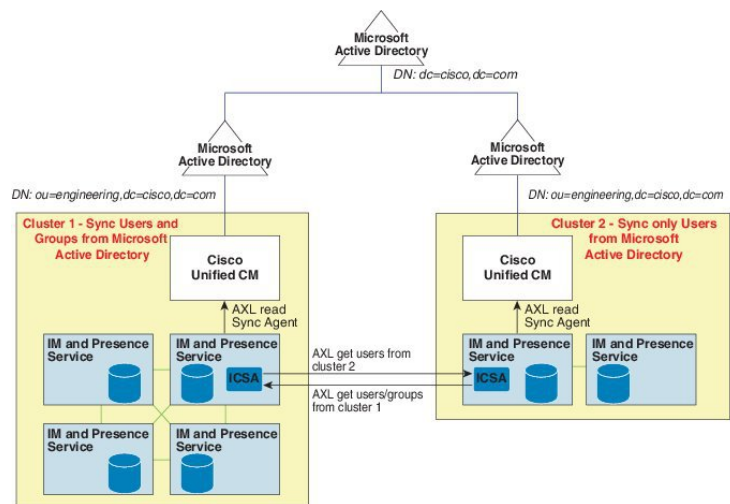


주의 이 구축 모델을 사용하는 경우 하나의 클러스터에서만 그룹 데이터를 동기화하십시오. 엔터프라이즈 그룹 기능은 실패하는 경우 예상대로 작동하지 않습니다.

Cisco Unified CM IM and Presence 관리 > 프레즌스 > 클러스터링 간 창에서 설정을 확인할 수 있습니다.

클러스터 간 피어 테이블에서 엔터프라이즈 그룹 **LDAP** 설정 파라미터의 상태를 확인합니다. 충돌 없음은 피어 간에 잘못된 구성이 없음을 의미합니다. 충돌이 발견되면 Enterprise GroupConflicts 링크를 클릭하고 나타나는 세부 정보 버튼을 클릭합니다. 세부 보고서에 대한 보고 창이 열립니다.

그림 13: 엔터프라이즈 그룹 구축 모델 2



엔터프라이즈 그룹 제한 사항

표 60: 엔터프라이즈 그룹 제한 사항

제한 사항	설명
모든 사용자 차단	<p>Cisco Jabber 사용자가 Cisco Jabber 정책 설정에서 "모든 사용자 차단" 기능을 활성화하면 차단은 차단 사용자의 연락처 목록에 연락처로 나열되지 않은 한 다른 Jabber 사용자가 IM and Presence를 차단 사용자와 함께 보거나 교환할 수 없습니다.</p> <p>예를 들어 Cisco Jabber 사용자(Andy)는 개인 Jabber 설정 내에서 모든 사용자 차단을 활성화했습니다. 다음 목록은 Andy의 차단이 Andy의 개인 연락처 목록에 포함되거나 포함되지 않을 수 있는 다른 Jabber 사용자에게 미치는 영향을 보여줍니다. 차단 외에도 Andy는 다음과 같은 개인 연락처 목록을 가지고 있습니다.</p> <ul style="list-style-type: none"> • Bob 포함 - Bob은 Andy의 개인 연락처 목록에 있기 때문에 차단에도 불구하고 그는 여전히 IM을 보내고 Andy의 프레즌스를 볼 수 있습니다. • Carol 생략 - Carol은 Andy의 프레즌스를 볼 수 없거나 차단으로 인해 IM을 보낼 수 없습니다. • 개인 연락처로 Deborah를 생략합니다. 그러나 Deborah의 멤버인 Andy 연락처로 나열가 엔터프라이즈 그룹 — Deborah Andy의 프레즌스 보거나 Andy Im을 보내기 차단 됩니다. <p>Deborah는 Andy의 연락처 목록에 있는 엔터프라이즈 그룹의 구성원임에도 불구하고 Andy의 프레즌스를 보거나 IM을 Andy에게 보내는 것이 차단됩니다. 엔터프라이즈 그룹 연락처 동작에 대한 자세한 내용은 CSCvg48001을 참조하십시오.</p>
10.x 클러스터의 인터클러스터 피어링	<p>엔터프라이즈 그룹은 릴리스 11.0(1) 이상에서 지원됩니다.</p> <p>동기화된 그룹에 10.x 인터클러스터 피어의 그룹 구성원이 포함되어 있는 경우 상위 클러스터의 사용자가 10.x 클러스터에서 동기화된 구성원을 볼 수 없습니다. 이는 엔터프라이즈 그룹 동기화를 위해 11.0(1)에서 도입된 데이터베이스 업데이트로 인한 것입니다. 이 업데이트는 10.x 릴리즈의 일부가 아닙니다.</p> <p>상위 클러스터에 있는 사용자가 10.x 클러스터에 있는 그룹 구성원의 프레즌스를 확인할 수 있도록하려면 상위 클러스터의 사용자가 10.x 사용자를 수동으로 자신의 연락처 목록에 추가해야 합니다. 수동으로 추가된 사용자에게는 프레즌스 문제가 없습니다.</p>
멀티 레벨 그룹화	<p>멀티 레벨 그룹화는 그룹 동기화에 허용되지 않습니다.</p>

제한 사항	설명
그룹만 동기화	사용자 그룹과 사용자가 동일한 검색 기반에 있으면 그룹 전용 동기화가 허용되지 않습니다. 대신 사용자 그룹과 사용자는 동기화됩니다.
최대 사용자 그룹 수	Microsoft Active Directory 서버의 최대 15000개의 사용자 그룹을 Unified Communications Manager 데이터베이스와 동기화할 수 있습니다. 각 사용자 그룹에 1 ~ 200명의 사용자를 포함할 수 있습니다. Cisco Unified CM IM and Presence 관리 > 시스템 > 서비스 파라미터 창에서 정확한 수를 설정할 수 있습니다. 데이터베이스에서 최대 사용자 계정 수는 160,000을 초과할 수 없습니다.
사용자 그룹 마이그레이션	사용자 그룹을 한 조직 단위에서 다른 조직 단위로 이동하는 경우 원래 단위에서 전체 동기화를 수행한 후에 새 단위에서 전체 동기화를 수행해야 합니다.
로컬 그룹	로컬 그룹은 지원되지 않습니다. Microsoft Active Directory에서 동기화된 그룹만 지원됩니다.
IM and Presence 서비스 노드에 할당되지 않은 그룹 구성원	IM and Presence 서비스 노드에 할당되지 않은 그룹 구성원은 연락처 목록에 프렌즈 풍선이 회색으로 표시됩니다. 그러나 연락처 목록에 허용된 최대 사용자 수를 계산할 때 이 구성원이 고려됩니다.
Microsoft Office Communication Server에서 마이그레이션	Microsoft Office Communication Server에서 마이그레이션하는 동안 사용자가 IM and Presence 서비스 노드로 완전히 마이그레이션되어야 엔터프라이즈 그룹 기능이 지원됩니다.
LDAP 동기화	동기화가 진행되는 동안 LDAP 디렉터리 구성 창에서 동기화 옵션을 변경하면 기존 동기화는 영향을 받지 않습니다. 예를 들어 동기화가 진행 중일 때 동기화 옵션을 사용자 및 그룹에서 사용자로 만으로 변경하면 사용자와 그룹 동기화가 계속됩니다.
Edge를 통한 그룹 검색 기능	이 릴리스에서는 Edge를 통한 그룹 검색 기능이 제공되지만 완전히 테스트되지 않았습니다. 따라서 Edge를 통한 그룹 검색을 완벽하게 지원할 수는 없습니다. 향후 릴리스에서는 완벽한 지원이 제공될 것으로 예상됩니다.
Cisco 클러스터 간 동기화 에이전트 서비스 주기적 동기화	그룹 이름이나 그룹 구성원 이름이 외부 LDAP 디렉터리에서 업데이트되면 주기적 Cisco Intercluster 동기화 에이전트 서비스 동기화 후에만 Cisco Jabber 연락처 목록에서 업데이트됩니다. 일반적으로 Cisco 클러스터 간 동기화 에이전트 서비스 동기화는 30분마다 발생합니다.

제한 사항	설명
LDAP 구성에서 다른 동기화 계약을 통해 사용자와 사용자 그룹 동기화	<p>사용자 및 사용자 그룹이 동일한 동기화 계약의 일부로 Cisco Unified Communications Manager 데이터베이스에 동기화된 경우 동기화 후 Cisco Unified Communications Manager 데이터베이스에서 사용자 및 그룹 연결이 예정대로 업데이트됩니다. 그러나 사용자 및 사용자 그룹이 다른 동기화 계약의 일부로 동기화된 경우 첫 번째 동기화 후 사용자와 그룹이 데이터베이스에 연결되지 않을 수 있습니다. 데이터베이스의 사용자 및 그룹 연결은 동기화 계약이 처리되는 순서에 따라 다릅니다. 사용자가 그룹보다 먼저 동기화되는 경우 그룹이 연결을 위해 데이터베이스에서 사용 가능하지 않을 수 있습니다. 이 경우 그룹과의 동기화 계약이 사용자와의 동기화 계약 이전에 예약되도록 해야 합니다. 그렇지 않으면 그룹이 데이터베이스와 동기화된 후 사용자는 사용자 및 그룹으로 설정된 동기화 유형을 통해 다음 수동 또는 정기 동기화 후에 그룹과 연결됩니다. 계약 동기화 유형이 사용자 및 그룹으로 설정된 경우에만 사용자 및 해당 그룹 정보가 매핑됩니다.</p>
엔터프라이즈 그룹에 대한 테스트된 OVA 정보	<p>테스트된 시나리오</p> <p>두 클러스터인 클러스터 A와 클러스터 B를 포함한 interCluster 구축에서:</p> <p>클러스터 A는 Active Directory에서 동기화된 160K의 사용자 중 IM and Presence 서비스에 대해 15K OVA와 15K 사용자가 활성화됩니다. 15K OVA 클러스터의 사용자당 테스트 및 지원되는 평균 기업 그룹 수는 13개의 엔터프라이즈 그룹입니다.</p> <p>클러스터 B는 Active Directory에서 동기화된 160K의 사용자 중 IM and Presence 서비스에 대해 25K OVA와 25K 사용자가 활성화됩니다. 25K OVA 클러스터의 사용자당 테스트 및 지원되는 평균 기업 그룹 수는 8개의 엔터프라이즈 그룹입니다.</p> <p>사용자 등록 명부에 있는 사용자의 개인 연락처와 사용자 등록 명부에 있는 기업 그룹의 연락처의 테스트되고 지원되는 합계는 200보다 작거나 같습니다.</p> <p>참고 클러스터가 2개 이상인 환경에서는 이러한 번호가 지원되지 않습니다.</p>
연락처 목록 내보내기	<p>벌크 관리 > 연락처 목록 > 연락처 목록 내보내기를 사용하여 사용자의 연락처 목록을 내보낼 경우 연락처 목록 CSV 파일에는 Jabber 클라이언트에 있던 엔터프라이즈 그룹의 세부 정보는 포함되지 않습니다.</p>



XIII 부

디바이스 관리

- 헤드셋 및 액세서리 관리, 721 페이지
- 헤드셋 서비스, 739 페이지
- IVR 및 전화 서비스를 사용한 기본 전화 마이그레이션, 749 페이지
- 비디오 엔드포인트 관리, 771 페이지



55 장

헤드셋 및 액세서리 관리

- 헤드셋 및 액세서리 관리 개요, 721 페이지
- 헤드셋 및 액세서리 관리를 위한 기능 호환성, 721 페이지
- 워크플로: 헤드셋 서비스 가용성 구성, 723 페이지
- 헤드셋 및 액세서리 템플릿 관리, 728 페이지
- 펌웨어 관리, 732 페이지
- 헤드셋 및 액세서리 재고 목록 관리, 733 페이지
- 헤드셋 및 액세서리 문제 해결 및 진단, 737 페이지

헤드셋 및 액세서리 관리 개요

헤드셋 및 액세서리 관리는 Cisco 헤드셋 배포를 개선하여 관리자가 Cisco Unified Communications Manager에서 헤드셋 서비스 가용성을 관리하도록 합니다. Cisco Unified CM 관리에서 관리자는 다음을 수행할 수 있습니다.

- 무선 전원 범위, 오디오 대역폭 및 블루투스 설정/해제와 같은 헤드셋 설정을 원격으로 구성합니다.
- 헤드셋 또는 액세서리 펌웨어를 정의하고 제어합니다.
- 배포에 있는 모든 헤드셋 및 액세서리의 세부 재고 목록을 얻습니다.
- 원격 PRT, CMR(통화 관리 레코드)의 헤드셋 메트릭 및 경보가 있는 헤드셋을 진단하고 문제 해결합니다.

헤드셋 및 액세서리 관리를 위한 기능 호환성

Cisco 헤드셋 및 액세서리 관리는 다음 릴리스의 Unified Communications Manager에서 지원됩니다.

- 12.x 릴리스용 릴리스 12.5(1)SU4

Unified Communications Manager 버전과 함께, 기능 지원은 Cisco 헤드셋 및 액세서리, Cisco IP 전화기 및 Cisco Jabber의 펌웨어 버전에 따라 달라집니다. 다음 표에는 사용 중인 헤드셋 및 액세서리, 전화

기 및 Unified Communications Manager 버전에 따라 사용 가능한 헤드셋 및 액세서리 관리 기능이 나열되어 있습니다.



참고 Cisco 헤드셋 및 액세서리 관리 기능은 12.0(x) 또는 12.5(1)에서 지원되지 않습니다. 이전 버전의 경우, defaultheadsetconfig.json 구성 파일 및 TFTP를 통해 IP 전화기에 대한 헤드셋 및 액세서리 구성 템플릿을 수동으로 전송하는 기능이 제한적으로 지원될 수 있습니다. 자세한 내용은 헤드셋 관리 지침서를 참조하십시오.

표 61: Cisco IP 전화기에 대한 헤드셋 서비스 가능성 기능

서비스 가능성 기능	Unified CM 12.5(1) 또는 이전 + 전화기 펌웨어 12.1(1) 또는 이전	Unified CM 12.5(1)SU1 이상** + 전화기 펌웨어 12.1(1) 또는 이전	Unified CM 12.5(1) 또는 이전 + 전화기 펌웨어 12.5(1)	Unified CM 12.5(1)SU1 이상** + 전화기 펌웨어 12.5(1)	Unified CM 12.5(1) 또는 이전 + 전화기 펌웨어 12.5(1) SR3	Unified CM 12.5(1)SU1 이상** + 전화기 펌웨어 12.5(1)SR3
수동 원격 구성	—	—	X	해당 없음	X	—
Unified CM의 헤드셋 펌웨어 업그레이드	—	—	—	—	—	X
Unified CM을 통한 원격 헤드셋 및 액세서리 구성	—	—	—	—	—	X
Unified CM의 헤드셋 및 액세서리 재고 목록	—	—	—	—	—	X*
전화기 UI에 대한 구성 재설정	—	—	—	—	X	X
헤드셋 통화 관리 레코드(CMR)	—	—	—	—	—	X*

- *이 기능은 헤드셋 펌웨어 1.5 이상이 있는 헤드셋에서만 사용할 수 있습니다.
- **이 기능은 12.0.x 및 12.5(1) 릴리스에서는 지원되지 않습니다.
- 해당 없음 이전 버전에서 Unified CM 12.5(1) 이상으로 업그레이드하는 경우 대부분의 Cisco IP 전화기는 자동으로 전화기 펌웨어 12.5(1) SR3 이상으로 업그레이드됩니다.

표 62: Cisco Jabber용 헤드셋 서비스 가능성 기능

서비스 가능성 기능	Unified CM 12.5(1) 또는 이전 + Jabber 버전 12.5(1) 또는 이전	Unified CM 12.5(1)SU1 이상** + Jabber 버전 12.5(1) 또는 이전	Unified CM 12.5(1) 또는 이전 + Jabber 버전 12.6(1)	Unified CM 12.5(1) 이상** + Jabber 버전 12.6(1)	Unified CM 12.5(1) 또는 이전 + Jabber 버전 12.6(1) MR	Unified CM 12.5(1) 이상** + Jabber 버전 12.6(1)MR
Unified CM을 통한 헤드셋 펌웨어 업그레이드	—	—	—	—	—	X
Unified CM을 통한 원격 헤드셋 및 액세서리 구성	—	—	—	X	—	X
Unified CM의 헤드셋 및 액세서리 재고 목록	—	—	—	X*	—	X*
로컬 구성 재설정	—	—	—	—	X	X
로컬 UI 구성	—	—	X	X	X	X
로컬 헤드셋 및 액세서리 버전 표시	—	—	—	—	X	X

- * 이 기능은 헤드셋 펌웨어 1.5 이상이 있는 헤드셋만 검색할 수 있습니다.
- **이 기능은 12.0.x 및 12.5(1) 릴리스에서는 지원되지 않습니다.

타사 헤드셋 및 액세서리 지원

타사 헤드셋 또는 액세서리를 구축하는 경우에는 Unified Communications Manager가 Cisco Unified CM 관리 인터페이스에서 바로 타사 헤드셋 또는 액세서리에 대한 제한된 정보를 사용하여 헤드셋 및 액세서리 재고 목록 관리를 지원합니다. Unified Communications Manager는 헤드셋 또는 액세서리 구성 템플릿, 펌웨어, 진단 및 타사 헤드셋 용 헤드셋 CMR을 지원하지 않습니다.

워크플로: 헤드셋 서비스 가용성 구성

Cisco 헤드셋 서비스 가용성 기능의 설정을 안내하는 다음 워크플로를 사용합니다.

이 워크플로를 완료한 후에는 헤드셋 또는 액세서리 설정을 구성하고, 헤드셋 또는 액세서리 최신 펌웨어 로드를 유지 관리하고, 사용자에게 헤드셋 또는 액세서리를 연결하고, 헤드셋 기반 Extension Mobility를 활성화하고, 재고 목록을 유지할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	Cisco 헤드셋 서비스 활성화, 724 페이지	Cisco Unified Serviceability에서 Cisco 헤드셋 서비스를 켭니다.
단계 2	헤드셋 COP 파일 준비, 725 페이지	COP 파일을 사용하여 최신 헤드셋/액세서리 펌웨어를 설치하고 업그레이드해야 합니다.
단계 3	헤드셋 사용자를 위한 사용자 프로파일 구성, 726 페이지	사용자에 대한 사용자 프로파일을 아직 구성하지 않은 경우 이 절차를 사용하여 프로파일을 설정합니다. 모든 사용자 프로파일이 구성된 경우 이 작업을 건너뛸 수 있습니다.
단계 4	최종 사용자에게 사용자 프로파일 적용, 727 페이지	최종 사용자에게 사용자 프로파일을 할당합니다. 이미 사용자 프로파일을 할당한 경우에는 이 작업을 건너뛸 수 있습니다.
단계 5	헤드셋 및 액세서리 템플릿 구성, 731 페이지	Cisco 헤드셋 및 액세서리 템플릿에 대한 기본 설정 및 펌웨어를 구성합니다. 해당 사용자 프로파일을 사용하는 사용자가 이 헤드셋 및 액세서리 템플릿에 할당되도록 사용자 프로파일을 템플릿에 연결합니다.
단계 6	헤드셋 및 액세서리 재고 목록 보기, 735 페이지	Cisco Unified CM 인터페이스를 통해 배포된 헤드셋 및 액세서리 재고 목록을 볼 수 있는지 확인합니다.

Cisco 헤드셋 서비스 활성화

Cisco Unified CM 관리 인터페이스를 통해 Cisco 헤드셋 및 액세서리를 관리하기 전에 Cisco Unified Communications Manager 서비스 가용성에서 **Cisco** 헤드셋 서비스를 켜십시오.



참고 Cisco CallManager 서비스가 이미 실행 중인 경우 모든 Unified Communications Manager 노드에서 Cisco 헤드셋 서비스를 활성화해야 합니다. Cisco Unified CM 관리 인터페이스를 사용하여 헤드셋 또는 액세서리를 관리하려는 Unified Communications Manager 노드에서 Cisco 헤드셋 서비스를 활성화해야 합니다. Cisco 헤드셋 서비스를 활성화하면 Cisco CallManager 서비스가 자동으로 활성화됩니다. 필요하지 않은 경우 Cisco CallManager 서비스를 비활성화합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 **Cisco Unified Serviceability**로 이동하고 이동을 클릭합니다.

단계 2 도구 > 서비스 활성화를 선택합니다.

단계 3 CM 서비스 섹션에서 **Cisco** 헤드셋 서비스 확인란을 선택하고 저장을 선택합니다.

다음에 수행할 작업

헤드셋 COP 파일을 준비합니다.

헤드셋 COP 파일 준비

COP 파일을 사용하여 최신 헤드셋 펌웨어를 설치하고 업그레이드할 수 있습니다. 헤드셋 COP 파일에는 구성 데이터와 함께 다양한 헤드셋 또는 액세서리 모델의 모든 펌웨어 버전이 포함되어 있습니다.



참고 COP 파일을 설치하기 전에 Cisco 헤드셋 서비스가 켜져 있고 실행 중인지 확인합니다.

헤드셋 COP 파일이 Unified Communications Manager의 모든 노드에 설치되어 있는지 확인합니다.

1. Cisco 헤드셋 또는 액세서리 사용을 시작하려면 먼저 COP 파일을 Unified Communications Manager 시스템에 설치하거나 업그레이드합니다.

헤드셋 또는 액세서리를 엔드포인트에 연결하면 헤드셋 및 액세서리 템플릿 구성 변경 사항이 적용됩니다. Unified Communications Manager에서 헤드셋 및 액세서리 템플릿 구성에 대한 업데이트를 수행하는 경우 엔드포인트는 연결된 헤드셋 또는 액세서리에 이러한 구성 업데이트를 적용합니다.

모든 구성 업데이트는 COP 파일의 헤드셋 및 액세서리 템플릿 버전에 따라 달라집니다. 최신 COP 파일에서 헤드셋 및 액세서리 템플릿 버전이 더 높을 경우에는 Unified Communications Manager의 구성 파일이 업데이트됩니다. COP 파일의 구성 파일이 업그레이드된 경우, Unified Communications Manager의 헤드셋 및 액세서리 템플릿 버전은 템플릿 버전에 관계없이 업데이트되며, 그 반대의 경우도 마찬가지입니다. 다음 목록에서는 COP 파일 업그레이드 후의 다양한 템플릿 버전 업데이트 시나리오를 보여줍니다.

- Unified Communications Manager가 현재 헤드셋 및 액세서리 템플릿 버전 1-10과 함께 설치되어 있고, 헤드셋 및 액세서리 템플릿 버전 1-12가 있는 Unified Communications Manager 서버를 업그레이드하는 경우, 선택한 헤드셋 및 액세서리 템플릿 버전은 1-12입니다. Unified Communications Manager는 더 높은 헤드셋 및 액세서리 템플릿 버전을 선택합니다.
- Unified Communications Manager가 현재 헤드셋 및 액세서리 템플릿 버전 1-10과 함께 설치되어 있고, 헤드셋 및 액세서리 템플릿 버전 1-9가 있는 Unified Communications Manager 서버를 업그레이드하는 경우, 선택한 헤드셋 및 액세서리 템플릿 버전은 1-10입니다. Unified Communications Manager는 더 높은 헤드셋 및 액세서리 템플릿 버전을 선택합니다.
- Unified Communications Manager가 현재 헤드셋 및 액세서리 템플릿 버전 1-10과 함께 설치되어 있고, 헤드셋 및 액세서리 템플릿 버전 1-12가 있는 COP 파일을 설치하는 경우, 선택한 헤드셋 및 액세서리 템플릿 버전은 1-12입니다. COP 파일을 사용하여 설치된 헤드셋 및 액세서리 템플릿이 선호되는 옵션입니다.

- Unified Communications Manager가 현재 헤드셋 및 액세서리 템플릿 버전 1-10과 함께 설치되어 있고, 헤드셋 및 액세서리 템플릿 버전 1-9가 있는 COP 파일을 설치하는 경우, 선택한 헤드셋 및 액세서리 템플릿 버전은 1-9입니다. COP 파일을 사용하여 설치된 헤드셋 및 액세서리 템플릿이 선호되는 옵션입니다.
- 헤드셋 템플릿 및 액세서리 버전 1-12가 있는 COP 파일이 설치되어 있고, 헤드셋 및 액세서리 템플릿 버전 1-10이 있는 Unified Communications Manager 서버를 업그레이드하는 경우, 선택한 헤드셋 및 액세서리 템플릿 버전은 1-12입니다. Unified Communications Manager는 더 높은 헤드셋 및 액세서리 템플릿 버전을 선택합니다.

헤드셋 사용자를 위한 사용자 프로파일 구성

사용자에 대한 사용자 프로파일을 아직 구성하지 않은 경우 이 절차를 사용하여 프로파일을 설정합니다. 헤드셋 및 액세서리 템플릿은 사용자 프로파일을 통해 사용자에게 할당됩니다. 이미 사용자 프로파일을 구성한 경우에는 이 작업을 건너뛸 수 있습니다.



참고 배포 요구에 따라 서로 다른 사용자 그룹에 대한 여러 사용자 프로파일을 구성합니다. 기본적으로 모든 사용자 프로파일은 시스템 기본 헤드셋 템플릿에 할당됩니다. 헤드셋 및 액세서리 템플릿을 구성할 때 사용자 정의된 템플릿에 이러한 템플릿을 할당할 수 있습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 사용자 설정 > 사용자 프로파일.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 사용자 프로파일의 이름 및 설명을 입력합니다.
- 단계 4 사용자의 데스크폰, 모바일 및 데스크탑 디바이스 및 원격 대상/디바이스 프로파일에 적용할 유니버설 디바이스 템플릿을 할당합니다.
- 단계 5 이 사용자 프로파일의 사용자에게 대한 전화 회선에 적용할 범용 회선 템플릿을 할당합니다.
- 단계 6 이 사용자 프로파일의 사용자가 자신의 전화기를 프로비저닝하는 데 셀프 프로비저닝 기능을 사용할 있도록하려면 다음을 수행합니다.
 - a) 최종 사용자에게 자신의 전화기 프로비저닝 허용 확인란을 선택합니다.
 - b) 최종 사용자가 이렇게 많은 전화기를 가지고 있으면 프로비저닝 제한 필드에 사용자가 프로비저닝하도록 허용되는 전화기의 최대 수를 입력합니다. 최대값은 20입니다.
- 단계 7 이 사용자 프로파일과 연결된 Cisco Jabber 사용자가 모바일 및 원격 액세스 기능을 사용할 수 있도록하려면 모바일 및 원격 액세스 활성화 확인란에 체크 표시합니다.

참고 기본적으로 이 확인란은 선택되어 있습니다. 이 확인란을 선택 취소하면 **Jabber** 정책 섹션이 비활성화되고 기본적으로 서비스 클라이언트 없음 정책 옵션이 선택됩니다.

참고 이 설정은 Cisco Jabber 사용자의 경우에만 필수입니다. 비 Jabber 사용자는 이 설정이 없어도 모바일 및 원격 액세스를 사용할 수 있습니다. 모바일 및 원격 액세스 기능은 Jabber 모바일 및 원격 액세스 사용자에게 대해서만 적용 가능하며, 다른 엔드포인트 또는 클라이언트에게는 적용되지 않습니다.

단계 8 이 사용자 프로파일에 대해 Jabber 정책을 할당합니다. Jabber 데스크톱 클라이언트 정책 및 Jabber 모바일 클라이언트 정책 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 서비스 없음 - 이 정책은 모든 Cisco Jabber 서비스에 대한 액세스를 비활성화합니다.
- IM & 프레즌스만 해당—이 정책은 인스턴트 메시징 및 프레즌스 기능을 활성화합니다.
- IM & 프레즌스, 음성 및 영상 통화—이 정책은 음성 또는 영상 디바이스가 있는 모든 사용자에게 대해 인스턴트 메시징, 프레즌스, 음성 메일 및 전화 회의 기능을 활성화합니다. 이것이 기본 옵션입니다.

참고 Jabber 데스크톱 클라이언트는 Windows용 Cisco Jabber와 Mac용 Cisco Jabber 사용자를 포함합니다. Jabber 모바일 클라이언트는 iPad 및 iPhone용 Cisco Jabber 사용자와 Android용 Cisco Jabber 사용자를 포함합니다.

단계 9 사용자가 Unified Communications 셀프 서비스 포털을 통해 Extension Mobility 또는 클러스터 간 Extension Mobility에 대한 최대 로그인 시간을 설정하도록 허용하려면 최종 사용자가 **Extension Mobility**를 최대 로그인 시간을 설정하도록 허용 확인란을 선택합니다.

참고 기본적으로 최종 사용자가 **Extension Mobility**를 최대 로그인 시간을 설정하도록 허용 확인란은 선택 해제되어 있습니다.

단계 10 저장을 클릭합니다.

최종 사용자에게 사용자 프로파일 적용

사용자가 생성한 사용자 프로파일에 연결합니다. 사용자 프로파일은 최종 사용자와 연결되어야 하며, 제어되는 디바이스 아래에 디바이스 MAC을 추가하여 헤드셋 및 액세서리 템플릿 구성 변경 사항을 적용해야 합니다.



참고 이미 모든 사용자를 해당 사용자 프로파일에 할당한 경우 이 작업을 건너뛸 수 있습니다.

프로시저

단계 1 Cisco Unified Communications Manager 데이터베이스에 새 최종 사용자를 수동으로 추가하려면 다음을 수행하십시오.

- Cisco Unified CM 관리에서 사용자 관리 > 최종 사용자를 선택합니다.
- 새로 추가를 클릭합니다.
- 사용자 ID 및 성을 입력합니다.
- 드롭다운 목록에서 사용자 순위를 선택합니다.

- e) 최종 사용자 구성 창에서 필드를 완료합니다. 필드 설명은 온라인 도움말을 참조하십시오.
- f) 저장을 클릭합니다.

단계 2 최종 사용자를 디바이스와 연결하려면 다음을 수행합니다.

- a) Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.
- b) Cisco IP 전화기 또는 디바이스를 선택합니다.
- c) 디바이스 정보 아래에서 사용자를 소유자로 선택하고 소유자 사용자 ID를 선택합니다.
- d) 저장을 클릭하고 구성 변경 사항을 적용하려면 구성 적용을 클릭합니다.

헤드셋 및 액세서리 템플릿 관리

헤드셋 및 액세서리 템플릿을 Cisco Unified Communications Manager의 사용자 프로파일에 할당하여 사용자에게 대한 기본 헤드셋 설정을 구성할 수 있습니다. 헤드셋 및 액세서리 템플릿에서는 사용자 프로파일을 연결하는 옵션을 제공합니다. Unified Communications Manager는 두 가지 유형의 헤드셋 및 액세서리 템플릿을 지원합니다.

표준 기본 헤드셋 구성 템플릿

이 템플릿은 모든 헤드셋 및 액세서리 모델 시리즈에 대한 공장 기본 설정을 포함하는 시스템 기본 템플릿입니다. 이 템플릿에는 모든 헤드셋 또는 액세서리 모델 시리즈에 대해 시스템에 설치된 최신 헤드셋 및 액세서리 펌웨어가 지원하는 헤드셋 또는 액세서리 설정이 포함되어 있습니다. 프로파일 구성 설정을 변경할 수는 있지만 기본 설정을 편집할 수는 없습니다.



참고 Cisco Unified Serviceability 사용자 인터페이스에서 **Cisco** 헤드셋 서비스가 활성화된 경우에만 표준 기본 헤드셋 구성 템플릿이 생성됩니다.

기본적으로 관리자가 이러한 사용자 프로파일을 사용자 정의된 헤드셋 템플릿에 연결하지 않는 한, 모든 사용자 프로파일은 표준 헤드셋 템플릿에 연결됩니다. 표준 기본 헤드셋 템플릿의 복사본을 만들어 헤드셋 또는 액세서리 펌웨어 버전을 포함한 매개 변수의 사용자 지정 값으로 사용자 지정 템플릿을 만들 수 있습니다.

시스템 생성 사용자 지정 헤드셋 템플릿

전체 Cisco 헤드셋 서비스 가용성 기능을 지원하지 않는 일부 이전 릴리스에서는 관리자가 defaultheadsetconfig.json 구성 파일 및 TFTP를 통해 헤드셋 및 액세서리 템플릿을 수동으로 구성하고 배포할 수 있습니다. 이전 릴리스에서 이 방법을 사용한 다음 이 릴리스로 업그레이드하면 구성 파일이 시스템 생성 사용자 정의 헤드셋 템플릿으로 변환되어 헤드셋 및 액세서리 구성 템플릿 창에 표시됩니다. 업그레이드를 수행하면 구성 파일을 사용하는 사용자 및 디바이스가 이 사용자 지정 템플릿에 연결됩니다.

사용자 지정 헤드셋 설정 템플릿

Cisco Unified CM 관리에서 디바이스 > 헤드셋 및 액세서리 > 헤드셋 및 액세서리 템플릿 창을 사용하여 구축 요구 사항에 따라 헤드셋 및 액세서리 템플릿을 사용자 정의합니다. 동일한 템플릿의 다른 모델에 다른 헤드셋 파라미터를 할당할 수 있습니다. 다른 헤드셋 또는 액세서리 모델에 다른 펌웨어 로드를 할당할 수도 있습니다. 사용자 프로파일을 사용자 지정 헤드셋 템플릿에 연결하여 사용자 지정 헤드셋 또는 액세서리 설정을 특정 사용자 집합에 할당할 수 있습니다.

표 63: 헤드셋 및 액세서리 구성 템플릿 설정

필드	설명
헤드셋 및 액세서리 템플릿 구성	
이름	헤드셋 및 액세서리 템플릿을 식별하는 고유한 이름을 입력합니다.
설명	템플릿 사용을 식별하는 설명을 입력합니다.
모델 및 펌웨어 설정	
모델 시리즈 선택	디바이스에 안정적인 고품질 사운드를 제공하는, 지원되는 헤드셋 또는 액세서리 모델을 선택합니다.
추가	표준 템플릿의 경우 헤드셋 또는 액세서리 모델의 기본 사전 정의 펌웨어 버전 및 설정을 볼 수 있습니다. 기본값은 편집할 수 없습니다. 사용자 정의 템플릿의 경우 추가를 클릭하여 새 헤드셋 또는 액세서리 모델 및 관련 설정을 추가합니다. 같은 템플릿에 있는 다른 기존 헤드셋 또는 액세서리 모델은 추가할 수 없습니다. 사용자 정의 템플릿에는 다른 헤드셋 또는 액세서리 모델을 추가할 수 있습니다. 하지만 헤드셋 또는 액세서리 모델당 펌웨어 하나만 사용할 수 있습니다. 헤드셋 매개 변수에 대한 자세한 내용은 아래의 "헤드셋 구성 매개 변수" 표를 참조하십시오. 표준 기본 헤드셋 템플릿 구성의 경우 헤드셋 COP 파일을 설치하여 설정만 편집할 수 있습니다.
펌웨어	필요한 펌웨어 버전을 선택합니다. <ul style="list-style-type: none"> 현재 버전으로 유지 - 헤드셋 또는 액세서리를 기존 펌웨어 버전(즉, 헤드셋 또는 액세서리 펌웨어 버전을 최신 펌웨어 버전으로 업그레이드하지 않음)으로 유지하려면 이 옵션을 선택합니다. 최신 - 헤드셋 또는 액세서리 펌웨어 버전을 시스템의 최신 펌웨어 버전으로 업그레이드하려면 이 옵션을 선택합니다.
삭제	사용자 정의 템플릿의 경우 삭제를 클릭하여 헤드셋 및 액세서리 템플릿에서 헤드셋 또는 액세서리 모델을 제거합니다.
프로필 구성	

필드	설명
사용 가능한 사용자 프로파일	<p>이 헤드셋 및 액세서리 템플릿과 함께 사용할 수 있는 구성된 사용자 프로파일을 나열합니다.</p> <p>사용자 프로파일을 이 템플릿에 연결하려면 프로파일을 선택하고 아래쪽 화살표를 클릭하여 할당된 사용자 프로파일로 템플릿을 옮깁니다.</p> <p>참고 기본적으로 모든 사용자 프로파일은 표준 기본 헤드셋 구성 템플릿에 할당됩니다. 사용자 프로파일을 다른 템플릿에 연결하려면 새 템플릿을 만들고 사용자 프로파일을 새 템플릿에 할당합니다.</p>
할당된 사용자 프로파일	<p>이 헤드셋 및 액세서리 구성 템플릿을 사용하게 될 사용자 프로파일을 나열합니다. 이 프로파일에 할당된 사용자의 경우, 등록 과정에서 헤드셋 및 액세서리 구성 템플릿의 설정이 Cisco 헤드셋 또는 액세서리에 적용됩니다.</p> <p>화살표를 클릭하여 Available User Profiles(사용 가능한 사용자 프로파일) 목록에 있는 새 사용자 프로파일을 추가합니다.</p>

다음 표에서는 각 헤드셋 및 액세서리 템플릿의 파라미터에 대해 설명합니다.



참고 온프레미스 및 다중 플랫폼 헤드셋 서비스 가능성 기능은 RJ-9 연결을 통해 사용할 수 없습니다.

표 64: Cisco 헤드셋 300 시리즈 파라미터

파라미터	범위	기본값	부재
펌웨어 소스	UCM 또는 Cisco Cloud에서 허용(펌웨어가 업그레이드 전용), UCM 전용으로 제한(펌웨어가 업그레이드 또는 다운그레이드될 수 있음)	UCM 또는 Cisco Cloud에서 허용	<p>헤드셋의 펌웨어 업그레이드 소스를 제어합니다.</p> <p>기본적으로 사용자는 Unified CM에 연결된 디바이스 및 소프트웨어 또는 클라우드 연결 디바이스 또는 소프트웨어를 통해 헤드셋을 업그레이드할 수 있습니다. Unified CM 소스를 통해서만 펌웨어 변경을 허용하도록 헤드셋을 제한할 수 있습니다.</p>
스피커 볼륨	0 - 15	7	<p>헤드셋의 사운드 수준을 제어합니다. 15는 큰 반면 0은 매우 낮습니다.</p> <p>사무실 환경에서의 주변 소음에 기반하여 이 설정을 구성합니다.</p>

파라미터	범위	기본값	부재
마이크 게인	더 작게 - 더 크게	기본값	통화 중 다른 사람에게 소리가 얼마나 크게 들리는지 제어합니다. 더 작게는 사용자가 조용한 소리를 내는 것을 의미하고 더 크게는 크게 소리를 내는 것을 의미합니다. 사무실 환경에서의 주변 소음에 기반하여 이 설정을 구성합니다.
측음	꺼짐 - 높음	낮음	헤드셋을 통해 들을 수 있는 사용자 자신의 목소리 크기를 제어합니다. 꺼짐은 측음을 해제하고 높음은 사용자가 헤드셋 마이크에서 자신의 음성을 훨씬 더 선명하게 들을 수 있다는 것을 의미합니다.
이퀄라이저	가장 따뜻함 - 가장 밝음	기본값	이퀄라이저 설정을 제어합니다. 따뜻함 설정은 헤드셋에서 더 많은 저음을 들을 수 있고, 밝음 설정은 더 많은 고음을 들을 수 있음을 의미합니다.

헤드셋 및 액세서리 템플릿 구성

이 절차를 사용하여 Cisco 헤드셋 및 액세서리에 적용할 수 있는 사용자 정의된 설정으로 헤드셋 및 액세서리 템플릿을 구성합니다. 사용자 지정 템플릿을 만들거나 시스템 정의 표준 기본 헤드셋 템플릿을 사용할 수 있습니다.



참고 표준 기본 헤드셋 구성 템플릿은 시스템 정의 템플릿입니다. 표준 기본 헤드셋 템플릿에 새 사용자 프로파일을 할당할 수 있지만 템플릿을 편집할 수는 없습니다. 기본적으로 모든 사용자 프로파일은 이 템플릿에 할당됩니다. 이 템플릿에서 사용자 프로파일의 연결을 해제하려면 프로파일을 새 템플릿에 할당해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 헤드셋 및 액세서리 > 헤드셋 및 액세서리 템플릿을 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 기존 템플릿을 편집하려면 템플릿을 선택합니다.
- 새 템플릿을 만들려면 기존 템플릿을 선택하고 복사를 클릭합니다. 기존 설정이 새 템플릿에 적용됩니다.

단계 3 템플릿에 대한 이름 및 설명을 추가합니다.

- 단계 4 모델 및 펌웨어 설정] 아래에서 이 템플릿에 적용할 사용자 지정된 헤드셋 및 액세서리 설정을 할당합니다. 새 설정을 추가하려면 추가 버튼을 클릭하고 설정을 구성합니다.
- 단계 5 위쪽 및 아래쪽 화살표를 사용하여 이 템플릿을 할당하려는 사용자 프로파일을 할당된 사용자 프로파일 목록 상자로 이동합니다. 해당 프로파일에 할당된 모든 사용자도 이 헤드셋 및 액세서리 템플릿에 할당됩니다.
- 단계 6 저장을 클릭합니다.
- 단계 7 기본값으로 설정 버튼을 사용하여 기본 템플릿 설정으로 돌아갑니다.
- 단계 8 구성 적용을 클릭합니다.

표준 기본 헤드셋 구성 템플릿의 경우 구성 적용 버튼이 다음 항목에 적용됩니다.

- 할당된 사용자 프로파일 목록에 추가한 사용자가 소유한 디바이스
- 익명의 디바이스

사용자 지정된 헤드셋 구성 템플릿의 경우 구성 적용 버튼은 할당된 사용자 프로파일 목록에 추가한 사용자가 소유한 디바이스에만 적용됩니다.

펌웨어 관리

Unified Communications Manager에 연결된 대부분의 전화기 및 디바이스는 Cisco 헤드셋 500 시리즈 및 Cisco 헤드셋 700 시리즈를 지원합니다. 헤드셋 또는 액세서리를 전화기에 연결하기 전에 최신 전화기 펌웨어 릴리스 및 디바이스 패키지를 설치합니다. 헤드셋 또는 액세서리를 처음 연결하면 필요한 펌웨어를 다운로드하고 업그레이드 프로세스를 시작합니다.

지정된 헤드셋 또는 액세서리 모델의 경우 다음 두 가지 펌웨어 옵션이 지원됩니다.

- 현재 버전으로 유지 - 헤드셋 또는 액세서리를 기존 펌웨어 버전(즉, 헤드셋 또는 액세서리 펌웨어 버전을 최신 펌웨어 버전으로 업그레이드하지 않음)으로 유지하려면 이 옵션을 선택합니다.
- 최신 - 헤드셋 또는 액세서리를 업그레이드하거나 다운그레이드하려면 이 옵션을 선택합니다. 해당 펌웨어 또는 액세서리가 현재 헤드셋의 이전 릴리스인 경우에는 시스템에서 선택한 소프트웨어를 설치하고 실행합니다.

예를 들어, 최신으로 **1-5-1-10**을 선택하면 헤드셋 또는 액세서리에 현재 **1-5-1-9** 또는 **1-5-1-11**이 있는지 여부에 관계 없이 펌웨어가 헤드셋 또는 액세서리에 설치됩니다.

펌웨어 고려 사항

- 표준 헤드셋 템플릿에 할당된 사용자는 항상 최신 헤드셋 또는 액세서리 펌웨어와 설정을 수신합니다.
- 헤드셋 템플릿 구성에 표시된 설정(표준 및 사용자 지정 모두)은 항상 모든 헤드셋 및 액세서리 모델 시리즈에 대한 최신 펌웨어로 설정됩니다.

헤드셋 및 액세서리 재고 목록 관리

Cisco IP 전화기는 헤드셋 및 액세서리가 연결된 상태이거나 연결이 끊어진 상태에 있을 때마다 헤드셋 및 액세서리 재고 목록 데이터를 Unified Communications Manager에게 보냅니다. Unified Communications Manager는 이 서버에 배포된 모든 헤드셋 및 액세서리에 대한 재고 목록 요약 보고서 또는 사용자 지정 재고 목록 보고서를 생성할 수 있도록 재고 목록 데이터를 저장합니다.

보고서 정보에는 헤드셋 또는 액세서리 직렬 및 모델 번호, 도킹 스테이션 세부 정보, 펌웨어, 사용되는 구성 템플릿, 공급 업체 세부 정보, 디바이스에 대한 헤드셋 또는 액세서리 연결 상태 등이 포함됩니다.

헤드셋 및 액세서리 재고 목록

Cisco Unified CM 관리에서 디바이스 > 헤드셋 및 액세서리 > 헤드셋 및 액세서리 재고 목록 창을 사용하여 서버에 배포된 모든 헤드셋 및 액세서리의 전체 목록을 볼 수 있습니다. 이 정보를 사용하여 배포된 모든 헤드셋 및 액세서리에 대한 보고서를 생성할 수 있습니다. 디바이스의 일련 번호를 클릭하면 팝업 창에서 개별 헤드셋 및 액세서리의 세부 정보를 볼 수 있습니다.

표 65: 헤드셋 및 액세서리 재고 목록 설정

필드	설명
일련 번호	헤드셋 또는 액세서리의 일련 번호입니다. 이 번호는 개별 헤드셋 또는 액세서리마다 고유합니다. 참고 비 Cisco 헤드셋 또는 액세서리의 경우 디바이스 이름이 일련 번호로 사용됩니다. 여러 전화기에서 동일한 비 Cisco 헤드셋 또는 액세서리를 사용하면 중복 헤드셋 또는 액세서리 레코드가 생성됩니다. 참고 특정 헤드셋 또는 액세서리의 일련 번호를 찾는 방법에 대한 자세한 내용은 해당 헤드셋 또는 액세서리 모델에 대한 헤드셋 관리 지침서를 참조하십시오.
모델	헤드셋 또는 액세서리의 모델 번호입니다.
공급업체	공급업체 세부 정보를 표시합니다.
유형	헤드셋 연결 유형(유선, DECT 무선 또는 알 수 없음)을 나타냅니다.
펌웨어	헤드셋 또는 액세서리의 최신 펌웨어 로드를 표시합니다.
사용자	전화기 또는 디바이스를 사용하여 최종 사용자의 정보를 표시합니다.
연결된 전화기 소유자 사용자 ID	전화기 또는 디바이스를 사용하여 최종 사용자의 정보를 표시합니다. 연결된 헤드셋 또는 액세서리가 없을 경우 필드는 비어 있습니다.

필드	설명
헤드셋/액세서리 소유자	헤드셋 또는 액세서리의 일련 번호와 연결된 최종 사용자 정보를 표시합니다.
템플릿	헤드셋 또는 액세서리 구성 템플릿의 이름을 표시합니다.
상태(이후)	헤드셋 또는 액세서리 활동의 상태를 표시합니다. 연결됨 또는 연결 끊김 일 수 있습니다.
도크 모델	도킹 모델 스테이션의 유형을 표시합니다.
디바이스 이름	헤드셋 또는 액세서리가 연결된 디바이스의 이름입니다.
디바이스 모델	Cisco IP 전화기 또는 Cisco Jabber 모델 번호를 표시합니다. 예를 들어, CP-8865는 Cisco IP 전화기 모델입니다. CSF는 Mac용 Cisco Jabber 또는 Windows용 Cisco Jabber에 대한 디바이스 유형입니다.
소프트웨어 버전	사용된 소프트웨어의 최신 버전을 표시합니다. 전화기 펌웨어 또는 Jabber 소프트웨어 버전일 수 있습니다.
헤드셋/액세서리 경과 시간(일수)	헤드셋 또는 액세서리의 지속 기간을 표시합니다. 레코드가 삭제되면 헤드셋 또는 액세서리 지속 시간이 재설정됩니다.

헤드셋 및 액세서리 재고 목록 다운로드



중요 이 섹션은 12.5(1)SU4 및 릴리스 14 이후부터 적용할 수 있습니다.

Cisco Unified Communications Manager 관리에서 헤드셋 및 액세서리 > 헤드셋 및 액세서리 재고 목록 메뉴 경로에서 관련 링크 드롭다운 목록에서 헤드셋 및 액세서리 재고 목록 다운로드를 선택하여 CSV 파일 형식으로 헤드셋 및 액세서리의 세부 정보를 다운로드합니다.

이 정보를 사용하여 헤드셋 및 액세서리 사용, 배포에 있는 타사 헤드셋 및 헤드셋 새로 고침 등의 사용 사례에 대한 데이터를 분석할 수 있습니다.

헤드셋 및 액세서리 재고 목록 관리 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	헤드셋 및 액세서리 재고 목록 보기, 735 페이지	서버에 구축된 헤드셋 및 액세서리를 나열합니다.
단계 2	전화기 소유자를 헤드셋 또는 액세서리 소유자와 연결, 735 페이지	헤드셋이나 액세서리를 사용자에게 연결합니다.

헤드셋 및 액세서리 재고 목록 보기

서버에 배포된 모든 헤드셋 및 액세서리의 전체 목록을 볼 수 있습니다. 이 정보를 사용하여 배포된 모든 헤드셋 및 액세서리에 대한 보고서를 생성할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 헤드셋 및 액세서리 > 헤드셋 및 액세서리 재고 목록을 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 서버에 배포된 헤드셋의 전체 목록을 보려면 찾기를 선택합니다.
- 검색 상자에 하나 이상의 검색 조건을 입력하고 찾기를 선택합니다.

전화기 소유자를 헤드셋 또는 액세서리 소유자와 연결

이 절차를 사용하여 벌크 헤드셋 또는 액세서리를 사용자에게 연결할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 헤드셋 및 액세서리 > 헤드셋 및 액세서리 재고 목록

단계 2 서버에 구축된 헤드셋 또는 액세서리의 전체 목록을 보려면 찾기를 클릭합니다.

단계 3 모두 선택을 클릭하거나 필요한 일련 번호를 선택하고 전화기 소유자를 헤드셋/액세서리 소유자로 연결을 클릭하여 헤드셋이나 액세서리를 사용자에게 연결합니다.

참고 헤드셋이나 액세서리는 이미 연결되어 있거나 연결할 전화기 소유자가 없는 경우 연결할 수 없습니다. 헤드셋 또는 액세서리 연결은 페이지를 다시 로드한 후 "헤드셋/액세서리 소유자" 열에 표시됩니다.

최대 15개의 헤드셋 또는 액세서리를 특정 사용자에게 연결할 수 있습니다. 특정 사용자에게 대한 최대 제한에 도달하면 나머지 헤드셋이나 액세서리는 연결되지 않으며 오류가 표시됩니다.

단계 4 (선택 사항) 필요한 일련 번호를 선택하고 헤드셋/액세서리 소유자 연결 해제 를 클릭하여 선택한 사용자의 헤드셋 또는 액세서리 일련 번호를 연결 해제합니다.

참고 헤드셋이나 액세서리 소유자와 연결되지 않은 헤드셋 또는 액세서리는 연결을 해제할 수 없습니다.

단계 5 (선택 사항) 최종 사용자 구성 및 헤드셋 또는 액세서리 연결 세부 정보를 보려면 연결된 전화기 소유자 사용자 ID 또는 헤드셋/액세서리 소유자 열에서 사용자 이름 링크를 클릭합니다.

참고 최종 사용자 구성 창에 헤드셋 또는 액세서리 연결 및 연결 해제 세부 정보가 표시됩니다.

헤드셋 및 액세서리 재고 목록 요약

Cisco Unified CM 관리에서 디바이스 > 헤드셋 및 액세서리 > 헤드셋 및 액세서리 재고 목록 요약 창을 사용하여 헤드셋 및 액세서리 재고 목록 요약 창에서 구축된 헤드셋 및 액세서리의 집계 요약을 볼 수 있습니다.

모델별 헤드셋 및 액세서리 재고 목록

필드	설명
헤드셋/액세서리 모델	헤드셋 또는 액세서리의 모델 번호입니다.
수량	배포의 각 모델 유형에 대한 헤드셋 또는 액세서리 수를 나열합니다. 참고 수량 열의 링크를 클릭하면 모델 유형별로 필터링된 자세한 헤드셋 및 액세서리 재고 목록 페이지로 이동합니다.

상태별 헤드셋 및 액세서리 재고 목록

헤드셋/액세서리 모델, 활성, 비활성 또는 할당되지 않은 열의 하이퍼링크를 클릭하여 각 상태에 대한 자세한 헤드셋 및 액세서리 재고 목록 페이지로 이동합니다.

필드	설명
헤드셋/액세서리 모델	헤드셋 또는 액세서리의 모델 번호입니다.
활성화	최근 30일 이내에 헤드셋 또는 액세서리가 연결되었습니다.
비활성	최근 30일 이내에 헤드셋 또는 액세서리가 연결되지 않았습니다.
할당되지 않음	사용자 ID가 시스템에 없거나 인벤토리 레코드에 사용자 ID 매핑이 없습니다.

구축된 헤드셋 및 액세서리의 집계 요약 가져오기

헤드셋 및 액세서리 재고 목록 요약 창에서 구축된 헤드셋 및 액세서리의 집계 요약을 볼 수 있습니다.

프로시저

Cisco Unified CM 관리에서 디바이스 > 헤드셋 및 액세서리 > 헤드셋 및 액세서리 재고 목록 요약을 선택합니다.

모델 또는 헤드셋 및 액세서리 상태별로 헤드셋 및 액세서리 재고 목록 분석을 볼 수 있습니다.

헤드셋 및 액세서리 문제 해결 및 진단

Unified Communications Manager 또는 Cisco Unified Real-Time Monitoring Tool(RTMT)을 구성하여 Cisco IP 전화기에 연결된 헤드셋 또는 액세서리에 대한 PRT(문제 보고서 도구) 로그를 수집할 수 있습니다. PRT에는 통화 품질, 사용된 코덱, 오디오 설정, 무선 설정 및 경고 로그에 대한 데이터가 포함됩니다.

Unified Communications Manager는 헤드셋 및 액세서리에 대한 통화 진단 세부 정보를 저장합니다. Cisco IP 전화기는 Unified Communications Manager에서 CMR을 업데이트하기 위해 BYE 메시지 또는 BYE 메시지에 대한 200 OK 응답으로 Headset-Stat 헤더의 헤드셋 또는 액세서리 진단 데이터를 보냅니다.

Cisco IP 전화기는 헤드셋 및 액세서리 진단 데이터를 Unified Communications Manager와 공유하며, 이 정보는 CMR 레코드에 있는 다음 필드에 저장됩니다.

- SN—헤드셋 또는 액세서리의 일련 번호입니다.
- 매트릭스 - RSSI 프레임 오류, 연결 삭제 이유, 비컨 이동, 오디오 설정 및 DECT 대역폭과 같은 헤드셋 및 액세서리 메트릭입니다.

CMR 레코드를 내보내고 보는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager*용 통화 보고 및 청구 관리 가이드를 참조하십시오.



참고 헤드셋 CMR 레코드는 Cisco 헤드셋 500 시리즈에 적용되지만 700 시리즈에는 적용되지 않습니다.

Unified CM에서 엔드포인트에 대한 PRT 생성

이 절차를 사용하여 엔드포인트에서 PRT(문제 보고 도구)를 트리거합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 2 찾기를 클릭하고 헤드셋이 연결된 전화기를 하나 이상 선택합니다.

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

단계 4 저장을 클릭합니다.

Cisco 통합 커뮤니케이션 매니저는 전화기에서 원격으로 로그 수집을 시작하고 "고객 지원 업로드 URL" 파라미터에 구성된 로그 서버에 업로드하는 SIP 알림 메시지를 전송합니다.

RTMT에서 엔드포인트에 대한 PRT 생성

디바이스 또는 엔드포인트는 진단 및 문제 해결에 대한 각 중요 이벤트에 대한 알람을 생성합니다. 이러한 알람은 Cisco Unified Real-Time Monitoring Tool(RTMT) 사용자 인터페이스의 추적 모음 메뉴 또는 디바이스 모니터링 메뉴에 있는 PRT(문제 보고 도구)를 사용하여 생성됩니다.

프로시저

단계 1 추적 및 Log Central 옵션을 엽니다.

단계 2 추적 및 Log Central 트리 계층 구조에서 PRT 생성을 선택합니다.
PRT 생성 마법사가 나타납니다.

단계 3 Cisco Unified CM 관리 사용자 인터페이스의 전화기 찾기 및 나열 페이지에 구성된 디바이스 이름을 입력합니다.

단계 4 PRT 생성을 클릭합니다.

생성된 보고서는 고객 지원 업로드 URL에서 업로드됩니다. 다운로드 옵션은 고객 지원 업로드 URL 매개 변수가 Cisco Unified CM 관리 사용자 인터페이스의 엔터프라이즈, 프로파일 또는 디바이스 수준에서 구성된 경우에만 사용할 수 있습니다.

참고 엔터프라이즈, 프로파일 또는 디바이스 수준 구성 페이지 설정에서 고객 지원 업로드 URL 매개 변수를 선택합니다. 그렇지 않으면 PRT가 생성되지 않습니다.



56 장

헤드셋 서비스

- 헤드셋 서비스 개요, 739 페이지
- 헤드셋 서비스 사전 요건, 740 페이지
- 헤드셋 서비스 관리자 구성 작업 흐름, 740 페이지
- 헤드셋 서비스 최종 사용자 연결 작업 흐름, 744 페이지

헤드셋 서비스 개요

헤드셋 서비스를 사용하면 Cisco 헤드셋을 지원되는 디바이스에 연결하여 헤드셋 기반 Extension Mobility 및 앞으로 많은 향후 통합된 사용자 환경을 제공할 수 있습니다.

헤드셋 기반 Extension Mobility는 헤드셋 서비스에 도입된 첫 번째 기능입니다. Cisco 헤드셋을 Extension Mobility 기능이 활성화된 디바이스에 연결할 때 Extension Mobility 로그인 및 로그아웃에 대한 매끄러운 로그인 경험을 제공합니다.

헤드셋 서비스를 사용하면 관리자와 최종 사용자가 자체 소유 디바이스, 공유 공간 및 일반 영역 디바이스와 같은 모든 디바이스의 헤드셋을 연결할 수 있습니다. 이 연결은 인증을 제공하고 사용자에게 사용자 정의된 경험을 만드는 데 도움이 됩니다. 이 기능은 유선 및 무선 헤드셋을 모두 지원합니다.

헤드셋을 연결하면 사용자의 ID를 헤드셋에 할당합니다. 사용자 ID가 필요한 서비스에 로그인할 수 있습니다.

이 Unified Communications Manager 인터페이스를 사용하면 관리자가 다음 작업을 수행할 수 있습니다.

- 일련 번호를 사용하여 최종 사용자와 헤드셋을 연결 및 연결 해제합니다.
- 헤드셋 기반 Extension Mobility를 활성화합니다.
- 벌크 사용자를 헤드셋 연결로 가져오고 내보냅니다.



참고 EMCC(Extension Mobility Cross Cluster)에는 헤드셋 기반 Extension Mobility 로그인 지원되지 않습니다.

헤드셋 기반 Extension Mobility 로그인은 모바일 및 원격 액세스(MRA)를 지원하는 디바이스에서 작동합니다. 호환되는 전화기 펌웨어 버전은 14.1(1)입니다.

동일한 사용자 ID가 헤드셋과 전화기를 모두 제어하는 경우 헤드셋 기반 Extension Mobility 로그인이 작동하지 않습니다.

헤드셋 서비스 사전 요건

- 최종 사용자가 이미 Unified Communications Manager에서 생성되었는지 확인합니다.
- 헤드셋을 사용하는 Extension Mobility 로그인인 경우 사용자 디바이스에서 Extension Mobility가 활성화되어 있는지 확인합니다. 그리고 Cisco 헤드셋을 사용하여 사용자가 Extension Mobility 로그인을 수행 하거나 로그아웃할 수 있도록 헤드셋에서 **Extension Mobility** 로그인 및 로그아웃 허용 옵션이 활성화됩니다.



참고 헤드셋 기반 Extension Mobility 기능은 88XX 및 78XX 시리즈 Cisco IP 전화기의 최신 펌웨어만 지원합니다.

헤드셋 서비스 관리자 구성 작업 흐름

관리자는 다음 작업을 사용하여 헤드셋을 사용자와 연결하고 헤드셋 기반 Extension Mobility를 활성화할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	사용자에게 헤드셋 연결, 741 페이지	일련 번호를 사용자와 연결하고 분리하는 방법을 지정합니다.
단계 2	최종 사용자 헤드셋 연결 관리, 741 페이지	선택 사항: 최종 사용자가 디바이스에 대한 헤드셋 연결을 만들 수 있습니다.
단계 3	헤드셋 기반 Extension Mobility 활성화, 742 페이지	Unified Communications Manager에서 헤드셋에 대한 Extension Mobility를 활성화합니다.
단계 4	핀리스 Extension Mobility 로그인 활성화, 743 페이지	핀리스 Extension Mobility 로그인을 활성화합니다.

	명령 또는 동작	목적
단계 5	Extension Mobility 헤드셋 로그아웃 타이머 구성, 743 페이지	헤드셋에 대한 자동 로그 아웃 시간 초과 설정을 구성합니다.

사용자에게 헤드셋 연결

이 절차를 사용하여 헤드셋을 사용자와 연결합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. **사용자 관리 > 최종 사용자**

단계 2 **찾기**를 클릭하고 헤드셋을 연결하려는 기존 사용자를 선택합니다.

단계 3 연결된 헤드셋 섹션에서 할당할 헤드셋의 일련 번호를 입력합니다.

단계 4 **저장**을 클릭합니다.

단계 5 선택한 사용자에게 더 많은 헤드셋을 연결하려는 경우 (+)을 클릭합니다.

참고 최대 15 개의 헤드셋을 특정 사용자에게 연결할 수 있습니다. 이 헤드셋 일련 번호는 개별 헤드셋마다 고유합니다. 동일한 헤드셋을 두 사용자와 연결할 수 없습니다. 헤드셋 연결을 다른 사용자에게 이동하려면 먼저 첫 번째 사용자의 헤드셋 연결을 해제해야 합니다.

특정 헤드셋의 일련 번호를 찾는 방법에 대한 자세한 내용은 해당 헤드셋 모델에 대한 헤드셋 관리 설명서를 참조하십시오.

단계 6 (선택 사항) (-)을 클릭하여 선택한 사용자의 헤드셋 일련 번호 연결을 해제합니다.

단계 7 헤드셋의 재고 목록 세부 정보를 보려면 세부 정보 보기 링크를 클릭합니다. 자세한 내용은 헤드셋 세부 정보를 보려면 '헤드셋 및 액세서리 관리' 장의 헤드셋 재고 목록 설정 섹션을 참조하십시오.

최종 사용자 헤드셋 연결 관리

선택 사항: 이 절차를 사용하여 최종 사용자가 헤드셋 연결 메뉴 옵션을 사용하여 헤드셋을 디바이스 화면에서 연결할 수 있도록 Unified Communication Manager의 설정을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. **시스템 > 엔터프라이즈 매개 변수**.

단계 2 엔터프라이즈 매개 변수 구성 섹션에서 다음 중 하나를 선택하여 최종 사용자 헤드셋을 디바이스에 연결합니다.

- 헤드셋이 디바이스에 처음 연결될 때 헤드셋 연결 화면을 표시하려면 사용자에게 모든 디바이스에서 헤드셋 연결 시작을 선택합니다. 기본적으로 이 매개 변수 값이 선택되어 있습니다.

- 헤드셋 연결 화면에 대해서만 **Extension Mobility** 활성화 디바이스에서 헤드셋 연결을 시작하도록 사용자에게 헤드셋 연결을 선택하여 **Extension Mobility** 활성화 디바이스에만 표시되도록 합니다.
- 모든 디바이스에서 헤드셋 연결 화면을 비활성화하려면 사용자에게 모든 디바이스에서 헤드셋 연결을 시작하도록 사용자에게 묻지 않음을 선택합니다. 이 설정은 사용자가 디바이스 메뉴에서 직접 헤드셋 연결을 시작하는 것을 막지는 못합니다.

참고 설정의 변경 사항은 최종 사용자와 이미 연결된 헤드셋에는 적용되지 않습니다.

단계 3 저장을 클릭하고 구성 변경 사항을 적용하려면 구성 적용을 클릭합니다.

팁 자세한 설명을 보려면 엔터프라이즈 매개 변수 구성 창에서 매개 변수 이름 또는 물음표 (?) 아이콘을 클릭합니다.

헤드셋 기반 **Extension Mobility** 활성화

이 절차를 사용하여 사용자가 연결된 헤드셋에서 **Extension Mobility**에 로그인할 수 있도록 합니다.

시작하기 전에

사용자가 헤드셋을 사용하여 **Extension Mobility**에 로그인하고, 사용 후 로그아웃할 수 있도록 IP 전화 기 및 디바이스 프로파일을 **Extension Mobility** 서비스에 구성해야 합니다. 자세한 내용은 [Extension Mobility에 구독, 443 페이지](#)의 내용을 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 필드에서 Cisco **Extension Mobility** 서비스를 실행하는 노드를 선택합니다.

단계 3 서비스 필드에서 **Cisco Extension Mobility**를 선택합니다.

단계 4 헤드셋 기반 **Extension Mobility** 필드에서 다음 중 하나를 선택하여 **Extension Mobility** 로그인을 위해 연결된 헤드셋을 사용합니다.

- **Extension Mobility** 로그인을 사용하여 헤드셋 사용자가 로그인하도록 허용하려면 헤드셋을 사용하여 **Extension Mobility** 로그인 및 로그아웃 허용을 선택합니다. 기본적으로 이 매개 변수 값이 선택되어 있습니다.
- **Extension Mobility** 로그인을 사용하여 헤드셋 사용자가 로그인하는 것을 제한하려면 헤드셋을 사용하여 **Extension Mobility** 로그인 및 로그아웃 허용 안 함을 선택합니다. 이 옵션을 선택하면 최종 사용자가 헤드셋을 연결할 때 **Extension Mobility** 로그인 또는 로그아웃 화면이 표시되지 않습니다.

단계 5 저장을 클릭합니다.

핀리스 **Extension Mobility** 로그인 활성화

사용자와 연결된 헤드셋을 사용하여 핀이 없는 **Extension Mobility** 로그인에 이 절차를 사용합니다.



참고 이 기능은 릴리스 12.5(1)SU3 이후부터 지원됩니다.

시작하기 전에

서비스 매개 변수 구성 > 헤드셋 연결 후 자동 로그인 타이머(초) 필드에 **Extension Mobility** 프로파일
에 자동으로 로그인하기 전에 시스템이 사용자 입력을 기다리는 최대 시간을 지정합니다.



참고 지정된 최대 지속 시간은 헤드셋 기반 로그인에 대한 **PIN** 항목이 필요 없음으로 설정된 경우에만 적용됩니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 필드에서 Cisco Extension Mobility 서비스를 실행하는 노드를 선택합니다.

단계 3 서비스 필드에서 **Cisco Extension Mobility**를 선택합니다.

단계 4 헤드셋 기반 로그인에 대한 **PIN** 항목 필드에서 다음 중 하나를 선택하여 핀이 없는 **Extension Mobility**
로그인을 활성화하거나 비활성화합니다.

- 사용자에게 **Extension Mobility** 로그인을 위한 **PIN**을 입력하라는 메시지를 표시하려면 필요를 선택합니다. 기본적으로 이 매개 변수 값이 선택되어 있습니다.
- 1분 내에 **Extension Mobility**에 사용자를 자동으로 로그인하려면 필요하지 않음을 선택합니다. 사용자에게 전화기 UI의 **PIN** 세부 정보를 입력하라는 메시지가 표시되지 않습니다.

중요 사용자가 설정된 시간 내에 자동으로 로그아웃하거나 유선 또는 무선 헤드셋을 사용하여 수동으로 로그아웃하면 지정된 기간 내에 자동 로그인되지 않도록 사용자가 취소 버튼을 클릭하는 것이 좋습니다.

단계 5 저장 버튼을 클릭합니다.

Extension Mobility 헤드셋 로그아웃 타이머 구성

이 절차를 사용하여 자동 로그아웃 시간 초과 설정을 구성합니다.



참고 서비스 매개 변수 구성 창에서 헤드셋 기반 Extension Mobility 서비스 매개 변수가 **Extension Mobility** 로그인 및 로그아웃에 헤드셋 허용 안 함으로 설정된 경우 자동 로그아웃 타이머 값을 구성해도 아무런 영향을 미치지 않습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 서비스 > 서비스 매개 변수.

단계 2 서버 필드에서 Cisco Extension Mobility 서비스를 실행하는 노드를 선택합니다.

단계 3 서비스 필드에서 **Cisco Extension Mobility**를 선택합니다.

단계 4 헤드셋 연결이 끊어진 후 자동 로그아웃 타이머 필드에 사용자를 자동으로 로그아웃하기 전에 헤드셋이 디바이스에서 연결이 끊어질 때 시스템이 사용자 입력을 기다릴 수 있는 최대 기간 값을 입력합니다.

참고 기본적으로 이 값은 5분으로 설정됩니다. 최대 값을 15분으로 설정할 수 있습니다.

단계 5 저장을 클릭합니다.

헤드셋 서비스 최종 사용자 연결 작업 흐름

최종 사용자는 다음 작업을 사용하여 헤드셋을 연결하고 연결된 ID를 사용하여 Extension Mobility를 사용하여 로그인할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	사용자 헤드셋 연결, 745 페이지	최종 사용자에게 헤드셋 연결을 만듭니다.
단계 2	헤드셋 연결 건너뛰기, 745 페이지	특정 최종 사용자에 대한 헤드셋 연결을 건너뛸 수 있습니다.
단계 3	헤드셋을 사용하여 Extension Mobility 로그인, 746 페이지	Extension Mobility 로그인에 연결된 헤드셋을 사용하도록 사용자 정의된 환경을 활성화합니다.
단계 4	헤드셋을 사용하여 Extension Mobility에서 사용자 로그아웃, 746 페이지	기본 설정 시간 내에 Extension Mobility에서 헤드셋을 로그아웃하는 데 도움이 됩니다.

사용자 헤드셋 연결

이 절차를 사용하여 헤드셋을 사용자에게 할당합니다.

프로시저

단계 1 헤드셋을 Cisco IP 전화기에 연결합니다.

사용자에게 헤드셋 연결 팝업 화면이 IP 전화기 화면에 나타납니다.

디바이스가 공유 공간 또는 일반 영역에 있거나 사용자가 디바이스와 연결된 경우 사용자 이름이 자동으로 채워집니다. 디바이스가 익명인 경우 사용자 **ID** 필드는 비어 있으며 모든 최종 사용자가 사용자 인증서를 제공하는 헤드셋을 연결할 수 있습니다.

단계 2 사용자 **ID**와 **PIN**을 입력하거나 수정합니다. 인증서를 모르는 경우 관리자에게 문의하십시오.

단계 3 제출을 클릭합니다.

헤드셋 메시지를 성공적으로 연결하면 사용자 이름과 함께 표시됩니다.

잘못된 인증서(사용자 **ID** 또는 **PIN**)를 세 번 이상 입력하는 경우 Cisco IP 전화기에 오류 메시지가 표시됩니다.

헤드셋 연결이 실패하는 경우 헤드셋 연결을 해제한 후 다시 연결하여 유효한 인증서를 제공하거나 관리자에게 문의할 수 있습니다.

단계 4 (선택 사항) Cisco IP 전화기를 통해 헤드셋을 수동으로 연결하려면 설정 > 액세서리 > **Cisco** 헤드셋 설정 > 사용자 연결을 선택합니다.

참고 헤드셋의 연결이 끊어진 경우 사용자 연결 옵션은 회색으로 표시됩니다. 활성화하려면 헤드셋을 디바이스에 연결합니다.

헤드셋 연결 건너뛰기

이 절차를 사용하여 헤드셋을 사용자와 연결하는 것을 건너뛸 수 있습니다.

프로시저

단계 1 헤드셋을 Cisco IP 전화기에 연결합니다.

단계 2 헤드셋을 사용자에게 연결하기 전에 종료를 클릭합니다.

단계 3 헤드셋을 연결하지 않으려면 예를 클릭합니다.

헤드셋 연결 화면에 디바이스에 대한 추가 연결 프롬프트가 표시되지 않습니다. 동일한 헤드셋이 다른 디바이스에 연결되어 있는 경우 사용자에게 헤드셋 연결 팝업 화면이 Cisco IP 전화기 화면에 표시되고 연결 프로세스를 통해 이동합니다.

헤드셋을 사용하여 **Extension Mobility** 로그인

이 절차를 사용하여 사용자와 연결된 헤드셋을 사용하여 **Extension Mobility**로 로그인합니다.

프로시저

단계 1 헤드셋을 Cisco IP 전화기에 연결합니다.

단계 2 헤드셋이 연결되어 있지 않은 경우 다음을 수행합니다.

- a) 사용자 **ID** 및 **PIN**을 입력하여 헤드셋을 사용자와 연결합니다.
- b) 제출을 클릭합니다.

로그인 화면에는 연결된 사용자 **ID**와 함께 성공 메시지가 표시되고 사용자가 **Extension Mobility** 기능을 사용하여 로그인할 수 있습니다.

- c) 로그인을 클릭하여 **Extension Mobility** 로그인을 완료합니다.

단계 3 헤드셋이 사용자와 이미 연결되어 있는 경우 다음을 수행합니다.

- a) **Extension Mobility** 기능을 사용하여 로그인하려면 **PIN**을 입력합니다.
- b) 필요한 사용자 프로파일을 선택합니다.
- c) 제출을 클릭합니다.

단계 4 사용자가 이미 디바이스의 **Extension Mobility**에 로그인되어 있고 다른 사용자가 이전에 연결된 헤드셋에 꽂는 경우 로그아웃 화면이 나타나고 사용자가 이전에 로그인한 사용자를 로그아웃할 수 있습니다.

단계 5 예를 클릭하여 이전 프로파일에서 로그아웃합니다.

단계 6 **Extension Mobility** 기능을 사용하여 로그인하려면 **PIN**을 입력합니다.

단계 7 제출을 클릭합니다.

참고 디바이스 프로파일이 변경될 때마다 전화기가 재설정되고 사용자 프로파일이 원래 프로파일로 변경 됩니다.

헤드셋을 사용하여 **Extension Mobility**에서 사용자 로그아웃

이 절차를 사용하여 **Extension Mobility** 기능이 활성화된 디바이스에서 헤드셋에서 로그아웃합니다.

프로시저

단계 1 Cisco IP 전화기에서 헤드셋의 연결을 끊습니다.

단계 2 로그아웃을 클릭합니다.

참고 전화기가 재설정되고 디바이스 프로파일이 원래 디바이스 프로파일로 변경됩니다.

진행 중인 통화 중에 헤드셋의 연결을 끊으면(1 ~ 1 통화 또는 전화회의 통화) 통화가 종료되지 않으며 통화가 종료될 때만 **Extension Mobility** 로그아웃이 발생합니다.

수동으로 로그아웃하지 않았거나 무선 헤드셋의 범위를 벗어나면 설정된 시간 내에 자동으로 로그아웃됩니다. 기본적으로 설정된 시간은 5분입니다. 자세한 내용은 [Extension Mobility 헤드셋 로그아웃 타이머 구성, 743 페이지](#) 섹션을 참고하십시오.

단계 3 현재 **Extension Mobility** 세션을 유지하려면 취소를 클릭합니다. 기본 설정 시간 내에 다시 연결하여 사용자 프로파일을 유지하고 재설정을 방지합니다.



57 장

IVR 및 전화 서비스를 사용한 기본 전화 마이그레이션

- IVR 및 전화 서비스를 사용한 기본 전화 마이그레이션 개요, 749 페이지
- 전화기 마이그레이션 사전 요건, 752 페이지
- 셀프 프로비저닝 IVR을 사용하는 전화기 마이그레이션 작업 흐름, 753 페이지
- 전화기 마이그레이션 서비스를 사용하여 전화기 마이그레이션 작업 흐름, 760 페이지
- 전화기 마이그레이션 보고서 보기, 764 페이지
- Cisco Unified CM 관리 인터페이스를 사용하여 전화기 마이그레이션, 764 페이지
- 마이그레이션 시나리오, 765 페이지

IVR 및 전화 서비스를 사용한 기본 전화 마이그레이션 개요

전화기 마이그레이션 기능은 Unified Communications Manager에 기본 제공되는 쉽고 직관적인 Cisco IP 전화기 마이그레이션 솔루션입니다. 이는 더 이상 사용되지 않거나 결함이 있는 전화기를 대체하는 비용과 복잡성을 최소화합니다. 최종 사용자나 관리자는 솔루션을 사용하여 간단한 사용자 인터페이스를 사용하여 이전 전화기의 모든 설정을 새 전화기로 쉽게 마이그레이션할 수 있습니다. 솔루션은 전화기를 마이그레이션하는 데 다음 방법을 지원합니다.

- 셀프 프로비저닝 **IVR** 서비스 사용
- 전화기 마이그레이션 서비스 사용
- **Cisco Unified CM** 관리 인터페이스 사용

다음 표는 다양한 전화기 마이그레이션 옵션의 빠른 비교를 제공합니다.

표 66: 서로 다른 전화기 마이그레이션 옵션 및 고려 사항

	셀프 프로비저닝 IVR 서비스 사용	전화기 마이그레이션 서비스 사용	Unified CM 관리 인터페이스 사용
최종 사용자 또는 관리자 구동 전화 마이그레이션	최종 사용자(셀프 서비스)	최종 사용자(셀프 서비스)	관리자
자동 등록 필요	예	아니요	아니요
마이그레이션 단계	<ul style="list-style-type: none"> • 새 전화기 자동 등록 • 자체 프로비저닝 IVR 번호 다이얼 • 음성 프롬프트 따르기 	<ul style="list-style-type: none"> • 네트워크에 새 전화기 연결 • 기본 내선 번호 및 PIN의 키(선택 사항) 	<ul style="list-style-type: none"> • Cisco Unified CM 관리 인터페이스에 로그인 • 이전 전화기의 전화기 구성 페이지에서 "전화기 마이그레이션" 옵션 선택 • 전화기 유형(모델 및 프로토콜) 및 새 전화기의 MAC 주소 입력
관리자 참여	중간	낮음	높음



참고 셀프 프로비저닝 IVR 서비스 및 전화기 마이그레이션 서비스를 사용하는 전화기 마이그레이션에서는 최종 사용자가 전화기를 셀프 서비스로 쉽게 마이그레이션할 수 있습니다. 관리자는 이러한 방법을 사용하여 최종 사용자 또는 일반 전화기(예: 로비 전화기)를 대신하여 전화기를 마이그레이션할 수 있습니다.



참고 전화기 마이그레이션 중에 최종 사용자가 PIN을 기억하지 못하는 경우 관리자는 필요한 경우 사용자에게 셀프 관리 포털에 로그인하여 PIN을 변경하도록 권고해야 합니다.

전화기 마이그레이션을 위한 엔터프라이즈 매개 변수

마이그레이션은 엔터프라이즈 매개 변수 구성 페이지의 다음 두 매개 변수에 따라 달라집니다.

- 최종 사용자에 대한 대체 전화기를 프로비저닝할 때 - 기존 전화기 유지(기본 옵션) 또는 해당 최종 사용자의 기존 전화기 삭제를 선택할 수 있습니다. 기존 전화기 유지 옵션을 선택한 경우 마이그레이션 중 기존 전화기가 마이그레이션된 것으로 표시되고 전화기 찾기 및 나열 페이지에서 필터링하여 마이그레이션 보고서를 생성할 수 있습니다.



참고 관리자가 전화기 마이그레이션에 대해 기존 전화기 유지 옵션을 선택하기로 결정한 경우, 총 두 라이선스가 사용됩니다. 즉, 기존 전화기에 대한 라이선스와 마이그레이션을 위해 선택한 새 전화기에 대한 라이선스입니다.



참고 전화기 마이그레이션 중에 관리자가 전화기 마이그레이션에 대한 기존 전화기 유지 옵션을 선택하기로 결정하면 인터콤 DN이 새 디바이스로 마이그레이션되지 않습니다. 해당 최종 사용자에게 대한 기존 전화기 삭제 옵션을 선택하면 인터콤 DN 정보도 마이그레이션됩니다.

- 마이그레이션된 전화기에 대한 보안 프로파일 - 이 옵션은 전화기 마이그레이션 중에 마이그레이션된 전화기에 적용되는 보안 프로파일 유형(이전 전화기가 보안 모드임)을 결정합니다. 비보안 프로파일을 선택하면 디바이스가 비보안 모드로 표시됩니다.
- 전화기 마이그레이션 사용자 식별 프롬프트 - 이 매개 변수는 사용자가 셀프 서비스 사용자 ID를 사용하거나 기본 내선 번호를 사용하여 전화기 마이그레이션을 진행할 수 있는지 여부를 결정합니다. 최종 사용자 셀프 서비스 사용자 ID 사용 옵션을 선택하면 전화기 마이그레이션을 진행하기 전에 고유한 셀프 서비스 사용자 ID를 입력하라는 메시지가 최종 사용자에게 표시됩니다. 최종 사용자 기본 내선 번호 사용 옵션을 선택한 경우 기본 내선 번호를 입력한 후에 전화기를 마이그레이션할 수 있습니다. 이 모드에서 동일한 DN이 서로 다른 라우트 파티션에 있는 경우 IVR 또는 전화 마이그레이션 서비스를 사용하여 전화기를 마이그레이션할 수 없습니다.

기본값은 최종 사용자 기본 내선 번호 사용입니다.

안전한 전화기 마이그레이션을 위해 다음과 같은 표준 범용 전화기 보안 프로파일 템플릿이 추가되었습니다. 기존 전화기 보안 프로파일을 기반으로 새 전화기는 이러한 새 프로파일 중 하나를 선택합니다.

- 범용 디바이스 템플릿 - 보안 프로파일 - 비보안
- 범용 디바이스 템플릿 - 보안 프로파일 - 인증됨
- 범용 디바이스 템플릿 - 보안 프로파일 - 암호화됨
- 범용 디바이스 템플릿 - 보안 프로파일 - 암호화됨 - Device_TFTP
- 범용 디바이스 템플릿 - 보안 프로파일 - 암호화된 EC 기본 설정

다음 표에는 전화기 마이그레이션 후의 새 디바이스 보안 프로파일 매핑이 나열되어 있습니다.

표 67: 전화기 보안 프로파일 마이그레이션 데이터

기존 보안 프로파일 설정				새 매핑된 프로파일 이름
디바이스 보안 모드	TFTP 암호화 구성	전송 유형	키 순서	
비보안	아니요	TCP	RSA	범용 디바이스 템플릿 - 보안 프로파일 - 비보안
인증됨	아니요	TLS	RSA	범용 디바이스 템플릿 - 보안 프로파일 - 인증됨
암호화됨	아니요	TLS	RSA	범용 디바이스 템플릿 - 보안 프로파일 - 암호화됨
암호화됨	예	TLS	RSA	범용 디바이스 템플릿 - 보안 프로파일 - 암호화됨 - Device_TFTP
암호화됨	예	TLS	EC 기본, RSA 백업	범용 디바이스 템플릿 - 보안 프로파일 - 암호화됨 - Device_TFTP
암호화됨	아니요	TLS	EC 기본, RSA 백업	범용 디바이스 템플릿 - 보안 프로파일 - 암호화된 EC 기본 설정

전화기 마이그레이션 사전 요건

셀프 프로비저닝 IVR 사용

최종 사용자가 마이그레이션을 위해 셀프 프로비저닝을 사용할 수 있으려면 먼저 다음을 구성해야 합니다.

- 자동 등록을 활성화합니다.
- 최종 사용자에게 기본 내선 번호가 있어야 합니다. 전화기 또는 디바이스에서 기본 DN이 항상 회선 1인지 확인합니다.

- 최종 사용자는 범용 회선 템플릿, 범용 디바이스 템플릿 및 셀프 프로비저닝을 활성화한 사용자 프로파일 또는 기능 그룹 템플릿에 연결해야 합니다.
- 올바른 "CTI 라우트 포인트" 및 "애플리케이션 사용자" 구성이 선택되었는지 확인합니다.
- 셀프 프로비저닝 IVR 서비스를 활성화합니다.

전화기 마이그레이션 서비스 사용

최종 사용자가 마이그레이션을 위해 전화기 마이그레이션 서비스를 사용할 수 있으려면 먼저 다음을 구성해야 합니다.

- 자동 등록을 비활성화합니다.
- 최종 사용자에게 기본 내선 번호가 있어야 합니다. 전화기 또는 디바이스에서 기본 DN이 항상 회선 1인지 확인합니다.
- 지원되는 전화기 모델: 88XX, 78XX, 8832 및 7832.
- 지원되는 최소 전화기 버전은 릴리스 12.8.1 이상입니다.

셀프 프로비저닝 IVR을 사용하는 전화기 마이그레이션 작업 흐름

다음 작업 흐름을 사용하여 전화기 마이그레이션 절차를 안내합니다.

이 워크플로우를 완료한 후에는 셀프 프로비저닝 IVR 서비스를 구성하고, 이전 또는 결함 있는 Cisco IP 전화기를 마이그레이션하거나, 마이그레이션한 전화기 목록을 추적할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	셀프 프로비저닝 서비스 활성화, 754 페이지	Cisco 통합 서비스 가용성에서 셀프 프로비저닝 IVR 및 CTI 매니저 서비스를 활성화합니다.
단계 2	셀프 프로비저닝을 위한 자동 등록 활성화, 754 페이지	셀프 프로비저닝을 위한 자동 등록 매개 변수를 활성화합니다.
단계 3	CTI 라우트 포인트 구성, 755 페이지	CTI 라우트 포인트를 구성하여 셀프 프로비저닝 IVR 서비스를 처리합니다.
단계 4	CTI 라우트 포인트에 디렉터리 번호 할당, 756 페이지	사용자가 전화하려는 내선 번호를 구성하여 셀프 프로비저닝 IVR에 액세스하고 해당 내선 전화를 CTI 라우트 포인트에 연결합니다.

	명령 또는 동작	목적
단계 5	셀프 프로비저닝을 위한 애플리케이션 사용자 구성, 756 페이지	셀프 프로비저닝 IVR을 위한 애플리케이션 사용자를 구성합니다. CTI 라우트 포인트를 애플리케이션 사용자와 연결합니다.
단계 6	셀프 프로비저닝을 위한 시스템 구성, 757 페이지	셀프 프로비저닝 시스템 설정을 구성합니다.
단계 7	사용자 프로파일에서 셀프 프로비저닝 활성화, 758 페이지	사용자가 할당된 사용자 프로파일에서 전화기를 셀프 프로비저닝할 수 있습니다.
단계 8	다음 절차 중 하나를 사용하여 전화기를 마이그레이션합니다. <ul style="list-style-type: none"> 셀프 프로비저닝 IVR을 사용하여 전화기 마이그레이션(관리자), 758 페이지 셀프 프로비저닝 IVR을 사용하여 전화기 마이그레이션(전화기 사용자), 759 페이지 	사용자에게 적용되는 마이그레이션 절차를 선택합니다. 관리자 또는 전화기 사용자가 셀프 프로비저닝 IVR을 사용하여 전화기를 마이그레이션할 수 있습니다.
단계 9	전화기 마이그레이션 보고서 보기, 764 페이지	마이그레이션에 따라 마이그레이션한 Cisco IP 전화기를 표시하는 보고서를 봅니다.

셀프 프로비저닝 서비스 활성화

이 절차를 사용하여 셀프 프로비저닝 기능을 지원하는 서비스를 활성화합니다. 셀프 프로비저닝 IVR과 Cisco CTI 관리자 서비스가 모두 실행되고 있는지 확인하십시오.

프로시저

단계 1 Cisco Unified 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.

단계 2 서버 드롭다운 목록에서 퍼블리셔 노드를 선택하고 이동을 클릭합니다.

단계 3 CM 서비스에서 Cisco CTI 관리자를 확인합니다.

단계 4 CTI 서비스 아래에서 셀프 프로비저닝 IVR을 확인합니다.

단계 5 저장을 클릭합니다.

셀프 프로비저닝을 위한 자동 등록 활성화

셀프 프로비저닝을 위해 이 절차를 사용하여 퍼블리셔에서 자동 등록 매개변수를 구성해야만 합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 시스템 > **Cisco Unified CM**을 선택합니다.
 - 단계 2 퍼블리셔 노드를 클릭합니다.
 - 단계 3 프로비저닝된 전화기에 적용하려는 범용 디바이스 템플릿을 선택합니다.
 - 단계 4 프로비저닝된 전화기에 대한 전화 회선에 적용하려는 범용 회선 템플릿을 선택합니다.
 - 단계 5 시작 디렉터리 번호 및 종료 디렉터리 번호 필드를 사용하여 프로비저닝된 전화기에 적용할 디렉터리 번호의 범위를 입력합니다.
 - 단계 6 이 **Cisco Unified Communications Manager**에서 자동 등록 비활성화됨 확인란을 선택 취소합니다.
 - 단계 7 SIP 등록에 사용될 포트를 확인합니다. 대부분의 경우 기본 설정에서 포트를 변경할 필요가 없습니다.
 - 단계 8 저장을 클릭합니다.
-

CTI 라우트 포인트 구성

이 절차를 사용하여 셀프 프로비저닝 IVR에 대한 CTI 라우트 포인트를 구성합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 디바이스 > **CTI** 라우트 포인트를 선택합니다.
 - 단계 2 다음 단계 중 하나를 완료합니다.
 - a) 찾기를 클릭하고 기존 CTI 라우트 포인트를 선택합니다.
 - b) 새로 추가를 클릭하여 새 CTI 라우트 포인트를 만듭니다.
 - 단계 3 디바이스 이름 필드에 라우트 포인트를 식별하는 고유 이름을 입력합니다.
 - 단계 4 디바이스 풀 드롭다운 목록에서 이 디바이스에 대한 속성을 지정하는 디바이스 풀을 선택합니다.
 - 단계 5 위치 드롭다운 목록에서 이 CTI 라우트 포인트에 대한 해당 위치를 선택합니다.
 - 단계 6 **TRP(Trusted Relay Point)** 사용 드롭다운 목록에서 Unified Communications Manager에서 이 미디어 엔드포인트로 TRP 디바이스에 삽입하도록 설정할 것인지 여부를 선택합니다. 기본 설정은 이 디바이스와 연결된 일반 디바이스 구성 설정을 사용하는 것입니다.
 - 단계 7 **CTI** 라우트 포인트 구성 창에서 나머지 필드를 완료합니다. 필드와 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
 - 단계 8 저장을 클릭합니다.
-

CTI 라우트 포인트에 디렉터리 번호 할당

이 절차를 사용하여 사용자가 셀프 프로비저닝 IVR에 액세스하기 위해 전화를 거는 내선 번호를 설정합니다. 셀프 프로비저닝을 위해 사용하려는 CTI 라우트 포인트에 이 내선 번호를 연결해야 합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 디바이스 > **CTI** 라우트 포인트를 선택합니다.
 - 단계 2 찾기를 클릭하고 셀프 프로비저닝을 위해 설정한 CTI 라우트 포인트를 선택합니다.
 - 단계 3 연결에서 회선 [1] - 새 **DN** 추가를 클릭합니다.
디렉터리 번호 구성 창이 표시됩니다.
 - 단계 4 디렉터리 번호 필드에 사용자가 셀프 프로비저닝 IVR 서비스에 액세스하기 위해 전화를 걸려고 하는 내선 번호를 입력합니다.
 - 단계 5 저장을 클릭합니다.
 - 단계 6 디렉터리 번호 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
 - 단계 7 저장을 클릭합니다.
-

셀프 프로비저닝을 위한 애플리케이션 사용자 구성

셀프 프로비저닝 IVR에 대한 애플리케이션 사용자를 설정하고 생성한 CTI 라우트 포인트를 애플리케이션 사용자에게 연결해야 합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 사용자 > 애플리케이션 사용자를 선택합니다.
 - 단계 2 다음 단계 중 하나를 수행합니다.
 - a) 기존 애플리케이션 사용자를 선택 하려면 찾기를 클릭하고 애플리케이션 사용자를 선택합니다.
 - b) 새 애플리케이션 사용자를 만들려면 새로 추가를 클릭합니다.
 - 단계 3 사용자 **ID** 텍스트 상자에 애플리케이션 사용자의 고유 ID를 입력합니다.
 - 단계 4 애플리케이션 사용자에게 대한 **BLF** 프리젠스 그룹을 선택합니다.
 - 단계 5 다음 단계를 수행하여 생성한 CTI 라우트 포인트를 애플리케이션 사용자에게 연결합니다.
 - a) 생성한 CTI 라우트 포인트가 사용 가능한 디바이스 목록 상자에 나타나지 않는 경우, 추가 라우트 포인트 찾기]를 클릭합니다.
생성한 CTI 라우트 포인트는 사용 가능한 디바이스로 표시됩니다.
 - b) 사용 가능한 디바이스 목록에서 셀프 프로비저닝을 위해 생성한 CTI 라우트 포인트를 선택하고 아래쪽 화살표를 클릭합니다.
제어된 디바이스 목록에 CTI 라우트 포인트가 표시됩니다.

단계 6 애플리케이션 사용자 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 7 저장을 클릭합니다.

셀프 프로비저닝을 위한 시스템 구성

이 절차를 사용하여 셀프 프로비저닝을 위해 시스템을 구성합니다. 셀프 프로비저닝을 통해 네트워크 사용자는 관리자에게 연락하지 않고서도 IVR 시스템을 통해 자신의 데스크폰을 추가할 수 있습니다.



참고 셀프 프로비저닝 기능을 사용하려면 엔드 유저가 사용자 프로파일에서도 기능을 활성화해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 사용자 관리 > 셀프 프로비저닝을 선택합니다.

단계 2 다음 라디오 버튼 중 하나를 클릭하여 셀프 프로비저닝 IVR에서 엔드 유저를 인증할 것인지 여부를 구성합니다.

- 인증 필요—셀프 프로비저닝 IVR을 사용하려면 엔드 유저가 암호, PIN 또는 시스템 인증 코드를 입력해야 합니다.
- 인증 필요 없음—엔드 유저가 인증 없이 셀프 프로비저닝 IVR에 액세스할 수 있습니다.

단계 3 셀프 프로비저닝 IVR이 인증을 요구하도록 구성된 경우, 다음 라디오 버튼 중 하나를 클릭하여 IVR에서 엔드 유저를 인증하는 방법을 구성합니다.

- 엔드 유저에게만 인증 허용—엔드 유저가 암호나 PIN을 입력해야 합니다.
- 사용자(암호/PIN 사용) 및 관리자(인증 코드 사용)에 대한 인증 허용—엔드 유저가 인증 코드를 입력해야 합니다. 이 옵션을 선택하는 경우, 인증 코드 텍스트 상자에 0~20 사이의 정수를 입력하여 인증 코드를 구성합니다.

단계 4 IVR 설정 목록 상자에서 화살표를 사용하여 IVR 프롬프트에 사용할 언어를 선택합니다. 사용 가능한 언어 목록은 시스템에 설치된 언어 팩에 따라 달라집니다. 추가 언어 팩을 다운로드하려면 cisco.com의 다운로드 섹션을 참조하십시오.

단계 5 CTI 라우트 포인트 드롭다운 목록에서 셀프 프로비저닝 IVR에 대해 구성한 CTI 라우트 포인트를 선택합니다.

단계 6 애플리케이션 사용자 드롭다운 목록에서 셀프 프로비저닝을 위해 구성한 애플리케이션 사용자를 선택합니다.

단계 7 저장을 클릭합니다.

사용자 프로파일에서 셀프 프로비저닝 활성화

사용자가 전화기를 셀프 프로비저닝할 수 있으려면, 기능이 할당된 사용자 프로파일에서 기능을 활성화해야 합니다.



참고 사용자가 사용 중인 사용자 프로파일을 모르는 경우 최종 사용자 구성 창에서 사용자 설정을 열고 사용자 프로파일 필드를 확인하여 올바른 프로파일을 가져올 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 사용자 관리 > 사용자 설정 > 사용자 프로파일을 선택합니다.

단계 2 사용자가 할당된 사용자 프로파일 찾기 및 선택을 클릭합니다.

단계 3 사용자 프로파일에 범용 회선 템플릿 및 범용 디바이스 템플릿을 할당합니다.

단계 4 셀프 프로비저닝을 위한 사용자 설정 구성:

- 최종 사용자에게 자신의 전화기 프로비저닝 허용 확인란을 선택합니다.
- 사용자가 프로비저닝할 수 있는 전화기 수에 대한 제한을 입력합니다. 기본값은 10입니다.
- 사용자가 셀프 프로비저닝을 사용하여 이전에 할당된 전화기를 다시 할당하려는 경우, 이전 디바이스의 최종 사용자와 연결된 사용자 프로파일 페이지에서 다른 최종 사용자에게 이미 할당된 전화기의 프로비저닝 허용 설정을 선택합니다. 이전 디바이스에 연결된 사용자 프로파일에서이 확인란이 활성화 된 경우에만 사용자가 이전에 할당 된 전화기를 다시 할당할 수 있습니다.

단계 5 저장을 클릭합니다.

전화기 마이그레이션 작업

셀프 프로비저닝 인증이 설정된 후 다음 절차 중 하나를 사용하여 전화기를 마이그레이션합니다.

셀프 프로비저닝 IVR을 사용하여 전화기 마이그레이션(관리자)

관리자는 이 절차를 사용하여 최종 사용자를 대신하여 Cisco IP 전화기를 마이그레이션하거나 일반 전화기를 마이그레이션할 수 있습니다(예: 로비 전화기).

시작하기 전에

마이그레이션을 진행하기 전에 이전 전화기가 "등록되지 않음" 상태인지 확인합니다. 새 전화기를 네트워크에 연결하고 전화기가 등록될 때까지 기다린 다음 마이그레이션 작업을 수행할 수 있습니다. 마이그레이션이 성공적으로 완료되면 디바이스는 사용자 전화기 구성 데이터에 다시 등록됩니다.

프로시저

단계 1 새 전화기에서 셀프 프로비저닝 IVR에 할당된 내선 번호로 전화를 겁니다.

단계 2 기존 전화기를 교체하려면 2를 누릅니다

단계 3 최종 사용자 전화기 또는 일반 전화기의 기본 내선 번호를 입력한 후 파운드 키(#)를 입력합니다.

단계 4 인증 코드를 입력한 후 파운드 키(#)를 입력합니다.

인증이 성공한 후에 마이그레이션이 시작됩니다. 마이그레이션을 수행하면 최종 사용자의 이전 전화기에서 마이그레이션한 구성 설정으로 전화기가 다시 시작됩니다.

셀프 프로비저닝 IVR을 사용하여 전화기 마이그레이션(전화기 사용자)

전화기 사용자는이 절차를 사용하여 새 Cisco IP 전화기를 마이그레이션할 수 있습니다.

시작하기 전에

마이그레이션을 진행하기 전에 이전 전화기가 "등록되지 않음" 상태인지 확인합니다. 새 전화기를 네트워크에 연결하고 전화기가 등록될 때까지 기다린 다음 마이그레이션 작업을 수행할 수 있습니다. 마이그레이션이 성공적으로 완료되면 디바이스는 사용자 전화기 구성 데이터에 다시 등록됩니다.

프로시저

단계 1 새 Cisco IP 전화기에서 셀프 프로비저닝 IVR에 할당된 내선 번호로 전화를 겁니다.

단계 2 기존 전화기를 교체하려면 2를 누릅니다

단계 3 전화기의 기본 내선 번호를 입력한 다음 파운드 키(#)를 입력합니다.

단계 4 핀(PIN) 번호를 입력한 다음 파운드 키(#)를 입력합니다.

인증이 성공한 후에 마이그레이션이 시작됩니다. 마이그레이션이 성공적으로 완료되면 이전 전화기에서 마이그레이션한 구성 설정으로 전화기가 다시 시작됩니다.

참고 전화기가 다른 사용자에게 할당된 경우, 관리자가 사용자의 사용자 프로파일 창에서 다른 최종 사용자에게 이미 할당된 전화의 프로비저닝 허용 옵션을 활성화한 경우 전화기 사용자가 전화기를 다시 프로비저닝할 수 있습니다. 관리자에게 이 옵션에 대해 문의하십시오.

전화기 마이그레이션 서비스를 사용하여 전화기 마이그레이션 작업 흐름

다음 작업 흐름을 사용하여 전화기 마이그레이션 서비스를 사용하는 전화기 마이그레이션 절차를 안내합니다.

이 워크플로를 완료한 후 이전 또는 결함 있는 Cisco IP 전화기를 마이그레이션하거나 마이그레이션된 전화기 목록을 추적할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	자동 등록 비활성화, 760 페이지	전화기 마이그레이션 전에 자동 등록 매개 변수를 비활성화합니다.
단계 2	기본 전화기 로드 설정, 761 페이지	전화기 마이그레이션 서비스를 수행하기 전에 기본 전화기 로드를 구성합니다.
단계 3	셀프 프로비저닝 인증 구성, 761 페이지	필수 셀프 프로비저닝 인증 설정을 구성합니다.
단계 4	다음 절차 중 하나를 사용하여 전화기를 마이그레이션합니다. <ul style="list-style-type: none"> 전화기 마이그레이션 서비스를 사용하여 전화기 마이그레이션(관리자), 762 페이지 전화기 마이그레이션 서비스를 사용하여 전화기 마이그레이션(전화기 사용자), 763 페이지 	사용자에게 적용되는 마이그레이션 절차를 선택합니다. 관리자 또는 전화기 사용자가 전화기 마이그레이션 서비스를 사용하여 전화기를 마이그레이션할 수 있습니다.
단계 5	전화기 마이그레이션 보고서 보기, 764 페이지	마이그레이션에 따라 마이그레이션한 Cisco IP 전화기를 표시하는 보고서를 봅니다.

자동 등록 비활성화

전화기 마이그레이션 서비스를 사용하려면 자동 등록을 비활성화해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > **Cisco Unified CM**을 선택합니다.

단계 2 퍼블리셔 노드를 클릭합니다.

단계 3 Cisco Unified Communications Manager에서 자동 등록 비활성화된 확인란을 선택합니다.

단계 4 SIP 등록에 사용될 포트를 확인합니다. 대부분의 경우 기본 설정에서 포트를 변경할 필요가 없습니다.

단계 5 저장을 클릭합니다.

기본 전화기 로드 설정

이 절차를 사용하여 전화기 마이그레이션 서비스를 수행하기 전에 기본 전화기 로드를 설정합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 디바이스 기본값을 선택합니다.

단계 2 마이그레이션에 필요한 전화기 모델을 선택합니다.

단계 3 전화기 로드를 입력하고 전화기 로드의 로드 교체 버튼을 클릭하여 기본 전화기 로드를 만듭니다.

단계 4 저장을 클릭합니다.

셀프 프로비저닝 인증 구성

전화기 마이그레이션 서비스는 셀프 프로비저닝 시스템 설정을 사용하여 전화기 마이그레이션 전에 사용자를 인증합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 사용자 관리 > 셀프 프로비저닝을 선택합니다.

단계 2 다음 라디오 버튼 중 하나를 클릭하여 셀프 프로비저닝에서 최종 사용자를 인증할 것인지 여부를 구성합니다.

- 인증 필요—셀프 프로비저닝을 사용하려면 최종 사용자가 암호, PIN 또는 시스템 인증 코드를 입력해야 합니다.
- 인증 필요 없음—최종 사용자가 인증 없이 셀프 프로비저닝에 액세스할 수 있습니다.

단계 3 셀프 프로비저닝 기능이 인증을 요구하도록 구성된 경우, 다음 라디오 버튼 중 하나를 클릭하여 셀프 프로비저닝 옵션에서 최종 사용자를 인증하는 방법을 구성합니다.

- 엔드 유저에게만 인증 허용—엔드 유저가 암호나 PIN을 입력해야 합니다.
- 사용자(암호/PIN 사용) 및 관리자(인증 코드 사용)에 대한 인증 허용—엔드 유저가 인증 코드를 입력해야 합니다. 이 옵션을 선택하는 경우, 인증 코드 텍스트 상자에 0 ~ 20 사이의 정수를 입력하여 인증 코드를 구성합니다.

단계 4 저장을 클릭합니다.

전화기 마이그레이션 작업

셀프 프로비저닝 인증이 설정된 후 다음 절차 중 하나를 사용하여 전화기를 마이그레이션합니다.

전화기 마이그레이션 서비스를 사용하여 전화기 마이그레이션(관리자)

관리자는 이 절차를 사용하여 최종 사용자를 대신하여 Cisco IP 전화기를 마이그레이션하거나 일반 전화기를 마이그레이션할 수 있습니다(예: 로비 전화기).

시작하기 전에

마이그레이션을 진행하기 전에 이전 전화기가 "등록되지 않음" 상태인지 확인합니다. 새 전화기를 네트워크에 연결하려면 전화기 마이그레이션 또는 프로비전 프롬프트가 표시되고 마이그레이션 프로세스가 시작될 때까지 기다립니다. 마이그레이션이 성공적으로 완료되면 디바이스는 사용자 전화기 구성 데이터에 다시 등록됩니다.

프로시저

단계 1 새 Cisco IP 전화기를 네트워크에 연결합니다.

단계 2 기존 전화기를 교체하려면 2 옵션을 선택합니다.

참고 관리자가 활성화 코드 기반 디바이스 온보딩을 구성하지 않았거나 전화기 마이그레이션이 활성화 코드를 지원하지 않는 11.5(1)SU8 버전의 Unified Communications Manager에서 수행된 경우 전화기에는 기본 내선 번호를 입력할 수 있는 화면이 표시됩니다.

단계 3 전화기의 기본 내선 번호를 입력합니다.

단계 4 인증 코드를 입력합니다.

인증이 성공한 후에 마이그레이션이 시작됩니다. 마이그레이션이 성공적으로 완료되면 이전 전화기에서 마이그레이션한 구성 설정으로 전화기가 다시 시작됩니다.

참고 디바이스 기본값 구성 페이지에서 온프레미스 온보딩 방법 옵션이 자동 등록으로 선택된 시나리오를 고려하십시오. 전화기 마이그레이션을 수행하는 동안 오류 메시지가 표시될 때 종료 또는 뒤로 버튼을 누르면 예상된 지연 시간이 지나면 초기 전화기 마이그레이션 화면으로 바로 이동합니다. 이 지연은 자동 등록이 Unified Communications Manager 서버에서 비활성화되면 Unified CM에 다시 등록하려고 시도하는 전화기 때문에 발생합니다.

참고 기본 내선 번호가 동일한 사용자에 대해 디바이스가 둘 이상 있는 경우에는 디바이스를 선택하라는 메시지가 표시됩니다. 자세한 내용은 [전화기 마이그레이션 서비스 — 여러 디바이스에 할당된 사용자, 766 페이지](#)의 내용을 참조하십시오.

전화기 마이그레이션 서비스를 사용하여 전화기 마이그레이션(전화기 사용자)

전화기 사용자는 이 절차를 사용하여 IVR 이외의 방법을 사용하여 새 Cisco IP 전화기로 마이그레이션할 수 있습니다. 전화기를 네트워크에 연결하면 전화기가 부팅을 시도하고 자동 구성합니다. 기본 전화기 로드에서 사용자는 '새 전화기 프로비저닝' 또는 '기존 전화기 교체' 중 하나를 선택하는 옵션을 선택할 수 있습니다.



참고 최종 사용자는 이전 장치의 소유자인 경우에만 마이그레이션을 수행해야 합니다.

시작하기 전에

마이그레이션을 진행하기 전에 이전 전화기가 "등록되지 않음" 상태인지 확인합니다. 새 전화기를 네트워크에 연결하려면 전화기 마이그레이션 또는 프로비전 프롬프트가 표시되고 마이그레이션 프로세스가 시작될 때까지 기다립니다. 마이그레이션이 성공적으로 완료되면 디바이스는 사용자 전화기 구성 데이터에 다시 등록됩니다.

프로시저

단계 1 새 Cisco IP 전화기를 네트워크에 연결합니다.

단계 2 기존 전화기를 교체하려면 2 옵션을 선택합니다.

참고 관리자가 활성화 코드 기반 디바이스 온보딩을 구성하지 않았거나 전화기 마이그레이션이 활성화 코드를 지원하지 않는 11.5(1)SU8 버전의 Unified Communications Manager에서 수행된 경우 전화기에는 기본 내선 번호를 입력할 수 있는 화면이 표시됩니다.

단계 3 전화기의 기본 내선 번호를 입력합니다.

단계 4 PIN을 입력합니다.

인증이 성공한 후에 마이그레이션이 시작됩니다. 마이그레이션이 성공적으로 완료되면 이전 전화기에서 마이그레이션한 구성 설정으로 전화기가 다시 시작됩니다.

참고 디바이스 기본값 구성 페이지에서 온프레미스 온보딩 방법 옵션이 자동 등록으로 선택된 시나리오를 고려하십시오. 전화기 마이그레이션을 수행하는 동안 오류 메시지가 표시될 때 종료 또는 뒤로 버튼을 누르면 예상된 지연 시간이 지나면 초기 전화기 마이그레이션 화면으로 바로 이동합니다. 이 지연은 자동 등록이 Unified Communications Manager 서버에서 비활성화되면 Unified CM에 다시 등록하려고 시도하는 전화기 때문에 발생합니다.

참고 기본 내선 번호가 동일한 사용자에게 디바이스가 둘 이상 있는 경우에는 디바이스를 선택하라는 메시지가 표시됩니다. 자세한 내용은 [전화기 마이그레이션 서비스 — 여러 디바이스에 할당된 사용자, 766 페이지](#)의 내용을 참조하십시오.

전화기 마이그레이션 서비스 COP 파일

11.5(1)부터 11.5(1)SU7까지 Unified Communications Manager 버전을 실행 중인 경우, 전화기 마이그레이션 서비스 COP 파일(ciscocm-migration-service-11-5-1.zip)을 설치하여 기본 전화기 마이그레이션 기능 지원을 받으십시오.

COP 파일 설치의 일부로서, Unified Communications Manager에 대해 'Tftp 다시 시작' 서비스가 자동으로 수행됩니다.



참고 전화기 마이그레이션 서비스 COP 파일 설치 후에도 Unified CM을 업그레이드할 계획이라면, 기본 전화기 마이그레이션 기능을 기본으로 지원하는 릴리스 버전으로 Unified CM 서버를 업그레이드해야 합니다.

전화기 마이그레이션 보고서 보기

이 절차를 사용하여 마이그레이션한 모든 Cisco IP 전화기의 목록을 봅니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 2 전화기 찾기 및 나열 페이지의 전화기 찾기 위치 드롭다운 목록에서 마이그레이션(이전 전화기)을 선택합니다.

단계 3 찾기를 클릭합니다.

마이그레이션한 모든 이전 디바이스 목록을 볼 수 있습니다. 이 목록은 엔터프라이즈 매개 변수 페이지에서 기존 전화기 유지 옵션이 구성된 경우에만 채워집니다.

Cisco Unified CM 관리 인터페이스를 사용하여 전화기 마이그레이션

이 절차를 사용하여 Cisco Unified CM 관리 인터페이스의 전화 템플릿 또는 전화 유형(및 프로토콜) 옵션을 사용하여 전화기를 마이그레이션합니다.

프로시저

단계 1 전화기 찾기 및 나열 창(디바이스 > 전화기)에서 마이그레이션할 Cisco IP 전화기를 찾습니다.

단계 2 마이그레이션할 Cisco IP 전화기의 전화기 구성 창의 관련 링크 드롭다운 목록에서 전화기 마이그레이션을 선택합니다.

단계 3 전화기를 마이그레이션하려면 다음 옵션 중 하나를 사용할 수 있습니다.

- a) 전화 템플릿—전화기 구성을 마이그레이션할 전화기 모델에 대한 전화 템플릿을 선택합니다.
- b) 전화 유형(및 프로토콜)—전화기 구성을 마이그레이션할 Cisco IP 전화기 모델을 선택합니다.

단계 4 구성을 마이그레이션할 새 Cisco Unified IP Phone의 **MAC** 주소를 입력합니다.

단계 5 (선택 사항) 새 전화기의 설명을 입력합니다. 마이그레이션 고려 사항 및 구성 설정에 대한 자세한 내용은 *Cisco Unified CM* 관리 온라인 도움말 페이지를 참조하십시오.

단계 6 저장을 클릭합니다.

새 전화기에서 기능이 손실될 수 있다는 경고 메시지가 표시되면 확인을 클릭합니다. 마이그레이션 후에는 새 디바이스가 이전 전화기의 설정을 상속합니다.

마이그레이션 시나리오

공유 회선을 사용하는 전화기

기존 전화기에 여러 디바이스가 있는 기본 DN 공유 회선이 있는 시나리오를 고려하십시오. 이러한 디바이스는 동일한 사용자나 여러 사용자가 담당할 수 있습니다. 공유 회선을 사용하여 셀프 프로비저닝 IVR 또는 전화 마이그레이션 서비스 방법을 사용하여 새 Cisco IP 전화기에서 이전 전화기를 마이그레이션하려는 경우, 회선 1로 DN을 사용하는 디바이스를 소유하는 사용자에게 대해서만 마이그레이션이 가능합니다. 여기서 공유 회선 기능 설정은 전화기 마이그레이션 후에 전달됩니다.

이전 전화기에서 공유 회선 기능을 지원하지 않는 경우 전화기 마이그레이션 후 이전 전화 회선이 제거됩니다. 새 전화기는 전화기 마이그레이션 후 이전 전화 회선을 유지합니다.

프록시 TFTP에서 실행 중인 전화기 마이그레이션 서비스

전화기 마이그레이션 서비스를 사용하는 기본 전화기 마이그레이션은 Cisco 프록시 TFTP 서버 구축 모델을 지원합니다.

프록시 TFTP에서 실행되는 전화기 마이그레이션 서비스는 모든 원격 클러스터에서 기본 내선을 검색하고 전화기 마이그레이션을 완료하기 위해 전화기를 홈 또는 로컬 전화기 마이그레이션 서비스로 재전송합니다.

프록시 설정 환경에서 Unified Communications Manager 서버는 원격 클러스터에서 동일한 DN을 사용하는 디바이스를 찾습니다. 오프 클러스터 중 하나에서 동일한 DN을 사용하는 등록됨 또는 등록되지 않음 상태의 디바이스가 두 개 이상인 경우 해당 특정 오프 클러스터의 디바이스는 전화기 마이그레이션에 고려되지 않습니다. 이는 릴리스 11.5(1)SU8에 대한 알려진 제한 사항입니다.



참고 프록시 TFTP에서는 마이그레이션 후 전화기가 이전 전화기에서 마이그레이션한 구성 설정으로 다시 시작됩니다. 마이그레이션이 성공한 후에 다시 시작하기 위해 전화기에서 두 개의 재설정 주기가 사용됩니다.

전화기 마이그레이션 서비스 — 여러 디바이스에 할당된 사용자

마이그레이션을 위한 기본 내선 번호가 동일한 사용자에 대해 디바이스가 둘 이상 있는 경우에는 디바이스를 선택하라는 메시지가 표시됩니다.

다음 표에서는 가능한 다양한 마이그레이션 시나리오를 보여줍니다.

표 68: 디바이스 목록 및 마이그레이션 시나리오

	전화기 마이그레이션 전 디바이스 상태	마이그레이션 중 전화기 표시
시나리오 1	디바이스 1 - 등록됨 디바이스 2 — 등록되지 않음	디바이스 2의 전화기 구성 설정이 마이그레이션됩니다.
시나리오 2	디바이스 1 - 등록됨 디바이스 2 - 등록됨 디바이스 3 - 등록되지 않음	디바이스 3의 전화기 구성 설정이 마이그레이션됩니다.
시나리오 3	디바이스 1 - 등록됨 디바이스 2 — 등록되지 않음 디바이스 3 - 등록되지 않음	설명, 전화 모델 및 MAC 주소를 포함하는 디바이스 목록을 표시합니다. 사용자는 전화기 마이그레이션에 필요한 목록에서 디바이스를 선택해야 합니다.
시나리오 4	디바이스 1 - 등록되지 않음 디바이스 2 — 등록되지 않음 디바이스 3 - 등록되지 않음	설명, 전화 모델 및 MAC 주소를 포함하는 디바이스 목록을 표시합니다. 사용자는 전화기 마이그레이션에 필요한 목록에서 디바이스를 선택해야 합니다.
시나리오 5	디바이스 1 - 등록됨 디바이스 2 - 등록됨 디바이스 3 - 등록됨	설명, 전화 모델 및 MAC 주소를 포함하는 디바이스 목록을 표시합니다. 사용자는 전화기 마이그레이션에 필요한 목록에서 디바이스를 선택해야 합니다.

	전화기 마이그레이션 전 디바이스 상태	마이그레이션 중 전화기 표시
시나리오 6:	3개 이상의 디바이스가 등록되거나 등록되지 않은 상태입니다.	설명, 전화 모델 및 MAC 주소를 포함하는 디바이스 목록을 표시합니다. 사용자는 전화기 마이그레이션에 필요한 목록에서 디바이스를 선택해야 합니다.

Unified CM 매개 변수 설정을 기반으로 하는 디바이스 표시

다음 표에는 Cisco Unified Communications Manager 및 관련 구성 설정의 릴리스 버전에 기반을 둔 새 전화기의 마이그레이션 화면 동작이 나열되어 있습니다.

표 69: 다양한 Unified CM 매개 변수 설정을 기반으로 하는 디바이스 표시

관리자가 미리 구성된 전화기 또는 디바이스	엔터프라이즈 수준에서 활성화된 자동 등록	디바이스 기본값 수준에서 온보딩 방법	전화기 마이그레이션 서비스가 없는 동작	전화기 마이그레이션 서비스가 있는 동작
아니요	예	—	디바이스는 네트워크에 자동으로 등록됩니다.	디바이스는 네트워크에 자동으로 등록됩니다.
아니요	아니요	—	디바이스는 네트워크에 등록을 재시도하고 백오프 타이머 설정을 기반으로 재시도를 계속합니다.	전화기 대체 화면에 기본 확장과 PIN을 입력하라는 메시지가 표시됩니다.
예	해당 없음	—	디바이스는 미리 구성된 설정을 사용하여 등록됩니다.	디바이스는 미리 구성된 설정을 사용하여 등록됩니다.
아니요	예	활성화 코드로 설정된 디바이스 유형	전화기의 시작 화면에 "활성화 코드 입력"이라는 메시지가 표시됩니다.	전화기 대체 화면에 "새 전화기 프로비저닝" 또는 "기존 전화기 교체" 중 하나를 선택하라는 메시지가 표시됩니다.

관리자가 미리 구성한 전화기 또는 디바이스	엔터프라이즈 수준에서 활성화된 자동 등록	디바이스 기본값 수준에서 온보딩 방법	전화기 마이그레이션 서비스가 없는 동작	전화기 마이그레이션 서비스가 있는 동작
아니요	아니요	자동 등록으로 설정된 디바이스 유형	디바이스는 네트워크에 등록을 재시도하고 포기합니다.	전화기 대체 화면에 "기존 전화기 교체"라는 메시지가 표시됩니다.
아니요	아니요	활성화 코드로 설정된 디바이스 유형	전화기의 시작 화면에 "활성화 코드 입력"이라는 메시지가 표시됩니다.	전화기 대체 화면에 "새 전화기 프로비저닝" 또는 "기존 전화기 교체" 중 하나를 선택하라는 메시지가 표시됩니다.
예	해당 없음	해당 없음	디바이스는 네트워크에 등록을 재시도하고 백오프 타이머 설정을 기반으로 재시도를 계속합니다.	디바이스는 미리 구성된 설정을 사용하여 등록됩니다.

Extension Mobility를 사용하는 전화기

이전 전화기가 Extension Mobility 로그인을 지원하는 시나리오에서 새 디바이스는 Extension Mobility 기능도 지원합니다. 이전 전화기가 마이그레이션 전에 로그인된 경우, 로그인한 Extension Mobility 사용자는 전화기 마이그레이션 중에 자동으로 로그아웃됩니다. 사용자는 새 전화기에서 새로운 Extension Mobility 로그인을 수행해야 합니다.



참고 기본 전화기 마이그레이션은 최종 사용자 Extension Mobility 디바이스 프로파일 마이그레이션을 지원하지 않습니다.

CTI 제어된 디바이스

기존 디바이스가 전화기 마이그레이션 전에 CTI 제어되는 경우 새 디바이스도 CTI 제어됩니다. 이는 전화기 마이그레이션 후 디바이스 구성 설정이 수행되기 때문입니다.

키 확장 모듈을 사용하는 전화기

이전 전화기에 연결된 KEM(키 확장 모듈)이 새 전화기 모델과 호환되지 않는 경우 전화기 마이그레이션 후 새 전화기의 KEM '확장 모듈 정보' 구성 설정이 손실됩니다.

다음 표에서는 다양한 시나리오에 대해 설명합니다.

표 70: KEM 마이그레이션 시나리오

시나리오	이전 전화기(모델 79xx)	새 전화기(모델 88xx)	마이그레이션 후 예상되는 동작
<ul style="list-style-type: none"> 기존 전화기에 연결된 KEM 1이 새 전화기와 호환됩니다. 사용자는 이전 전화기에서 KEM 1을 제거하고 새 전화기에 연결합니다. 	KEM 1	KEM 1	KEM 1 구성 설정이 수행됩니다.
<ul style="list-style-type: none"> 기존 전화기에 연결된 KEM 1이 새 전화기와 호환되지 않습니다. 사용자가 새 전화기에 호환되는 KEM 2(새로운 브랜드 또는 사용됨)를 연결합니다. 	KEM 1	KEM 2	KEM 1 구성 설정이 KEM 2에 대해 수행됩니다.
<ul style="list-style-type: none"> 이전 전화기에 연결된 KEM 1은 더 이상 사용되지 않습니다. 사용자가 새 전화기에 새 KEM 3을 연결합니다. 	KEM 1	KEM 3	KEM 1 구성 설정이 KEM 3에 대해 수행됩니다.

제품별 구성 매개 변수

전화기 마이그레이션 중에는 이전 전화기의 제품별 매개 변수도 마이그레이션됩니다. 새 전화기는 전화기가 이해하는 매개 변수만 고려합니다. 나머지 매개 변수는 기본값으로 설정됩니다.

'회선 모드' 매개 변수가 전화기 마이그레이션 중에 이미 구성된 경우 '회선 모드' 구성 설정이 수행됩니다. 그 외에 이 매개 변수는 기본적으로 '세션 회선 모드'로 설정됩니다.

그리고 전화기 마이그레이션 중에 "기본 회선의 모든 통화 표시" 매개 변수가 이전 전화기에서 구성된 경우 새 전화기에는 전화기 마이그레이션 후 "기본 회선의 모든 통화 표시" 매개 변수가 유지됩니다.

다. 전화기 마이그레이션 전에 이 매개 변수가 구성되지 않은 경우 전화기 마이그레이션 후에 기본적으로 활성화됩니다.

전화기 버튼 템플릿

SCCP 전화기 모델을 SIP 전화기 모델로 마이그레이션하면 SIP 전화기는 자신이 이해하는 매개 변수만 고려합니다. 또한 SIP 전화기 모델에서 기본 구성 값을 사용합니다(예: 표준 SIP 프로파일).

이전 전화기에 고유한 사용자 정의 전화기 버튼 템플릿이 있는 경우 전화기 마이그레이션 후 새 전화기에 사용자 정의 전화기 버튼 템플릿이 유지됩니다. 표준 전화기 버튼 템플릿의 경우 새 디바이스에는 전화기 모델에 해당하는 표준 전화기 버튼 템플릿이 사용됩니다.

표 71: 전화기 버튼 템플릿 - 마이그레이션 시나리오

이전 디바이스	전화기 버튼 템플릿	전화기 마이그레이션을 위해 선택된 새 디바이스	전화기 마이그레이션 후 새 디바이스의 전화기 버튼 템플릿
Cisco Unified IP Phone 7965 SCCP	표준 7965 SCCP	Cisco IP 전화기 8861	표준 8861 SIP
Cisco Unified IP Phone 7965 SCCP	범용 디바이스 템플릿 버튼 레이아웃	Cisco IP 전화기 8861	범용 디바이스 템플릿 버튼 레이아웃
Cisco Unified IP Phone 7965 SCCP	사용자 정의 7965 SCCP	Cisco IP 전화기 8861	사용자 정의 7965 SCCP
Cisco Unified IP Phone 8851 SIP	표준 8851 SIP	Cisco IP 전화기 8861	표준 8861 SIP

협업 디바이스 — 실내 시스템, 데스크 및 IP 전화기

- 비디오 엔드포인트 디바이스를 다른 비디오 엔드포인트 디바이스로만 마이그레이션할 수 있습니다.
- Unified Communications Manager는 CSF(데스크톱용 Jabber), TCT(iPhone용 Jabber), TAB(iPad용 Jabber) 또는 BOT(Android용 Jabber) 디바이스에 대한 전화기 마이그레이션을 지원하지 않습니다.
- 전화기 마이그레이션 서비스를 사용하여 비디오 엔드포인트를 마이그레이션할 수 없습니다.
- 이전 비디오 엔드포인트 디바이스가 잠긴 상태에 있는 경우 새 비디오 엔드포인트 디바이스는 전화기 마이그레이션 후 잠긴 상태를 유지하지 않습니다.



58 장

비디오 엔드포인트 관리

- 비디오 엔드포인트 관리 개요, 771 페이지
- 비디오 엔드포인트 관리 기능 호환성, 772 페이지
- 비디오 엔드포인트 프로비저닝을 위한 마이그레이션 고려 사항, 773 페이지
- 비디오 엔드포인트 마이그레이션 보고서, 774 페이지
- 프로비저닝 및 마이그레이션 시나리오, 775 페이지

비디오 엔드포인트 관리 개요

이 기능은 관리자가 Cisco TelePresence 비디오 엔드포인트의 프로비저닝 및 관리 작업을 단순화합니다. 관리자는 Unified Communications Manager에서 Cisco TelePresence 엔드포인트에 대한 설정을 지정하고 해당 제품별 구성 설정을 엔드포인트에 푸시할 수 있습니다.

12.5(1)SU1 릴리스 이전에는 제한된 제품별 구성 집합만 Unified Communications Manager에서 엔드포인트의 부분 구성을 수행하는 엔드포인트로 푸시되었습니다. 관리자는 Cisco TelePresence Management Suite 또는 TelePresence 엔드포인트의 웹 인터페이스를 이용하여 모든 설정을 구성해야 했습니다. Unified Communications Manager의 전화기 구성 창에는 사용자가 엔드포인트에 표시하는 것과 일치하는 Cisco TelePresence 엔드포인트에 대한 전체 제품별 구성 레이아웃이 포함되어 있습니다. 이 업데이트를 사용하면 관리자가 사용자를 대신하여 설정을 적용하고 해당 설정을 사용자에게 푸시할 수 있습니다.



참고 BAT(벌크 관리 도구) 전화 템플릿 구성 페이지에는 엔드포인트 매개 변수의 전체 목록을 지원하는 탭 레이아웃에 새로운 모델 관련 구성이 표시됩니다. 전체 매개 변수 집합을 가져오거나 엔드포인트의 특정 매개 변수를 대량으로 수정할 수 있습니다.

비디오 엔드포인트 관리 기능은 다음과 같은 이점을 제공합니다.

- TelePresence 엔드포인트는 Unified Communications Manager에서 완벽하게 프로비저닝할 수 있습니다. Unified Communications Manager 사용자 인터페이스에 나열된 엔드포인트 매개 변수는 Cisco TelePresence 모델의 고급 구성 설정에 나열된 것과 동일한 순서로 되어 있습니다. 다양한 고급 매개 변수에 대한 자세한 내용은 협업 엔드포인트 관리자 설명서에서 해당 모델을 참조하십시오.

- 새로운 제품별 구성 레이아웃 — 새 레이아웃은 탭 레이아웃의 모델 특정 구성에 대해 자세히 설명합니다. 이는 제한된 매개 변수 집합에만 액세스할 수 있는 이전 플랫 형식에서 업그레이드하는 것입니다. 새 레이아웃을 사용하면 Cisco Unified CM 관리 인터페이스에서 Cisco TelePresence 설정의 전체 목록을 확인할 수 있습니다.
- 비디오 엔드포인트에서 구성 데이터 자동 마이그레이션 — 엔드포인트에서 Unified Communications Manager로 데이터를 자동으로 동기화하여 엔드포인트 구축을 단순화합니다. 공장 설정으로 재설정하거나 제품 반품 및 교체(RMA)하는 경우 엔드포인트 구성을 완전히 복원할 수 있습니다.



참고 CE(협업 엔드포인트) 소프트웨어 9.8 이상을 지원하는 엔드포인트는 전화기 구성 페이지의 제품별 구성 필드에 이 새로운 프로비저닝 레이아웃을 사용할 수 있습니다. 9.8 이전 CE 소프트웨어 버전을 사용하는 경우 모든 새 고급 매개 변수 집합을 볼 수 있습니다. 그러나 CE 소프트웨어 버전을 9.8 이상으로 업그레이드하는 경우에만 새로운 매개 변수 집합이 작동합니다. 지원되는 매개 변수의 하위 집합은 사용자 인터페이스에서 각 매개 변수 값의 오른쪽에 "#"으로 표시됩니다. 디바이스 유형이 새 프로비저닝 프레임워크를 지원할 수 있지만 추가 매개 변수를 표시하지 않는 경우에는 디바이스 팩을 Unified Communications Manager에 로드해야 합니다.

비디오 엔드포인트 관리 기능 호환성

다음 표에서는 비디오 엔드포인트 관리 기능 및 Unified Communications Manager 및 CE(협업 엔드포인트) 버전과의 호환성에 대해 자세히 설명합니다.

Unified Communications Manager 버전	CE 엔드포인트 버전	예상된 동작
12.5(1) SU1	9.8 이상	<p>12.5(1) SU1 전에 추가된 디바이스:</p> <ul style="list-style-type: none"> • 성공적으로 백업되는 디바이스에 대한 고급 구성 UI(탭 레이아웃) • 아직 백업해야 하는 디바이스에 대한 제한된 구성 UI(플랫 레이아웃) <p>UI/BAT/AXL을 통해 추가된 새 디바이스:</p> <ul style="list-style-type: none"> • 고급 구성 UI <p>참고 CE 9.8 이상을 실행하는 것이 좋습니다.</p>

Unified Communications Manager 버전	CE 엔드포인트 버전	예상된 동작
12.5(1) SU1	9.7 이하	<p>12.5(1) SU1 전에 추가된 디바이스:</p> <ul style="list-style-type: none"> 제한된 구성 UI <p>UI/BAT/AXL을 통해 추가된 새 디바이스:</p> <ul style="list-style-type: none"> 제한된 매개 변수 집합만 적용되는 고급 구성 UI <p>참고 CE 9.7 이전 버전에서 마이그레이션하는 경우 마이그레이션 중에 기존 엔드포인트 구성을 유지할 수 없습니다. 마이그레이션된 디바이스가 등록되면 Unified CM은 기존 구성을 기본 설정으로 덮어씁니다.</p>
12.5 (1) 이하	9.8 이상	제한된 구성 UI

비디오 엔드포인트 프로비저닝을 위한 마이그레이션 고려 사항

Unified Communications Manager 업그레이드 후 자동 백업

Unified Communications Manager 12.5(1)SU1로 업그레이드하는 경우 지원되는 엔드포인트 유형에 대한 기존 구성 데이터가 엔드포인트에서 Unified Communications Manager로 자동으로 마이그레이션됩니다.

1. Unified Communications Manager를 버전 12.5(1)SU1 이상으로 업그레이드합니다.
2. Unified Communications Manager에 엔드포인트를 등록합니다.
3. 그런 다음 Unified Communications Manager는 전체 제품별 구성 매개 변수 집합을 요청하는 엔드포인트에 SIP 알림 메시지를 보냅니다.
4. CE 9.8 이상으로 업그레이드되는 엔드포인트는 SIP 참조 메시지를 사용하여 Unified Communications Manager(xConfiguration 형식)로 전체 구성 데이터 집합을 전송합니다.
5. Unified Communications Manager는 이 구성 데이터를 처리하고 Cisco Unified CM 관리 인터페이스에서 Cisco TelePresence 설정(고급 구성 UI)의 전체 목록을 채웁니다.



참고 Unified CM이 엔드포인트의 데이터를 성공적으로 백업할 수 있는 경우에만 Unified Communications Manager 서버에 새 레이아웃으로 전체 엔드포인트 구성 설정이 표시됩니다.

구성 제어 모드

구축 요구 사항에 따라 관리자는 Cisco Unified CM 관리 인터페이스에서 다양한 구성 제어 모드를 구성할 수 있습니다. 엔드포인트 또는 Unified Communications Manager 또는 두 가지 모두에서 구성 설정을 중앙에서 제어할 지 여부를 결정할 수 있습니다.

전화기 구성 페이지의 제품별 구성 레이아웃 섹션으로 이동하고 기타 탭의 “일반 설정” 아래에 있는 구성 제어 모드를 선택하여 다양한 모드를 제어합니다. 다음은 다양한 구성 제어 모드입니다.

- **Unified CM 및 엔드포인트(기본값)** - Unified Communications Manager 및 엔드포인트에서 엔드포인트 데이터를 프로비저닝하는 데 사용되는 멀티 프라임 소스로 작동하게 하려면 이 모드를 사용합니다. Unified CM 및 엔드포인트가 구성된 모드인 경우 로컬에서 엔드포인트를 통해 생성된 업데이트는 모두 Unified CM 서버와 동기화됩니다.
- **Unified CM** — Unified Communications Manager에서 엔드포인트 데이터를 프로비저닝하는 중앙 집중식 기본 소스로 작동하고 로컬로 엔드포인트에서 수행한 구성을 수락하지 않으려면 이 모드를 사용합니다.
- **엔드포인트** - 엔드포인트가 구성 데이터의 중앙 집중식 기본 소스로 작동하도록 하려면 이 모드를 사용합니다. 이 모드에서 엔드포인트는 Unified Communications Manager에서 구성 데이터를 무시하고 로컬로 수행한 변경 사항을 동기화하지 않습니다. 이 모드는 일반적으로 AV(오디오 표시) 통합자가 엔드포인트를 설치하고 엔드포인트에서 구성을 제어 하려고 할 때 사용됩니다.



참고 엔드포인트 모드에서 CE 디바이스는 릴리스 12.5(1)SU1 이전에 지원되었던 제한된 세트의 매개 변수를 계속 받아들입니다. Unified Communications Manager는 이러한 매개 변수를 "#" 기호로 표시합니다. CE 디바이스는 12.5(1)SU1 릴리스부터 지원되는 확장된 매개 변수 집합을 무시합니다.

주문형 구성 가져오기 기능

관리자는 전화기에서 구성 가져오기 옵션을 사용하여 해당 지점에서 CE 9.8 엔드포인트 디바이스의 요청 시 구성 변경 사항을 가져올 수 있습니다.

전화기 구성 페이지의 제품별 구성 레이아웃 섹션으로 이동하고 페이지 상단 모서리에 있는 전화기에서 구성 가져오기 버튼을 클릭하여 요청 시 CE 9.8 엔드포인트에서 데이터 구성을 가져옵니다. 이 옵션은 엔드포인트가 등록된 상태에서만 활성화됩니다.

비디오 엔드포인트 마이그레이션 보고서

확장 구성 백업이 있는 비디오 엔드포인트는 릴리스 12.5(1)SU1에 대한 전화기 찾기 및 나열 창에서도 도입된 새 필터입니다. 관리자는 자동으로 마이그레이션된 CE 엔드포인트 수와 마이그레이션되지 않은 CE 엔드포인트 수에 대한 세부 정보를 검색할 수 있습니다. 이 정보를 기반으로 정정 조치를 취할 수 있습니다.



참고 전화기 찾기 및 나열 창에서 확장 구성 백업을 사용한 비디오 엔드포인트 필터는 CE(Collaboration Endpoint) 소프트웨어 9.8 이상을 사용하는 비디오 엔드포인트에만 적용됩니다.

프로비저닝 및 마이그레이션 시나리오

다음 표에서는 다양한 프로비저닝 및 마이그레이션 시나리오에 대해 설명합니다. 이러한 모든 시나리오에서는 TelePresence 비디오 엔드포인트를 Unified CM에서 제품별 구성 프로비저닝을 지원하는 CE 릴리스로 업그레이드 한다고 가정합니다. Unified CM에서는 이러한 설정이 제품별 구성 섹션에 표시되지만, 엔드포인트에서는 고급 구성 아래에 표시됩니다.

표 72: 비디오 엔드포인트에 대한 프로비저닝 및 마이그레이션 시나리오

작업	기존 구성 요약	수행할 작업
새 비디오 엔드포인트 프로비저닝	<ul style="list-style-type: none"> • 새로운 디바이스 • 디바이스가 Unified CM에서 설정되지 않았음 • 디바이스 또는 Unified CM에 기존 설정이 없음 	9.8의 최소 릴리스 12.5(1)SU1 및 CE 엔드포인트에서 Unified CM을 사용하면 새 엔드포인트를 프로비저닝하고 Unified CM에서 제품별 구성을 관리할 수 있습니다.

작업	기존 구성 요약	수행할 작업
VCS에서 기존 비디오 엔드포인트 마이그레이션	<ul style="list-style-type: none"> 기존 디바이스 디바이스가 Unified CM에서 설정되지 않았음 디바이스가 구성 되어 있지만 Unified CM에 구성이 없음 	<p>Cisco TelePresence Video Communications Server에서 Cisco Unified Communications Manager로 기존 비디오 엔드포인트를 마이그레이션하는 경우:</p> <p>Unified CM에서 전화기 구성 창을 통한 전화기 추가:</p> <ul style="list-style-type: none"> Unified CM에 전화기를 추가하되 <u>저장을 클릭하지 마십시오.</u> 전화기를 등록합니다. 등록 후에는 전화기의 기존 고급 구성 설정이 Unified CM에 업로드되고 전화기 구성 창에 제품별 구성으로 표시됩니다. 전화기 구성 창에서 새 설정을 구성하고 저장을 클릭합니다. 프로비저닝된 설정이 전화기로 다운로드됩니다. <p>자세한 절차는 Unified CM에 비디오 엔드포인트 마이그레이션 추가, 776 페이지의 내용을 참조하십시오.</p> <p>별크 관리를 통해 전화기 추가</p> <p>프로비저닝하는 데 사용하는 csv 파일 또는 BAT 템플릿에 제품별 구성 필드가 포함되어 있지 않은지 확인합니다.</p> <p>AXL을 통해 전화기 추가</p> <p>AXL 요청에 제품별 구성 필드가 포함되어 있지 않은지 확인합니다.</p>
등록된 비디오 엔드포인트를 사용하여 이전 버전의 Unified CM에서 업그레이드	<ul style="list-style-type: none"> 기존 디바이스 디바이스는 Unified CM의 사전 12.5 릴리스에서 프로비저닝됩니다. Unified CM에는 디바이스에 대해 제한된 제품별 구성 설정이 있습니다. 	<p>CE 엔드포인트가 지원되는 버전인 경우, Unified CM을 업그레이드할 때 엔드포인트의 고급 구성 설정을 디바이스 등록 후 자동으로 Unified CM으로 가져와 전화기 구성 창의 제품별 구성 섹션 아래에 표시됩니다.</p> <p>등록 후에는 원하는 설정 외에도 구성 제어 모드를 설정할 수 있습니다.</p>

Unified CM에 비디오 엔드포인트 마이그레이션 추가

Cisco TelePresence Video Communications Server에서 Unified Communications Manager로 기존 Cisco TelePresence 비디오 엔드포인트를 마이그레이션하는 경우, 이 절차를 사용하여 엔드포인트의 기존 고급 구성을 Unified CM의 전화기 구성 창에서 관리할 수 있도록 전화기 구성 창을 통해 Unified CM에 CE 엔드포인트를 추가합니다.



참고 이 절차를 자세히 따르십시오. 디바이스 등록 후에도 엔드포인트의 설정이 Unified CM에 자동으로 업로드되지 않습니다.



참고 이 절차에서는 Unified CM 전화기 구성 창에서 템플릿에서 새로 추가 설정을 사용합니다. 벌크 관리 또는 AXL과 같은 도구를 사용하여 엔드포인트를 추가할 수도 있습니다.

시작하기 전에

마이그레이션하기 전에 펌웨어를 CE 9.8 이상으로 업그레이드하는 것이 좋습니다. CE 9.7 또는 이전 버전에서는 기본 설정을 사용하여 등록하는 동안 Unified CM이 기존 엔드포인트 구성을 덮어씁니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 2 템플릿에서 새로 추가를 클릭하고 다음 전화기 세부 정보를 입력합니다.

- 전화기 유형 드롭다운 목록에서 모델을 선택합니다.
- 엔드포인트의 **MAC** 주소를 입력합니다.
- 디바이스 템플릿에서 범용 디바이스 템플릿을 선택합니다.
- 전화기에 추가할 디렉터리 번호를 선택합니다. 없는 경우 새로 만들기를 클릭하고 디렉터리 번호를 구성합니다.
- 소유자 사용자 **ID** 드롭다운 목록에서 디바이스를 생성할 사용자를 선택합니다.

단계 3 추가를 클릭합니다. 전화기 구성이 전화기 구성을 채우는 범용 디바이스 템플릿 설정과 함께 표시됩니다. 제품별 구성 섹션은 전화기의 기존 설정 대신에 기본 설정을 사용하여 표시됩니다.

참고 전화기 구성 창의 새로 추가를 사용하여 디바이스를 추가할 수도 있지만 이 방법을 사용하려면 설정을 수동으로 입력해야 합니다.

단계 4 저장을 클릭하지 마십시오. 설정을 저장하는 경우에는 Unified CM이 전화기에서 기존 설정을 로드하지 않습니다. 실수로 저장한 경우 복구 단계에 대한 이 절차의 맨 아래에 있는 문제 해결 메모로 바로 이동하십시오.

단계 5 전화기를 등록합니다.

등록하는 동안 전화기의 기존 고급 구성 설정이 Unified CM으로 발신되고 전화기 구성 창의 제품별 구성 섹션에 표시됩니다.

단계 6 전화기 구성 창에서 구성 제어 모드 필드를 구성하여 엔드포인트 설정을 관리하는 방법을 구성합니다.

- **Unified CM** 및 엔드포인트(기본값) - Unified Communications Manager 및 엔드포인트에서 엔드포인트 데이터를 프로비저닝하는 데 사용되는 멀티 프라임 소스로 작동하게 하려면 이 모드를 사용합니다. Unified CM 및 엔드포인트가 구성된 모드인 경우 로컬에서 엔드포인트를 통해 생성

된 모든 업데이트는 Unified CM과 동기화되며, Unified CM에서 변경한 내용이 엔드포인트에 동기화됩니다.

- **Unified CM** — Unified Communications Manager에서 엔드포인트 데이터를 프로비저닝하는 중앙 집중식 기본 소스로 작동하고 로컬로 엔드포인트에서 수행한 구성을 수락하지 않으려면 이 모드를 사용합니다.
- **엔드포인트** - 엔드포인트가 구성 데이터의 중앙 집중식 기본 소스로 작동하도록 하려면 이 모드를 사용합니다. 이 모드에서 엔드포인트는 기존 설정을 유지하고, Unified Communications Manager에서 구성 데이터를 무시하고, 로컬로 수행한 변경 사항을 동기화하지 않습니다. 이 모드는 일반적으로 AV(오디오 표시) 통합자가 엔드포인트를 설치하고 엔드포인트에서 구성을 제어 하려고 할 때 사용됩니다.

참고 엔드포인트에서 기존 설정을 유지하려면 엔드포인트가 등록 프로세스 전체를 완료한 후부터 엔드포인트 모드를 선택하는 것이 좋습니다. 이 절차를 완료한 후에는 구성을 다른 모드 중 하나로 전환할 수 있습니다.

단계 7 원하는 전화기 설정을 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 8 저장을 클릭합니다.

Unified Communications Manager에 프로비저닝된 설정이 엔드포인트로 다운로드됩니다.



참고 디바이스 등록 전에 전화기 구성 창에서 실수로 저장을 클릭한 경우, 디바이스가 등록 될 때 엔드포인트의 기존 고급 구성 설정이 Unified CM으로 로드되지 않습니다. 복구하려면 디바이스 등록 전에 다음을 수행하십시오.

- Unified CM에서 구성 제어 모드를 엔드포인트로 설정하고 저장을 클릭합니다.
- 전화기가 Unified CM에 등록되도록 합니다.
- 등록 후 전화기 구성 창의 디바이스 구성으로 돌아가서 디바이스에서 구성 가져오기 버튼을 클릭합니다. 설정으로 인해 전화기의 기존 고급 구성을 Unified CM으로 가져옵니다. 이 버튼은 디바이스 등록이 완료될 때 까지는 표시되지 않습니다.
- 구성을 완료하기 위해 절차의 6단계로 돌아갑니다.



XIV 부

고급 통화 처리

- [통화 제어 검색 구성, 781 페이지](#)
- [외부 전화 제어 구성, 791 페이지](#)
- [통화 대기열 구성, 801 페이지](#)
- [통화 조절 구성, 813 페이지](#)
- [논리적 파티션 구성, 817 페이지](#)
- [위치 인식 구성, 829 페이지](#)
- [유연한 DSCP 표시 및 비디오 프로모션 구성, 837 페이지](#)
- [SIP에서 발신자 번호 및 청구 번호 분리, 845 페이지](#)
- [SIP OAuth 모드, 861 페이지](#)



59 장

통화 제어 검색 구성

- 통화 제어 탐색(CCD) 개요, 781 페이지
- 통화 제어 탐색(CCD) 사전 요건, 781 페이지
- 통화 제어 탐색(CCD) 구성 작업 흐름, 782 페이지
- 통화 제어 탐색(CCD) 상호 작용, 788 페이지
- 통화 제어 탐색(CCD) 제한 사항, 789 페이지

통화 제어 탐색(CCD) 개요

CCD(통화 제어 탐색)를 사용하여 디렉터리 번호 패턴과 같은 기타 주요 특성과 함께 Unified Communications Manager 정보를 광고합니다. SAF(서비스 광고 프레임워크) 네트워크를 사용하는 다른 통화 제어 엔티티에는 광고된 정보를 사용하여 동적으로 라우팅 작업을 구성하고 적용할 수 있습니다. SAF를 사용하는 모든 엔티티가 다른 키 정보와 함께 디렉터리 번호 패턴을 광고합니다. 다른 원격 통화 제어 엔티티는 이 브로드캐스트의 정보를 학습하고 통화의 라우팅 작업을 조정할 수 있습니다.

통화 제어 탐색(CCD) 사전 요건

- SAF 사용 기능이 있는 SIP 또는 H.323 클러스터 간(게이트키퍼에서 제어하지 않음) 트렁크
- SAF 네트워크를 지원하고 사용하는 원격 통화 제어 엔티티(예: 다른 Unified Communications Manager 또는 Cisco Unified Communications Manager Express 서버)
- SAF 포워더로 구성되는 Cisco IOS 라우터

통화 제어 탐색(CCD) 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	Cisco IOS 라우터를 지원하는 설명서를 참조하십시오. Cisco Feature Navigator(http://www.cisco.com/go/cfn)를 사용하여 특정 소프트웨어 릴리스, 기능 집합 또는 플랫폼을 지원하는 Cisco IOS 및 Catalyst OS 소프트웨어 이미지를 결정할 수 있습니다.	Cisco IOS 라우터를 SAF 포워더로 구성합니다.
단계 2	SAF 보안 프로파일 구성, 783 페이지	SAF 포워더에 대한 SAF 보안 프로파일을 구성하여 SAF 포워더와 Unified Communications Manager의 보안 연결을 제공합니다.
단계 3	SAF 포워더 구성, 784 페이지	SAF에 대해 구성된 Cisco IOS 라우터인 SAF 포워더를 구성합니다. 원격 통화 제어 엔티티가 호스팅된 DN 패턴을 광고할 때 로컬 클러스터에 통보합니다. 또한 SAF 포워더는 구성하는 각각의 구성 및 등록 트렁크에 대한 로컬 클러스터의 게시 요청을 수신합니다. 게시 요청에는 Cisco Unified Communications Manager에 대한 호스팅된 DN 패턴, PSTN 장애 조치 구성, 트렁크의 수신 포트 및 SIP 트렁크의 경우 트렁크의 URI가 포함된 SIP 경로 헤더 필드가 포함됩니다.
단계 4	SIP 또는 H.323 클러스터 간 트렁크 구성, 784 페이지	SAF 지원을 위해 SIP 또는 H.323 클러스터 간(게이트키퍼에서 제어하지 않음) 트렁크를 구성합니다. 로컬 클러스터는 CCD 요청 서비스에 할당된 SAF 사용 트렁크를 사용하여 발신 전화를 SAF 네트워크를 사용하는 원격 통화 제어 엔티티로 전송합니다.
단계 5	호스팅된 DN 그룹 구성, 785 페이지	호스팅된 DN 패턴의 컬렉션인 호스팅된 DN 그룹을 구성합니다. 호스팅된 DN 그룹을 CCD 광고 서비스에 할당한 다음에 CCD 광고 서비스에서 호스팅된 DN 그룹의 일부인 호스팅된 DN 패턴 전체를 광고합니다. CCD 광고 서비스당 호스팅된 DN 그룹 하나만 할당할 수 있습니다.

	명령 또는 동작	목적
단계 6	호스팅된 DN 패턴 구성, 785 페이지	Unified Communications Manager에 속하는 디렉터리 번호 패턴인 호스팅된 DN 패턴을 구성합니다. CCD 광고 서비스는 이러한 패턴을 SAF 네트워크를 사용하는 다른 원격 통화 제어 엔티티에 광고합니다. 이러한 패턴을 호스팅된 DN 그룹에 연결하면 여러 패턴을 CCD 광고 서비스에 쉽게 연결할 수 있습니다.
단계 7	광고 서비스 구성, 786 페이지	Unified Communications Manager에서 클러스터에 대해 호스팅된 DN 및 PSTN 장애 조치 구성을, SAF 네트워크를 사용하는 원격 통화 제어 엔티티에 광고할 수 있는 통화 제어 검색 광고 서비스를 구성합니다.
단계 8	통화 제어 탐색(CCD)에 대한 파티션 구성, 786 페이지	통화 제어 검색 파티션을 구성하여 학습 패턴이 이 파티션 아래의 숫자 분석에 삽입되는지 확인합니다.
단계 9	요청 서비스 구성, 787 페이지	로컬 클러스터가 SAF 네트워크에서 광고를 검색할 수 있도록 하려면 한 통화 제어 검색 요청 서비스에서 SAF 네트워크를 사용하는 원격 통화 제어 엔티티의 광고를 수신하도록 구성합니다. 또한, CCD 요청 서비스는 설정된 패턴이 숫자 분석에 삽입되도록 합니다.
단계 10	설정된 패턴 차단, 787 페이지	원격 통화 제어 엔티티가 로컬 Unified Communications Manager에 전송하는 학습 패턴을 차단합니다. 더 이상 사용하지 않을 학습 패턴에 대해 이 절차를 수행합니다.

SAF 보안 프로파일 구성

SAF 포워더에 대한 SAF 보안 프로파일을 구성하여 SAF 포워더 및 Unified Communications Manager 간에 보안 연결을 제공합니다.



팁 라우터(SAF 포워더)에 입력한 것과 동일한 사용자 이름 및 암호를 사용합니다.

시작하기 전에

Cisco IOS 라우터를 SAF 포워더로 구성합니다. (<http://www.cisco.com/%20go/cfn>의 Cisco Feature Navigator를 참조하십시오.)

프로시저

단계 1 Cisco Unified CM 관리에서 고급 기능 > **SAF** > **SAF** 보안 프로파일을 선택합니다.

단계 2 **SAF** 보안 프로파일 구성 창에서 필드를 구성합니다.

필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 3 저장을 클릭합니다.

SAF 포워더 구성

SAF에 대해 구성된 Cisco IOS 라우터인 SAF 포워더를 구성합니다. 원격 통화 제어 엔티티가 호스팅된 DN 패턴을 광고할 때 로컬 클러스터에 통보합니다. 또한 SAF 포워더는 구성하는 각각의 구성 및 등록 트렁크에 대한 로컬 클러스터의 게시 요청을 수신합니다. 게시 요청에는 Cisco Unified Communications Manager에 대한 호스팅된 DN 패턴, PSTN 장애 조치 구성, 트렁크의 수신 포트 및 SIP 트렁크의 경우 트렁크의 URI가 포함된 SIP 경로 헤더 필드가 포함됩니다.



팁 선택한 **Cisco Unified Communications Manager** 창에 둘 이상의 노드가 나타나면 클라이언트 레이블 값에 @를 추가합니다. 그렇지 않으면 각 노드가 동일한 클라이언트 레이블을 사용하여 SAF 포워더에 등록하면 오류가 발생할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 고급 기능 > **SAF** > **SAF** 포워더를 선택합니다.

단계 2 **SAF** 포워더 구성 창에서 필드를 구성합니다.

필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 3 저장을 클릭합니다.

SIP 또는 H.323 클러스터 간 트렁크 구성

SAF 지원을 위해 SIP 또는 H.323 클러스터 간(게이트키퍼에서 제어하지 않음) 트렁크를 구성합니다. 로컬 클러스터는 CCD 요청 서비스에 할당된 SAF 사용 트렁크를 사용하여 발신 전화를 SAF 네트워크를 사용하는 원격 통화 제어 엔티티로 전송합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 다음 작업 중 하나를 수행합니다.

- SIP 트렁크용:

1. 트렁크 서비스 유형 유형 드롭다운 목록에서 통화 제어 검색을 선택합니다. 드롭다운 목록 상자에서 트렁크 서비스 유형을 선택한 후에는 유형을 변경할 수 없습니다.
2. 다음을 클릭합니다.
3. 트렁크 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

- 클러스터간 트렁크(게이트키퍼에서 제어하지 않음):

1. 다음을 클릭합니다.
2. SAF 활성화 확인란을 선택합니다.
3. 트렁크 구성 창에서 다른 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

호스팅된 DN 그룹 구성

호스팅된 DN 패턴의 컬렉션인 호스팅된 DN 그룹을 구성합니다. 호스팅된 DN 그룹을 CCD 광고 서비스에 할당한 다음에 CCD 광고 서비스에서 호스팅된 DN 그룹의 일부인 호스팅된 DN 패턴 전체를 광고합니다. CCD 광고 서비스당 호스팅된 DN 그룹 하나만 할당할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 통화 제어 검색 > 호스트 DN 그룹을 선택합니다.

단계 2 호스트 DN 그룹 구성 창에서 필드를 구성합니다.

필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 3 저장을 클릭합니다.

호스팅된 DN 패턴 구성

Unified Communications Manager에 속하는 디렉터리 번호 패턴인 호스팅된 DN 패턴을 구성합니다. CCD 광고 서비스는 이러한 패턴을 SAF 네트워크를 사용하는 다른 원격 통화 제어 엔티티에 광고함

니다. 이러한 패턴을 호스팅된 DN 그룹에 연결하면 여러 패턴을 CCD 광고 서비스에 쉽게 연결할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 통화 제어 검색 > 호스팅된 **DN** 패턴을 선택합니다.

단계 2 호스팅된 **DN** 패턴 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 3 저장을 클릭합니다.

광고 서비스 구성

Unified Communications Manager에서 클러스터에 대해 호스팅된 DN 및 PSTN 장애 조치 구성을, SAF 네트워크를 사용하는 원격 통화 제어 엔티티에 광고할 수 있는 통화 제어 검색 광고 서비스를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 통화 제어 탐색 > 어드버타이징 서비스를 선택합니다.

단계 2 어드버타이징 서비스 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 3 저장을 클릭합니다.

통화 제어 탐색(CCD)에 대한 파티션 구성

통화 제어 검색 파티션을 구성하여 학습 패턴이 이 파티션 아래의 숫자 분석에 삽입되는지 확인합니다.



참고 CCD 파티션은 Cisco Unified Communications Manager 관리의 통화 라우팅 > 제어 클래스 > 파티션 밑에 표시되지 않습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 통화 제어 검색 > 파티션을 선택합니다.

단계 2 통화 제어 검색 파티션 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 3 저장을 클릭합니다.

요청 서비스 구성



주의 학습된 패턴 접두사 또는 경로 파티션 필드를 업데이트하면 시스템 성능에 영향을 줄 수 있습니다. 시스템 성능 문제를 방지하도록 사용량이 적은 시간에 이러한 필드를 업데이트하는 것이 좋습니다.

로컬 클러스터가 SAF 네트워크에서 광고를 검색할 수 있도록 하려면 한 통화 제어 검색 요청 서비스에서 SAF 네트워크를 사용하는 원격 통화 제어 엔티티의 광고를 수신하도록 구성합니다. 또한, CCD 요청 서비스는 설정된 패턴이 숫자 분석에 삽입되도록 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 통화 제어 검색 > 요청 서비스를 선택합니다.

단계 2 요청 서비스 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 3 저장을 클릭합니다.

SAF 네트워크를 사용하도록 원격 통화 제어 엔티티를 구성합니다. (원격 통화 제어 엔티티에 대한 설명서를 참조하십시오.)

설정된 패턴 차단

원격 통화 제어 엔티티가 로컬 Unified Communications Manager에 전송하는 학습 패턴을 차단합니다. 더 이상 사용하지 않을 학습 패턴에 대해 이 절차를 수행합니다.

시작하기 전에

SAF 네트워크를 사용하도록 원격 통화 제어 엔티티를 구성합니다. 원격 통화 제어 엔티티를 지원하는 설명서를 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 통화 제어 검색 > 학습 패턴 차단을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 다음 필드 중 하나를 구성합니다.

- 학습 패턴 필드에서 차단하려는 학습 패턴을 정확히 입력해야 합니다. Cisco Unified Communications Manager에서 차단하려는 정확한 패턴을 입력해야 합니다.

- 학습 패턴 접두사 필드에 패턴 앞에 붙는 접두사를 기준으로 학습 패턴을 차단할 접두사를 입력합니다.

예제:

학습 패턴의 경우 235XX를 차단하려면 235XX를 입력합니다.

예제:

학습 패턴 접두사의 경우 +1을 사용하는 패턴을 차단하려면 +1을 입력합니다.

단계 4 원격 전화 컨트롤 엔티티 필드에 차단할 패턴을 광고하는 원격 전화 컨트롤 엔티티의 이름을 입력합니다.

단계 5 원격 IP 필드에 학습 패턴을 차단할 원격 전화 컨트롤 엔티티의 IP 주소를 입력합니다.

단계 6 저장을 클릭합니다.

통화 제어 탐색(CCD) 상호 작용

표 73: 통화 제어 탐색(CCD) 상호 작용

기능	상호 작용
알람	Cisco Unified Serviceability에는 통화 제어 검색 기능을 지원하는 알람이 있습니다. 알람을 구성하는 방법에 대한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html 에서 Cisco 통합 서비스 가용성 관리 가이드를 참조하십시오.
BLF 가입	SAF 학습 패턴의 BLF 상태를 가입하는 경우 Unified Communications Manager에서는 SIP 트렁크를 통해 원격 클러스터에 SIP 가입 메시지를 보냅니다. 이 기능은 SAF 사용 SIP 트렁크에서만 지원됩니다.
벌크 관리 도구	벌크 관리 도구에서 SAF 보안 프로파일, SAF 착신 전환기, CCD 어드버타이징 서비스, CCD 요청 서비스, 호스팅된 DN 그룹 및 호스팅된 DN 패턴 등에 대한 구성을 가져오거나 내보낼 수 있습니다.
통화 세부 정보 레코드	Unified Communications Manager에서는 재전송 사유로 통화가 PSTN 장애 조치 번호로 재전송됨을 나타내는 SS_RFR_SAF_CCD_PSTNFAILOVER를 사용하여 onBehalfOf를 AFCCDRequestingService로 재전송할 수 있습니다.

기능	상호 작용
수신 착신자 설정	<p>H.323 프로토콜은 국제 이스케이프 문자 +를 지원하지 않습니다. H.323 게이트웨이 또는 트렁크를 통한 착신 전화에 대한 SAF 및 통화 제어 검색에 올바른 DN 패턴이 사용되게 하려면 서비스 매개 변수, 디바이스 풀, H.323 게이트웨이 또는 H.323 트렁크 창에서 착신자 수신 설정을 구성해야 합니다. 즉, 착신자 수신 설정을 구성하면 착신 전화가 H.323 게이트웨이 또는 트렁크에서 오는 경우 Unified Communications Manager는 원래 트렁크 또는 게이트웨이를 통해 전송된 값으로 착신자 번호를 다시 변환합니다.</p> <p>예를 들어 발신자가 Unified Communications Manager A를 대상으로 +19721230000으로 전화를 건다고 가정합니다.</p> <p>Unified Communications Manager A는 +19721230000을 수신하고 통화를 H.323 트렁크로 보내기 전에 이 번호를 55519721230000으로 변환합니다. 이 경우, 구성에서는 국제 이스케이프 문자 +를 제거해야 하며 555를 [국제] 유형 통화 앞에 추가해야 함을 나타냅니다.</p> <p>이 착신 전화가 트렁크를 통해 오는 경우 Unified Communications Manager B는 55519721230000을 수신하고 번호를 다시 +19721230000으로 변환합니다. 그러면 발신자가 전송하는 이 값을 번호 분석에 사용할 수 있습니다. 이 경우, 착신자 수신 설정에 대한 구성에서는 555를 제거하고 +1을 [국제] 유형의 착신자 번호 앞에 추가해야 함을 나타냅니다.</p>
다이제스트 인증	<p>Unified Communications Manager는 다이제스트 인증(TLS 없는)을 사용하여 SAF 착신 전화기에 인증합니다. Unified Communications Manager에서 SAF 착신 전환기로 메시지를 전송하면 Unified Communications Manager가 SHA1 체크섬을 계산해서 메시지의 MESSAGE-INTEGRITY 필드에 포함합니다.</p>
QSIG	<p>H.323 구성 창의 QSIG 변형 및 ASN.1 ROSE OID 인코딩 설정은 CCD 광고 서비스에서 광고합니다. 이러한 설정은 터널링된 착신 통화의 QSIG 메시지의 디코딩에 영향을 미칩니다. 통화 제어 검색의 경우, 발신 통화에 영향을 미치지 않습니다.</p> <p>원격 통화 제어 엔티티가 H.323 트렁크를 통한 발신 통화의 QSIG 터널링이 필요한지 여부를 결정합니다. 원격 통화 제어 엔티티가 QSIG 터널링이 필요하다고 광고할 경우, Cisco Unified CM 관리의 H.323 구성 창의 QSIG 지원이 필요하지 않다고 표시되더라도, QSIG 메시지가 발신 통화의 메시지로 터널링됩니다.</p>

통화 제어 탐색(CCD) 제한 사항

모든 클러스터는 같은 AS(자율 시스템) 내의 광고되거나 설정된 경로로 제한됩니다.



60 장

외부 전화 제어 구성

- 외부 전화 제어 개요, 791 페이지
- 외부 전화 제어 사전 요건, 792 페이지
- 외부 전화 제어 구성 작업 흐름, 792 페이지
- 외부 전화 제어 상호 작용, 798 페이지
- 외부 전화 제어 제한 사항, 800 페이지

외부 전화 제어 개요

외부 통화 제어에서 Cisco Unified Routing Rules Interface를 사용하여 보조 라우트 서버가 Unified Communications Manager를 위한 콜 라우팅 결정을 내리도록 합니다. 외부 통화 제어를 구성할 때 Unified Communications Manager에서는 발신자 및 착신자 정보가 포함된 라우트 요청을 보조 라우트 서버에 대해 발행합니다. 해당 서버가 요청을 수신하고, 적절한 비즈니스 논리를 적용하고, 적용할 추가 콜 라우팅 방법에 대한 시스템 지침인 라우트 응답을 반환합니다.

임시 라우터 서버는 통화를 허용, 전환 또는 거부하고, 발신자 및 착신자 정보를 수정하고, 발신자에게 알림을 재생하고, 임시 음성 메일 및 IVR 서버가 발신자/착신자 정보를 제대로 해석할 수 있도록 통화 기록을 재설정하고, 통화가 전환 또는 거부된 이유를 나타내는 사유 코드를 기록하도록 시스템에 지시할 수 있습니다.

외부 전화 제어는 다음 기능을 제공합니다.

- 최고 품질 음성 라우팅 - 모든 통화 참가자에게 최고의 음성 품질을 제공하는 음성 게이트웨이를 통해 통화를 전송할 수 있도록 보조 라우트 서버에서 네트워크 링크 가용성, 대역폭 사용, 대기 시간, 지터 및 MOS 점수를 모니터링합니다.
- 최소 비용 라우팅 - 추가 라우트 서버는 가장 비용 효율적인 링크를 통해 통화가 라우팅되도록 로컬 액세스 및 전송 영역(LATA)과 LATA 간 요금제, 트렁크 비용 및 버스트 활용 비용과 같은 통신업체 계약 정보로 구성됩니다.
- 교신 차단 - 보조 라우트 서버에 연결성을 결정하는 회사 정책을 구성합니다(예: 사용자 1이 사용자 2에게 전화를 걸 수 있는지 여부).

외부 전화 제어 사전 요건

이 기능을 사용하려면 시스템에 통화를 처리하는 방법을 지시하는 Cisco Unified 라우팅 규칙 XML 인터페이스가 필요합니다.

자세한 내용은 <https://developer.cisco.com>의 *Cisco Unified* 라우팅 규칙 인터페이스 개발자 설명서 (CURRI 설명서)를 참조하십시오.

외부 전화 제어 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	외부 전화 제어를 위한 발신 검색 공간 구성, 793 페이지	라우트 서버에서 전환 의무를 보낼 때 사용할 시스템의 발신 검색 공간을 구성합니다. 발신 검색 공간은 디바이스에 할당되어 있는 정렬된 라우트 파티션 목록으로 구성됩니다. 발신 검색 공간은 통화를 완료하려고 시도할 때 발신 디바이스에서 검색하는 파티션을 결정합니다.
단계 2	외부 전화 제어 프로파일 구성, 794 페이지	외부 전화 제어 프로파일을 구성하여 보조 라우트 서버의 URI, 통화 전환에 사용되는 발신 검색 공간, 시스템이 보조 라우트 서버의 응답을 기다리는 시간을 나타내는 타이머 등을 제공합니다.
단계 3	변환 패턴에 프로파일 할당, 794 페이지	외부 통화 제어와 함께 사용할 변환된 패턴의 경우 외부 통화 제어 프로파일을 패턴에 할당합니다. 변환 패턴과 일치하는 통화가 발생하면 시스템에서 즉시 통화 라우팅 쿼리를 보조 라우트 서버로 전송하고 보조 라우트 서버는 통화 처리 방법을 시스템에 지시합니다.
단계 4	(선택 사항) 라우트 서버 인증서를 신뢰할 수 있는 저장소로 가져오기, 795 페이지	라우트 서버가 HTTPS를 사용하는 경우, 라우트 서버에 대한 인증서를 시스템 노드의 신뢰할 수 있는 저장소로 가져옵니다. 경로 서버에 라우팅 쿼리를 보낼 수 있는 클러스터의 각 노드에서 이 작업을 수행해야 합니다. 외부 전화 제어 프로파일에서 기본 또는 보조 웹 서비스 URI에 대해 HTTPS를 사용하는 경우 시스템이 구성된 보조 라우트 서버에 대한 TLS 연결

	명령 또는 동작	목적
		을 통해 상호 인증하는 데 인증서를 사용합니다.
단계 5	(선택 사항) SSC(자가서명 인증서)를 라우트 서버로 내보내기, 795 페이지	<p>라우트 서버가 HTTPS를 사용하는 경우 Cisco Unified Communications Manager 자체 서명 인증서를 라우트 서버로 내보냅니다. 경로 서버에 라우팅 쿼리를 보낼 수 있는 클러스터의 각 노드에서 이 작업을 수행해야 합니다. 기본 및 중복 라우트 서버가 HTTPS를 통해 Cisco Unified Communications Manager에 인증될 수 있게 하려면 시스템에 지시문을 보내는 각 보조 라우트 서버로 가져올 수 있는 SSC(자가서명 인증서)를 생성해야 합니다.</p> <p>기본 및 중복 보조 라우트 서버에 연결할 수 있는 클러스터의 각 노드에 대해 이 절차를 수행합니다.</p>
단계 6	(선택 사항) Chaperone 기능 구성, 796 페이지	라우트 서버의 라우팅 규칙이 샤프롱(chaperone)이 통화를 모니터링하거나 기록해야 하는 경우 샤프롱 기능을 구성합니다. 샤프롱은 통화에 회사 정책을 안내하고 통화를 모니터링하며 통화를 녹음할 수 있도록 지정된 전화기 사용자입니다.
단계 7	(선택 사항) 사용자 정의된 알림 구성, 797 페이지	라우팅 규칙에서 일부 통화에 대해 알림이 생성되어야 하고 Cisco에서 제공하는 알림을 사용하지 않으려는 경우 다음 절차를 수행합니다.

외부 전화 제어를 위한 발신 검색 공간 구성

라우트 서버에서 전환 의무를 보낼 때 사용할 시스템의 발신 검색 공간을 구성합니다. 발신 검색 공간은 디바이스에 할당되어 있는 정렬된 라우트 파티션 목록으로 구성됩니다. 발신 검색 공간은 통화를 완료하려고 시도할 때 발신 디바이스에서 검색하는 파티션을 결정합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 제어 클래스 > 발신 검색 공간을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 이름 필드에 이름을 입력합니다.

각 발신 검색 공간 이름은 시스템에 고유해야 합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.

단계 4 설명 필드에 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.

단계 5 사용 가능한 파티션 드롭다운 목록에서 다음 단계 중 하나를 수행합니다.

- 단일 파티션의 경우 해당 파티션을 선택합니다.
- 여러 파티션의 경우 컨트롤(**CTRL**) 키를 누른 상태에서 해당 파티션을 선택합니다.

단계 6 상자 사이에서 아래쪽 화살표를 선택하여 선택한 파티션 필드로 파티션을 이동합니다.

단계 7 (선택 사항) 선택한 파티션 상자 오른쪽의 화살표 키를 사용하여 선택한 파티션의 우선 순위를 변경합니다.

단계 8 저장을 클릭합니다.

외부 전화 제어 프로파일 구성

외부 전화 제어 프로파일을 구성하여 보조 라우트 서버의 URI, 통화 전환에 사용되는 발신 검색 공간, 시스템이 보조 라우트 서버의 응답을 기다리는 시간을 나타내는 타이머 등을 제공합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 외부 전화화 제어 프로파일을 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 찾기를 클릭한 후 결과 목록에서 기존 외부 전화 제어 프로파일을 선택하여 기존 외부 전화 제어 프로파일에 대한 설정을 수정하고 검색 기준을 입력합니다.
- 새 외부 전화 제어 프로파일을 추가하려면 새로 추가를 클릭합니다.

단계 3 외부 전화 제어 프로파일 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

변환 패턴에 프로파일 할당

외부 전화 제어 프로파일을 구성하여 보조 라우트 서버의 URI, 통화 전환에 사용되는 발신 검색 공간, 시스템이 보조 라우트 서버의 응답을 기다리는 시간을 나타내는 타이머 등을 제공합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 콜 라우팅 > 변환 패턴을 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 찾기를 클릭한 다음 결과 목록에서 기존 변환 패턴을 선택하여 기존 변환 패턴에 대한 설정을 수정하고 검색 기준을 입력합니다.
- 새로 추가를 클릭하여 변환된 패턴을 새로 추가합니다.

단계 3 외부 통화 제어 프로파일 드롭다운 목록에서 패턴에 할당할 외부 통화 제어 프로파일을 선택합니다.

단계 4 변환 패턴 구성 창에서 필요한 경우 다른 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

라우트 서버 인증서를 신뢰할 수 있는 저장소로 가져오기

라우트 서버가 HTTPS를 사용하는 경우, 라우트 서버에 대한 인증서를 시스템 노드의 신뢰할 수 있는 저장소로 가져옵니다. 경로 서버에 라우팅 쿼리를 보낼 수 있는 클러스터의 각 노드에서 이 작업을 수행해야 합니다. 외부 전화 제어 프로파일에서 기본 또는 보조 웹 서비스 URI에 대해 HTTPS를 사용하는 경우 시스템이 구성된 보조 라우트 서버에 대한 TLS 연결을 통해 상호 인증하는 데 인증서를 사용합니다.

프로시저

단계 1 Cisco Unified 운영 체제 관리에서 보안 > 인증서 관리를 선택합니다.

단계 2 인증서 업로드를 클릭합니다.

단계 3 인증서 업로드 팝업 창의 인증서 이름 드롭다운 목록에서 **CallManager-trust**를 클릭하고 보조 라우트 서버의 인증서를 찾습니다.

단계 4 파일 업로드 필드에 인증서가 나타나면 업로드를 클릭합니다.

단계 5 (선택 사항) 시스템에서 이중화 보조 라우트 서버에 연결할 수 있는 경우 이 절차를 다시 수행합니다.

SSC(자가서명 인증서)를 라우트 서버로 내보내기

라우트 서버가 HTTPS를 사용하는 경우 Unified Communications Manager SSC(자가서명 인증서)를 라우트 서버로 내보냅니다. 경로 서버에 라우팅 쿼리를 보낼 수 있는 클러스터의 각 노드에서 이 작업을 수행해야 합니다. 기본 및 중복 라우트 서버가 HTTPS를 통해 Unified Communications Manager에 인증될 수 있게 하려면 시스템에 지시문을 보내는 각 보조 라우트 서버로 가져올 수 있는 SSC(자가서명 인증서)를 생성해야 합니다.

기본 및 중복 보조 라우트 서버에 연결할 수 있는 클러스터의 각 노드에 대해 이 절차를 수행합니다.

프로시저

-
- 단계 1 Cisco Unified Operating 관리에서 보안 > 인증서 관리를 선택합니다.
- 단계 2 인증서 목록 창에서 새로 생성을 클릭합니다.
- 단계 3 인증서 이름 드롭다운 목록에서 **CallManager**를 선택합니다.
- 단계 4 지금 생성을 클릭합니다.
- 단계 5 인증서 찾기 및 나열 창에서 방금 생성한 **CallManager.pem** 인증서를 선택합니다.
- 단계 6 인증서 파일 데이터가 표시되면 다운로드를 클릭하여 인증서를 보조 라우트 서버로 내보내는 데 사용할 수 있는 위치로 인증서를 다운로드합니다.
- 단계 7 지시문을 보내는 각 보조 라우트 서버로 인증서를 내보냅니다.
-

Chaperone 기능 구성

라우트 서버의 라우팅 규칙이 샤프롱(chaperone)이 통화를 모니터링하거나 기록해야 하는 경우 샤프롱 기능을 구성합니다. 샤프롱은 통화에 회사 정책을 안내하고 통화를 모니터링하며 통화를 녹음할 수 있도록 지정된 전화기 사용자입니다.

Unified Communications Manager는 보조 라우트 서버에서 지정하는 대로 샤프롱 기능을 지원하기 위해 다음과 같은 기능을 제공합니다.

- 수신 통화를 chaperone, 힌트 그룹 또는 chaperones 목록으로 재전송합니다.
- 통화를 녹음하는 기능을 제공하는 chaperone을 제공합니다.

chaperone이 발신자에게 연결되었거나 chaperone 전화회의가 구축된 경우 전화기의 녹음 소프트웨어 또는 PLK(프로그래밍 가능한 라인 키)(전화기 모델에 따라 다름)가 활성화되고 chaperone이 통화 녹음을 호출할 수 있습니다. 통화 녹음은 현재 통화에서만 발생하며 현재 통화가 종료되면 통화 녹음이 중단됩니다. 샤프롱이 녹음 소프트웨어 또는 PLK를 누르면 녹음 상태를 나타내는 메시지에 전화기가 표시됩니다.

프로시저

-
- 단계 1 녹음을 활성화할 전화기의 경우 전화기 구성 창에서 빌트-인 브리지(BIB)를 켜기로 설정합니다.
- 단계 2 녹음 프로파일을 만듭니다.
- a) 디바이스 > 디바이스 설정 > 녹음 프로파일을 선택합니다.
 - b) 감독받는 전화회의를 녹음할 수 있는 전화기의 통화 녹음 프로파일을 만듭니다.
- 단계 3 녹음 프로파일을 회선 표시에 적용합니다.
- 단계 4 레코더를 가리키는 SIP 트렁크 추가
- 단계 5 SIP 트렁크를 가리키는 라우트 패턴을 만듭니다.
- 단계 6 다음 서비스 매개 변수를 구성합니다.

- a) 관찰 대상에게 녹음 알림 신호음 재생
- b) 연결된 관찰 대상에게 녹음 알림 신호음 재생

단계 7 표준 샤프롱 전화기 소프트키 템플릿을 샤프롱이 사용하는 전화기에 할당합니다.

단계 8 전화기가 이미 구성된 경우 새 전화기에 대해 통화 라우팅 > 디렉터리 이름 또는 디바이스 > 전화기에서 다음 단계를 수행합니다.

- a) 샤프롱 전화기에 대해 디렉터리 번호(DN)를 하나만 구성합니다.
- b) 샤프롱 전화기의 DN에 대해 녹음 옵션 드롭다운 목록 상자에서 디바이스 호출 통화 녹음 활성화를 선택합니다.
- c) 샤프롱 전화기의 DN에 대해 최대 통화 수 설정에 2를 입력하고 통화 중 트리거 설정에 1을 입력합니다.

단계 9 녹음 소프트키를 지원하는 Cisco Unified IP Phone의 경우 전화회의, 녹음 및 통화종료 소프트키만 연결된 상태의 전화기에 표시되도록 표준 샤프롱 전화기 소프트키 템플릿이 구성되어 있는지 확인합니다.

단계 10 녹음 PLK(프로그램 가능 회선 키)를 지원하는 Cisco Unified IP Phone의 경우 전화기 버튼 템플릿 구성 창에서 [PLK]를 구성합니다.

단계 11 (선택 사항) 클러스터에 샤프롱이 둘 이상인 경우에는 샤프롱 힌트 목록에 할당할 샤프롱 회선 그룹에 샤프롱 DN을 추가합니다.

이 단계를 통해 사용 가능한 chaperone이 통화를 모니터링합니다.

사용자 정의된 알림 구성

라우팅 규칙에서 일부 통화에 대해 알림이 재생되어야 하고 Cisco에서 제공하는 알림을 사용하지 않으려는 경우 다음 절차를 수행합니다.



팁 알림 식별자에는 포함된 공백을 사용하지 마십시오.

다른 언어 로캘이 설치된 경우 이 알림에 대해 다른 .wav 파일을 업로드하여 해당 로캘과 함께 사용할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 미디어 리소스 > 공지사항을 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 새 알림을 추가하려면:
 - a) 새로 추가를 클릭합니다.
 - b) 알림 ID 필드에 알림 ID를 입력합니다.
 - c) 설명에 알림에 대한 설명을 입력합니다.

- d) 기본 알림 드롭다운 목록에서 원하는 경우 기본 Cisco 제공 알림을 선택합니다.
- e) 저장을 클릭합니다.
 - 알림에 대한 사용자 정의 .wav 파일을 업로드하려면:
 - a) 파일 업로드를 클릭합니다.
 - b) 로컬 드롭다운 목록에서 알림에 대한 로컬 언어를 선택합니다.
 - c) 파일 선택을 클릭한 다음 업로드할 .wav 파일을 선택합니다.
 - d) 파일 업로드를 클릭합니다.
 - e) 업로드가 완료되면 닫기를 클릭하여 창을 새로 고치고 업로드된 알림을 표시합니다.

외부 전화 제어 상호 작용

표 74: 외부 전화 제어 상호 작용

기능	상호 작용
최고 통화 품질 라우팅	보조 라우트 서버에서 통화에 사용할 게이트웨이를 결정하고, 음성 품질을 고려하여 라우팅 규칙을 설정할 수 있습니다. 예를 들어, 게이트웨이 A는 최상의 음성 품질을 제공하므로 통화에 사용됩니다. 이 경우 보조 라우트 서버는 네트워크 링크 사용 가능성, 대역폭 사용량, 대기 시간, 지터 및 MOS(평균 평가점)을 모니터링하여 모든 통화 참가자에게 최상의 음성 품질을 제공하는 음성 게이트웨이를 통해 통화가 전송되는지 확인합니다.
통화 세부 정보 레코드	통화 세부 정보 레코드에는 외부 전화 제어 기능이 표시될 수 있습니다. 예를 들어 통화 세부 정보 레코드에는 보조 라우트 서버에서 통화를 허용했는지, 아니면 거부했는지 표시될 수 있습니다. 또한, 통화 세부 정보 레코드에는 Unified Communications Manager가 보조 라우트 서버의 결정을 받지 못한 경우 Unified Communications Manager가 통화를 차단했는지, 아니면 허용했는지 표시될 수 있습니다.
통화 착신 전환	외부 전화 제어에서는 변환 패턴 수준에서 통화를 차단하지만, 통화 착신 전환에서는 디렉터리 번호 수준에서 통화를 차단합니다. 외부 전화 제어는 착신 전환보다 우선 순위가 높습니다. 착신 전환을 호출하는 통화의 경우, Unified Communications Manager는 변환 패턴이 외부 전화 제어 프로파일 에 할당된 경우 라우팅 쿼리를 보조 라우트 서버로 보냅니다. 착신 전환은 보조 라우트 서버에서 계속 의무와 함께 허용 결정을 Cisco Unified Communications Manager로 보내는 경우에만 트리거됩니다. 참고 외부 전화 제어를 지원하는 통화 전환 흡수 서비스 매개 변수 및 착신 전환을 지원하는 착신 전환 통화 흡수 서비스 매개 변수는 별개입니다.

기능	상호 작용
통화 당겨받기	전화기 사용자가 통화 당겨받기 기능을 사용하여 통화를 당겨받으려고 할 때는 외부 전화 제어가 호출되지 않습니다. Unified Communications Manager는 통화의 해당 부분에 대한 라우팅 쿼리를 보조 라우트 서버로 보내지 않습니다.
샤프롱(Chaperone)	샤프롱은 필요 시 통화에 회사 정책을 안내하고 통화를 모니터링하며 통화를 녹음할 수 있도록 지정된 전화기 사용자입니다. 통화에 연결된 당사자들이 샤프롱이 없을 때 대화할 수 없도록 하는 샤프롱 제한이 있습니다.
Cisco Unified Mobility	<p>Unified Communications Manager는 다음 Cisco Unified Mobility 기능에 대해 보조 라우트 서버의 라우트 결정을 따릅니다.</p> <ul style="list-style-type: none"> • 모바일 음성 액세스 • 엔터프라이즈 기능 액세스 • DVO(Dial-via-Office) 역방향 콜백 <p>Unified Communications Manager는 다음 Cisco Unified Mobility 기능에 대한 라우팅 쿼리를 보내지 않습니다.</p> <ul style="list-style-type: none"> • 휴대폰 당겨받기 • 사무실 전화 당겨받기 • 세션 전환
전화회의	전화기 사용자가 전화회의를 생성하는 경우 기본 통화 및 상담 통화에 대해 외부 전화 제어가 호출될 수 있습니다.
디렉터리 번호	디렉터리 번호를 4자리 또는 5자리 내선 번호(기업 내선 번호)로 구성할 때 온넷 다이얼링이 4자리 또는 5자리를 지원하는 경우 2가지 변환 패턴을 구성해야 합니다. 첫 번째 변환 패턴은 발신 및 착신 번호 전역화를 지원하고, 두 번째 변환 패턴은 발신 및 착신 번호 지역화를 지원합니다.
DND(Do Not Disturb)	기본적으로, 사용자에게 대한 DND 설정은 보조 라우트 서버의 사용자 규칙이 보조 라우트 서버에서 계속 의무를 보냄을 나타내는 경우에 적용됩니다. 예를 들어 보조 라우트 서버에서 계속 의무를 보내는 경우 사용자 측에 DND-R이 활성화되어 있으면 Unified Communications Manager는 통화를 거부합니다.
비상 통화 처리	<p>주의</p> <p>비상 통화(예: 911 또는 9.11)에 대한 명시적 패턴 세트를 구성하는 것이 좋습니다. 그러면 통화 처리 방법에 대한 지침을 위해 경로 서버에 연결할 필요 없이 통화가 적절한 대상(예: Cisco Emergency Responder 또는 게이트웨이)으로 전송될 수 있습니다.</p>

기능	상호 작용
호전환	전화기 사용자가 호전환하는 경우 기본 통화와 상담 통화 모두에 대해 외부 전화 제어가 호출될 수 있습니다. 그러나 Unified Communications Manager는 호전환되는 상대방과 호전환 대상 간의 모든 라우팅 규칙을 보조 라우트 서버에서 시행할 수 없습니다.

외부 전화 제어 제한 사항

표 75: 외부 전화 제어 제한 사항

제한 사항	설명
당사자 추가	<p>샤프롱이 당사자를 추가하려면 통화를 보류해야 하므로 전화회의가 시작된 이후 전화기를 사용하여 당사자를 전화회의에 추가할 수 없습니다.</p> <p>전화회의의 다른 당사자는 전화회의에 당사자를 추가할 수 있습니다. Cisco CallManager 서비스를 지원하는 고급 애드-혹 컨퍼런스 활성화 서비스 매개 변수 구성에 따라 다른 당사자가 참가자를 전화회의에 추가할 수 있는지 여부가 결정됩니다. 서비스 매개 변수가 True로 설정된 경우 다른 당사자가 전화회의에 참가자를 추가할 수 있습니다.</p>
통화 전환	샤프롱은 전화기를 사용하여 전화회의 통화를 다른 당사자에게 호전환할 수 없습니다.
전화회의 로그아웃	샤프롱이 전화회의에서 나가면 전체 전화회의가 종료됩니다.
전화회의 소프트키	샤프롱이 전화회의를 생성한 다음, 사용 가능한 경우 전화기의 전화회의 소프트키가 비활성화됩니다.
보류	샤프롱은 전화기를 사용하여 전화회의 통화를 보류할 수 없습니다.
녹음	샤프롱이 전화회의에 참가해야 하는 당사자에게 상담 전화를 걸기 전에 녹음을 시작하면 Unified Communications Manager는 샤프롱이 상담 통화를 하는 동안 녹음을 일시 중지하고 전화회의가 구축된 이후 녹음이 재개됩니다.



61 장

통화 대기열 구성

- [통화 대기 개요, 801 페이지](#)
- [통화 대기 사전 요건, 803 페이지](#)
- [통화 대기 작업 흐름, 803 페이지](#)
- [통화 지정 보류 상호 작용, 810 페이지](#)
- [통화 대기 제한 사항, 811 페이지](#)
- [통화 대기가 포함된 힌트 파일럿의 성능 및 확장성, 811 페이지](#)

통화 대기 개요

Unified Communications Manager는 통화 대기를 제공하여 힌트 구성원이 응답할 수 있을 때까지 대기열에 발신자를 배치합니다. 관리자는 통화를 상담사에게 확장하기 전에 발신자가 초기 인사말 알림을 수신하도록 기본값을 설정할 수 있습니다. 또는 기본값을 변경하여 발신자가 대기열에 배치된 후에 대기 중 음악 또는 대기 중으로 설정된 후에만 초기 알림이 재생되도록 할 수 있습니다. 발신자가 지정된 시간 동안 대기열에 유지될 경우 통화에 응답하거나 최대 대기 타이머가 만료될 때까지 구성되어 있는 간격으로 보조 알림이 재생됩니다.

수신 통화가 힌트 파일럿에 도달하면 다음 기능이 제공됩니다.

- 발신자는 계속하기 전에 초기 사용자 지정 인사말 알림에 연결될 수 있습니다.
- 한 명 이상의 회선 구성원이 힌트 파일럿에 로그인되어 있고 유휴 상태이며 대기열에 통화가 없는 경우 가장 긴 시간 동안 유휴 상태였던 회선 구성원으로 통화가 확장됩니다.
- 통화에 응답하는 회선 구성원이 없을 경우 발신자는 대기열에 추가되지 않습니다. 통화가 "로그인되거나 등록된 힌트 구성원 응답이 없는 경우" 설정을 기준으로 새 대상으로 라우팅되거나 끊깁니다.
- 회선 구성원이 대기열이 활성화된 통화에 응답하지 않을 경우 회선 그룹 창에서 응답이 없는 경우 힌트 구성원 자동 로그아웃 설정이 선택된 경우에만 해당 회선 구성원이 힌트 그룹에서 로그오프됩니다.
- 모든 구성원이 통화 중일 경우에만 통화가 대기열에 추가됩니다.
- 대기열에서 대기 중인 발신자는 대기 중 음악과 반복되는(사용자 지정 가능) 주기적 알림을 들을 수 있습니다.

- 회선 구성원이 유휴 상태가 된 후 여러 헌트 그룹에서 가장 오래 대기한 발신자가 유휴 회선 구성원으로 확장됩니다. 유휴 회선 번호가 통화에 응답하지 않을 경우 발신자는 대기열의 이전 위치로 복귀됩니다.
- 대기 중인 통화가 최대 대기 시간을 초과하거나 대기열에서 허용되는 최대 발신자 수를 초과하는 경우, 통화를 대체 번호로 라우팅하거나, 헌트 파일럿이 구성된 방식에 따라 연결을 끊을 수 있습니다. 대체 번호는 다음 중 하나일 수 있습니다.
 - 대기를 활성화 또는 비활성화한 헌트 파일럿 DN
 - 보이스메일 DN
 - 회선 DN
 - 공유 DN
- 회선 구성원은 대기열 사용 헌트 파일럿의 대기열 상태를 표시할 수 있습니다. 대기열 상태 표시는 다음과 같은 정보를 제공합니다.
 - 헌트 파일럿 패턴
 - 각 헌트 파일럿에서 대기열에 추가된 발신자 수
 - 최대 대기 시간

통화 대기는 기존 헌트 파일럿과 연계하여 작동하지만 대기 또는 비대기 헌트 파일럿에 대한 헌팅 작업 동작은 달라지지 않습니다. 통화 대기를 활성화한 헌트 파일럿은 다음과 같은 기능을 제공합니다.

- 대기-활성화 헌트 파일럿 통화는 회선 구성원이 한 번에 하나씩만 수신할 수 있습니다. 2개의 대기-활성화 헌트 파일럿 통화를 한 명의 회선 구성원에게 제공할 수 없습니다. 회선 구성원은 DN으로 직접 통화를 수신하거나 비-대기 헌트 파일럿의 통화를 수신할 수 있습니다.
- 헌트 파일럿에 의해 라우팅되는 응답하지 않는 회선 구성원은 자동으로 로그아웃됩니다. 대기-활성화 헌트 파일럿 통화를 수신한 회선 구성원이 초과가 발생하기 전에 통화에 응답하지 않을 경우 디바이스에서 자동으로 로그아웃됩니다. 공유 회선 배포의 경우 동일한 공유 회선으로 구성된 모든 디바이스가 로그아웃됩니다. 회선 그룹 설정 창에서 응답이 없는 경우 헌트 구성원 자동 로그아웃을 선택하여 이 동작을 구성할 수 있습니다. 회선 구성원은 이 확인란을 선택한 경우에만 로그아웃됩니다.

통화 대기열 모니터링 또는 알림 모니터링에 대한 자세한 내용은 *Cisco Unified* 실시간 모니터링 도구 관리 지침서를 참조하십시오.

통화가 대기열 사용 헌트 파일럿의 헌트 구성원으로 확장되는 동안 대기 알림을 재생하기 전에 연결된 통화 상태로 변경하도록 인바운드 통화를 구성할 수 있습니다.

보안 통화 대기



중요 이 섹션은 14SU2 이후 릴리스부터 적용할 수 있습니다.

보안 통화가 힌트 파일럿에 추가되고 모든 회선 그룹이 사용 중인 경우 대기열에서 대기 중인 발신자는 라이브 상담사가 통화에 응답할 때까지 대기 중 음악 및 반복되는 (사용자 지정 가능) 정기 알람을 들을 수 있습니다. 이 프로세스 중에 통화는 일시적으로 보류됩니다. 엔드포인트에서 SRTP 폴백 기능이 지원되지 않는 경우 지정 보류 중 (비보안 장치)에 발신된 통화는 암호화 불일치로 인해 꺼집니다.

Unified Communications Manager는 기본 통화 대기열에 대한 보안 통화 지원을 향상하여 임시 보류 통화의 암호화 기능을 활성화하고 통화 드롭 다운을 방지할 수 있습니다. Unified CM는 SRTP 폴백 옵션 상태와 관계 없이 발신된 SRTP(실시간 전송 프로토콜) 전용 통화를 보안 통화로 처리합니다.

통화 대기 사전 요건

- 클러스터의 하나 이상의 노드에서 Cisco IPVMS(IP Voice Media Streaming)를 활성화해야 합니다.
- 클러스터에 있는 하나 이상의 서버에서 실행 중인 Cisco CallManager 서비스
- Cisco CallManager 서비스와 동일한 서버에서 실행 중인 Cisco RIS Data Collector 서비스
- Cisco Unified Communications Manager 로컬 설치 관리자(영어 이외의 전화기 로컬 또는 국가별 신호음을 사용하려는 경우)

통화 대기 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	알림 구성, 803 페이지	.wav 파일 업로드를 통해 알람을 구성합니다.
단계 2	대기 중 음악 구성, 805 페이지	대기 중 음악(MoH) 오디오 소스를 구성합니다.
단계 3	힌트 파일럿 대기 구성, 808 페이지	응답될 때까지 대기열에 있는 통화에 대해 통화 대기 보류 옵션을 활성화합니다.
단계 4	응답이 없는 경우 힌트 구성원 자동 로그아웃, 810 페이지	회선 구성원이 자동으로 힌트 목록을 로그아웃시킬 수 있습니다.

알림 구성

Cisco Unified Communications Manager를 사용하면 다음을 수행할 수 있습니다.

- 기존 Cisco 제공 알람을 사용합니다.
- 알람을 재생할 메시지나 신호음을 변경합니다.

- 사용자 정의 알림 .wav 파일을 삽입합니다.
- 알림에 대한 로깅을 할당합니다.
- 알림에 대한 설명을 변경합니다.
- 알림을 재생할 메시지나 신호음을 변경합니다.

기능 알림은 힌트 파일럿 통화 대기 또는 외부 전화 제어와 연계하여 특정 기능(예: MOH(대기 중 음약))에 사용됩니다.

최대 50개의 기능 알림을 사용할 수 있습니다. 이러한 알림은 Cisco에서 제공하는 오디오 파일일 수도 있고 업로드된 사용자 정의 wav 파일일 수도 있습니다.

모든 사용자 정의 알림 wav 파일은 클러스터의 모든 서버에 업로드되어야 합니다.

프로시저

단계 1 Cisco Unified Communications Manager 관리에서 미디어 리소스 > 알림을 선택합니다.

알림 찾기 및 나열 창이 표시됩니다.

단계 2 사용할 알림에 대한 하이퍼링크를 선택합니다.

예제:

Hyperlink—Wait_In_Queue_Sample

알림 설명을 편집하거나 업로드한 경우 사용자 정의된 알림을 선택할 수 있습니다.

단계 3 사용자 정의 알림에 사용할 .wav 파일을 업로드하려면 파일 업로드를 클릭합니다.

파일 업로드 창이 열립니다.

단계 4 파일 업로드 창에서 로깅을 선택하고 파일 이름을 입력하거나 .wav 파일을 탐색하여 선택한 다음 파일 업로드를 클릭합니다.

업로드 프로세스가 시작되며 파일에 따라 몇 분이 걸릴 수 있습니다. 처리가 완료되면 상태가 업데이트됩니다.

단계 5 업로드 창을 종료하려면 닫기를 클릭합니다.

알림 구성 창이 새로 고침되고 업로드된 파일 상태가 업데이트됩니다.

단계 6 사용자 정의된 알림을 재생하려면 알림 구성 창의 로깅별 알림 창에서 활성화 확인란이 선택되어 있는지 확인합니다.

단계 7 알림 구성 창에서 변경을 수행한 후 저장을 클릭합니다.

다음에 수행할 작업

알림 파일은 클러스터 내 서버 간에 전파되지 않으므로 클러스터의 각 노드에서 알림을 업로드해야 합니다. 클러스터 내 각 서버에서 Cisco Unified Communications Manager 관리를 탐색하여 업로드 프로세스를 반복합니다.

대기 중 음악 구성

MoH(대기 중 음악)를 구성하여 발신자가 처음으로 보류될 때 선택적 초기 인사말 알림을 재생하고 주기적으로 반복되는 알림을 재생할 수 있습니다. 이러한 알림은 시스템에 업로드된 Cisco 제공 오디오 파일 또는 파일을 사용할 수 있습니다.

다음 절차를 수행하여 대기 중 음악 오디오 소스를 추가 또는 업데이트하거나, 기존 오디오 소스를 오디오 스트림 번호와 연결하거나, 새 사용자 지정 오디오 소스를 업로드합니다.

프로시저

- 단계 1 Cisco Unified Communications Manager에서 미디어 리소스 > 대기 중 음악 오디오 소스를 선택합니다.
대기 중 음악 오디오 소스 찾기 및 나열 창이 표시됩니다.
- 단계 2 대기 중 음악 오디오 소스를 새로 추가하려면 새로 추가를 클릭합니다. 대기 중 음악 오디오 소스를 업데이트하려면 대기 중 음악 오디오 소스를 찾습니다. 지정한 검색 기준에 따라, 시스템은 모든 기준과 일치하는 레코드에 대한 검색 결과를 표시합니다.
- 단계 3 [대기 중 음악에 대한 오디오 소스 필드, 805 페이지](#)에 설명된 대로 적절한 설정을 입력합니다.
- 단계 4 저장을 클릭합니다.
창의 맨 아래에 있는 목록 상자에는 새 대기 중 음악 오디오 소스가 표시됩니다. MOH 오디오 소스 파일 상태 창을 보면 추가된 오디오 소스의 MOH 오디오 변환 상태를 알 수 있습니다.

대기 중 음악에 대한 오디오 소스 필드

표 76: MoH 오디오 소스 정보

필드	설명
MoH 오디오 스트림 번호	이 필드를 사용하여 이 MoH 오디오 소스의 스트림 번호를 선택합니다. 드롭다운 목록을 클릭하고 목록에서 값을 선택합니다. 기존 MoH 오디오 소스의 경우 이 값은 MOH 오디오 소스 제목에 나타납니다.
MoH 오디오 소스 파일	이 필드를 사용하여 이 MoH 오디오 소스의 파일을 선택합니다. 드롭다운 목록을 클릭하고 값을 선택합니다.
MoH 오디오 소스 이름	이 필드에 MoH 오디오 소스의 고유한 이름을 입력합니다. 이 이름에는 문자, 숫자, 공백, 대시, 점(주기) 및 밑줄과 같은 최대 50개의 유효한 문자가 포함됩니다.
멀티캐스팅 허용	선택된 MOH 오디오 소스가 멀티캐스팅을 허용하도록 지정하려면 이 확인란을 선택합니다.

필드	설명
MoH 오디오 소스 파일 상태	<p>이 창은 선택된 MOH 오디오 소스의 소스 파일에 대한 다음 정보를 표시합니다.</p> <ul style="list-style-type: none"> • InputFileName • ErrorCode • ErrorText • DurationSeconds • DiskSpaceKB • LowDateTime • HighDateTime • OutputFileList • MOH 오디오 변환 완료 날짜 <p>참고 OutputFileList는 ULAW, ALAW, G.729 및 와이드밴드 wav 파일 및 상태 옵션에 대한 정보를 포함합니다.</p>

표 77: 알림 설정

필드	설명
초기 알림	<p>드롭다운 목록에서 초기 알림을 선택합니다.</p> <p>참고 초기 알림 없음으로 MoH를 선택하려면 선택되지 않음 옵션을 선택합니다.</p> <p>다음 초기 알림 정보를 보려면 세부 정보 보기 링크를 클릭합니다.</p> <ul style="list-style-type: none"> • 알림 ID • 설명 • 기본 알림 <p>참고</p> <ul style="list-style-type: none"> • 멀티캐스팅 허용 오디오 소스를 선택하지 않고 대기열 사용 기능이 있는 힌트 파일럿 통화에 대한 초기 알림통화가 대기 상태에 있는 경우 알림 재생으로 설정된 경우에만 MOH 서버에서 재생됩니다. • 멀티캐스팅 허용 확인란을 선택했거나 대기열 사용 기능이 있는 힌트 파일럿 통화에 대한 초기 알림이 힌트 구성원에게 라우팅하기 전에 알림 재생으로 설정된 경우 ANN에서 재생합니다.

필드	설명
대기열 사용 기능이 있는 헌트 파일럿 통화에 대한 초기 알림	<p>다음 중 하나를 선택하여 초기 알림을 재생할 시기를 결정합니다.</p> <ul style="list-style-type: none"> • 헌트 구성원에게 라우팅하기 전에 알림 재생 • 통화가 대기 상태에 있는 경우 알림 재생
주기적 알림	<p>드롭다운 목록에서 주기적 알림을 선택합니다.</p> <p>참고 주기적 알림 없음으로 MoH를 선택하려면 선택되지 않음 옵션을 선택합니다.</p> <p>다음 주기적 알림 정보를 보려면 세부 정보 보기 링크를 클릭합니다.</p> <ul style="list-style-type: none"> • 알림 ID • 설명 • 기본 알림 <p>참고 MOH 서버가 다른 설정과 상관없이 주기적 알림을 재생합니다.</p>
주기적 알림 간격	<p>주기적 알림 간격을 지정하는 값(초)을 입력합니다. 유효한 값은 10-300입니다. 기본값은 30입니다.</p>
로케일 알림	<p>로캘 알림은 설치된 로캘 설치 패키지에 따라 다릅니다.</p> <p>참고 • MoH에서 재생하는 프롬프트는 로캘 알림에 대한 설정을 사용합니다.</p> <p> • ANN에서 재생하는 프롬프트는 발신자의 사용자 로케일을 사용합니다.</p>

표 78: MoH(대기 중 음악) 오디오 소스

필드	설명
(MoH 오디오 소스 목록)	<p>이 목록 상자에는 추가하는 MOH 오디오 소스가 표시됩니다. MOH 오디오 소스를 구성하려면 MOH 오디오 소스의 오디오 스트림 번호를 선택합니다.</p> <p>오디오 소스 ID는 대기 중 음악 서버의 오디오 소스를 나타내는 ID입니다. 오디오 소스는 소스 스트림 대기 중 음악 서버가 스트리밍 데이터를 가져오는 디스크의 파일 또는 고정 디바이스를 포함할 수 있습니다. MOH 서버는 최대 51개의 오디오 소스 ID를 지원할 수 있습니다. 오디오 소스 ID로 나타내는 각 오디오 소스는 필요에 따라 유니캐스트 및 멀티캐스트 모드로 스트림할 수 있습니다.</p> <p>참고 <None>을 선택한 경우 MoH 오디오 소스에 대해 시스템 기본 값 MoH 오디오 소스 서비스 매개 변수(기본 네트워크 보류 MoH 오디오 소스 ID)가 사용됩니다.</p>
파일 업로드	<p>드롭다운 목록에 나타나지 않은 MOH 오디오 소스 파일을 업로드하려면 파일 업로드를 클릭합니다. 파일 업로드 창에서 오디오 소스 파일의 라우트를 입력하거나 찾아보기를 클릭하여 파일을 탐색합니다. 오디오 소스 파일을 찾은 다음 파일 업로드 버튼을 클릭하여 업로드를 완료합니다. 오디오 파일이 업로드된 후 [업로드 결과] 창에 업로드 결과가 표시됩니다. 이 창을 닫으려면 단기를 클릭합니다.</p> <p>참고 파일을 업로드하면 파일이 Unified Communications Manager 서버에 업로드되고 오디오 변환을 수행하여 MOH를 위한 코덱별 오디오 파일을 생성합니다. 원본 파일의 크기에 따라 완료되는 데 몇 분이 소요될 수 있습니다.</p> <p>참고 오디오 소스 파일을 MoH 서버로 업로드하면 파일이 한 대의 MoH 서버로만 업로드됩니다. 각 서버에서 Cisco Unified Communications Manager 관리를 사용하여 클러스터의 각 MoH 서버로 오디오 소스 파일을 업로드해야 합니다. MOH 오디오 소스 파일은 클러스터의 다른 MoH 서버로 자동으로 전파되지 않습니다.</p>

헌트 파일럿 대기 구성

헌트 파일럿의 통화 중 통화 분배 기능을 통해 분배된 통화가 지정된 시간에 헌트 구성원이 처리할 수 있는 통화보다 많은 경우 통화 대기 기능에서는 이러한 통화를 받을 수 있을 때까지 대기열에서 보류합니다.

대기를 활성화하는 경우 헌트 응답 없음 착신 전환과 헌트 통화 중 착신 전환이 모두 자동으로 비활성화됩니다. 반대로 헌트 응답 없음 착신 전환이나 헌트 통화 중 착신 전환을 활성화하는 경우 대기가 자동으로 비활성화됩니다.

프로시저

- 단계 1** Cisco Unified Communications Manager 관리에서 통화 라우팅 > 경로/헌트 > 헌트 파일럿을 선택하여 헌트 파일럿을 구성합니다.
- 단계 2** 대기를 위해 구성해야 하는 헌트 파일럿을 선택합니다.
- 단계 3** 헌트 파일럿 구성 창의 대기 섹션으로 이동합니다.
- 단계 4** 대기를 활성화하려면 대기열 통화 확인란을 선택합니다.
- 단계 5** 드롭다운 목록 상자에서 알람을 재생하고 대기열 보류 기능을 제공하는 데 사용되는 MoH(대기 중 음악) 소스를 선택합니다.
- MoH 소스는 유니캐스트나 멀티캐스트로 구성할 수 있습니다. 발신자의 MRGL(미디어 리소스 구성 목록) 구성은 멀티캐스트 또는 유니캐스트에 우선합니다.
- 소스를 선택하지 않으면 기본 네트워크 보류 MoH/MoH 소스 및 알람이 사용됩니다.
- MoH 소스 알람 로컬은 알람에 사용되는 언어를 결정하는 데 사용됩니다. 헌트 파일럿당 한 가지 유형의 언어 알람만 재생될 수 있습니다.
- 단계 6** 대기열에 허용된 최대 발신자 수 필드에 이 헌트 파일럿에 대해 대기열에 허용되는 발신자 수를 정수 값으로 입력합니다.
- 기본값은 32입니다. 필드 범위는 1-100입니다.
- 단계 7** 대기열에 있는 최대 발신자 수에 도달한 경우 다음 옵션 중 하나를 선택합니다.
- 후속 통화의 연결을 끊으려면 통화 연결 끊기를 선택합니다.
 - 후속 통화를 보조 대상으로 라우팅해야 하는 경우 통화를 이 대상으로 라우트를 선택합니다. 특정 디바이스 DN, 공유 회선 DN 또는 다른 헌트 파일럿 DN을 제공합니다.
 - (선택 사항) 드롭다운 목록에서 전체 대기열 발신 검색 공간을 선택할 수도 있습니다. 통화를 완료하려고 할 때 검색할 파티션을 결정하는 데 사용됩니다.
- 단계 8** 대기열에서의 최대 대기 시간 필드에 정수 값을 입력하여 대기열에서의 최대 대기 시간(초)을 설정합니다.
- 기본값은 900초입니다. 필드 범위는 10초에서 3600초까지입니다.
- 단계 9** 최대 대기 시간에 도달하는 경우 다음 옵션 중 하나를 선택합니다.
- 해당 통화의 연결을 끊으려면 통화 연결 끊기를 선택합니다.
 - 해당 통화를 보조 대상으로 라우팅해야 하는 경우 통화를 이 대상으로 라우트를 선택합니다. 특정 디바이스 DN, 공유 회선 DN 또는 다른 헌트 파일럿 DN을 제공합니다.
 - (선택 사항) 드롭다운 목록에서 최대 대기 시간 발신 검색 공간을 선택할 수도 있습니다. 통화를 완료하려고 할 때 검색할 파티션을 결정하는 데 사용됩니다.
- 단계 10** 수신 통화 시 로그인되거나 등록된 회선 구성원이 없는 경우 다음 옵션 중 하나를 선택합니다.
- 통화의 연결을 끊으려면 통화 연결 끊기를 선택합니다.
 - 통화가 보조 대상으로 전송되어야 하는 경우 통화를 이 대상으로 라우트를 선택합니다. 특정 디바이스 DN, 공유 회선 DN 또는 다른 헌트 파일럿 DN을 제공합니다.

- (선택 사항) 드롭다운 목록에서 발신 검색 공간에 로그인되거나 등록된 헛트 구성원 없음을 선택할 수도 있습니다. 통화를 완료하려고 할 때 검색할 파티션을 결정하는 데 사용됩니다.

단계 11 저장을 클릭합니다.

응답이 없는 경우 헛트 구성원 자동 로그아웃

회선 구성원이 자동으로 헛트 목록을 로그오프 시킬 수 있습니다. 상담사가 대기열 사용 헛트 파일럿 통화에 응답하지 않을 경우, 해당 상담사는 헛트 그룹에서 로그오프되고 전화기의 "HLOG" 소프트웨어를 눌러 헛트 파일럿에 로그인할 때까지 추가 헛트 파일럿 통화를 수신하지 않습니다.

회선 구성원은 "헛트로그" 소프트웨어 또는 PLK를 사용하여 다시 로그인할 수 있습니다.

프로시저

- 단계 1 Cisco Unified Communications Manager 관리에서 통화 라우팅 > 라우트/헛트 > 회선 그룹을 선택하여 회선 그룹을 구성합니다.
- 단계 2 회선 그룹 찾기 및 나열 창에서 구성해야 하는 회선 그룹을 선택합니다.
- 단계 3 회선 그룹 구성 창의 헛트 옵션 섹션으로 이동합니다.
- 단계 4 응답이 없는 경우 헛트 구성원 자동 로그아웃 확인란이 선택되어 있는지 확인합니다.
- 단계 5 저장을 클릭합니다.

통화 지정 보류 상호 작용

기능	상호 작용
SIP Rel1XX 옵션	<p>통화가 SIP ICT를 통해 대기가 활성화된 헛트 파일럿으로 라우팅될 경우 SIP ICT는 SIP Rel1XX 옵션이 1xx에 SDP가 포함된 경우 PRACK 보내기로 설정된 SIP 프로파일을 사용합니다. 그 결과, 통화가 회선 구성원에게 확장되기 전에 모든 통화에 초기 알림이 재생됩니다.</p> <p>Cisco Unified CM 관리의 디바이스디바이스 설정SIP 프로파일 > 트렁크 특정 구성 아래에서 대기 알림을 실행하기 전에 착신 전화 연결 확인란을 선택하는 경우 SIP ICT에 대한 위의 기존 상호 작용은 적용되지 않습니다.</p> <p>대기 알림을 실행하기 전에 착신 전화 연결 확인란을 선택하지 않으면 SIP ICT에 대한 상호 작용은 동일하게 유지됩니다. 그러나 PSTN 측의 발신자가 언제든지 초기 알림을 들을 수 있다는 보장은 없습니다. 통화 중 연결 메시지가 수신될 때까지 PSTN 공급자가 음성 경로를 열지 않으면 PSTN 측에서 발신자가 초기 알림을 듣지 못합니다.</p>

기능	상호 작용
헌트 파일럿 및 헌트 그룹	<ul style="list-style-type: none"> • 헌트 파일럿에 대해 통화 대기가 활성화된 경우 헌트 그룹의 로그오프 알림 기능이 변경됩니다. 헌트 파일럿에 대해 통화 대기가 활성화된 경우 사용자가 헌트 그룹에서 로그아웃하거나 대기열에서 순서를 놓쳐 로그오프된 경우는 헌트 그룹 로그오프 알림이 재생되지 않습니다. • 헌트 목록에 여러 회선 그룹이 있는 경우 이러한 회선 그룹은 응답이 없는 경우 헌트 구성원 자동 로그아웃 설정이 동일해야 합니다. • 헌트 파일럿은 모든 헌트 구성원이 로그아웃된 경우에도 여전히 통화를 대기열에 배치합니다. 회선 그룹 구성원을 두 개 이상의 회선 그룹에 추가해서는 안 되며 두 번째 회선 그룹에 추가되는 경우에도 이러한 두 번째 회선 그룹은 동일한 헌트 목록에 있지 않아야 합니다. • 모든 헌트 옵션은 [다음 구성원 시도 후 헌트 목록에서 다음 그룹 시도]로 설정해야 합니다.

통화 대기 제한 사항

다음 일반 제한 사항이 통화 대기에 적용됩니다.

- H.323 빠른 시작은 통화 대기를 지원하지 않습니다.
- 대기열 상태 PLK는 SCCP 및 SIP: 6921, 6941, 6945, 6961, 7911G, 7931G, 7942G, 7945G, 7942G, 7965G, 7975G, 8961, 8945, 8941, 9951, 9971, 7800 및 8800 시리즈 모두에 대한 LCD 디스플레이 전화기에만 지원됩니다.
- 헌트 그룹 로그아웃(HLog)은 Cisco EMCC(Extension Mobility Cross Cluster)와 호환되지 않습니다. 통화 대기는 EMCC를 사용하여 구축해서는 안 됩니다.
- Unified Communications Manager는 통화 대기와 함께 Unified Mobility를 지원하지 않습니다.
- H.323와 SIP 간 상호 연동 시나리오에서 사용자는 초기 알림, MoH, 정지 알림 또는 상호 연동 지원이 발생하여 기본 통화 대기 흐름에서 통화 실패를 관찰하지 못할 수 있습니다. 이러한 시나리오에서는 SIP 프로토콜만 사용하는 것이 좋습니다.

통화 대기가 포함된 헌트 파일럿의 성능 및 확장성

다음과 같은 성능 및 확장성 제한 사항이 적용됩니다.

- 단일 Unified CM 클러스터는 최대 15,000개 헌트 목록 디바이스를 지원합니다.
- 단일 Unified CM 가입자는 노드별로 통화 대기가 활성화된 최대 100개의 헌트 파일럿을 지원합니다.

- 헌트 목록 디바이스는 각 헌트 목록에 10개 IP Phone이 있는 1500개 헌트 목록 조합, 각 헌트 목록에 20개 IP Phone이 있는 750개 헌트 목록 조합 또는 비슷한 조합일 수 있습니다.



참고 통화 커버리지에 대해 브로드캐스트 알고리즘을 사용하는 경우, 헌트 목록 디바이스의 수는 BHCA(최번시 통화 시도) 수에 따라 제한을 받습니다. 10대의 전화기를 포함하고 브로드캐스트 알고리즘을 사용하는 헌트 목록이나 헌트 그룹을 가리키는 헌트 파일럿에서 BHCA 10은 BHCA 10인 10대의 전화기와 동일합니다.

- 대기열에 32명의 발신자가 허용되도록 구성할 경우, 통화 대기가 활성화된 헌트 파일럿의 최대 수는 Unified CM 가입자 노드당 100개입니다. 노드당 대기열 슬롯의 총 수(결합된 노드에서 모든 통화 대기열 활성화 헌트 파일럿에 대해 "대기열에 허용되는 최대 발신자 수"의 값)는 3200으로 제한됩니다. 각 헌트 파일럿에 대해 대기열에 있는 최대 동시 발신자의 수는 100입니다. 이는 헌트 파일럿 당 100명의 발신자가 대기열에서 허용되고 최대 헌트 파일럿의 수가 32로 감소한다는 의미입니다. 모든 헌트 리스트 전반에 걸친 최대 설정된 수는 통화 대기가 활성화되어도 변하지 않습니다.
- 구성할 수 있는 각 헌트 파일럿에 대한 대기열의 최대 대기 시간은 0-3600초 범위입니다(기본값 900). 헌트 목록에서 수를 늘리면 Unified Communications Manager 서비스 매개변수에 지정된 다이얼 플랜 초기화 타이머를 늘려야 할 수 있습니다. 1500개 헌트 목록이 구성되어 있으면 다이얼 플랜 초기화 타이머를 600초로 설정하시는 것을 권장합니다.
- 통화 대기와 함께 브로드캐스트 알고리즘을 사용할 때 단일 회선 그룹에 35개 미만의 디렉터리 번호를 사용하는 것이 좋습니다. 또한 브로드캐스트 회선 그룹의 수는 BHCC(통화 중 시간 통화 완료율)에 따라 달라집니다. 통합 CM 시스템에 여러 개의 브로드캐스트 회선 그룹이 있는 경우 회선 그룹의 최대 디렉터리 번호 수는 35 미만이어야 합니다. 모든 브로드캐스트 회선 그룹에 대한 BHCA(최번시 통화 시도)의 수는 초당 설정된 35회 통화를 초과하지 않아야 합니다.



62 장

통화 조절 구성

- 통화 조절 개요, 813 페이지
- 통화 조절 구성 작업 흐름, 814 페이지

통화 조절 개요

통화 조절을 사용하면 시스템에서 새 통화 시도를 자동으로 조절하거나 거부할 수 있습니다. 조건에 의해 사용자에게 오프훅 전환 및 다이얼톤 수신 간격 동안 지연이 발생하는 경우 시스템은 이 동작을 수행합니다.

이러한 지연이 발생할 수 있는 몇 가지 요소는 다음과 같습니다.

- 많은 통화 활동
- 낮은 CPU 가용성
- 라우팅 루프
- 디스크 I/O 제한
- 디스크 단편화

시스템은 통화 조절 관련 매개 변수에 지정된 값을 사용하여 다이얼톤 지연 가능성을 결정하고 더 이상 통화 조절이 필요하지 않은 시기를 결정합니다.

다이얼톤의 과도한 지연을 방지하기 위해 조절이 필요한 경우 시스템이 코드 옐로우 상태로 전환되고 새로운 통화 시도는 조절(거부)됩니다.

시스템이 통화 조절 서비스 매개 변수에 구성된 임계값을 초과한 것으로 다이얼톤 지연을 계산하면 Unified Communications Manager는 새로운 통화를 거부합니다. 통화 조절이 활성화되는 경우 새 통화를 시도하는 사용자에게 다시걸기 신호음이 수신되며, 전화기 모델에 따라 전화기 디스플레이에 프롬프트도 표시될 수 있습니다.

통화 조절은 사용자가 시스템 관리자에게 불만을 제기하거나 시스템이 중단되었는지 또는 전화기가 고장 났는지 여부를 질문할 수 있는 과도한 지연 유형을 효과적으로 방지합니다. 시스템에서 지속적으로 시스템을 모니터링하여 그러한 지연의 발생 시기를 예상합니다.

다이어턴 지연이 통화 조절 서비스 매개 변수 지침을 벗어나지 않는 경우 Cisco Unified Communications Manager에서 코드 옐로우 상태를 종료하여 통화 조절을 중단하고 다시 새 통화가 허용됩니다.

통화 조절 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	통화 조절 구성, 814 페이지	시스템에서 과도한 통화 활동, 낮은 CPU 사용 가능성 및 디스크 조각화와 같은 조건을 감지하면 자동으로 통화 조절을 활성화합니다.
단계 2	메모리 조절 구성, 815 페이지	시스템에 대한 메모리 조절 기능을 구성합니다.

통화 조절 구성

통화 조절은 시스템에서 통화량이 많은 작업, 낮은 CPU 가용성 및 디스크 조각화와 같은 조건을 감지하면 자동으로 수행됩니다. 이러한 조건이 수정되면 시스템에서 자동으로 제한을 종료합니다. 통화 조절은 고급 서비스 매개 변수를 통해 구성됩니다. 대부분의 구축의 경우 기본 설정만으로도 충분합니다.



주의 고객 지원의 영향을 받지 않는 한 통화 제한 매개 변수를 수정하지 않는 것이 좋습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개 변수를 선택합니다.
- 단계 2 서버 드롭다운 목록에서 서버를 선택합니다.
- 단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.
- 단계 4 고급을 클릭합니다.
- 단계 5 통화 조절 아래에서 cll 조절 서비스 매개 변수에 대한 값을 구성합니다. 매개 변수 도움말 설명이 필요한 경우, GUI에서 매개 변수 이름을 클릭합니다.
 - 코드 옐로우 시작 지연(Code Yellow Entry Latency)
 - 코드 옐로우 종료 지연(Code Yellow Exit Latency) 달력
 - 코드 옐로우 기간(Code Yellow Duration)
 - 최대 허용 이벤트 수
 - 시스템 스로틀 샘플 크기

단계 6 저장을 클릭합니다.

메모리 조절 구성

이 절차를 사용하여 시스템에 대한 메모리 조절 기능을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 2 서버 드롭다운 목록에서 Unified Communications Manager 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 고급을 클릭합니다.

단계 5 메모리 조절 활성화 매개 변수를 **True**로 설정합니다.

단계 6 메모리 조절 영역의 추가 서비스 매개 변수에 대한 값을 구성합니다. 매개 변수 도움말의 경우 GUI에서 매개 변수 이름을 클릭합니다.

단계 7 저장을 클릭합니다.



63 장

논리적 파티션 구성

- 논리적 파티셔닝 개요, 817 페이지
- 논리적 파티셔닝 구성 작업 흐름, 817 페이지
- 논리적 파티셔닝 상호 작용, 824 페이지
- 논리적 파티션 제한 사항, 826 페이지

논리적 파티셔닝 개요

논리적 파티션을 사용하면 통화 분리에 대한 규정 요구 사항을 충족하는 동안 단일 시스템에서 PSTN 및 VoIP 통화를 지원할 수 있습니다. 예를 들어, 인도의 규정 제약 조건 아래에서 외부 전화기에서 수신 또는 발신되는 모든 통화는 모든 연결의 전체 길이에 대해 로컬 또는 장거리 서비스 공급업체에 전달되고 해당 전화 요금을 사용하여 전달되어야 합니다. 발신자의 위치 및 착신 전화 번호에 따라 PSTN 또는 VoIP 네트워크에 적절하게 통화를 라우팅하는 단일 Unified Communications Manager 클러스터를 생성할 수 있습니다.

논리적 파티션은 서로 통신할 수 있는 VoIP 디바이스 세트를 정의합니다. 사용자는 PSTN에 대해 한 회선을 사용하고 VoIP에 한 회선을 사용하는 것을 기억할 필요가 없습니다. 오프 넷 전화를 거는 전화기는 PSTN 게이트웨이와 통신하는 경우에만 허용됩니다. 이는 두 네트워크가 VoIP 및 PSTN 통화를 별도로 처리하는 것과 비슷하지만 이중 인프라의 비용을 사용하지 않습니다.

논리적 파티셔닝 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	논리적 파티셔닝 활성화, 818 페이지	논리적 파티셔닝을 활성화합니다.
단계 2	<p>지오로케이션 구성, 819 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> • 지오로케이션 만들기, 819 페이지 • 지오로케이션 할당, 819 페이지 	지오로케이션 구성은 위치를 정의하고 디바이스에 할당하는 2단계 프로세스입니다. 클러스터의 모든 디바이스에서 사용되는 기본 위치를 설정할 수도 있습니다.

	명령 또는 동작	목적
	<ul style="list-style-type: none"> 기본 지오로케이션 설정, 820 페이지 	
단계 3	논리적 파티셔닝 기본 정책 구성, 820 페이지	지오로케이션 또는 지오로케이션 필터와 연결되지 않은 디바이스에 대한 기본 정책을 설정합니다. 이 정책은 이러한 디바이스 간의 PSTN 통화를 허용하거나 거부합니다.
단계 4	논리적 파티션 확인을 방지하도록 디바이스를 구성합니다., 821 페이지	파티션 확인에서 디바이스 및 디바이스폴을 구체적으로 제외할 수 있습니다.
단계 5	<p>지오로케이션 필터 구성, 821 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> 지오로케이션 필터 규칙 만들기, 822 페이지 지오로케이션 필터 할당, 822 페이지 기본 지오로케이션 필터 설정, 823 페이지 	논리적 파티셔닝은 위치를 기반으로 각 디바이스에 고유 식별자를 할당합니다. 한 디바이스가 다른 디바이스에 전화를 걸 때 이러한 식별자를 사용하여 통화가 허용되는지 여부와 적절한 라우팅을 결정합니다. 이 식별자를 생성하는 데 사용되는 필드를 선택할 수 있습니다. 예를 들어, 건물 내에서 방 또는 층에 따라서 다른 정책을 적용할 수 있습니다.
단계 6	논리적 파티셔닝 정책 레코드 집합 정의, 823 페이지	지오로케이션 간 통화를 허용하거나 거부하는 논리적 파티셔닝 정책 집합을 정의합니다. 지오로케이션 간 통화를 계속 진행할 수 있으면 시스템에서 이러한 정책에 따라 지정된 지오로케이션 간에 통화가 허용되는지 확인합니다.
단계 7	(선택 사항) 위치 전환 활성화, 824 페이지	클러스터 간에 디바이스에 대한 지오로케이션 정보를 전달하려는 경우 위치 전달을 구성합니다.

논리적 파티셔닝 활성화

이 절차를 사용하여 논리적 파티션 기능을 설정합니다.

프로시저

단계 1 [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 2 논리적 파티셔닝 활성화 엔터프라이즈 매개 변수의 경우 드롭다운 목록에서 **True**를 선택합니다.

단계 3 저장을 클릭합니다.

지오로케이션 구성

지오로케이션 구성은 위치를 정의하고 디바이스에 할당하는 2단계 프로세스입니다. 클러스터의 모든 디바이스에서 사용되는 기본 위치를 설정할 수도 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	지오로케이션 만들기, 819 페이지	지오로케이션 위치를 지정하는 지오로케이션을 구성합니다. 이러한 기능은 디바이스를 논리적 파티션 등의 규제 기능과 연결하는 데 사용됩니다. 지오로케이션은 국가 규정과 같은 정책 결정에 사용됩니다.
단계 2	지오로케이션 할당, 819 페이지	디바이스 또는 디바이스풀에 지오로케이션을 할당합니다.
단계 3	기본 지오로케이션 설정, 820 페이지	이 클러스터의 모든 디바이스 및 디바이스풀에 대한 기본 지오로케이션을 지정합니다.

지오로케이션 만들기

이 절차를 사용하여 시스템의 디바이스에 할당할 수 있는 지오로케이션을 만듭니다. 논리적 파티션에 대해 지오로케이션을 사용할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 지오로케이션 구성을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 지오로케이션에 대한 이름을 입력합니다.

단계 4 지오로케이션 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

단계 6 추가 지오로케이션을 더 생성하려면 이 절차를 반복합니다.

지오로케이션 할당

디바이스 또는 디바이스풀에 지오로케이션을 할당합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴 항목 중 하나를 선택합니다.

- 장치 > 전화기
- 디바이스 > 트렁크.
- 디바이스 > 게이트웨이
- 시스템 > 디바이스폴.

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 디바이스 또는 디바이스폴에 대한 설정을 수정하려면 찾기를 클릭합니다. 검색 조건을 입력한 다음 결과 목록에서 기존 디바이스 또는 디바이스폴을 선택합니다.
- 새로 추가를 클릭하여 새 디바이스 또는 디바이스폴을 추가합니다. 디바이스의 경우 필요에 따라 디바이스 유형 및 프로토콜을 선택하고 다음을 클릭합니다.

단계 3 지오로케이션 드롭다운 목록에서 구성된 지오로케이션을 선택합니다.

단계 4 저장을 클릭합니다.

기본 지오로케이션 설정

이 클러스터의 모든 디바이스 및 디바이스폴에 대한 기본 지오로케이션을 지정합니다.

프로시저

단계 1 [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 2 기본 지오로케이션 드롭다운 목록에서 구성된 지오로케이션을 선택합니다. 기본값은 미지정입니다.

단계 3 저장을 클릭합니다.

단계 4 구성 적용을 클릭합니다.

단계 5 (선택 사항) 특정 디바이스 또는 디바이스폴에 대해 이 기본값을 무시해야 하는 경우 디바이스 구성 또는 디바이스폴 구성 창에서 값을 입력한 다음 저장을 클릭합니다.

논리적 파티셔닝 기본 정책 구성

지오로케이션 또는 지오로케이션 필터와 연결되지 않은 디바이스에 대한 기본 정책을 설정합니다. 이 정책은 이러한 디바이스 간의 PSTN 통화를 허용하거나 거부합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 논리적 파티셔닝 정책 구성을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 논리적 파티셔닝 정책 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

참고 허용 값이 포함된 정책이 나중에 거부로 변경되면 거부로 유지됩니다. 반대의 경우도 마찬가지입니다. 이전에 거부로 설정된 정책은 나중에 허용으로 변경됩니다. **Cisco** 통합 보고 > 지오로케이션 정책 보고서는 중복되는 정책을 식별하는 데 도움이 될 수 있습니다.

논리적 파티션 확인을 방지하도록 디바이스를 구성합니다.

파티션 확인에서 디바이스 및 디바이스폴을 구체적으로 제외할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴 항목 중 하나를 선택합니다.

- 장치 > 전화기
- 디바이스 > 트렁크.
- 디바이스 > 게이트웨이
- 시스템 > 디바이스폴.

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 디바이스 또는 디바이스폴에 대한 설정을 수정하려면 찾기를 클릭합니다. 검색 조건을 입력한 다음 결과 목록에서 기존 디바이스 또는 디바이스폴을 선택합니다.
- 새로 추가를 클릭하여 새 디바이스 또는 디바이스폴을 추가합니다. 디바이스의 경우 필요에 따라 디바이스 유형 및 프로토콜을 선택하고 다음을 클릭합니다.

단계 3 지오로케이션 드롭다운 목록에서 미지정을 선택합니다.

단계 4 저장을 클릭합니다.

지오로케이션 필터 구성

논리적 파티셔닝은 위치를 기반으로 각 디바이스에 고유 식별자를 할당합니다. 한 디바이스가 다른 디바이스에 전화를 걸 때 이러한 식별자를 사용하여 통화가 허용되는지 여부와 적절한 라우팅을 결정합니다. 이 식별자를 생성하는 데 사용되는 필드를 선택할 수 있습니다. 예를 들어, 건물 내에서 방 또는 층에 따라 서로 다른 정책을 적용할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	지오로케이션 필터 규칙 만들기, 822 페이지	지오로케이션 필터를 구성하여 지오로케이션 식별자를 만드는 데 사용할 필드를 선택합니다. 이 기능은 지오로케이션 개체의 하위 집합에 대한 정책 결정을 내리는 데 사용됩니다.
단계 2	지오로케이션 필터 할당, 822 페이지	
단계 3	기본 지오로케이션 필터 설정, 823 페이지	기본 지오로케이션 필터 엔터프라이즈 매개 변수를 구성하여 클러스터에 대한 기본 지오로케이션 필터를 지정합니다. 이 매개 변수는 지오로케이션 필터와 연결되지 않은 모든 디바이스 및 디바이스폴에 대한 기본 지오로케이션 필터 설정을 결정합니다.

지오로케이션 필터 규칙 만들기

이 절차를 사용하여 논리적 파티션 결정에 사용할 수 있는 지오로케이션 필터를 만들 수 있습니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 시스템 > 지오로케이션 필터를 선택합니다.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 필터에 대한 이름 및 설명을 입력합니다.
- 단계 4 논리적 파티션 결정에 사용할 항목에 해당하는 확인란을 선택합니다.
- 단계 5 지오로케이션 필터 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.
- 단계 6 저장을 클릭합니다.
- 단계 7 이러한 단계를 반복하여 추가 지오로케이션 필터를 생성합니다.
-

지오로케이션 필터 할당

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴 항목 중 하나를 선택합니다.
- 장치 > 전화기
 - 디바이스 > 트렁크.
 - 디바이스 > 게이트웨이

- 시스템 > 디바이스폴.

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 디바이스 또는 디바이스폴에 대한 설정을 수정하려면 찾기를 클릭합니다. 검색 조건을 입력한 다음 결과 목록에서 기존 디바이스 또는 디바이스폴을 선택합니다.
- 새로 추가를 클릭하여 새 디바이스 또는 디바이스폴을 추가합니다. 디바이스의 경우 필요에 따라 디바이스 유형 및 프로토콜을 선택하고 다음을 클릭합니다.

단계 3 지오로케이션 필터 드롭다운 목록에서 구성된 지오로케이션 필터를 선택합니다.

단계 4 저장을 클릭합니다.

기본 지오로케이션 필터 설정

프로시저

단계 1 [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 2 기본 지오로케이션 드롭다운 목록에서 구성된 지오로케이션을 선택합니다. 기본값은 미지정입니다.

단계 3 저장을 클릭합니다.

단계 4 구성 적용을 클릭합니다.

단계 5 (선택 사항) 특정 디바이스 또는 디바이스폴에 대해 이 기본값을 무시해야 하는 경우 디바이스 구성 또는 디바이스폴 구성 창에서 기본 지오로케이션 필터 값을 지정한 다음 저장을 클릭합니다.

논리적 파티셔닝 정책 레코드 집합 정의

지오로케이션 간 통화를 허용하거나 거부하는 논리적 파티셔닝 정책 집합을 정의합니다. 지오로케이션 간 통화를 계속 진행할 수 있으려면 시스템에서 이러한 정책에 따라 지정된 지오로케이션 간에 통화가 허용되는지 확인합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 논리적 파티션 정책 구성.

단계 2 다음 작업 중 하나를 수행합니다.

- 찾기를 클릭하여 기존 논리적 파티셔닝 정책에 대한 설정을 수정합니다. 검색 조건을 입력한 다음 결과 목록에서 기존 논리적 파티셔닝 정책을 선택합니다.
- 새로 추가를 클릭하여 논리적 파티셔닝 정책을 새로 추가합니다.

단계 3 논리적 파티셔닝 정책 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

참고 구성 값 없이 정책을 비워 두면 빈 지오로케이션 정책이 되며, 빈 논리적 파티셔닝 구성을 사용하여 특정 디바이스 유형에 대한 논리적 정책을 구성하면 Unified Communications Manager에서 구성된 디바이스 유형에 정책 값(허용 또는 거부)을 추가합니다.

단계 4 저장을 클릭합니다.

위치 전환 활성화

위치 전환은 클러스터 간에 지오로케이션 정보를 공유하는 데 사용되는 선택적 구성입니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 트렁크를 선택합니다.
- 새로 추가를 클릭하여 새 트렁크를 구성합니다.

단계 3 트렁크 구성 창에서 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 4 지오로케이션 정보 영역에서 지오로케이션 및 지오로케이션 필터를 선택합니다.

단계 5 위치 전환을 활성화하려면 지오로케이션 정보 보내기 확인란을 선택합니다.

단계 6 저장을 클릭합니다.

논리적 파티셔닝 상호 작용

표 79: 논리적 파티셔닝 상호 작용

기능	상호 작용
애드-혹 컨퍼런스, 참가, 회선 간 통화 참가, 통화 착신 전환, 통화 전달	다음과 같은 경우에 논리적 파티션 처리가 발생하지 않습니다. <ul style="list-style-type: none"> • 모든 참가자가 VoIP 전화기를 사용하는 경우 • 지오로케이션 또는 지오로케이션 필터가 연결된 디바이스가 없을 경우

기능	상호 작용
참여, 회의끼기 및 원격 재개	<p>다음과 같은 경우에 논리적 파티션 처리가 발생하지 않습니다.</p> <ul style="list-style-type: none"> 발신자 및 수신자 디바이스가 모두 VoIP 전화기인 경우 논리적 파티셔닝 정책 확인이 무시됩니다. 회의끼기/참여를 사용하는 참가자에 대해서는 논리적 파티션 정책 확인이 발생하지 않으며 논리적 파티션 거부 시나리오를 금지할 수 없습니다.
Cisco Unified Mobility	<p>다음과 같은 경우에 논리적 파티션 처리가 발생하지 않습니다.</p> <ul style="list-style-type: none"> 지오로케이션 또는 지오로케이션 필터가 관련 디바이스와 연결되지 않습니다. 듀얼 모드 전화기가 사용된 경우에는 논리적 파티션 지원이 없습니다.
CTI 처리	<p>다음과 같은 경우에 논리적 파티션 처리가 발생하지 않습니다.</p> <ul style="list-style-type: none"> 지오로케이션 또는 지오로케이션 필터와 연결된 디바이스가 없을 경우 처리가 발생하지 않습니다. 관련된 모든 디바이스가 VoIP 전화기를 지정하는 경우에는 처리가 발생하지 않습니다.
Extension Mobility	<p>다음과 같은 경우에 논리적 파티션 처리가 발생하지 않습니다.</p> <ul style="list-style-type: none"> 지오로케이션 또는 지오로케이션 필터는 Cisco Extension Mobility에 로그인된 VoIP 전화기 또는 발신 디바이스 또는 착신 디바이스와 연결되지 않습니다. Cisco Extension Mobility에 로그인된 VoIP 전화기는 VoIP 전화기에 통화를 걸거나 받습니다.
Meet-Me 전화회의	<p>다음과 같은 경우에 논리적 파티션 처리가 발생하지 않습니다.</p> <ul style="list-style-type: none"> 모든 참가자가 VoIP 전화기를 사용하는 경우 처리는 발생하지 않습니다. 지오로케이션 또는 지오로케이션 필터가 디바이스와 연결되지 않은 경우 해당 디바이스에 대해 정책 확인이 이루어지지 않습니다.

기능	상호 작용
라우트 목록 및 헌트 파일럿	다음과 같은 경우에 논리적 파티션 처리가 발생하지 않습니다. <ul style="list-style-type: none"> 발신자 및 착신자 디바이스가 둘 다 VoIP 전화기인 경우, 처리가 발생하지 않습니다. 모든 디바이스가 지오로케이션 및 지오로케이션 필터와 연결되어야 합니다. 지오로케이션 및 지오로케이션 필터와 모두 연결되지 않은 디바이스가 있을 경우, 처리가 발생하지 않습니다.
공유 회선	다음과 같은 경우에 논리적 파티션 처리가 발생하지 않습니다. <ul style="list-style-type: none"> 발신자 디바이스와 착신자 디바이스가 모두 VoIP 전화기인 경우 처리하지 않습니다. 지오로케이션 또는 지오로케이션 필터가 연결된 디바이스가 없는 경우 처리하지 않습니다.

논리적 파티션 제한 사항

표 80: 논리적 파티션 제한 사항

제한 사항	설명
참여/회의끼기	참여/회의끼기가 발생 하지 않고 통화 인스턴스가 삭제됩니다. 회의끼기/참여를 사용하는 참가자에 대해서는 논리적 파티션 정책 확인이 발생하지 않으며 논리적 파티션 거부 시나리오를 금지할 수 없습니다.
BLF 프리젠스	BLF 프리젠스 알림은 논리적 파티셔닝 정책에 대해 확인되지 않습니다.
Cisco Extension Mobility	Cisco Extension Mobility가 다른 지오로케이션에 있는 전화기에 로그인할 때 로컬 라우트 그룹이 구성되면 발신 PSTN 통화가 발생할 수 있습니다. 수신 PSTN 통화는 전화기로 걸리지 않지만 다시걸기 신호음은 재생됩니다.
Cisco Unified MeetingPlace	시스템은 Cisco Unified MeetingPlace 또는 Cisco Unified MeetingPlace Express가 관련된 통화에 논리적 파티셔닝 기능을 지원하지 않습니다.
전화회의	전화회의 체인의 전화회의 간 참가자에 대해서는 논리적 파티셔닝 확인이 지원되지 않습니다. 예를 들어 지금 미팅 및 임시 체인 전화회의에는 논리적 파티셔닝이 거부된 참가자가 있을 수 있습니다.
H.225 게이트키퍼 제어 트렁크	Cisco Unified Communications Manager는 게이트키퍼로 제어되는 H.225 트렁크를 통해 지오로케이션 정보를 전달하지 않습니다.

제한 사항	설명
H.323 및 MGCP 게이트웨이	Cisco Unified Communications Manager는 지오로케이션 정보를 H.323 또는 MGCP 게이트웨이로 전달하지 않습니다. SIP 트렁크 확인란에서 SIP 게이트웨이에 대한 통신을 비활성화할 수 있습니다.
휴대폰 당겨받기	휴대폰에서 전화를 받은 후에는 논리적 파티셔닝 거부 처리가 발생합니다. 휴대폰으로 전화가 걸리기 전에는 논리적 파티셔닝 정책 확인이 발생하지 않습니다(기본 SNR 통화의 경우에 발생). 휴대폰에서 통화에 응답한 후에는 시스템에서 논리적 파티셔닝 정책을 확인합니다.
Q.SIG 인터클러스터 트렁크	Q. SIG 프로토콜을 사용하는 ICT(인터클러스터 트렁크)는 발신자 또는 수신 디바이스에 대한 지오로케이션 정보를 전달할 수 없습니다. Q.SIG 터널링된 프로토콜을 선택하면 “지오로케이션 정보 보내기”에 대한 ICT 구성이 비활성화됩니다.
다시걸기 신호음	논리적 파티셔닝 정책으로 인해 연결된 통화가 해제되면 IOS H.323 및 SIP 게이트웨이에서 다시걸기 신호음이 제공되지 않습니다.
공유 회선 활성 통화	제한된 논리적 파티셔닝 시나리오의 경우 일부 기능에서 공유 회선 통화를 허용되는 범주로 바꾸더라도 공유 회선에서는 통화 지속 시간 동안 활성 통화 정보가 삭제됩니다.
사용자 에이전트 서버	정책이 거부되면 이 지오로케이션을 받는 논리적 파티셔닝 인식 클러스터의 논리적 파티셔닝 정책 확인에서 통화를 취소할 수 있습니다.



64 장

위치 인식 구성

- 위치 인식 개요, 829 페이지
- 위치 인식 사전 요건, 831 페이지
- 위치 인식 구성 작업 흐름, 832 페이지

위치 인식 개요



중요 위치 인식에 대한 Meraki 액세스 포인트 지원은 릴리스 12.5(1)SU6 및 14릴리스 14SU1 이후에서만 적용됩니다.

위치 인식은 관리자가 회사 네트워크에 연결하는 실제 위치를 결정할 수 있습니다. 무선 네트워크의 경우 무선 액세스 포인트 인프라와 현재 해당 액세스 포인트에 연결된 모바일 디바이스를 볼 수 있습니다. 유선 네트워크의 경우 이더넷 스위치 인프라를 보고 해당 스위치에 현재 연결되어 있는 디바이스를 확인할 수 있습니다. 이를 통해 전화를 건 건물, 층 및 큐브를 확인할 수 있습니다.

Cisco Unified CM 관리 > 고급 기능 > 디바이스 위치 추적 서비스 > 스위치 및 액세스 포인트 > 스위치 및 액세스 포인트 찾기 및 나열 창에서 네트워크 인프라를 볼 수 있습니다.

이 기능은 다음 정보를 사용하여 Unified Communications Manager 데이터베이스를 동적으로 업데이트합니다.

- 각 인프라 디바이스에 대한 IP 주소, 호스트 이름 및 BSSID 정보(해당되는 경우)를 포함하여 스위치 및 무선 액세스 포인트와 같은 네트워크 인프라 디바이스.
- 다음을 포함하여 각 인프라 디바이스에 대한 연결된 엔드포인트:
 - 무선 네트워크의 경우 현재 무선 액세스 포인트에 연결된 디바이스 목록.
 - 유선 네트워크의 경우 현재 이더넷 스위치에 연결된 디바이스 및 디바이스 유형 목록.

Cisco Emergency Responder 통합

위치 인식은 Cisco Emergency Responder와 같은 통합 애플리케이션을 통해 비상 통화를 하는 사용자의 실제 위치를 결정하는 데 도움이 됩니다. 위치 인식이 활성화되면 Cisco Emergency Responder는 새 무선 액세스 포인트와 관련된 모바일 디바이스 또는 데스크폰이 새 이더넷 스위치에 연결된 후 몇 분 이내에 새로운 디바이스와 인프라 연결을 인식합니다.

Cisco Emergency Responder를 처음 시작하면 현재 디바이스에 대한 Unified Communications Manager 데이터베이스를 네트워크 인프라 연결에 쿼리합니다. 이후 2분마다 Cisco Emergency Responder는 기존 연결에 대한 업데이트를 확인합니다. 결과적으로, 모바일 발신자가 로밍 상황에서 비상 전화를 거는 경우에도 Cisco Emergency Responder에서 발신자의 실제 위치를 신속하게 파악하여 적절한 건물, 층 또는 큐브로 긴급 서비스를 보낼 수 있습니다.

무선 네트워크 업데이트

무선 인프라에 대한 위치 인식을 활성화하려면 Unified Communications Manager를 Cisco 무선 LAN 컨트롤러와 동기화하도록 구성할 수 있습니다. Unified Communications Manager를 최고 50개의 컨트롤러와 동기화할 수 있습니다. 동기화 프로세스 중에 Unified Communications Manager가 컨트롤러에서 관리하는 액세스 포인트 인프라를 사용하여 데이터베이스를 업데이트합니다. Cisco Unified CM 관리에서 각 액세스 포인트에 연결된 모바일 클라이언트 목록을 비롯하여 무선 액세스 포인트에 대한 상태를 볼 수 있습니다.

모바일 클라이언트가 액세스 포인트 간에 로밍하면 엔드포인트로부터의 SIP 및 SCCP 신호 처리에서 새 디바이스를 Unified Communications Manager에 액세스 포인트 연결로 전달하여 데이터베이스를 업데이트합니다. Cisco Emergency Responder는 연결을 변경한 새 엔드포인트에 대해 몇 분마다 Unified Communications Manager 데이터베이스를 쿼리하여 새 연결을 알아냅니다. 따라서 모바일 클라이언트가 비상 전화를 걸 경우 Cisco Emergency Responder는 통화를 수행한 사용자의 실제 위치에 대한 정확한 정보를 가집니다.

무선 액세스 포인트 컨트롤러에 대한 정기적인 동기화 일정을 가지고 있는 경우에는 Unified Communications Manager가 각 동기화를 수행하여 데이터베이스에서 동적으로 액세스 포인트를 추가하고 업데이트합니다.

벌크 관리를 사용하여 액세스 포인트 삽입

타사 무선 액세스 포인트 컨트롤러를 사용하거나 Cisco Prime Infrastructure에서 액세스 포인트를 내보내려는 경우 벌크 관리 도구를 사용하여 CSV 파일의 무선 액세스 포인트 인프라를 Unified Communications Manager 데이터베이스에 벌크 삽입할 수 있습니다. 벌크 삽입 후 모바일 디바이스의 다음 위치 업데이트는 현재 액세스 포인트 연결을 사용하여 데이터베이스를 업데이트합니다.

그러나, 벌크 관리에서는 새 액세스 포인트가 무선 네트워크에 추가될 때 액세스 포인트 인프라를 동적으로 업데이트할 수 없습니다. 벌크 삽입 후 추가된 액세스 포인트를 통해 모바일 통화가 발신되는 경우, 해당 액세스 포인트는 데이터베이스에 레코드가 없는 경우에는 Unified Communications Manager가 새 액세스 포인트의 BSSID와 일치시킬 수 없으며, 무선 디바이스에 대한 인프라를 알 수 없는 AP로 표시합니다.

벌크 관리 도구에 대한 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 지침서의 "인프라 디바이스 관리" 장을 참조하십시오.

유선 네트워크 업데이트

유선 인프라에 대한 위치 인식 기능을 활성화 하는 데는 구성이 필요하지 않습니다. 이 기능은 자동으로 활성화됩니다.

유선 전화기가 등록되면 전화기와 Cisco Unified Communications Manager 간의 신호가 스위치 인프라를 사용하여 데이터베이스를 동적으로 업데이트합니다. 특정 스위치에 연결된 전화기 목록을 포함하여 Cisco Unified CM 관리의 회사의 스위치 인프라에 대한 세부 정보를 볼 수 있습니다.

모바일 디바이스와 달리 유선 디바이스는 일반적으로 한 스위치에서 다른 스위치로 로밍되지 않습니다. 전화기가 이동하는 경우, 작업자가 회사 내에서 책상을 전환할 때 발생할 수 있는 것처럼, 새 위치에서 전화기가 다시 등록될 후 데이터베이스가 새 스위치 정보로 업데이트됩니다. Cisco Unified Communications Manager에서 새 스위치는 이동된 전화기를 연결된 엔드포인트로 표시합니다.

스위치가 더 이상 사용되지 않고 네트워크 인프라에서 제거되면 해당 스위치가 Cisco Unified Communications Manager 내에 표시된 상태로 유지됩니다. 인프라 보기에서 이전 스위치를 제거하려면 액세스 포인트 및 스위치 구성 창에서 스위치를 비활성화해야 합니다.

위치 인식을 위해 지원되는 엔드포인트

다음 엔드포인트는 위치 인식을 통한 추적을 지원합니다.

- Cisco Unified 무선 IP 전화기 7925G
- Cisco Unified 무선 IP 전화기 7925G-EX
- Cisco Unified 무선 IP 전화기 7926G
- Cisco Jabber 클라이언트 — 12.5(1)SU1 지원됨
- Cisco Wireless IP Phone 8821—12.5(1)SU1부터 지원됨
- Webex 앱 — 12.5(1)SU1부터 지원됨

이러한 엔드포인트는 스테이션 정보 메시지를 통해 Cisco Unified Communications Manager에 대한 업스트림 인프라 정보(예: BSSID)를 제공합니다. Cisco Emergency Responder는 AXL 변경 알림을 사용하여 연결된 액세스 포인트를 통해 이러한 디바이스를 추적합니다.

디바이스 추적이 작동하려면 Cisco Unified Communications Manager에서 무선 액세스 포인트를 정의해야 합니다. 무선 액세스 포인트 컨트롤러를 동기화하거나 벌크 관리를 사용하여 무선 액세스 포인트 인프라를 가져오는 방법으로 이 작업을 수행할 수 있습니다.

위치 인식 사전 요건

이 기능을 사용하여 Cisco Unified Communications Manager 데이터베이스를 여러 Cisco 무선 LAN 컨트롤러와 동기화할 수 있습니다. Cisco 무선 LAN 컨트롤러 하드웨어와 액세스 포인트 인프라를 설정해야 합니다. 자세한 내용은 컨트롤러 설명서를 참조하십시오.

위치 인식 구성 작업 흐름

Cisco Unified Communications Manager에서 위치 인식을 설정하려면 다음 작업을 완료하십시오.

시작하기 전에

프로시저

	명령 또는 동작	목적
단계 1	무선 인프라 동기화를 위한 서비스 시작, 832 페이지	Cisco 통합 서비스 가용성에서 위치 인식 기능을 지원하는 서비스를 시작합니다.
단계 2	무선 액세스 포인트 컨트롤러 구성, 833 페이지	Cisco 무선 액세스 포인트 컨트롤러와 데이터베이스를 동기화합니다. 동기화에서 무선 인프라를 데이터베이스로 가져옵니다. 팁 자동 업데이트에 대한 동기화 일정을 설정합니다.
단계 3	인프라 디바이스 삽입, 834 페이지	(선택 사항) Cisco Prime Infrastructure에서 무선 인프라를 추가하거나 타사 무선 LAN 컨트롤러를 사용하는 경우 벌크 관리를 사용하여 CSV 파일에서 데이터베이스를 업데이트합니다. 참고 이 방법을 사용하여 자동 업데이트를 설정할 수는 없습니다.
단계 4	추적에서 인프라 디바이스 비활성화, 835 페이지	(선택 사항) 동기화에 추적하지 않으려는 액세스 포인트가 포함된 경우(예: 동기화가 실험실에서 액세스 포인트를 가져오는 경우) 액세스 포인트를 비활성화하고 Cisco Unified Communications Manager 액세스 포인트에 대한 업데이트를 추적하지 않습니다.

무선 인프라 동기화를 위한 서비스 시작

이 절차를 사용하여 위치 인식 기능을 지원하기 위해 Cisco 무선 LAN 컨트롤러와의 동기화를 지원하는 서비스를 시작할 수 있습니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에 로그인하고 도구 > 서비스 활성화를 선택합니다.

단계 2 서버 드롭다운 목록에서 퍼블리셔 노드를 선택합니다.

단계 3 다음 서비스가 선택되었는지 확인합니다.

- Cisco CallManager
- Cisco AXL 웹 서비스
- Cisco Wireless Controller 동기화 서비스

단계 4 (선택 사항) 벌크 관리를 사용하여 CSV 파일에서 네트워크 인프라를 가져오려면 벌크 프로비저닝 서비스를 선택했는지 확인합니다.

단계 5 저장을 클릭합니다.

무선 액세스 포인트 컨트롤러 구성

이 절차를 사용하여 데이터베이스를 Cisco 무선 액세스 포인트 컨트롤러와 동기화합니다. 동기화 중에 Unified Communications Manager가 컨트롤러에서 관리하는 무선 액세스 포인트 인프라를 사용하여 데이터베이스를 업데이트합니다. 최대 50개의 무선 액세스 포인트 컨트롤러를 추가할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 고급 기능 > 디바이스 위치 추적 서비스 > 무선 액세스 포인트 컨트롤러를 선택합니다.

단계 2 구성할 컨트롤러를 선택합니다.

- 찾기를 클릭하고 컨트롤러를 선택하여 기존 컨트롤러를 편집합니다.
- 새 컨트롤러를 추가하려면 새로 추가를 클릭합니다.

단계 3 이름 필드에 컨트롤러의 IP 주소 또는 호스트 이름을 입력합니다.

단계 4 컨트롤러에 대한 설명을 입력합니다.

단계 5 컨트롤러에 대한 SNMP 메시징에 사용될 SNMP 설정을 완료합니다.

- a) **SNMP** 버전 드롭다운 목록에서 컨트롤러가 사용하는 SNMP 버전 프로토콜을 선택합니다.
- b) 나머지 SNMP 인증 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- c) **SNMP** 설정 테스트를 클릭하여 유효한 SNMP 설정을 입력했는지 확인합니다.

단계 6 데이터베이스를 정기적으로 업데이트하도록 예약된 동기화를 구성하려면 다음을 수행합니다.

- a) 예약된 동기화를 활성화하여 인프라 디바이스 검색 확인란을 선택합니다.
- b) 매일 재동기화 수행 필드에서 동기화 일정을 만듭니다.

단계 7 저장을 클릭합니다.

단계 8 (선택 사항) 즉시 데이터베이스를 업데이트하려면 동기화를 클릭합니다.

선택 사항. 동기화가 추적하지 않을 액세스 포인트(예: 랩 장비 또는 사용 중이 아닌 액세스 포인트)를 가져오는 경우 추적에서 액세스 포인트를 제거할 수 있습니다.

인프라 디바이스 삽입

이 절차를 사용하여 CSV 파일에서 Unified Communications Manager 데이터베이스에 무선 액세스 포인트 인프라의 벌크 가져오기를 완료할 수 있습니다. Cisco Prime Infrastructure에서 내보낸 CSV 파일을 가져오거나 타사 무선 액세스 포인트 컨트롤러에서 액세스 포인트를 가져오려는 경우 이 절차를 사용할 수 있습니다.

시작하기 전에

다음과 같은 설명 열에 CSV(쉼표로 구분된 값) 형식으로 된 데이터 파일이 있어야 합니다.

- 액세스 포인트 또는 스위치 이름
- IPv4 주소
- IPv6 주소
- BSSID—WAP(Wireless Access Protocol) 인프라 디바이스에 필요합니다.
- 설명—위치 식별자, 스위치 유형과 위치의 조합 또는 다른 의미 있는 식별자



참고 IPv4 및 IPv6 주소를 모두 정의하거나, IPv4 또는 IPv6 주소를 정의할 수 있습니다.

Meraki 액세스 포인트의 경우에는 Unified Communications Manager에서 데이터베이스의 기본 서비스 설정 식별자(BSSID)를 기본 BSSID에 정규화한 후 이를 업데이트합니다. Meraki 액세스 포인트를 위한 BSSID 마스킹 계산에 대한 자세한 내용은 [Cisco Meraki BSSID MAC 주소 계산](#)을 참조합니다.

비 Meraki 액세스 포인트의 경우에는 Unified CM에서 마지막 바이트를 0으로 마스킹하여 데이터베이스의 BSSID를 업데이트합니다.

이 마스킹 로직은 Unified CM이 액세스 포인트의 개별 채널에 대한 BSSID와 달리 액세스 포인트를 고유하게 식별할 수 있도록 합니다.

프로시저

단계 1 벌크 관리 > 인프라 디바이스 > 인프라 디바이스 삽입을 선택합니다.

인프라 디바이스 삽입 구성 창이 표시됩니다.

단계 2 파일 이름 필드에서 이 트랜잭션에 대해 생성한 CSV 데이터 파일을 선택합니다.

단계 3 작업 정보 영역에 작업 설명을 입력합니다.

기본 설명은 인프라 디바이스 삽입입니다.

단계 4 작업을 실행할 시기를 선택합니다.

- 즉시 실행 라디오 버튼을 선택하여 즉시 작업을 실행합니다.
- 나중에 실행하도록 작업을 예약하려면 나중에 실행 라디오 버튼을 선택합니다.

단계 5 제출을 클릭합니다.

작업을 즉시 실행하도록 선택하면 작업이 실행됩니다.

단계 6 나중에 작업을 실행하기로 선택하면 작업 실행 시기를 예약합니다.

- a) 벌크 관리 > 작업 스케줄러를 선택합니다.
 - b) 찾기를 클릭하고 방금 생성한 작업을 선택합니다.
 - c) 작업 스케줄러 창에서 작업을 실행하려는 시기를 예약합니다.
 - d) 저장을 클릭합니다.
- 예약된 시간에 작업이 실행됩니다.

추적에서 인프라 디바이스 비활성화

동기화에 추적하지 않을 액세스 포인트 또는 스위치가 포함되어 있는 경우(예: 동기화가 실험실 장비 또는 액세스 포인트를 사용하지 않는 경우) 액세스 포인트 또는 스위치를 추적에서 비활성화할 수 있습니다. Unified Communications Manager가 액세스 포인트 또는 스위치의 상태를 업데이트하지 않습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 고급 기능 > 디바이스 위치 추적 서비스 > 스위치 및 액세스 포인트를 선택합니다.

단계 2 찾기를 클릭하고 추적을 중지하려는 스위치 또는 액세스 포인트를 선택합니다.

단계 3 선택한 항목 비활성화를 클릭합니다.

관련 설명서

시스템 구성을 완료하고 시스템을 실행한 후에는 다음 장의 작업을 사용하여 인프라를 지속적으로 관리할 수 있습니다.

"인프라 관리", [Cisco Unified Communications Manager 및 IM and Presence 서비스용 관리 가이드](#)



65 장

유연한 DSCP 표시 및 비디오 프로모션 구성

- 유연한 DSCP 표시 및 비디오 프로모션 개요, 837 페이지
- 사용자에 대한 사용자 정의 QoS 설정, 838 페이지
- 트래픽 클래스 레이블, 839 페이지
- DSCP 설정 구성 작업 흐름, 839 페이지
- 유연한 DSCP 표시 및 비디오 프로모션 상호 작용, 843 페이지
- 유연한 DSCP 표시 및 비디오 프로모션 제한 사항, 843 페이지

유연한 DSCP 표시 및 비디오 프로모션 개요

디바이스 및 애플리케이션에는 DSCP(차별화된 서비스 코드 포인트) 표시가 사용되어 IP 통신의 QoS(서비스 품질) 처리를 나타냅니다. 예를 들어, 데스크톱 비디오 엔드포인트는 비디오 미디어 스트림에 대한 멀티미디어 전화회의 AF41 표시를 사용하는 반면, 고화질 비디오 룸 시스템은 실시간 대화형 CS4 표시를 사용할 수 있습니다. 애플리케이션에서 동일한 유형의 애플리케이션에 대한 IP 통신을 보내고 받을 때 DSCP 표시는 대칭적이며, 각 애플리케이션에서 보내고 받는 IP 통신의 QoS 처리는 동일합니다. 그러나 애플리케이션에서 다른 유형의 애플리케이션을 통해 미디어를 보내고 받을 때 DSCP 표시는 비대칭이 될 수 있으며, 각 애플리케이션에서 보내고 받는 IP 통신의 QoS 처리는 일관성이 없을 수 있습니다. 예를 들어, 비디오 룸 시스템이 데스크톱 비디오 엔드포인트에서 수신하는 비디오 미디어 스트림의 QoS 처리는 비디오 룸 시스템의 예상 품질을 지원하기에 적합하지 않을 수 있습니다.

디바이스 및 애플리케이션은 설정된 세션 동안 적절한 대역폭을 사용할 수 있는지 확인하기 위해 CAC(통화 허용 제어)에 사용됩니다. 설정된 세션에서 사용하는 대역폭은 세션이 시작되고 끝날 때 업데이트됩니다. 사용 가능한 대역폭을 초과하는 새 세션을 설정하려고 하면 차단됩니다. 사용 가능한 대역폭의 양을 서로 다른 유형의 디바이스 및 애플리케이션에 대해 개별적으로 추적할 수 있습니다. 예를 들어, 데스크톱 비디오 엔드포인트 및 고화질 비디오 룸 시스템에서는 비디오 미디어 스트림을 보내고 받기 위해 대역폭에 대한 독립된 추적을 사용할 수 있습니다.

동일한 유형의 디바이스 및 애플리케이션에서 통신을 보내고 받는 경우 각 방향에서 동일한 유형의 대역폭 공제가 이루어집니다. 그러나 서로 다른 유형의 디바이스 및 애플리케이션에서 통신을 보내고 받는 경우 각 방향마다 서로 다른 유형의 대역폭 공제가 이루어져야 합니다. 또한 대역폭 공제는 일반적으로 IP 네트워크의 일반적인 동작을 반영하기 위해 설계상 대칭적입니다. 그 결과, 서로 다른 유형의 디바이스 및 애플리케이션에서 통신을 보내고 받는 경우 총 대역폭 공제는 실제로 사용되는

네트워크 대역폭의 양을 최대 2배까지 늘릴 수 있습니다. 대역폭 계정에서 이 불일치로 인해 새 세션을 불필요하게 차단하려 할 수 있습니다.

유연한 DSCP 표시 및 비디오 프로모션 기능을 사용하면 보다 유리한 CAC 및 QoS 처리를 받는 애플리케이션에 유리하도록 대역폭 계정의 불일치를 조정하는 비디오 프로모션 정책을 구성할 수 있습니다. 예를 들어, 데스크톱 비디오 엔드포인트와 고화질 비디오 룸 시스템 간의 세션을 비디오 룸 시스템에 맞게 조정하는 경우에는 해당 조정이 데스크톱 비디오 엔드포인트에 대한 승격으로 간주됩니다.

유형이 서로 다른 디바이스 및 애플리케이션 간에 조정이 적용되는 경우, 대역폭은 조정에 의해 선호되는 애플리케이션 유형에만 공제됩니다. 이 유형의 세션을 허용하기에 충분한 대역폭을 사용할 수 있는 경우 조정에서 선호하지 않는 유형의 디바이스 또는 애플리케이션은 조정에서 선호하는 유형의 디바이스 또는 애플리케이션에서 사용하는 DSCP 표시를 변경하라는 지침이 표시됩니다. 예를 들어, 고해상도 비디오 룸 시스템을 사용하는 세션에서 데스크톱 비디오 엔드포인트를 승격하는 경우, 데스크톱 비디오 엔드포인트는 비디오 룸 시스템과 동일한 유형의 애플리케이션인 것처럼 대역폭 계정이 발생합니다. 데스크톱 비디오 엔드포인트는 비디오 룸 시스템에서 사용하는 것으로 DSCP 표시를 변경하라고 지시합니다. QoS 처리는 양방향으로 일관성이 있으며, 비디오 룸 시스템과 동일한 유형의 디바이스와 애플리케이션 사이의 세션에 대해 대역폭이 공제되며, 데스크톱 비디오 엔드포인트 동일한 유형의 디바이스와 애플리케이션 간의 세션에 대해서는 대역폭이 공제되지 않습니다.

유연한 DSCP 표시 및 비디오 프로모션 기능을 활성화하는 경우 Unified Communications Manager는 각 협상된 미디어 스트림에 대한 DSCP 표시를 나타내는 트래픽 클래스 레이블을 데스크톱 비디오 디바이스에 동적으로 신호를 보냅니다.

사용자에 대한 사용자 정의 QoS 설정

SIP 프로파일 내에서 QoS(서비스 품질) 설정을 사용자 정의하고 해당 설정을 사용자에게 적용할 수 있습니다. SIP 프로파일 구성 창은 다음 유형의 QoS 설정으로 향상되었습니다.

- 오디오 및 비디오 스트림에 대한 사용자 정의 DSCP 값
- 오디오 및 비디오 스트림에 대한 사용자 정의 UDP 포트 범위

오디오 및 비디오에 대한 사용자 정의 DSCP 값

SIP 프로파일 내에서 오디오 및 영상 통화에 대한 DSCP 값을 구성하고 해당 프로파일을 사용하는 SIP 전화기에 적용할 수 있습니다. SIP 프로파일 구성 창에는 다음과 같은 유형의 통화에 대한 사용자 정의 DSCP 설정이 포함됩니다.

- 오디오 통화
- 영상 통화
- 영상 통화의 오디오 부분
- Telepresence 통화
- TelePresence 통화의 오디오 부분

회사에 영업 사원과 같은 직원 또는 CEO 집합이 있어, 대부분의 직원보다 높은 QoS 우선 순위 설정이 필요한 경우에는 SIP 프로파일 구성을 사용하여 해당 사용자에게 대한 사용자 정의 DSCP 값을 구성할 수 있습니다. SIP 프로파일 내의 설정은 해당 클러스터 수준 서비스 매개 변수 설정을 무시합니다.

오디오 및 비디오에 대한 사용자 정의 UDP 포트 범위

SIP 통화의 오디오 스트림 및 비디오 스트림에 대해 별도의 UDP 포트 범위를 구성할 수 있습니다. 일반적으로 비디오는 오디오 보다 훨씬 더 많은 대역폭을 필요로 하므로 각 미디어 유형에 대한 전용 포트 범위를 생성하면 네트워크 대역폭 관리가 간단해집니다. 또한 오디오 스트림이 상위 대역폭 비디오 스트림과 분리된 전용 채널을 갖도록 보장하여 오디오 스트림 성능이 저하되지 않도록 보호합니다.

SIP 프로파일의 미디어 포트 범위 필드를 오디오 및 비디오용 개별 포트 범위를 설정하여 이 구성을 적용할 수 있습니다. 그런 다음 SIP 프로파일을 전화기에 연결하여 구성을 전화기에 적용할 수 있습니다.

트래픽 클래스 레이블

유연한 DSCP 및 비디오 프로모션 기능은 TCL(트래픽 클래스 레이블)을 사용하여 SIP 엔드포인트에서 구성하는 비디오 프로모션 정책에 따라 통화별로 해당 DSCP를 표시하도록 동적으로 지시합니다. TCL은 미디어 회선당 정의된 SDP(SIP Session Description Protocol) 속성이므로, 영상 통화의 오디오 미디어 회선 및 비디오 미디어 회선에 대한 TCL 및 연결된 DSCP 표시가 다를 수 있습니다. 오디오 스트림에 다른 DSCP 표시를 선택하고 영상 통화의 비디오 스트림을 선택할 수 있습니다.

DSCP 설정 구성 작업 흐름

다음 작업을 수행하여 네트워크에 대한 DSCP 값과 비디오 승격 정책을 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	유연한 DSCP 표시 및 비디오 프로모션 정책 구성, 840 페이지	비디오 승격 정책을 구성하여 다양한 유형의 비디오를 처리합니다.
단계 2	사용자에 대한 사용자 정의 QoS 정책 구성, 841 페이지	회사에서 다른 사용자보다 높은 우선 순위를 필요로 하는 사용자가 있는 경우 오디오 및 비디오 스트림에 대한 사용자 정의 DSCP 값을 포함하는 SIP 프로파일을 구성합니다. 예를 들어 회사에 더 높은 우선 순위가 필요한 전화기 영업 사원이나 CEO가 있는 경우 해당 사용자의 전화기에 사용자 정의된 SIP 프로파일을 적용할 수 있습니다.

유연한 DSCP 표시 및 비디오 프로모션 정책 구성

다음 단계에 따라 비디오 승격 정책을 구성하여 다양한 유형의 비디오를 처리합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 시스템 > 서비스 매개 변수.

단계 2 서버 드롭다운 목록에서 매개 변수를 구성할 서버를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager(활성)** 서비스를 선택합니다.

서비스가 활성화 상태로 표시되지 않으면, Cisco Unified Serviceability에서 해당 서비스가 활성화되어 있는지 확인해야 합니다.

단계 4 데스크톱 비디오 엔드포인트를 몰입형 비디오 엔드포인트로 승격하는 비디오 승격 정책을 구성하려면 몰입형 영상 통화용 대역폭 풀 사용 매개 변수를 **False**로 설정하고 화상 통화 QoS 표시 정책 매개 변수를 몰입형으로 승격으로 설정합니다.

단계 5 다른 매개 변수를 구성하려면 서비스 매개 변수 구성 창의 해당 영역으로 스크롤하고 매개 변수 값을 업데이트합니다. 이러한 서비스 매개 변수 및 해당 구성 옵션에 대한 자세한 내용은 [유연한 DSCP 표시 및 비디오 프로모션 서비스 매개 변수, 840 페이지](#)의 내용을 참조하십시오.

단계 6 저장을 클릭합니다.

유연한 DSCP 표시 및 비디오 프로모션 서비스 매개 변수



참고 서비스 매개 변수에 대한 정보를 보려면 매개 변수 이름을 클릭하거나 서비스 매개 변수 구성 창에 표시되는 물음표(?)를 클릭합니다.

표 81: 유연한 DSCP 표시 및 비디오 프로모션 서비스 매개 변수

매개 변수	설명
클러스터 수준 매개 변수 (시스템 - QOS)	이 서비스 매개 변수 섹션에는 오디오 통화에 대한 DSCP, 영상 통화, 영상 통화의 오디오 부분, TelePresence 통화 및 TelePresence 통화의 오디오 부분을 포함하여 광범위한 오디오 및 영상 통화 유형에 대한 클러스터 수준 DSCP 값이 포함되어 있습니다. Cisco 지원 엔지니어의 지침이 있는 경우를 제외하고 이러한 매개 변수를 기본값으로 유지하는 것이 좋습니다.
클러스터 수준 매개 변수 (통화 허용 제어)	

매개 변수	설명
화상 통화 QoS 표시 정책	이 매개 변수를 사용하면 몰입형 엔드포인트를 위해 데스크톱 비디오 엔드포인트와 Cisco TelePresence 몰입형 비디오 엔드포인트 간의 대역폭 할당 불일치를 조정하는 몰입형 정책으로 수준 올리기를 구성할 수 있습니다. 프로모션이 수행되면 오디오 및 비디오 대역폭이 몰입형 대역폭 풀 할당에서 예약됩니다. 몰입형으로 프로모션하는 정책은 유연한 DSCP 표시와 몰입형 비디오 디바이스를 지원하는 데스크톱 비디오 디바이스 간의 통화에만 적용됩니다.
클러스터 수준 매개 변수(시스템 - 위치 및 지역)	
기본 지역 내 최대 몰입형 영상 통화 비트 레이트(오디오 포함)	이 매개 변수는 지역과의 관계를 위해 지역 구성 창에서 시스템 기본값 사용 옵션을 최대 몰입형 영상 통화 비트 전송률로 선택한 경우 특정 지역 내의 각 몰입형 영상 통화에 대한 기본 총 비트 전송률을 지정합니다.
기본 지역 간 최대 몰입형 영상 통화 비트 레이트(오디오 포함)	이 매개 변수는 특정 지역과 다른 지역 간의 몰입형 영상 통화에 대한 기본 총 비트 전송률을 지정합니다. 이 값은 다른 지역과의 관계에 대해 지역 구성 창에서 최대 몰입형 영상 통화 비트 전송률로 시스템 기본값 사용 옵션을 선택한 경우에 사용됩니다.
몰입형 영상 통화에 영상 통화용 대역폭 풀 사용	이 매개 변수는 Unified Communications Manager가 몰입형 영상 통화에 대한 데스크톱 비디오 대역폭 풀의 대역폭을 예약하는지 여부를 지정합니다.

사용자에 대한 사용자 정의 QoS 정책 구성

사용자에 대한 사용자 정의 QoS(서비스 품질) 정책을 설정하려면 다음 작업을 수행합니다. 회사 내 사용자 집합이 전화기 영업 사원 또는 CEO와 같은 회사의 나머지와 다른 QoS 요구 사항을 갖는 경우 사용자 정의 정책을 적용할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	SIP 프로파일에서 사용자 정의 QoS 설정 구성, 842 페이지	사용자 정의된 DSCP 값과 오디오 및 비디오 스트림에 대한 UDP 포트 범위를 사용하여 SIP 프로파일을 구성합니다.
단계 2	전화기에 사용자 정의 QoS 정책 적용, 842 페이지	SIP 프로파일을 전화기에 적용합니다. SIP 프로파일의 DSCP 설정은 DSCP 클러스터 수준 서비스 매개 변수 설정을 무시합니다.

SIP 프로파일에서 사용자 정의 QoS 설정 구성

이 SIP 프로파일을 사용하는 전화기에 대한 사용자 정의 DSCP 값 및 UDP 포트 범위를 구성합니다. 이러한 설정을 사용하여 네트워크 내 특정 전화기 및 사용자에게 적용할 수 있는 사용자 정의된 QoS 정책을 구성할 수 있습니다. 회사 내 특정 사용자(예: 영업 사원 또는 CEO)에 특정 QoS 설정을 적용하려는 경우 이 작업을 수행할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 2 다음 단계 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 SIP 프로파일을 선택합니다.
- 새로 추가를 클릭하여 새 SIP 프로파일을 만듭니다.

단계 3 미디어 포트 범위 필드에서 오디오 및 비디오 미디어를 모두 처리하는 단일 UDP 포트 범위를 할당할지 또는 오디오 및 비디오 스트림에 대해 별도의 포트 범위를 할당할지 여부를 선택합니다.

- 오디오 및 비디오 미디어에 대한 단일 포트 범위를 구성하려면 미디어 포트 시작 및 미디어 포트 중지 필드에 포트 범위를 입력합니다. 가능한 포트 값은 2048~65535입니다.
- 오디오 및 비디오 스트림에 대한 별도의 포트 범위를 원할 경우 오디오 포트 시작 및 오디오 포트 중지 필드를 사용하여 오디오 포트 범위를 입력합니다. 비디오 포트 시작 및 비디오 포트 중지 필드를 사용하여 비디오 포트 범위를 입력합니다. 가능한 각 포트 값은 2048~65535 사이입니다. 두 포트 범위는 겹치지 않아야 합니다.

단계 4 다음 필드에서 오디오 및 비디오 스트림에 대해 사용자 정의된 DSCP 값을 구성합니다.

- 음성 통화용 DSCP
- 영상 통화용 DSCP
- 영상 통화의 오디오 부분용 DSCP
- Telepresence 통화용 DSCP
- TelePresence 통화의 오디오 부분용 DSCP

참고 기본적으로 위의 각 필드는 해당하는 서비스 매개 변수의 값을 사용하도록 구성됩니다. 새 값을 할당하면 새 값이 서비스 매개 변수 설정을 무시합니다.

단계 5 **SIP** 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

전화기에 사용자 정의 QoS 정책 적용

이 절차를 사용하여 오디오 및 비디오 미디어에 대한 DSCP 값 및 UDP 포트 범위를 포함하여 사용자 정의된 QoS 설정을 포함하는 SIP 프로파일을 적용합니다. 이 SIP 프로파일을 전화기에 적용하면 전화기에서 SIP 프로파일의 사용자 정의 설정을 사용합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 2 다음 단계 중 하나를 수행하십시오.

- 찾기를 클릭하고 기존 전화기를 선택합니다.
- 새로 추가를 클릭하여 새 전화기를 생성합니다.

단계 3 SIP 프로파일 드롭다운 목록에서 사용자 정의 DSCP 값 및 UDP 포트 범위 값을 사용하여 설정 하는 SIP 프로파일을 선택합니다.

단계 4 전화기 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

유연한 DSCP 표시 및 비디오 프로모션 상호 작용

표 82: 유연한 DSCP 표시 및 비디오 프로모션 상호 작용

장치	상호 작용
SIP 인터클러스터 트렁크	유연한 DSCP 표시 및 비디오 프로모션 기능은 SIP 인터클러스터 트렁크를 통해 지원됩니다.
SCCP(Skinny Client Control Protocol) 디바이스	SCCP 디바이스에는 유연한 DSCP 표시 및 비디오 프로모션 기능이 지원됩니다.
통과 MTP	통화에 통과 MTP가 삽입되면 Unified Communications Manager는 MTP에 신호를 보내어 원래 비디오 스트림용 패킷을 내보냈던 엔드포인트 디바이스에서 예상되는 DSCP 표시로 패킷을 표시합니다. 통화의 두 엔드포인트에서 서로 다른 DSCP 표시(예: 비디오 승격이 없는 Cisco TelePresence 물입형 비디오 엔드포인트 및 데스크톱 비디오 엔드포인트)를 사용하는 경우, MTP가 각 스트림 방향으로 DSCP 표시를 유지합니다.

유연한 DSCP 표시 및 비디오 프로모션 제한 사항

표 83: 유연한 DSCP 표시 및 비디오 프로모션 제한 사항

제한 사항	설명
트렁크 및 게이트웨이	H.323 트렁크 및 MGCP(미디어 게이트웨이 제어 프로토콜) 게이트웨이에서는 유연한 DSCP 표시 및 비디오 프로모션 기능이 지원되지 않습니다.

제한 사항	설명
MLPP(Multilevel Precedence and Preemption)	다양한 MLPP(다중 수준 우선 순위 및 선점) 서비스 통화와 함께 유연한 DSCP 표시 및 비디오 프로모션 기능을 사용하지 않는 것이 좋습니다. MLPP 서비스 기능이 필요한 경우 영상 통화 QoS 표시 정책을 설정하고 몰입형 영상 통화 서비스 매개 변수에 대한 영상 통화용 대역폭 풀을 기본값으로 사용하는 것이 좋습니다. 영상 통화 QoS 표시 정책에 대한 기본값을 사용하고 몰입형 영상 통화에 영상 통화용 대역폭 풀 사용 서비스 매개 변수를 사용하는 경우 Unified Communications Manager 및 엔드포인트는 미디어 패킷에 MLPP DSCP 표시를 사용합니다.
SIP 비디오 엔드포인트	유연한 DSCP 표시 및 비디오 프로모션 기능은 데스크톱 SIP 비디오 엔드포인트 지원에 따라 달라집니다. 현재, Cisco DX650 시리즈 SIP 전화기만 필수 엔드포인트 지원을 제공합니다.



66 장

SIP에서 발신자 번호 및 청구 번호 분리

- 외부 표시 이름 및 번호 개요, 845 페이지
- 통화 처리, 846 페이지
- 디렉터리 번호 개요, 848 페이지
- SIP 프로파일 개요, 853 페이지
- SIP 트렁크 개요, 855 페이지
- 클러스터 간 SME 통화 흐름, 860 페이지

외부 표시 이름 및 번호 개요

별도의 발신자 및 프레젠테이션 번호를 포함하도록 Cisco Unified Communications Manager 관리를 구성할 수 있습니다.

이전 Cisco Unified Communications Manager 릴리스에서는 FROM 및 PAID 헤더의 PSTN으로 다른 번호를 전송하도록 회선 별로 구성할 수 없습니다. 사용자 그룹이 PSTN 사용자에게 동일한 발신 회선 식별 번호를 표시하도록 구성된 경우 비 지역 E.164 번호이며 대금 청구에 사용할 수 없습니다. 따라서 사용자의 실제 DDI는 프레젠테이션 번호와는 다른 필드에 전송되어야 합니다. 이번 릴리스에서는 Cisco Unified Communications Manager가 기존 ID 이름 및 번호와 다른 외부 표시 이름 및 번호를 지원합니다. 구성된 프레젠테이션 이름 및 번호는 다음 디바이스에 대한 표시 목적을 위한 것입니다.

- SIP
- SCCP
- SNRD(단일 번호 연락 대상)
- CTIRD
- SparkRD

구성 개요

다음 페이지에서 외부 표시 이름 및 번호 기능을 구성할 수 있습니다.

- 디렉터리 번호 구성

- SIP 프로파일 구성
- 트렁크 구성



참고

- SIP 프로파일 구성 페이지에서 외부 표시 정보를 구성할 때 SIP 프로파일 구성 페이지의 외부 표시 번호와 외부 표시 이름 값이 디렉터리 번호 페이지에 구성된 설정을 재정의하는 데 사용됩니다.
- 트렁크 구성 페이지에서 프레젠테이션 정보를 구성할 때 트렁크 구성 페이지의 프레젠테이션 번호와 프레젠테이션 이름 값이 SIP 프로파일 구성 및 디렉터리 번호 구성 페이지에서 구성한 설정을 재정의합니다.

통화 처리

이 섹션에서는 외부 표시 이름 및 번호 기능을 구성할 때 수신 및 발신 통화 동작에 대해 설명합니다.

착신 통화 프로세스

Cisco Unified Communications Manager는 PSTN 네트워크에서 시작된 통화가 있는 경우 FROM 및 PAID 헤더 정보를 찾습니다. FROM 헤더는 외부 표시 이름 및 번호(구성된 경우)를 포함합니다. 그러나 이것은 사용자의 실제 ID가 아니라 표시 용도로만 사용됩니다. PAID 헤더에는 사용자의 ID(원래 DN 또는 DDI)가 포함되어 있습니다.

FROM 및 PAID에 있는 번호가 다르고 SIP 프로파일 구성 페이지에서 외부 표시 이름 및 번호 사용 옵션이 활성화되어 있고 외부 표시 이름 및 번호 표시 서비스 매개 변수 값이 **True**로 설정된 경우, Cisco Unified Communications Manager는 착신 디바이스에서 FROM 헤더 정보(구성된 외부 표시 이름 및 번호)를 표시합니다. 마찬가지로, 옵션이 비활성화된 경우 Cisco Unified Communications Manager는 착신 디바이스에 PAID 헤더 정보(사용자의 원래 DN 또는 DDI)를 표시합니다.



참고

- 기본적으로 외부 표시 이름 및 번호 활성화는 선택되어 있지 않습니다.
- 서비스 매개 변수 외부 표시 이름 및 번호 표시의 기본값은 False입니다.

PSTN 네트워크에서 초대 수신됨

```
From: "Customer Care" <sip:1800000@example.com>;
To: <sip:someone@example.com>
P-Asserted-Identity: "Your personal adviser <sip:user1@example.com>"
Remote-Party-ID: "Your personal adviser <sip:user1@example.com>"
```

위의 예에서 FROM 헤더는 PAID 헤더와 다른 번호를 포함합니다. 외부 표시 이름 및 번호 활성화 확인란을 선택하고 외부 표시 이름 및 번호 표시를 **True**로 설정하는 경우 Cisco Unified Communications Manager는 착신 디바이스에 고객 관리/1800000를 표시합니다.

외부 표시 이름 및 번호 활성화 확인란을 선택 취소하거나 외부 표시 이름 및 번호 표시를 **False**로 설정하는 경우 Cisco Unified Communications Manager는 착신 디바이스에 **Your personal adviser / user1@example.com**을 표시합니다.

발신 통화 프로세스

외부 표시 이름 및 번호로 구성된 사용자가 SIP 프로파일에 구성된 외부 표시 이름 및 번호 활성화를 사용하여 SIP 트렁크를 통해 PSTN 네트워크에 대한 통화를 시작한다고 가정합니다. 그런 다음 Cisco Unified Communications Manager는 구성된 외부 표시 정보를 발신 SIP 메시지의 FROM 헤더로 전송하고 착신 디바이스에 표시합니다.

외부 표시 이름 및 번호 활성화 옵션을 비활성화하거나 외부 표시 번호 및 외부 표시 이름 필드가 구성되지 않은 경우 Cisco Unified Communications Manager는 FROM 및 PAID 헤더에 디렉터리 번호 정보를 전송하고 착신 디바이스에 표시합니다.

외부 표시 번호 마스크 작업

Cisco Unified Communications Manager를 사용하여 외부 표시 번호를 마스크하여 착신 디바이스에 표시할 수 있습니다. 디렉터리 번호 구성, SIP 프로파일 구성 및 트렁크 구성 페이지에서 표시 번호를 마스크할 수 있습니다.

외부 표시 번호 필드에 후행 X와 함께 숫자를 입력하면 X 값이 오른쪽에서 시작하여 왼쪽으로 디렉터리 번호 정보로 대체됩니다.

디렉터리 번호 설정의 마스크 작업

디렉터리 번호 5551234에 대한 디렉터리 번호 설정 페이지에서 외부 표시 번호를 180011XXXX로 마스크하는 경우 Cisco Unified Communications Manager는 착신 디바이스에 표시 번호로 1800111234를 표시합니다.

SIP 프로파일 구성에서 마스크 작업

디렉터리 번호 페이지의 외부 표시 번호가 180011XXXX라고 가정하고 디렉터리 번호 5551234에 대해 SIP 프로파일 구성 페이지에서 외부 표시 번호를 180022XXXX로 마스크하는 경우 Cisco Unified Communications Manager는 착신 디바이스에 표시 번호로 1800221234를 표시합니다.

트렁크 구성의 마스크 작업

디렉터리 번호 페이지의 외부 표시 번호가 180011XXXX이고 SIP 프로파일 구성 페이지에서는 180022XXXX라고 가정합니다. 디렉터리 번호 5551234에 대한 트렁크 구성 페이지에서 외부 표시 번호를 180033XXXX로 마스크하는 경우 Cisco Unified Communications Manager는 착신 디바이스에 표시 번호로 1800331234를 표시합니다.

디렉터리 번호 개요

Cisco Unified Communications Manager 관리에서 통화 라우팅 > 디렉터리 번호메뉴 경로를 사용하여 DN(디렉터리 번호)을 구성합니다. Cisco Unified Communications Manager 관리를 사용하여 특정 전화기에 할당된 DN을 구성 및 수정할 수 있습니다.

새 섹션 외부 표시 정보가 디렉터리 번호 구성 페이지에 추가됩니다. 이제 관리자가 외부 통화에 지원되는 디바이스에 표시할 표시 이름 및 선택 항목 번호를 구성할 수 있습니다. 관리자가 사용자 ID를 표시하고 싶지 않을 경우, 착신자 디바이스에서 구성된 외부 표시 번호와 외부 표시 이름을 익명으로 표시할 수 있는 권한이 있습니다.

디렉터리 번호 구성 작업

프로시저

	명령 또는 동작	목적
단계 1	다음 방법 중 하나를 사용하여 새 최종 사용자 추가: <ul style="list-style-type: none"> LDAP에서 최종 사용자 가져오기, 848 페이지 최종 사용자를 수동으로 추가, 849 페이지 	시스템이 회사 LDAP 디렉터리와 동기화된 경우 LDAP 디렉터리에서 새 최종 사용자를 직접 가져올 수 있습니다. 그렇지 않으면, 최종 사용자를 수동으로 추가 및 구성할 수 있습니다.
단계 2	다음 작업 중 하나를 수행하여 전화기를 새 사용자 또는 기존의 최종 사용자에게 할당합니다. <ul style="list-style-type: none"> 최종 사용자를 위한 새 전화기 추가, 851 페이지 최종 사용자에게 기존 전화기 이동, 851 페이지 	범용 디바이스 템플릿의 설정을 사용하여 최종 사용자에게 대한 새 전화기를 구성하기 위해 '새 전화기 추가' 절차를 사용할 수 있습니다. 또한 이미 구성된 기존 전화기를 할당하려면 '이동' 절차를 사용할 수 있습니다.
단계 3	DN에 외부 표시 정보 구성, 852 페이지	특정 전화기에 할당된 DN의 외부 표시 번호 및 외부 표시 이름을 구성합니다.

LDAP에서 최종 사용자 가져오기

새 최종 사용자를 회사 LDAP 디렉터리에서 수동으로 가져오려면 다음 절차를 수행합니다. LDAP 동기화 구성에 범용 회선 템플릿 및 디바이스 템플릿은 물론 DN 풀을 포함하는 기능 그룹 템플릿이 포함된 경우 가져오기 프로세스는 최종 사용자 및 기본 내선 번호를 자동으로 구성합니다.



참고 초기 동기화가 발생한 후에는 새 구성(예: 기능 그룹 템플릿 추가)을 LDAP 디렉터리 동기화에 추가할 수 없습니다. 기존 LDAP 동기화를 편집하려면 벌크 관리를 사용하거나 새 LDAP 동기화를 구성해야 합니다.

시작하기 전에

이 절차를 시작하기 전에 Cisco Unified Communications Manager가 회사 LDAP 디렉터리와 이미 동기화되었는지 확인하십시오. LDAP 동기화는 범용 회선 템플릿 및 디바이스 템플릿이 있는 기능 그룹 템플릿을 포함해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 2 찾기를 클릭하고 사용자가 추가한 LDAP 디렉터를 선택합니다.

단계 3 전체 동기화 수행을 클릭합니다.

Cisco Unified Communications Manager는 외부 LDAP 디렉터리와 동기화합니다. LDAP 디렉터리에 있는 새 최종 사용자를 Cisco Unified Communications Manager 데이터베이스로 가져옵니다.

다음에 수행할 작업

셀프 프로비저닝을 위해 사용자가 활성화된 경우 최종 사용자는 셀프 프로비저닝 대화형 음성 응답(IVR)을 사용하여 새 전화기를 프로비저닝할 수 있습니다. 그렇지 않으면 다음 작업 중 하나를 수행하여 전화기를 최종 사용자에게 할당합니다.

- [최종 사용자를 위한 새 전화기 추가, 851 페이지](#)
- [최종 사용자에게 기존 전화기 이동, 851 페이지](#)

최종 사용자를 수동으로 추가

새 최종 사용자를 추가하고 액세스 컨트롤 그룹 및 기본 회선 내선 번호로 해당 최종 사용자를 구성하려면 다음 절차를 수행합니다.



참고 사용자에게 할당할 역할 권한이 있는 액세스 컨트롤 그룹을 이미 설정했는지 확인합니다. 자세한 내용은 "사용자 액세스 관리" 장을 참조하십시오.

시작하기 전에

범용 회선 템플릿이 포함되어 있는 사용자 프로파일이 구성되었는지 확인합니다. 새 내선 번호를 구성해야 하는 경우 Cisco Unified Communications Manager는 범용 회선 템플릿의 설정을 사용하여 기본 내선 번호를 구성합니다.

프로시저

-
- 단계 1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 빠른 사용자/전화기 추가를 선택합니다.
- 단계 2** 사용자 ID 및 성을 입력합니다.
- 단계 3** 기능 그룹 템플릿 드롭다운 목록에서 기능 그룹 템플릿을 선택합니다.
- 단계 4** 저장을 클릭합니다.
- 단계 5** 사용자 프로파일 드롭다운 목록에서 선택한 사용자 프로파일에 범용 회선 템플릿이 포함되어 있는지 확인합니다.
- 단계 6** 액세스 컨트롤 그룹 구성원 섹션에서 + 아이콘을 클릭합니다.
- 단계 7** 사용자는 다음의 구성원입니다. 드롭다운 목록에서 액세스 컨트롤 그룹을 선택합니다.
- 단계 8** 기본 내선 번호 아래에서 + 아이콘을 클릭합니다.
- 단계 9** 내선 번호 드롭다운 목록에서 (사용 가능)으로 표시되는 DN을 선택합니다.
- 단계 10** 모든 회선 내선 번호가 (사용됨)으로 표시되는 경우 다음 단계를 수행합니다.
- a) 새로 만들기... 버튼을 클릭합니다.
새 내선 번호 추가 팝업이 표시됩니다.
 - b) 디렉터리 번호 필드에 새 회선 내선 번호를 입력합니다.
 - c) 회선 템플릿 드롭다운 목록에서 범용 회선 템플릿을 선택합니다.
 - d) 확인을 클릭합니다.
Cisco Unified Communications Manager는 범용 디바이스 템플릿의 설정을 사용하여 전화기를 구성합니다.
- 단계 11** (선택 사항) 빠른 사용자/전화기 추가 구성 창에서 추가 필드를 완료합니다.
- 단계 12** 저장을 클릭합니다.
-

다음에 수행할 작업

다음 절차 중 하나를 수행하여 전화기를 이 최종 사용자에게 할당합니다.

- [최종 사용자를 위한 새 전화기 추가, 851 페이지](#)
- [최종 사용자에게 기존 전화기 이동, 851 페이지](#)

최종 사용자를 위한 새 전화기 추가

신규 또는 기존 최종 사용자에게 새 전화기를 추가하려면 다음 절차를 수행합니다. 최종 사용자에게 대한 사용자 프로파일에 범용 디바이스 템플릿이 포함되어 있는지 확인합니다. Cisco Unified Communications Manager는 범용 디바이스 템플릿의 설정을 사용하여 전화기를 구성합니다.

시작하기 전에

최종 사용자를 추가하려면 다음 절차 중 하나를 수행합니다.

- [최종 사용자를 수동으로 추가, 849 페이지](#)
- [LDAP에서 최종 사용자 가져오기, 848 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 빠른 사용자/전화기 추가를 선택합니다.
 - 단계 2 찾기를 클릭하고 새 전화기를 추가하려는 최종 사용자를 선택합니다.
 - 단계 3 디바이스 관리를 클릭합니다.
[디바이스 관리] 창이 나타납니다.
 - 단계 4 새 전화기 추가를 클릭합니다.
[사용자에게 전화기 추가] 팝업이 표시됩니다.
 - 단계 5 제품 유형 드롭다운 목록에서 전화기 모델을 선택합니다.
 - 단계 6 디바이스 프로토콜 드롭다운에서 프로토콜로 SIP 또는 SCCP를 선택합니다.
 - 단계 7 디바이스 이름 텍스트 상자에 디바이스 MAC 주소를 입력합니다.
 - 단계 8 범용 디바이스 템플릿 드롭다운 목록에서 범용 디바이스 템플릿을 선택합니다.
 - 단계 9 전화기가 확장 모듈을 지원하는 경우 배포하려는 확장 모듈 수를 입력합니다.
 - 단계 10 Extension Mobility를 사용하여 전화에 액세스하려면 **Extension Mobility**에서 확인란을 선택합니다.
 - 단계 11 전화기 추가를 클릭합니다.
[새 전화기 추가] 팝업이 닫힙니다. Cisco Unified Communications Manager는 사용자에게 전화기를 추가하고 범용 디바이스 템플릿을 사용하여 전화기를 구성합니다.
 - 단계 12 전화기 구성을 추가 편집하려면 해당 연필 아이콘을 클릭하여 전화기 구성 창에서 전화기를 엽니다.
-

최종 사용자에게 기존 전화기 이동

기존 전화기를 새 사용자 또는 기존 최종 사용자에게 이동하려면 이 절차를 수행합니다.

프로시저

-
- 단계 1 [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 빠른/사용자 전화기 추가를 선택합니다.
- 단계 2 찾기를 클릭하고 기존 전화기를 이동할 사용자를 선택합니다.
- 단계 3 디바이스 관리 버튼을 클릭합니다.
- 단계 4 이 사용자로 이동할 전화기 찾기 버튼을 클릭합니다.
- 단계 5 이 사용자로 이동하려는 전화기를 선택합니다.
- 단계 6 선택 항목 이동을 클릭합니다.
-

DN에 외부 표시 정보 구성

특정 전화기에 할당된 DN에 대한 외부 표시 정보를 구성하려면 다음 절차를 수행합니다.

시작하기 전에

- SIP 프로파일 구성 페이지에서 외부 표시 이름 및 번호 활성화 확인란을 선택합니다.
- 최종 사용자를 추가하려면 다음 절차 중 하나를 수행합니다.
 - [최종 사용자를 수동으로 추가, 849 페이지](#)
 - [LDAP에서 최종 사용자 가져오기, 848 페이지](#)
- 다음 작업 중 하나를 수행하여 전화기를 새 사용자 또는 기존의 최종 사용자에게 할당합니다.
 - [최종 사용자를 위한 새 전화기 추가, 851 페이지](#)
 - [최종 사용자에게 기존 전화기 이동, 851 페이지](#)

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 콜 라우팅 > 디렉터리 번호를 선택합니다.
- 단계 2 디렉터리 번호 찾기 및 나열 페이지에서 다음 단계 중 하나를 수행합니다.
- DN을 업데이트하려면 찾기를 클릭하고 고유 ID를 표시할 디렉터리 번호를 선택합니다.
 - 새 디렉터리 번호를 생성하려면 새로 추가를 클릭합니다.
- 단계 3 외부 표시 정보 섹션에서 착신 디바이스에 표시할 이름과 번호를 입력합니다.
- 참고
- 외부 표시 번호 필드에는 최대 32자리의 숫자가 포함되며, [0-9, X, *, #, \, +] 문자가 포함될 수 있습니다.
 - 외부 표시 이름 필드에는 최대 50자까지 입력할 수 있습니다.

단계 4 (선택 사항), 구성된 외부 표시 번호 및 외부 표시 이름을 익명으로 표시하려면 익명 외부 표시 확인란을 선택합니다.

- 참고
- 기본적으로 익명 외부 표시 필드는 선택되어 있지 않습니다.
 - 익명 외부 표시 필드를 선택하는 경우:
외부 표시 번호 및 외부 표시 이름 필드는 편집할 수 없습니다. 이러한 필드의 항목도 사라집니다.

단계 5 디렉터리 번호 구성 페이지에서 나머지 필드를 완성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

SIP 프로파일 개요

SIP 프로파일은 일반 SIP 설정을 구성하는 템플릿입니다. 네트워크의 모든 SIP 트렁크 및 SIP 디바이스에 대한 SIP 프로파일을 할당해야 합니다. SIP 프로파일을 구성한 다음 해당 프로파일을 SIP 트렁크 또는 SIP 디바이스에 할당하면 시스템이 구성된 SIP 설정을 해당 트렁크 또는 디바이스에 적용합니다.

SIP 프로파일 구성 작업

프로시저

	명령 또는 동작	목적
단계 1	SIP 프로파일 구성, 853 페이지	이 절차를 사용하여 SIP 프로파일을 구성합니다.
단계 2	SIP 프로파일에 외부 표시 정보 구성, 854 페이지	SIP 프로파일에 대한 외부 표시 번호 및 외부 표시 이름을 구성합니다.

SIP 프로파일 구성

이 절차를 사용하여 이 프로파일을 사용하는 SIP 디바이스 및 트렁크에 할당할 수 있는 일반 SIP 설정으로 SIP 프로파일을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 2 다음 단계 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 프로파일을 편집할 SIP 프로파일을 선택합니다.
- 새로 추가를 클릭하여 새 프로파일을 생성합니다.

단계 3 SIP 전화기 및 트렁크에서 IPv4 및 IPv6 스택을 지원하도록 하려면, **ANAT** 활성화 확인란을 선택합니다.

단계 4 SDP 투명성 프로파일을 할당하여 **SDP** 투명성 프로파일 드롭다운 목록에서 SDP 상호운용성을 해결하려는 경우,

단계 5 정규화 또는 투명성 스크립트를 할당하여 정규화 스크립트 드롭다운 목록에서 SIP 상호운용성 문제를 해결하려는 경우, 스크립트를 선택합니다.

단계 6 (선택 사항) Cisco Unified Border Element 내에서 통화를 라우팅하기 위해 필요할 수 있는 전역 다이얼 플랜 복제 구축에 대한 **ILS** 설정된 대상 경로 문자열 보내기 확인란에 체크 표시를 합니다.

단계 7 **SIP** 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 8 저장을 클릭합니다.

SIP 프로파일에 외부 표시 정보 구성

이 절차를 사용하여 SIP 프로파일 구성 페이지에서 별도의 외부 표시 이름 및 번호를 구성합니다.

시작하기 전에

- **SIP** 프로파일 구성 페이지에서 외부 표시 이름 및 번호 활성화 확인란을 선택합니다.
- 서비스 매개 변수 구성 페이지의 클러스터 수준 매개 변수(디바이스 - 전화기) 섹션에서 외부 표시 이름 및 번호 매개 변수 값을 **True**로 설정합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 2 다음 단계 중 하나를 수행합니다.

- 기존 프로파일을 편집하려면, 찾기를 클릭하고 **SIP** 프로파일을 선택합니다.
- 새 프로파일을 추가하려면 새로 추가를 클릭합니다.

단계 3 외부 표시 정보 섹션에서 착신 디바이스에 표시할 이름과 번호를 입력합니다.

- 참고
- 외부 표시 번호 필드에는 최대 32자리의 숫자가 포함되며, [0-9, X, *, #, \, +] 문자가 포함될 수 있습니다.
 - 외부 표시 이름 필드에는 최대 50자를 입력할 수 있습니다.

단계 4 (선택 사항), 구성된 외부 표시 번호 및 외부 표시 이름을 익명으로 표시하려면 익명 외부 표시 확인란을 선택합니다.

- 참고
- 기본적으로 익명 외부 표시 필드는 선택되어 있지 않습니다.
 - 익명 외부 표시 필드를 선택하는 경우:
외부 표시 번호 및 외부 표시 이름 필드는 편집할 수 없습니다. 이러한 필드의 항목도 사라집니다.

단계 5 서비스 프로파일 구성 페이지의 나머지 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

SIP 트렁크 개요

통화 제어 신호 처리를 위해 SIP를 구축하는 경우, SIP 게이트웨이, SIP 프록시 서버, Unified Communications 애플리케이션, 원격 클러스터 또는 Session Management Edition과 같은 외부 디바이스에 Cisco Unified Communications Manager를 연결하는 SIP 트렁크를 구성합니다.

Cisco Unified CM 관리 내에서 SIP 트렁크 구성 창에 Cisco Unified Communications Manager에서 SIP 통화를 관리하기 위해 사용하는 SIP 신호 처리 구성이 포함됩니다.

SIP 트렁크는 기존 발신자 ID DN 및 발신자 이름과 다른 별도의 표시 이름 및 번호를 지원합니다. 새 확인란 익명 표시가 제공되어, 착신 디바이스에서 구성된 표시 이름과 번호를 익명으로 표시합니다.

트렁크 구성 작업

프로시저

	명령 또는 동작	목적
단계 1	SIP 트렁크 보안 프로파일 구성, 856 페이지	SIP 트렁크에 적용하려는 보안 설정을 사용하여 SIP 트렁크 보안 프로파일을 구성합니다. 예를 들어, SIP 신호 처리를 위해 다이제스트 인증, 디바이스 보안 모드 및 TLS 암호화를 구성할 수 있습니다. SIP 트렁크 보안 프로파일을 구성하지 않을 경우, Cisco Unified Communications Manager는 기본값으로 비보안 SIP 트렁크 보안 프로파일을 적용합니다.
단계 2	일반 디바이스 설정 구성, 857 페이지	트렁크에 대한 일반 디바이스 구성을 설정합니다. 듀얼 스택 트렁크의 경우, IP 주소 지정 기본 설정을 구성합니다.

	명령 또는 동작	목적
단계 3	SIP 트렁크 구성, 857 페이지	네트워크에서 SIP 트렁크를 구성합니다. 트렁크 구성 창에서 트렁크에 대한 SIP 설정을 구성합니다. SIP 프로파일, SIP 트렁크 보안 프로파일 및 일반 디바이스 구성을 SIP 트렁크에 할당합니다. 또한 트렁크 연결에 필요한 SIP 정규화 또는 투명성 스크립트를 할당합니다. 예를 들어, SIP 트렁크가 Cisco TelePresence VCS에 연결된 경우, <i>vcs-interop</i> 스크립트를 SIP 트렁크에 할당해야 합니다.
단계 4	SIP 트렁크에 표시 정보 구성, 858 페이지	SIP 트렁크 페이지에서 표시 이름 및 번호를 구성합니다.

SIP 트렁크 보안 프로파일 구성

다이제스트 인증 또는 TLS 신호 처리 암호화와 같은 보안 설정을 사용하여 SIP 트렁크 보안 프로파일을 구성합니다. 프로파일을 SIP 트렁크에 할당하면 트렁크는 보안 프로파일의 설정을 사용합니다.



참고 SIP 트렁크 보안 프로파일을 SIP 트렁크에 할당하지 않으면 Cisco Unified Communications Manager가 기본값으로 비보안 프로파일을 할당합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 보안 > **SIP** 트렁크 보안 프로파일을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 TLS를 사용하여 SIP 신호 처리 암호화를 활성화하려면 다음을 수행합니다.

- 디바이스 보안 모드 드롭다운 목록에서 암호화를 선택합니다.
- 수신 전송 유형 및 발신 전송 유형 드롭다운 목록에서 **TLS**를 선택합니다.
- 디바이스 인증을 위해 **X.509** 제목 이름 필드에 X.509 인증서의 제목 이름을 입력합니다.
- 수신 포트 필드에 TLS 요청을 수신하려는 포트를 입력합니다. TLS의 기본값은 5061입니다.

단계 4 다이제스트 인증을 활성화하려면 다음을 수행합니다.

- 다이제스트 인증 활성화 확인란에 체크 표시합니다.
- Nonce** 유효 타이머 값을 입력하여 시스템에서 새 nonce를 생성하기 전에 경과해야 하는 시간(초)을 나타냅니다. 기본값은 600(10분)입니다.
- 애플리케이션에 대한 다이제스트 인증을 활성화하려면 애플리케이션 수준 인증 활성화 확인란에 체크 표시합니다.

단계 5 **SIP** 트렁크 보안 프로파일 설정 창에서 추가 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

참고 트렁크가 설정을 사용할 수 있도록 트렁크 구성 창에서 프로파일을 트렁크에 할당해야 합니다.

일반 디바이스 설정 구성

일반 디바이스 구성은 사용자별 기능 특성 세트로 이루어집니다. IPv6을 구축하는 경우, 이 구성을 사용하여 SIP 트렁크 또는 SCCP 전화기에 대한 IPv6 기본 설정을 할당할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 일반 디바이스 구성을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 SIP 트렁크, SIP 전화기 또는 SCCP 전화기의 경우, **IP** 주소 지정 모드 드롭다운 목록에 대한 값을 다음과 같이 선택합니다.

- **IPv4** 전용—디바이스에서 미디어 및 신호 처리에 IPv4 주소만 사용합니다.
- **IPv6** 전용—디바이스에서 미디어 및 신호 처리에 IPv6 주소만 사용합니다.
- **IPv4 및 IPv6(기본값)**—디바이스는 듀얼 스택 디바이스로 어떤 것이든 사용할 수 있는 IP 주소 유형을 사용합니다. 해당 디바이스에 두 IP 주소 유형이 모두 구성된 경우, 신호 처리를 위해 디바이스에서 신호 처리를 위한 **IP** 주소 지정 모드 기본 설정 설정을 사용하고 미디어를 위해 디바이스에서 미디어를 위한 **IP** 주소 지정 모드 기본 설정 엔터프라이즈 매개변수를 사용합니다.

단계 4 이전 단계에서 IPv6을 구성한 경우, 신호 처리를 위한 **IP** 주소 지정 모드 드롭다운 목록에 대해 IP 주소 지정 기본 설정을 다음과 같이 구성합니다.

- **IPv4** —이중 스택 디바이스는 신호 처리를 위해 IPv4 주소를 선호합니다.
- **IPv6** —이중 스택 디바이스는 신호 처리를 위해 IPv6 주소를 선호합니다.
- 시스템 기본값 사용—신호 처리를 위한 **IP** 주소 지정 모드 기본 설정 엔터프라이즈 매개변수에 대한 설정을 사용합니다.

단계 5 일반 디바이스 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

SIP 트렁크 구성

이 절차를 사용하여 SIP 트렁크를 구성합니다. SIP 트렁크에 대해 최대 16개의 대상 주소를 할당할 수 있습니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 트렁크 유형 드롭다운 목록에서 **SIP** 트렁크를 선택합니다.
- 단계 4 프로토콜 유형 드롭다운 목록에서 구축과 일치하는 SIP 트렁크 유형을 선택하고 다음을 클릭합니다.
 - 없음(기본값)
 - 통화 제어 탐색(CCD)
 - 인터클러스터 내선 이동
 - Cisco Intercompany Media Engine
 - IP Multimedia System Service Control
- 단계 5 (선택 사항) 일반 디바이스 구성을 이 트렁크에 적용하려는 경우, 드롭다운 목록에서 구성을 선택합니다.
- 단계 6 트렁크에서 암호화된 미디어를 허용하는 경우, **SRTP** 허용됨 확인란에 체크 표시합니다.
- 단계 7 모든 클러스터 노드에 트렁크를 활성화하려면 모든 활성 **Unified CM** 노드 확인란에 체크 표시합니다.
- 단계 8 SIP 트렁크에 대한 대상 주소를 다음과 같이 구성합니다.
 - a) 대상 주소 텍스트 상자에 트렁크에 연결하려는 서버 또는 엔드포인트에 대한 IPv4 주소, FQDN(Fully Qualified Domain name) 또는 DNS SRV 레코드를 입력합니다.
 - b) 트렁크가 듀얼 스택 트렁크인 경우, 대상 주소 **IPv6** 텍스트 상자에 트렁크에 연결하려는 서버 또는 엔드포인트에 대한 IPv6 주소, FQDN(Fully Qualified Domain name) 또는 DNS SRV 레코드를 입력합니다.
 - c) 대상이 DNS SRV 레코드인 경우, 대상 주소가 **SRV**입니다 확인란에 체크 표시합니다.
 - d) 추가 대상을 추가하려면, (+)을 클릭합니다.
- 단계 9 **SIP** 트렁크 보안 프로파일 드롭다운에서 보안 프로파일을 할당합니다. 이 옵션을 선택하지 않는 경우, 비보안 프로파일이 할당됩니다.
- 단계 10 **SIP** 프로파일 드롭다운 목록에서 SIP 프로파일을 할당합니다.
- 단계 11 (선택 사항) 이 SIP 트렁크에 정규화 스크립트를 할당하려면 정규화 스크립트 드롭다운 목록에서 할당하려는 스크립트를 선택합니다.
- 단계 12 트렁크 구성 창에서 모든 추가 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 13 저장을 클릭합니다.

SIP 트렁크에 표시 정보 구성

이 절차를 사용하여 SIP 트렁크 페이지에서 표시 이름 및 번호를 구성합니다.

시작하기 전에

- SIP 프로파일 구성 페이지에서 외부 표시 이름 및 번호 활성화 확인란을 선택합니다.
- [SIP 트렁크 구성, 857 페이지](#)

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 트렁크 유형 드롭다운 목록에서 SIP 트렁크를 선택합니다.

단계 4 트렁크 서비스 유형 드롭다운 목록에서 구성할 SIP 트렁크 유형을 선택합니다.

- 없음(기본값): 트렁크는 통화 제어 탐색, 익스텐션 모빌리티 크로스 클러스터 (EMCC), Intercompany Media Engine 또는 IP 멀티미디어 시스템 서비스 제어에는 사용되지 않습니다.
- 통화 제어 탐색: 트렁크는 통화 제어 탐색 기능을 지원합니다.
- 익스텐션 모빌리티 크로스 클러스터 (EMCC): 트렁크는 익스텐션 모빌리티 크로스 클러스터 (EMCC)를 지원합니다.
- Cisco Intercompany Media Engine: 트렁크는 Intercompany Media Engine(IME)을 지원합니다. 이 유형의 트렁크를 구성하기 전에 IME 서버가 설치되어 있는지 확인합니다.
- IP 멀티미디어 시스템 서비스 제어: IP 멀티미디어 시스템 서비스를 지원하는 트렁크를 활성화하려면 이 옵션을 선택합니다.

단계 5 다음을 클릭합니다.

단계 6 표시 정보 섹션에서 착신 디바이스에 표시할 이름과 번호를 입력합니다.

- 참고
- 표시 번호 필드는 최대 32자리까지 허용하며 [0-9, X, *, #, \, +] 문자를 포함할 수 있습니다.
 - 표시 이름 필드에는 최대 50자를 입력할 수 있습니다.

단계 7 (선택 사항) 표시 이름과 번호를 익명으로 표시하려면 익명 표시 확인란을 선택합니다.

- 참고
- 기본적으로 익명 표시 필드는 선택되어 있지 않습니다.
 - 익명 외부 표시 필드를 선택하는 경우:
표시 번호 및 표시 이름 필드는 편집할 수 없습니다. 이러한 필드의 항목도 사라집니다.

단계 8 (선택 사항) SIP 트렁크에 구성된 표시 정보를 FROM 헤더로만 보내려면 다른 ID 헤더가 아닌 FROM 헤더에서만 표시 이름 및 번호 보내기 확인란을 선택합니다.

단계 9 트렁크 구성 창에서 모든 추가 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 10 저장을 클릭합니다.

클러스터 간 SME 통화 흐름

Cisco Unified Communications Manager Session Management Edition 소프트웨어는 주로 클러스터 간 또는 다양한 디바이스 간의 통화 라우팅에 사용되는 Cisco Unified Communications Manager와 동일합니다. 이 릴리스부터는 Cisco Unified Communications Manager가 클러스터 간 SME 통화를 지원합니다.

수신 통화

PSTN 네트워크의 사용자가 SIP 프로파일에서 외부 표시 이름 및 번호 활성화가 활성화된 상태에서 통화를 시작한다고 가정합니다. 외부 표시 이름 및 번호 표시서비스 매개 변수가 **True**로 설정된 경우 Cisco Unified Communications Manager는 표시 번호 정보를 X-Cisco-Presentation 헤더로 전송하고 착신 디바이스에 표시합니다. FROM 및 PAID 헤더에는 사용자의 DN 또는 DDI인 사용자의 ID가 포함됩니다.

외부 표시 이름 표시 및 번호 서비스 매개 변수가 **False**로 설정된 경우 Cisco Unified Communications Manager는 표시 번호 정보를 X-Cisco-Presentation 헤더로 전송합니다. FROM 및 PAID 헤더에는 사용자의 DN 또는 DDI가 포함되고 착신 디바이스에 표시됩니다.

발신 통화

외부 표시 이름 및 외부 표시 번호로 구성된 사용자는 클러스터 간 SIP 트렁크를 통해 PSTN 네트워크에 대한 통화를 시작합니다. 외부 표시 이름 및 번호 활성화 확인란이 SIP 프로파일에서 비활성화된 경우, Cisco Unified Communications Manager가 FROM 및 PAID 헤더에 원래 디렉터리 번호 정보를 전송하고 착신 디바이스에 표시하며 X-Cisco-Presentation 헤더에 구성된 외부 표시 정보를 표시합니다. 마찬가지로 SIP 프로파일에서 외부 프레젠테이션 이름 및 번호 활성화 확인란이 활성화된 경우 Cisco Unified Communications Manager는 FROM 헤더에 구성된 외부 표시 정보를 전송하고 착신 디바이스에 표시하고 PAID 헤더의 원래 디렉터리 번호를 표시합니다.



67 장

SIP OAuth 모드

- SIP OAuth 모드 개요, 861 페이지
- SIP OAuth 모드 사전 요건, 862 페이지
- SIP OAuth 모드 구성 작업 흐름, 862 페이지

SIP OAuth 모드 개요

Unified Communications Manager에 대한 보안 등록에는 CTL 파일 업데이트, 상호 인증서 신뢰 저장소 설정 등의 과정이 포함됩니다. 디바이스가 온-프레미스와 오프-프레미스 사이에서 전환되는 경우, 보안 등록이 완료될 때마다 LSC를 업데이트하고 CAPF(Certificate Authority Proxy Function) 등록을 갱신하는 것은 어렵습니다.

SIP OAuth 모드를 사용하면 보안 환경에서 모든 디바이스 인증에 대한 OAuth 새로 고침 토큰을 사용할 수 있습니다. 이 기능은 Unified Communications Manager의 보안을 향상시킵니다.

Unified Communications Manager에서는 엔드포인트가 제공하는 토큰을 확인하고 구성 파일을 인증 전용으로 사용합니다. SIP 등록 중 OAuth 토큰 유효성 검사는 Unified Communications Manager 클러스터 및 다른 Cisco 디바이스에서 OAuth 기반 인증이 활성화될 때 완료됩니다.

SIP 등록에 대한 OAuth 지원은 다음에 대해 확장됩니다.

- Cisco Unified Communications Manager 12.5 릴리스의 Cisco Jabber 디바이스
- Cisco Unified Communications Manager 릴리스 14 이후의 SIP 전화기



참고 기본적으로 SIP OAuth가 활성화된 경우 TFTP는 SIP 전화기에 대해 안전합니다. TFTP 파일 다운로드되는 보안 채널을 통해 인증된 전화기에 대해서만 발생합니다. SIP OAuth는 온-프레미스와 MRA를 통해 CAPF 온프레미스 없이 엔드 투 엔드 보안 신호 처리 및 미디어 암호화를 제공합니다.

다음은 OAuth에 대해 구성할 수 있는 전화기 보안 프로파일 유형입니다.

- iPhone용 Cisco 이중 모드(TCT 디바이스)
- Android용 Cisco 이중 모드(BOT 디바이스)

- Cisco Unified Client Service Framework(CSF 디바이스)
- 태블릿용 Cisco Jabber(TAB 디바이스)
- 범용 디바이스 템플릿
- Cisco 8811
- Cisco 8841
- Cisco 8851
- Cisco 8851NR
- Cisco 8861
- Cisco 7811
- Cisco 7821
- Cisco 7841
- Cisco 7861
- Cisco 8845
- Cisco 8865
- Cisco 8865NR
- Cisco 7832
- Cisco 8832
- Cisco 8832NR

SIP OAuth 모드 사전 요건

이 기능은 사용자가 다음을 이미 완료했다고 가정합니다.

- 모바일 및 원격 액세스가 구성되고 Unified Communication Manager와 Expressway 사이에 연결이 설정되어 있는지 확인합니다.
- Unified Communications Manager가 내보내기 제어 허용 기능을 통해 스마트 또는 가상 어카운트에 등록되어 있는지 확인합니다.
- 클라이언트 펌웨어가 SIP OAuth를 지원하는지 확인합니다.

SIP OAuth 모드 구성 작업 흐름

시스템에 대한 SIP OAuth를 구성하려면 다음 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 1	전화기 옛지 신뢰에 CA 인증서 업로드	CA 인증서를 전화기 옛지 신뢰에 업로드하여 토큰을 가져옵니다. 이 단계는 Cisco Jabber 디바이스에는 해당되지 않습니다.
단계 2	디바이스에 대한 OAuth 액세스 토큰 활성화	중요 이 단계는 14 이후 릴리스부터 적용할 수 있습니다. Cisco IP 전화기 7800 및 8800 엔터프라이즈 시리즈에서 SIP 등록에 대해 OAuth를 활성화합니다. 이 단계는 Cisco Jabber 디바이스에는 해당되지 않습니다.
단계 3	새로 고침 로그인 구성, 865 페이지	SIP OAuth를 통해 디바이스를 등록하려면 Unified Communications Manager의 로그인 흐름 새로 고침을 사용하여 oauth를 활성화합니다.
단계 4	OAuth 포트 구성, 865 페이지	OAuth 등록이 있는 각 노드에 대해 OAuth에 대한 포트를 할당합니다.
단계 5	Expressway-C에 대한 OAuth 연결 구성, 866 페이지	Expressway-C에 상호 인증된 TLS 연결을 구성합니다.
단계 6	SIP OAuth 모드 활성화, 867 페이지	퍼블리셔 노드에서 CLI 명령을 사용하여 OAuth 서비스를 활성화합니다.
단계 7	Cisco CallManager 서비스 다시 시작, 867 페이지	OAuth 등록이 포함된 모든 노드에서 이 서비스를 다시 시작합니다.
단계 8	전화기 보안 프로파일에서 디바이스 보안 모드 구성	엔드포인트에 대한 암호화를 구축하는 경우 전화기 보안 프로파일 내에서 OAuth 지원을 구성합니다.
단계 9	(선택 사항) MRA 모드에 대해 SIP OAuth 등록 전화기 구성	중요 이 단계는 14 이후 릴리스부터 적용할 수 있습니다. MRA 모드에서 SIP OAuth 등록 전화기를 구성합니다. 이 단계는 Cisco Jabber 디바이스에는 해당되지 않습니다.

전화기 옛지 신뢰에 CA 인증서 업로드

이 절차를 사용하여 Tomcat 서명 인증서의 루트 인증서를 전화기 옛지 신뢰에 업로드합니다.



참고 이 절차는 Cisco 전화기에 대해서만 수행되며 Cisco Jabber에는 적용되지 않습니다.

프로시저

단계 1 Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 2 인증서/인증서 체인 업로드를 클릭합니다.

단계 3 인증서/인증서 체인 업로드 창의 인증서 용도 드롭다운 목록에서 전화기 옛지 신뢰를 선택합니다.

단계 4 파일 업로드 필드에서 찾아보기를 클릭하고 인증서를 업로드합니다.

단계 5 업로드를 클릭합니다.

디바이스에 대한 OAuth 액세스 토큰 활성화



중요 이 섹션은 14 이후 릴리스부터 적용할 수 있습니다.

이 절차를 사용하여 전화기에 대한 OAuth 액세스 토큰을 활성화합니다.



참고 전화기의 SIP 등록에 대한 OAuth 지원에 대해서만 이 엔터프라이즈 매개 변수를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 2 SSO 및 OAuth 구성 섹션에서 디바이스에 대한 OAuth 액세스 토큰 값 드롭다운 목록이 암시적:이미 등록된 디바이스로 설정되어 있는지 확인합니다.

참고 디바이스에 대한 OAuth 액세스 토큰의 값을 명시적:활성화 코드 디바이스 온보딩 필요로 설정하여 SIP OAuth 등록을 위한 수신 토큰을 암시적으로 비활성화하고 활성화 코드를 통한 수신 토큰만 지원합니다. 그런 다음 보안 프로파일에 표시된 경우 SIP OAuth 등록에 토큰을 사용할 수 있습니다.

릴리스 14 이후부터는 엔터프라이즈 매개변수 디바이스용 OAuth 액세스 토큰의 기본값은 암시적:이미 등록된 디바이스입니다.

단계 3 저장을 클릭합니다.

새로 고침 로그인 구성

이 절차를 사용하여 Cisco Jabber 클라이언트에 대한 OAuth 액세스 토큰 및 새로 고침 토큰을 사용하여 새로 고침 로그인을 구성합니다.

프로시저

-
- 단계 1 [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.
 - 단계 2 SSO 및 OAuth 구성 아래에서 새로 고침 로그인을 사용한 OAuth 매개 변수를 활성화됨으로 설정합니다.
 - 단계 3 (선택 사항) SSO 및 OAuth 구성 섹션에서 다른 매개 변수를 설정합니다. 매개변수 설명이 필요한 경우, 매개변수 이름을 클릭합니다.
 - 단계 4 저장을 클릭합니다.
-

OAuth 포트 구성

이 절차를 사용하여 SIP OAuth에 사용되는 포트를 할당합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다., 시스템 > Cisco Unified CM.
 - 단계 2 SIP OAuth를 사용하는 각 서버에 대해 다음을 수행합니다.
 - 단계 3 서버를 선택합니다.
 - 단계 4 Cisco Unified Communications Manager TCP 포트 설정 아래에서 다음 필드에 대한 포트 값을 설정합니다.
 - SIP 전화기 OAuth 포트
기본값은 5090입니다. 허용 가능한 구성 가능 범위는 1024 ~ 49151입니다.
 - SIP 모바일 및 원격 액세스 포트
기본값은 5091입니다. 허용 가능한 구성 가능 범위는 1024 ~ 49151입니다.

참고 Cisco Unified Communications Manager는 SIP 전화기 OAuth 포트(5090)를 사용하여 TLS를 통해 Jabber 온프레미스 디바이스에서 SIP 회선 등록을 수신 대기합니다. 그러나 Unified CM은 SIP 모바일 원격 액세스 포트(기본값 5091)를 사용하여 mTLS를 통해 Expressway의 Jabber에서 SIP 회선 등록을 수신 대기합니다.

두 포트 모두 수신 TLS/mTLS 연결에 대해 Cisco Tomcat 인증서 및 Tomcat-trust를 사용합니다. Tomcat-trust 저장소에서 모바일 및 원격 액세스가 정확하게 작동하려면 SIP OAuth 모드에 대한 Expressway-C 인증서를 확인할 수 있어야 합니다.

다음의 경우에는 Expressway-C 인증서를 Cisco Unified Communications Manager의 Tomcat-Trust 인증서 저장소에 업로드하기 위한 추가 단계를 수행해야 합니다.

- Expressway-C 인증서 및 Cisco Tomcat 인증서가 동일한 CA 인증서에 의해 서명되지 않았습니다.
- Unified CM Cisco Tomcat 인증서는 CA에 서명이 되어 있지 않습니다.

단계 5 저장을 클릭합니다.

단계 6 SIP OAuth를 사용하는 각 서버에 대해 이 절차를 반복합니다.

Expressway-C에 대한 OAuth 연결 구성

이 절차를 사용하여 Cisco 통합 커뮤니케이션 매니저 관리에 Expressway-C 연결을 추가합니다. SIP OAuth를 사용하는 모바일 및 원격 액세스 모드의 디바이스에 대해 이 구성이 필요합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > **Expressway-C**.

단계 2 (선택 사항) **Expressway-C** 찾기 및 나열 창에서 찾기를 클릭하여 Expressway-C에서 Unified Communications Manager(으)로 푸시된 X.509 주체 이름/주체 대체 이름을 확인합니다.

참고 필요한 경우 값을 수정할 수 있습니다. 또는 항목이 누락된 경우 Expressway-C 정보를 추가합니다.

Expressway-C가 Unified Communications Manager와 다른 도메인에 있는 경우 관리자가 Cisco Unified CM 관리 사용자 인터페이스에 액세스하고 Unified CM 구성에서 Expressway C에 도메인을 추가해야 합니다.

단계 3 새로 추가를 클릭합니다.

단계 4 Expressway-C의 IP 주소, 호스트 이름 또는 정규화된 도메인 이름을 입력합니다.

단계 5 설명을 입력합니다.

단계 6 Expressway-C 인증서에서 Expressway-C의 X.509 주체 이름/주체 대체 이름을 입력합니다.

단계 7 저장을 클릭합니다.

SIP OAuth 모드 활성화

명령줄 인터페이스를 사용하여 SIP OAuth 모드를 활성화합니다. 퍼블리셔 노드에서 이 기능을 활성화하면 모든 클러스터 노드의 기능도 활성화됩니다.

시작하기 전에

14SU1 릴리스부터 프록시 TFTP가 활성화된 경우 오프 클러스터 Tomcat 인증서의 루트 CA 인증서를 프록시 전화기 옛지 신뢰로 복사해야 합니다.

프로시저

단계 1 Cisco Unified Communications Manager 노드에서 명령줄 인터페이스에 로그인합니다.

단계 2 `utils sipOAuth-mode enable` CLI 명령을 실행합니다.

릴리스 14부터 읽기 전용 클러스터 **SIPOAuth** 모드 엔터프라이즈 매개 변수가 활성화됨으로 업데이트됩니다.

Cisco CallManager 서비스 다시 시작

CLI를 통해 SIP OAuth를 활성화한 후 엔드포인트가 SIP OAuth를 통해 등록되는 모든 노드에서 Cisco CallManager 서비스를 다시 시작합니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에서 다음 메뉴를 선택합니다. 도구 > 제어 센터 > 기능 서비스.

단계 2 서버 드롭다운 목록에서 서버를 선택합니다.

단계 3 **Cisco CallManager** 서비스를 선택하고 다시 시작을 클릭합니다.

전화기 보안 프로파일에서 디바이스 보안 모드 구성

이 절차를 사용하여 전화기 보안 프로파일에서 디바이스 보안 모드를 구성하고 해당 전화기의 전화기 보안 프로파일 내에서 디바이스 보안 모드를 암호화로 설정한 경우에만 필요합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 보안 > 전화기 보안 프로파일에 체크 표시합니다.

단계 2 다음 중 하나를 수행합니다.

- 기존 전화기 보안 프로파일 검색

- 새로 추가를 클릭합니다.

단계 3 전화기 보안 프로파일 정보 섹션의 디바이스 보안 모드 드롭다운 목록에서 암호화를 선택합니다.

단계 4 전송 유형 드롭다운 목록에서 **TLS**를 선택합니다.

단계 5 **OAuth** 인증 활성화 확인란을 선택합니다.

단계 6 저장을 클릭합니다.

단계 7 전화기 보안 프로파일을 전화기에 연결합니다. 전화기 보안 프로파일을 적용하는 방법에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 보안 설명서](#)의 "전화기에 보안 프로파일 적용" 섹션을 참조하십시오.

참고 변경 내용을 적용하려면 전화기를 재설정합니다.

참고 SIP OAuth 모드가 활성화되면 다이제스트 인증 활성화 및 **TFTP** 암호화 구성 옵션이 지원되지 않습니다. 전화기에서 **https(6971)**를 통해 TFTP 구성 파일을 안전하게 다운로드하고 토큰을 인증에 사용합니다.

MRA 모드에 대해 SIP OAuth 등록 전화기 구성

이 절차를 사용하여 SIP OAuth 등록 전화기를 MRA 모드로 구성합니다.

시작하기 전에



중요 이 섹션은 14 이후 릴리스부터 적용할 수 있습니다.

전화기가 활성화 코드를 사용하도록 구성되어 있는지 확인합니다. 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)에서 활성화 코드를 사용하도록 등록 방법 설정 섹션을 참조하십시오.



참고 MRA를 통한 SIP OAuth를 사용할 때 사용자는 로그인에 사용자 이름/암호를 사용할 수 없지만 활성화 코드 기반 온보딩을 사용해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 전화기.

단계 2 찾기를 클릭하고 오프 프레미스 모드에 대해 구성하려는 디바이스를 선택합니다.

단계 3 디바이스 정보 섹션에서 다음을 수행합니다.

- **MRA**를 통한 활성화 코드 허용 확인란을 선택합니다.

- 활성화 코드 **MRA** 서비스 도메인 드롭다운 목록에서 필요한 MRA 서비스 도메인을 선택합니다. MRA 서비스 도메인을 구성하는 방법에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 MRA 서비스 도메인 구성 섹션을 참조하십시오.

참고 MRA를 통한 SIP OAuth 모드의 경우 활성화 코드만 사용하고 사용자 이름/암호 기반 로그인 사용하지 마십시오.

단계 4 프로토콜 특정 정보 섹션의 장치 보안 프로파일 드롭다운 목록에서 OAuth 활성화된 SIP 프로파일을 선택합니다. 전화기가 OAuth 펌웨어를 지원하는지 확인합니다. 보안 프로파일을 만드는 방법에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 전화기 보안 프로파일 구성 섹션을 참조하십시오.

단계 5 저장을 클릭하고 구성 적용을 클릭합니다.

참고 전화기가 MRA 모드로 전환되고 Expressway와 통신을 시작합니다. 내부 네트워크가 온프레미스에서 Expressway와의 통신을 허용하지 않는 경우, 전화기는 등록되지 않지만 오프프레미스에 전원이 공급되면 Expressway에 연결될 수 있습니다.



XV 부

QoS 관리

- [APIC-EM 컨트롤러를 사용하여 QoS 구성, 873 페이지](#)
- [AS-SIP 엔드포인트 구성, 879 페이지](#)
- [MLPP\(Multilevel Precedence and Preemption\) 구성, 893 페이지](#)



68 장

APIC-EM 컨트롤러를 사용하여 QoS 구성

- APIC-EM 컨트롤러 개요, 873 페이지
- APIC-EM 컨트롤러 사전 요건, 874 페이지
- APIC-EM 컨트롤러 구성 작업 흐름, 874 페이지

APIC-EM 컨트롤러 개요

APIC-EM 컨트롤러에서는 네트워크 트래픽 관리용 중앙 시스템을 제공하여 혼잡한 네트워크에서도 항상 대역폭을 보유하여 커뮤니케이션을 유지할 수 있게 해줍니다. Cisco Unified Communications Manager를 설정하여 APIC-EM 컨트롤러를 사용하여 SIP 미디어 플로우를 관리할 수 있습니다. 이를 통해 제공받는 이점은 다음과 같습니다.

- QoS 관리를 중앙에서 집중 처리함으로써, DSCP 값을 할당하기 위한 엔드포인트에 대한 필요를 없애 줍니다.
- 서로 다른 미디어 흐름에 대한 차등 QoS 처리를 적용합니다. 예를 들면, 비디오에 비해 오디오를 우선시하여 네트워크 대역폭이 낮을 때조차도 기본 오디오 커뮤니케이션이 항상 유지되도록 보장할 수 있습니다.
- SIP 프로파일 외부 QoS 설정을 통해 어떤 사용자가 APIC-EM을 사용할지 타겟팅할 수 있습니다. 예를 들면, Cisco Unified IP Phone 사용자가 Cisco Unified Communications Manager에서 DSCP 설정을 사용하는 동안, Cisco Jabber 사용자가 APIC-EM을 사용하여 미디어 플로우를 관리하도록 할 수 있습니다.

SIP 미디어 흐름 관리

APIC-EM을 사용하는 SIP 통화의 경우, Cisco Unified Communications Manager는 통화 시작 시 설정 중인 미디어 흐름을 APIC-EM에 통지하는 정책 요청을 APIC-EM 컨트롤러에 전송합니다. 정책 요청에는 소스 및 대상 디바이스에 대한 IP 주소 및 포트, 흐름에 대한 미디어 유형 및 프로토콜을 포함하여 통화에 대한 정보가 포함됩니다.

APIC-EM은 연결된 미디어 흐름에 대한 DSCP 값의 통화 흐름을 시작할 때 스위치에 알립니다. 이 스위치는 해당 DSCP 값을 개별 미디어 패킷에 삽입하여 엔드포인트에서 삽입하는 값을 덮어씁니다. 통화 흐름의 게이트웨이가 정체되는 경우 해당 게이트웨이는 더 높은 DSCP 값이 있는 패킷을 통해 먼저 전송됩니다. 이렇게 하면 우선 순위가 높은 오디오 및 비디오 스트림이 이메일, 인쇄 작업 또는

소프트웨어 다운로드와 같은 낮은 우선 순위 네트워크 트래픽에 의해 차단되지 않습니다. 통화가 종료되면 Cisco Unified Communications Manager가 APIC-EM에 알리고 APIC-EM에서 흐름을 삭제하도록 스위치에 알립니다.

외부 QoS 지원

Cisco Unified Communications Manager에서 APIC-EM을 사용하여 미디어 흐름을 관리하려면 외부 QoS 매개 변수를 시스템 수준에서 클러스터 수준 서비스 매개 변수를 통해, 그리고 디바이스 수준에서 SIP 프로파일을 통해 활성화해야 합니다.

APIC-EM 컨트롤러 사전 요건

APIC-EM을 사용하기 전에 다음 작업을 수행해야 합니다.

- Cisco Unified Communications Manager에서 여러 SIP 미디어 흐름에 대한 DSCP 우선 순위를 구성합니다. 자세한 내용은 [DSCP 설정 구성 작업 흐름, 839 페이지](#)를 참조하십시오.
- 네트워크 내에서 APIC-EM 컨트롤러 하드웨어를 구성합니다. 자세한 내용은 APIC-EM 컨트롤러와 함께 제공되는 하드웨어 설명서를 참조하십시오.

APIC-EM 컨트롤러 구성 작업 흐름

Cisco Unified Communications Manager에서 이러한 작업을 완료하여 APIC-EM 컨트롤러가 SIP 미디어 흐름을 관리하도록 합니다.

프로시저

	명령 또는 동작	목적
단계 1	APIC-EM 컨트롤러 구성, 875 페이지	APIC-EM 컨트롤러에서 Unified CM을 구성합니다.
단계 2	APIC-EM 컨트롤러 인증서 업로드, 875 페이지	APIC-EM 인증서를 Cisco 통합 OS 관리에 업로드합니다.
단계 3	APIC-EM 컨트롤러에 대한 HTTPS 연결 구성, 876 페이지	APIC-EM 서비스를 가리키는 HTTP 프로파일을 구성합니다.
단계 4	시스템에 대한 외부 QoS 서비스 활성화, 876 페이지	외부 QoS 활성화 서비스 매개 변수를 활성화하여 시스템에서 APIC-EM을 사용하여 미디어 흐름을 관리하도록 구성합니다. 디바이스에서 SIP 미디어 흐름 관리에 대한 APIC-EM을 사용하려면 서비스 매개 변수를 활성화해야 합니다.

	명령 또는 동작	목적
		참고 SIP 미디어 흐름 관리에 대한 APIC-EM을 사용하는 디바이스에 대해 SIP 프로파일 내에서 외부 QoS도 활성화해야 합니다.
단계 5	SIP 프로파일 수준에서 외부 QoS 서비스 구성, 877 페이지	SIP 프로파일 내에서 외부 QoS를 활성화합니다. 이 SIP 프로파일을 사용하는 모든 디바이스는 APIC-EM을 사용하여 SIP 미디어 흐름을 관리할 수 있습니다. SIP 프로파일 설정을 사용하여 APIC-EM에서 미디어 흐름을 관리하는 데 사용할 디바이스 및 디바이스 유형을 구성할 수 있습니다.
단계 6	SIP 프로파일을 전화기에 할당, 877 페이지	외부 QoS 사용 SIP 프로파일을 전화기에 연결합니다.

APIC-EM 컨트롤러 구성

APIC-EM 컨트롤러에서 이 절차를 사용하여 Cisco Unified Communications Manager를 사용자로 추가합니다. APIC-EM의 역할 기반 액세스 제어 기능은 Cisco Unified Communications Manager에게 APIC-EM 리소스에 대한 액세스 권한을 제공합니다.

프로시저

단계 1 APIC-EM 컨트롤러에서 설정 > 내부 사용자를 선택합니다.

단계 2 **ROLE_POLICY_ADMIN** 역할을 사용하여 새 사용자를 만듭니다. Cisco Unified Communications Manager의 **HTTP** 프로파일 창에 동일한 자격 증명을 입력해야 하므로 입력한 사용자 이름과 암호를 추적합니다.

단계 3 검색 탭으로 이동하여 CDP 또는 사용 가능한 디바이스의 IP 주소 범위에 대한 검색을 추가합니다.

단계 4 디바이스 재고 목록 탭을 선택하고 연결할 수 있는 디바이스를 선택합니다.

단계 5 정책 태그 설정을 클릭합니다.

단계 6 정책 태그를 만들고 디바이스에 대해 설정합니다.

단계 7 **EasyQoS** 탭에서 사용자가 만든 정책을 선택하고 **DynamicQoS**를 활성화합니다.

APIC-EM 컨트롤러 인증서 업로드

이 절차를 사용하여 Cisco Unified Communications Manager에 APIC-EM 컨트롤러 인증서를 업로드합니다.

프로시저

-
- 단계 1 Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
 - 단계 2 인증서/인증서 체인 업로드를 클릭합니다.
인증서/인증서 체인 업로드 팝업 창이 나타납니다.
 - 단계 3 인증서 용도 드롭다운 목록에서 **CallManager-trust**를 선택합니다.
 - 단계 4 인증서에 대한 설명을 입력합니다.
 - 단계 5 찾아보기를 클릭하여 인증서를 검색하고 선택합니다.
 - 단계 6 업로드를 클릭합니다.
-

APIC-EM 컨트롤러에 대한 HTTPS 연결 구성

이 절차를 사용하여 Cisco Unified Communications Manager를 APIC-EM 컨트롤러에 연결할 HTTP 프로파일을 설정합니다. 이 연결에서는 Cisco Unified Communications Manager가 HTTP 사용자 역할을 하고 APIC-EM이 HTTP 서버 역할을 합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 통화 라우팅 > **HTTP** 프로파일을 선택합니다.
 - 단계 2 서비스의 이름을 입력합니다.
 - 단계 3 이 HTTP 연결에 대한 사용자 이름과 암호를 입력합니다. 사용자 이름은 Cisco Unified Communications Manager에서 구성된 최종 사용자일 필요는 없지만, 사용자 이름과 암호는 APIC-EM 컨트롤러에 구성된 값과 일치해야 합니다.
 - 단계 4 웹 서비스 루트 **URI** 텍스트 상자에 APIC-EM 서비스의 IP 주소 또는 FQDN(Fully Qualified Domain Name)을 입력합니다.
 - 단계 5 HTTP 프로파일 창에서 나머지 필드를 구성합니다. 필드 및 해당 옵션에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.
 - 단계 6 저장을 클릭합니다.
-

시스템에 대한 외부 QoS 서비스 활성화

시스템에 대한 외부 QoS 서비스 활성화

이 절차를 사용하여 QoS 관리를 위해 외부 서비스를 사용하도록 Cisco Unified Communications Manager를 구성합니다. QoS에 대한 APIC-EM 컨트롤러를 사용하려면 이 서비스 매개 변수를 활성화해야 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 2 서버 드롭다운 목록에서 퍼블리셔 노드를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 4 외부 QoS 활성화 서비스 매개 변수의 값을 **True**로 설정합니다.

단계 5 저장을 클릭합니다.

참고 APIC-EM을 사용하여 디바이스에 대한 통화 흐름을 관리하려면 디바이스에 대한 SIP 프로파일 내에서도 외부 QoS를 활성화해야 합니다.

SIP 프로파일 수준에서 외부 QoS 서비스 구성

외부 QoS 활성화 클러스터 수준 서비스 매개 변수를 활성화한 경우 이 절차를 통해 이 SIP 프로파일을 사용하는 SIP 디바이스에 대한 외부 QoS를 활성화합니다.



참고 APIC-EM을 사용하여 QoS를 관리하려면 시스템 수준과 SIP 프로파일 모두에서 외부 QoS를 활성화해야 합니다.

프로시저

단계 1 [Cisco Unified CM 관리]에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 SIP 프로파일을 선택합니다.
- 새로 추가를 클릭하여 새 SIP 프로파일을 만듭니다.

단계 3 외부 QoS 활성화 확인란을 선택합니다. APIC-EM 컨트롤러를 사용하여 QoS를 관리하려면 이 SIP 프로파일을 사용하는 전화기에 대해 이 확인란을 선택해야 합니다.

단계 4 SIP 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

SIP 프로파일을 전화기에 할당

생성한 외부 QoS 사용 SIP 프로파일을 전화기에 할당하려면 이 절차를 사용합니다.



팁 벌크 관리 도구를 사용하여 한 번의 작업으로 다수의 전화기를 선택하는 SIP 프로파일을 업데이트합니다. 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 지침서를 참조하십시오.

프로시저

- 단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.
- 단계 2 찾기를 클릭하고 기존 전화기를 선택합니다.
- 단계 3 SIP 프로파일 드롭다운 목록에서 APIC-EM 컨트롤러를 사용하여 트래픽을 관리하는 전화기에 대해 업데이트된 SIP 프로파일을 선택합니다.
- 단계 4 전화기 구성 창의 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 5 저장을 클릭합니다.



69 장

AS-SIP 엔드포인트 구성

- [AS-SIP 개요, 879 페이지](#)
- [AS-SIP 사전 요건, 882 페이지](#)
- [AS-SIP 엔드포인트 구성 작업 흐름, 882 페이지](#)

AS-SIP 개요

AS-SIP(보증된 서비스 SIP) 엔드포인트는 MLPP, DSCP, TLS/SRTP 및 IPv6 요구 사항을 준수합니다. AS-SIP는 Unified Communications Manager에 여러 엔드포인트 인터페이스를 제공합니다.

대부분의 Cisco IP 전화기는 AS-SIP로 지원됩니다. 또한 타사 AS-SIP 엔드포인트 디바이스 유형을 사용하면 타사 AS-SIP 호환 엔드포인트를 구성하여 Cisco Unified Communications Manager에 사용할 수 있습니다. 또한 타사 AS-SIP 엔드포인트 디바이스 유형을 사용하면 타사 AS-SIP 호환 일반 엔드포인트를 구성하여 Cisco Unified Communications Manager에 사용할 수 있습니다.

AS-SIP 기능

다음과 같은 기능이 구현되거나 SIP 엔드포인트에 사용할 수 있게 됩니다.

- MLPP
- TLS
- SRTP
- 우선 수준을 위한 DSCP
- 오류 응답
- V.150.1 MER
- 컨퍼런스 팩토리 흐름 지원
- AS-SIP 회선 Early Offer

타사 AS-SIP 전화기

타사 전화기를 Cisco Unified Communications Manager에 제공하여 타사의 AS-SIP 엔드포인트 디바이스 유형을 사용할 수 있습니다.

AS-SIP를 실행 중인 타사 전화기는 Cisco Unified Communications Manager TFTP 서버를 통해 구성하지 않습니다. 고객은 기본 전화기 구성 메커니즘(일반적으로 웹 페이지 또는 TFTP 파일)을 사용하여 타사 전화기를 구성해야 합니다. 고객은 Cisco Unified Communications Manager 데이터베이스의 디바이스 및 회선 구성을 기본 전화기 구성과 동기화된 상태로 유지해야 합니다(예를 들면 전화기의 1002와 Cisco Unified Communications Manager의 1002). 또한, 회선의 디렉터리 번호를 변경하는 경우 고객은 Unified CM 관리와 기본 전화기 구성 메커니즘에서 모두 변경되도록 해야 합니다.

타사 전화기 식별

SIP를 실행 중인 타사 전화기는 MAC 주소를 전송하지 않으므로 사용자 이름을 사용하여 자체적으로 식별해야 합니다. REGISTER 메시지는 다음 헤더가 포함됩니다.

```
Authorization: Digest
username="swhite",realm="ccmsipline",nonce="GBauADss2qoWr6k9y3hGGVDAqnLfoLk5",uri="sip:172.18.197.224",
algorithm=MD5,response="126c0643a4923359ab59d4f53494552e"
```

사용자 이름인 **swhite**는 Cisco Unified CM 관리의 최종 사용자 구성 창에서 구성된 최종 사용자와 일치해야 합니다. 관리자는 전화기 구성 창의 다이제스트 사용자 필드에서 예를 들어 **swhite**라는 사용자를 사용하여 SIP 타사 전화기를 구성합니다.



참고 각 사용자 ID를 한 대의 타사 전화기에만 할당할 수 있습니다. 동일한 사용자 ID가 여러 전화기에 대해 다이제스트 사용자로 할당되는 경우 이러한 ID가 할당된 타사 전화기가 제대로 등록되지 않습니다.

타사 AS-SIP 전화기 및 Cisco IP 전화기 구성

다음 표에서는 Cisco Unified IP Phone과 AS-SIP를 실행하는 타사 전화기 사이의 구성 차이점을 간략히 비교하여 보여 줍니다.

표 84: Cisco IP 전화기와 타사 전화기 간의 구성 차이점 비교

AS-SIP를 실행하는 전화기	중앙 집중식 TFTP와 통합됨	MAC 주소 보내기	소프트키 파일 다운로드	다이얼 플랜 파일 다운로드	Unified Communications Manager 장애 조치 및 폴백 지원	재설정 및 재시작 지원
Cisco IP 전화기	예	예	예	예	예	예

AS-SIP를 실행하는 전화기	중앙 집중식 TFTP와 통합됨	MAC 주소 보내기	소프트키 파일 다운로드	다이얼 플랜 파일 다운로드	Unified Communications Manager 장애 조치 및 폴백 지원	재설정 및 재시작 지원
타사 AS-SIP 디바이스	아니요	아니요	아니요	아니요	아니요	아니요



참고 모든 Cisco IP 전화기가 AS-SIP로 지원되지는 않습니다. 지원 정보는 전화기 모델의 전화기 관리 지침서를 참조하십시오.

Cisco Unified CM 관리를 사용하여 SIP를 실행하는 타사 전화기를 구성합니다. 자세한 내용은 *Cisco Unified Communications Manager*용 시스템 구성 설명서의 "SIP 프로파일 구성" 항목을 참조하십시오. 관리자는 SIP를 실행하는 타사 전화기에서도 구성 단계를 수행해야 합니다. 다음 예를 참조하십시오.

- 전화기의 프록시 주소가 Cisco Unified Communications Manager의 IP 또는 FQDN(정규화된 도메인 이름)인지 확인합니다.
- 전화기의 디렉터리 번호가 Unified CM 관리에서 디바이스용으로 구성된 디렉터리 번호와 일치하는지 확인합니다.
- 전화기의 다이제스트 사용자 ID(인증 ID라고도 함)가 Cisco Unified CM 관리의 다이제스트 사용자 ID와 일치하는지 확인합니다.

자세한 내용은 타사 전화기와 함께 제공된 설명서를 참조하십시오.

AS-SIP 컨퍼런싱

기능 호출자(보류자, 호전환자 또는 전화회의 개시자)가 Cisco 전용 기능 신호 처리를 지원하는 경우 MOH가 대상(보류 상대방, 호전환 직전 피호전환자 또는 전화회의 참가 직전 회의 참가자)에 적용됩니다. 기능 호출자가 Cisco 전용 기능 신호 처리를 지원하지 않을 경우 MOH가 대상에 적용되지 않습니다. 또한, 엔드포인트가 컨퍼런스 믹서임을 명시적으로 알리는 경우 MOH가 대상에게 재생되지 않습니다. AS-SIP 컨퍼런싱에는 두 가지 형태가 있습니다.

- 로컬 믹싱
- 회의 팩터리

로컬 믹싱

Unified CM 측에서는 전화회의 개시자가 각각의 다른 전화회의 참석자마다 하나씩 단순히 통화 통화를 동시에 설정한 것처럼 보입니다. 이니시에이터는 로컬로 전화회의를 주최하며 이곳에서 음성이 믹싱됩니다. 컨퍼런스 주최자의 통화는 MOH 소스에 연결되지 않도록 하는 특수 신호 처리가 되어 있습니다.

회의 팩토리

컨퍼런스 주최자는 SIP 트렁크로부터 떨어져 있는 컨퍼런스 팩토리 서버에 전화를 겁니다. IVR 신호 처리를 통해 전화화의 개시자가 컨퍼런스 팩토리에 컨퍼런스 브리지를 예약하도록 지시합니다. 컨퍼런스 팩토리는 숫자 주소(전송 가능한 DN)를 전화화의 개시자에게 제공합니다. 그러면 전화화의 개시자는 브리지 가입을 설정하여 참가자를 추적할 전화화의 목록 정보를 수신합니다. 컨퍼런스 팩토리에서 MOH 소스에 연결되지 않도록 하는 특수 신호 처리를 전송합니다.

AS-SIP 사전 요건

충분한 디바이스 라이선스 단위를 사용할 수 있는지 확인합니다. 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "스마트 소프트웨어 라이선싱" 장을 참조하십시오.

AS-SIP 엔드포인트 구성 작업 흐름

감사 로깅을 구성하려면 다음 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 1	다이제스트 사용자 구성, 883 페이지	SIP 요청에 대해 다이제스트 인증을 사용하도록 최종 사용자를 구성합니다.
단계 2	SIP 전화기 보안 포트 구성, 884 페이지	Cisco Unified Communications Manager는 이 포트를 사용하여 TLS를 통한 SIP 회선 등록을 위한 SIP 전화를 수신합니다.
단계 3	서비스 다시 시작, 884 페이지	보안 포트를 구성한 후 Cisco CallManager 및 Cisco CTL Provider 서비스를 다시 시작합니다.
단계 4	AS-SIP용 SIP 프로파일 구성, 884 페이지	AS-SIP 엔드포인트와 SIP 트렁크를 위한 SIP 설정을 사용하여 SIP 프로파일을 구성합니다.
	참고	전화기 특정 매개 변수는 타사 AS-SIP 전화기에 다운로드되지 않으며, Cisco Unified Communications Manager에서만 사용됩니다. 타사 전화기에서는 동일한 설정을 로컬로 구성해야 합니다.

	명령 또는 동작	목적
단계 5	AS-SIP에 대한 전화기 보안 프로파일 구성, 885 페이지	전화기 보안 프로파일을 사용하여 TLS, SRTP 및 다이제스트 인증과 같은 보안 설정을 할당할 수 있습니다.
단계 6	AS-SIP 엔드포인트 구성, 886 페이지	Cisco IP 전화기 또는 타사 엔드포인트 및 AS-SIP 지원을 구성 합니다.
단계 7	디바이스를 최종 사용자에게 연결, 887 페이지	엔드포인트를 사용자와 연결합니다.
단계 8	AS-SIP에 대한 SIP 트렁크 보안 프로파일 구성, 887 페이지	SIP 트렁크 보안 프로파일을 사용하여 TLS 또는 다이제스트 인증과 같은 보안 기능을 SIP 트렁크에 할당할 수 있습니다.
단계 9	AS-SIP에 대한 SIP 트렁크 구성, 888 페이지	AS-SIP 지원을 사용하여 SIP 트렁크를 구성합니다.
단계 10	AS-SIP 기능 구성, 889 페이지	MLPP, TLS, V.150 및 IPv6과 같은 추가 AS-SIP 기능을 구성합니다.

다이제스트 사용자 구성

이 절차를 사용하여 최종 사용자를 다이제스트 인증을 사용하는 다이제스트 사용자로 구성합니다. 사용자와 연결된 디바이스는 사용자의 다이제스트 인증서를 통해 인증됩니다.

프로시저

단계 1 Cisco Unified CM 관리에서 사용자 관리 > 최종 사용자를 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 새 사용자를 생성하려면 새로 추가를 클릭합니다.
- 찾기를 클릭하고 기존 사용자를 선택합니다.

단계 3 다음 필수 필드가 완료되었는지 확인합니다.

- 사용자 ID
- 성

단계 4 다이제스트 인증서 필드에 암호를 입력합니다. 최종 사용자는 엔드포인트를 사용할 때 이 암호를 통해 자신을 인증해야 합니다.

단계 5 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 6 저장을 클릭합니다.

SIP 전화기 보안 포트 구성

다음 단계를 수행하여 SIP 전화기 보안 포트를 구성합니다. Cisco Unified Communications Manager는 이 포트를 사용하여 TLS를 통한 SIP 회선 등록을 위한 SIP 전화를 수신합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 시스템 > **Cisco Unified CM**을 선택합니다.
 - 단계 2 이 서버에 대한 **Cisco Unified Communications Manager TCP** 포트 설정 섹션에서 **SIP** 전화기 보안 포트 필드에 포트 번호를 지정하거나 기본값으로 설정된 필드를 그대로 둡니다. 기본값은 5061입니다.
 - 단계 3 저장을 클릭합니다.
 - 단계 4 구성 적용을 클릭합니다.
 - 단계 5 확인을 클릭합니다.
-

서비스 다시 시작

다음 단계에 따라 Cisco CallManager 및 Cisco CTL Provider 서비스를 다시 시작합니다.

프로시저

-
- 단계 1 Cisco Unified Serviceability 인터페이스에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.
 - 단계 2 서버 드롭다운 목록에서 Cisco Unified Communications Manager 서버를 선택합니다.
CM 서비스 영역에서 Cisco CallManager가 서비스 이름 옆에 표시됩니다.
 - 단계 3 Cisco CallManager 서비스에 해당하는 라디오 버튼을 클릭합니다.
 - 단계 4 재시작을 클릭합니다.
서비스가 다시 시작되고 서비스가 다시 시작되었습니다라는 메시지가 표시됩니다.
 - 단계 5 3단계와 4단계를 반복하여 Cisco CTL Provider 서비스를 다시 시작합니다.
-

AS-SIP용 SIP 프로파일 구성

이 절차를 사용하여 AS-SIP 엔드포인트와 SIP 트렁크를 위한 SIP 설정을 사용하여 SIP 프로파일을 구성합니다.

프로시저

-
- 단계 1 [Cisco Unified CM 관리]에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 SIP 프로파일을 만듭니다.
- 찾기를 클릭하고 기존 SIP 프로파일을 선택합니다.

단계 3 SIP 프로파일의 이름과 설명을 입력합니다.

단계 4 보증된 서비스 SIP 일지 확인란을 선택합니다.

참고 SIP 트렁크 및 타사 AS-SIP 전화기의 경우 이 확인란을 선택해야 합니다. AS-SIP을 지원하는 Cisco IP 전화기의 경우 필수 사항은 아닙니다.

단계 5 전화기에 사용된 매개 변수 J 섹션에서 예상하는 통화 유형에 대한 DSCP 우선 순위 값을 구성합니다.

참고 클러스터 수준 서비스 매개 변수를 통해 DSCP 값을 구성할 수도 있습니다. 그러나 SIP 프로파일 내의 DSCP 값은 SIP 프로파일을 사용하는 모든 디바이스에 대한 클러스터 수준 설정을 무시합니다.

단계 6 음성 및 영상 통화에 **Early Offer** 지원 드롭다운 목록에서 다음 옵션 중 하나를 선택하여 이 프로파일을 사용하는 SIP 트렁크에 대한 얼리 오퍼 지원을 구성합니다.

- 비활성화됨
- Best Effort(삽입된 MTP 없음)
- 필수(필요한 경우 MTP 삽입)

단계 7 SIP 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 8 저장을 클릭합니다.

AS-SIP에 대한 전화기 보안 프로파일 구성

이 절차를 사용하여 AS-SIP 엔드포인트에 대한 전화기 보안 프로파일을 구성합니다. 보안 프로파일을 사용하여 TLS 및 SRTP와 같은 보안 설정을 할당할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 보안 > 전화기 보안 프로파일에 체크 표시합니다.

단계 2 다음 단계 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 전화기 보안 프로파일을 만듭니다.
- 찾기를 클릭하여 기존 프로파일을 선택합니다.

단계 3 새 프로파일의 경우 전화기 보안 프로파일 드롭다운에서 옵션을 선택하고 전화기 모델 타사 AS-SIP 엔드포인트를 선택하고 다음을 클릭합니다.

- Cisco IP 전화기의 경우 전화기 모델을 선택하고 다음을 클릭합니다.

- 타사의 AS-SIP 엔드포인트인 경우 타사 **AS-SIP** 엔드포인트를 선택하고 다음을 클릭합니다.

단계 4 프로토콜의 경우 **SIP**을 선택하고 다음을 클릭합니다.

단계 5 프로토콜의 이름과 설명을 입력합니다.

단계 6 다음 설정 중 하나에 디바이스 보안 모드를 할당합니다.

- 인증됨 - Cisco Unified Communications Manager에서 TLS 설정을 사용하여 전화기에 대해 무결성 및 인증을 제공합니다.
- 암호화됨 - Cisco Unified Communications Manager에서 TLS 신호 처리를 사용하여 전화기에 대해 무결성 및 인증을 제공합니다. 또한 SRTP는 미디어 스트림을 암호화합니다.

단계 7 다이제스트 인증 활성화 확인란을 선택합니다.

단계 8 전화기 보안 프로파일 구성 창에서 남아 있는 필드를 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 9 저장을 클릭합니다.

AS-SIP 엔드포인트 구성

이 절차를 사용하여 AS-SIP 엔드포인트를 구성합니다. 대부분의 Cisco IP 전화기는 AS-SIP를 지원합니다. 또한 타사 엔드포인트에 대해 SIP로 구성할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 전화기 유형 드롭다운 목록에서 AS-SIP를 지원하는 Cisco IP 전화기를 선택합니다. 그렇지 않은 경우에는 타사 **AS-SIP** 엔드포인트를 선택합니다.

단계 4 다음을 클릭합니다.

단계 5 다음 필수 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

- 디바이스 신뢰 모드 — 타사의 AS-SIP 엔드포인트에만 해당됩니다. 신뢰 또는 신뢰 안 함을 선택합니다.
- MAC 주소
- 디바이스폴
- 전화기 버튼 템플릿
- 소유자 사용자 ID
- 디바이스 보안 프로파일 - AS-SIP로 설정된 전화기 보안 프로파일을 선택합니다.
- SIP 프로파일 - 사용자가 구성하는 AS-SIP 사용 가능 SIP 프로파일을 선택합니다.
- 다이제스트 사용자 - 다이제스트 사용자로 구성하는 사용자 ID를 선택합니다. 다이제스트 인증을 위해 사용자를 활성화해야 합니다.

- DTMF 수신 필요 - 엔드포인트에서 DTMF 숫자를 수락하도록 허용하려면 이 확인란을 선택합니다.
- 음성 및 영상 통화에 대한 Early Offer 지원 - Early Offer 지원을 활성화하려면 이 확인란을 선택합니다. 이 필드는 타사 전화기에 대해서만 표시됩니다.

단계 6 **MLPP** 및 기밀 액세스 수준 정보 섹션에서 필드를 구성합니다.

단계 7 저장을 클릭합니다.

단계 8 새 디렉터리 번호 추가:

- 왼쪽 탐색 모음에서 새 **DN** 추가를 클릭합니다. 디렉터리 번호 구성 창이 열립니다.
- 디렉터리 번호를 추가합니다.
- 디렉터리 번호 구성 창의 나머지 필드를 완료합니다.
- 저장을 클릭합니다.

단계 9 관련 링크 필드에서 디바이스 구성을 선택하고 이동을 클릭합니다.

단계 10 구성 적용을 클릭합니다.

디바이스를 최종 사용자에게 연결

이 절차를 사용하여 최종 사용자를 AS-SIP 엔드포인트에 연결합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 사용자 관리 > 최종 사용자

단계 2 찾기를 클릭하고 디바이스에 연결할 사용자를 선택합니다.

단계 3 디바이스 정보 영역에서 디바이스 연결을 클릭합니다.

[사용자 디바이스 연결] 창이 나타납니다.

단계 4 사용 가능한 디바이스 목록을 보려면 찾기를 클릭합니다.

단계 5 연결할 디바이스를 선택하고 선택 항목/변경 사항 저장을 클릭합니다.

단계 6 관련 링크에서 사용자로 돌아가기를 선택한 다음 이동을 클릭합니다.

최종 사용자 구성 창이 나타나고 선택한 연결 디바이스가 제어된 이바이스 창에 표시됩니다.

AS-SIP에 대한 SIP 트렁크 보안 프로파일 구성

이 절차를 사용하여 AS-SIP를 지원하는 SIP 트렁크에 대한 보안 프로파일을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 보안 > **SIP** 트렁크 보안 프로파일을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 보안 프로파일의 이름을 입력합니다.

단계 4 디바이스 보안 모드 드롭다운 목록에서 인증됨 또는 암호화됨을 선택합니다.

단계 5 수신 전송 유형 및 발신 전송 유형 필드가 자동으로 TLS로 변경됩니다.

단계 6 다이제스트 인증 활성화 확인란을 선택합니다.

단계 7 V.150을 구축하는 경우에는 SIP V.150 아웃바운드 SDP 제공 필터링 드롭다운 목록에 대한 값을 구성합니다.

단계 8 SIP 트렁크 보안 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 9 저장을 클릭합니다.

AS-SIP에 대한 SIP 트렁크 구성

이 절차를 사용하여 AS-SIP를 지원하는 SIP 트렁크를 설정합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 트렁크를 선택합니다.
- 새로 추가를 클릭하여 새 트렁크를 만듭니다.

단계 3 새 트렁크 유형의 경우 트렁크 유형 드롭다운 목록에서 SIP 트렁크를 선택합니다.

단계 4 트렁크 서비스 유형 드롭다운 목록에서 없음(기본값)을 선택하고 다음을 클릭합니다.

단계 5 트렁크에 대한 디바이스 이름을 입력합니다.

단계 6 디바이스 풀 드롭다운 목록에서 디바이스 풀을 선택합니다.

단계 7 대상 주소 필드에 트렁크를 연결하는 서버의 주소를 입력합니다.

단계 8 SIP 트렁크 보안 프로파일 드롭다운 목록에서 AS-SIP로 생성한 프로파일을 선택합니다.

단계 9 SIP 프로파일 드롭다운 목록에서 AS-SIP에 대해 설정된 SIP 프로파일을 선택합니다.

단계 10 트렁크 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 11 저장을 클릭합니다.

AS-SIP 기능 구성

이전 작업 흐름의 절차에서는 엔드포인트 및 트렁크에서 AS-SIP 지원을 구성하는 방법에 대해 설명합니다. 다음 표에서는 구축할 수 있는 AS-SIP 기능을 개략적으로 설명하고 각각에 대한 구성 참조를 제공합니다.

AS-SIP 기능	Configuration Description(컨피그레이션 설명)
Early Offer	<p>SIP Early Offer 기능을 사용하면 엔드포인트에서 INVITE 요청 중에 미디어를 협상하고 200OK 응답을 받을 수 있습니다. Early Offer에는 두 가지 모드가 있습니다.</p> <ul style="list-style-type: none"> • Best Effort Early Offer(삽입된 MTP 없음) • Mandatory Early Offer(필요한 경우 MTP 삽입) <p>다음 구성 창의 필드를 통해 Early Offer 지원을 구성합니다. 자세한 필드 설명은 온라인 도움말을 참조하십시오.</p> <p>SIP 프로파일 구성 창</p> <ul style="list-style-type: none"> • 음성 및 영상 통화에 대한 Early Offer 지원 - 이 필드를 구성하여 SIP 트렁크에서 Early Offer 지원을 활성화합니다. • Early Offer 및 Re-invite를 위한 SDP 세션 수준 대역폭 한정자 • 통화 중 INVITE에 전송-수신 SDP 전송 <p>전화기 구성 창(타사 AS-SIP 단말 디바이스 유형이 사용되는 경우에만)</p> <ul style="list-style-type: none"> • 음성 및 영상 통화에 대한 Early Offer 지원 - Early Offer 지원을 활성화하려면 이 확인란을 선택합니다.
회의 팩토리	<p>IMS 클라이언트에서 전화회의를 설정하는 데 사용하는 URI를 지정합니다.</p> <ol style="list-style-type: none"> 1. Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다. 2. 서버 드롭다운 목록에서 Cisco Unified Communications Manager 서버를 선택합니다. 3. 서비스 드롭다운 목록에서 Cisco CallManager를 선택합니다. 4. 클러스터 수준 매개 변수(기능 - 전화회의)에서 IMS 전화회의 팩토리 URI를 할당합니다. 5. 저장을 클릭합니다.

AS-SIP 기능	Configuration Description(컨피그레이션 설명)
DSCP 표시	<p>DSCP 설정을 사용하여 네트워크 내에서 QoS 및 대역폭을 관리할 수 있습니다. DSCP 설정은 통화별로 통화의 우선 순위가 지정된 트래픽 클래스 레이블을 할당하는 데 사용됩니다.</p> <p>서비스 매개 변수를 통해 클러스터 수준 DSCP 설정을 구성할 수 있으며 SIP 프로파일을 사용하여 해당 프로파일을 사용하는 사용자에게 대해 사용자 정의된 QoS 정책을 할당할 수 있습니다. 예를 들어, 임원(예: CEO) 또는 판매 팀의 통화의 더 높은 우선 순위를 할당하여 네트워크 대역폭 문제가 발생하는 경우 통화가 손실되지 않도록 할 수 있습니다.</p> <p>DSCP를 구성하려면 DSCP 설정 구성 작업 흐름, 839 페이지의 내용을 참조하십시오.</p>
IPv6	<p>기본값으로 Cisco Unified Communications Manager는 IPv4 주소 지정을 사용하도록 구성되어 있습니다. 하지만 시스템을 구성하여 IPv6 stack을 지원하여 IPv6 전용 엔드포인트로 SIP 네트워크를 구축할 수 있습니다.</p> <p>IPv6 구성에 대한 자세한 내용은 <i>Cisco Unified Communications Manager</i> 시스템 구성 설명서의 "듀얼 스택 IPv6 구성 작업 흐름" 장을 참조하십시오.</p>
MLPP(Multilevel Precedence and Preemption)	<p>MLPP(Multilevel Precedence and Preemption) 서비스를 사용하여 우선 통화를 연결할 수 있습니다. 이 기능으로 국가 비상 사태 또는 네트워크 성능 저하 상황과 같은 네트워크 스트레스 상황 동안 주요 담당자는 중요한 조직 및 개인에 대한 통신을 보장할 수 있습니다.</p> <p>MLPP를 구성하려면 MLPP(Multilevel Precedence and Preemption) 작업 흐름, 894 페이지의 내용을 참조하십시오.</p>
SRTP(Secure Real-Time Transport Protocol)	<p>보안 실시간 전송 프로토콜(SRTP)을 사용하여 통화의 미디어 스트림에 암호화 및 인증을 제공할 수 있습니다.</p> <p>전화기에서 사용하는 전화기 보안 프로파일 구성 내에서 전화기에 대해 SRTP를 구성할 수 있습니다. 디바이스 보안 모드 필드를 암호화됨으로 설정해야 합니다.</p>
TLS(전송 레이어 신호 처리)	<p>TLS(전송 레이어 보안)는 보안 포트 및 인증서 교환을 사용하여 두 시스템 또는 디바이스 간에 안전하고 신뢰할 수 있는 신호 처리 및 데이터 전송을 제공합니다.</p> <p>TLS를 구성하는 방법에 대한 자세한 내용은 <i>Cisco Unified Communications Manager</i>에 대한 보안 설명서의 "TLS 설정" 장을 참조하십시오.</p>

AS-SIP 기능	Configuration Description(컨피그레이션 설명)
V.150	<p>V.150 최소 필수 요구 사항 기능을 사용하면 IP 네트워크를 통한 모뎀에서 보안 전화를 걸 수 있습니다. 이 기능은 기존 PSTN(공중 전화 교환망)에서 작동하는 모뎀 및 전화 통신 디바이스의 대규모 설치 기반으로 전화 접속 모뎀을 사용합니다.</p> <p>V.150을 구성하는 자세한 내용은 <i>Cisco Unified Communications Manager</i>에 대한 보안 설명서의 "Cisco V. 150 최소 필수 요구 사항(MER)" 장을 참조하십시오.</p>



70 장

MLPP(Multilevel Precedence and Preemption) 구성

- MLPP(Multilevel Precedence and Preemption) 개요, 893 페이지
- MLPP(Multilevel Precedence and Preemption) 사전 요건, 893 페이지
- MLPP(Multilevel Precedence and Preemption) 작업 흐름, 894 페이지
- MLPP(Multilevel Precedence and Preemption) 상호 작용, 910 페이지
- MLPP(Multilevel Precedence and Preemption) 제한 사항, 911 페이지

MLPP(Multilevel Precedence and Preemption) 개요

MLPP(Multilevel Precedence and Preemption) 서비스를 사용하여 우선 통화를 연결할 수 있습니다. 올바르게 확인된 사용자는 우선 순위가 낮은 전화 통화를 우선 순위가 높은 통화로 선점할 수 있습니다. 인증된 사용자는 대상 기지국에 대한 통화 또는 완전히 가입된 TDM 트렁크를 통한 통화를 선점할 수 있습니다. 이 기능으로 국가 비상 사태 또는 네트워크 성능 저하 상황과 같은 네트워크 스트레스 상황 동안 주요 담당자는 중요한 조직 및 개인에 대한 통신을 보장할 수 있습니다.

MLPP(Multilevel Precedence and Preemption) 사전 요건

지원되는 SCCP 또는 SIP 전화기. 기능 지원 및 자세한 내용은 해당 전화기의 *Cisco IP* 전화기 관리 지침서 및 *Cisco IP* 전화기 사용 설명서를 참조 하십시오.

MLPP(Multilevel Precedence and Preemption) 작업 흐름

시작하기 전에

프로시저

	명령 또는 동작	목적
단계 1	<p>도메인 및 도메인 목록 구성, 895 페이지에 대해 다음 하위 작업을 수행합니다.</p> <ul style="list-style-type: none"> • MLPP(Multilevel Precedence and Preemption) 도메인 구성, 896 페이지 • 리소스 우선 순위 네임스페이스 네트워크 도메인 구성, 897 페이지 • 리소스 우선 순위 네임스페이스 네트워크 도메인 목록 구성, 897 페이지 	MLPP 가입자와 연결된 디바이스 및 리소스를 지정하기 위해 MLPP 도메인을 구성합니다.
단계 2	MLPP(Multilevel Precedence and Preemption)에 대한 일반 디바이스 구성, 898 페이지	일반 디바이스 구성에는 여러 사용자 및 해당 디바이스에 적용할 수 있는 MLPP 관련 정보가 포함됩니다. 각 디바이스가 일반 디바이스 구성과 연결되어 있는지 확인합니다. 이들 설정은 엔터프라이즈 매개 변수 설정을 무시합니다.
단계 3	MLPP(Multilevel Precedence and Preemption)에 대한 엔터프라이즈 매개 변수 구성, 898 페이지	엔터프라이즈 매개 변수를 설정하여 MLPP 표시 및 선점을 활성화합니다. 개별 디바이스 및 일반 디바이스 구성의 디바이스에 대한 MLPP 설정이 [기본값]인 경우 MLPP 관련 엔터프라이즈 매개 변수는 이러한 디바이스 및 일반 디바이스 구성에 적용됩니다.
단계 4	MLPP(Multilevel Precedence and Preemption)에 대한 파티션 구성, 900 페이지	연결성 특성이 비슷한 디렉터리 번호(DN) 및 라우트 패턴의 논리적 그룹을 만들기 위해 파티션을 구성합니다. 일반적으로 파티션에 배치되는 디바이스에는 DN 및 라우트 패턴이 포함됩니다. 이러한 엔티티는 사용자가 전화를 거는 DN과 연결됩니다. 간단하게 하기 위해 파티션 이름에는 일반적으로 특성이 반영됩니다.
단계 5	MLPP(Multilevel Precedence and Preemption)에 대한 발신 검색 공간 구성, 901 페이지	발신 검색 공간은 순서가 지정된 파티션 목록입니다. 발신 검색 공간은 통화를 완료하려고 시도할 때 IP 전화기, 스마트폰 및 게이

	명령 또는 동작	목적
		트웨이를 포함한 발신 디바이스에서 검색할 수 있는 파티션을 결정합니다.
단계 6	MLPP(Multilevel Precedence and Preemption)에 대한 경로 패턴 구성, 902 페이지	내부와 외부 모두의 통화를 라우팅하거나 차단하는 라우트 패턴을 구성합니다.
단계 7	MLPP(Multilevel Precedence and Preemption)에 대한 변환 패턴 구성, 903 페이지	통화를 배치한 후 라우팅하는 방법을 지정하는 변환 패턴을 구성합니다. 변환 패턴을 구성하면 시스템에서 필요에 따라 발신 번호 및 착신 번호를 조작할 수 있습니다. 시스템에서 패턴 일치가 발생했음을 식별하면 시스템에서 변환 패턴에 대해 구성된 발신 검색 공간을 사용하여 후속 일치를 수행합니다.
단계 8	게이트웨이에 대한 MLPP(Multilevel Precedence and Preemption) 구성, 904 페이지	Cisco Unified Communications Manager를 사용하면 비 IP 이동통신 디바이스와 통신할 수 있습니다.
단계 9	전화기에 대한 MLPP(Multilevel Precedence and Preemption) 구성, 905 페이지	
단계 10	디렉터리 번호를 구성하여 MLPP(Multilevel Precedence and Preemption) 통화 설정, 907 페이지	디바이스를 구성한 후에는 업데이트된 디바이스 구성 창에서 회선(디렉터리 번호)을 추가할 수 있습니다.
단계 11	다중 수준 우선 순위 및 선점에 대한 사용자 디바이스 프로파일 구성, 908 페이지	사용자 프로파일이 전화기에 할당되면, 해당 전화기는 사용자와 연결된 CSS를 포함하여, 할당된 사용자의 구성을 상속합니다. 그러나, 전화기 CSS는 사용자 프로파일을 무시할 수 있습니다. Cisco Unified Communications Manager는 패턴 일치가 발생하면 다이얼된 패턴과 연결된 우선 순위 수준을 통화에 할당합니다. 시스템은 해당 통화 요청을 할당된 우선 순위 수준을 가진 우선 순위 통화로 설정합니다.
단계 12	다중 수준 우선 순위 및 선점에 대한 디폴트 디바이스 프로파일 구성, 909 페이지	사용자 디바이스 프로파일이 없는 전화기 모델에 사용자가 로그인할 때마다 기본 디바이스 프로파일을 사용합니다. 기본 디바이스 프로파일은 특정 디바이스와 연결된 서비스 및 기능 세트로 구성됩니다.

도메인 및 도메인 목록 구성

MLPP 가입자와 연결된 디바이스 및 리소스를 지정하기 위해 MLPP 도메인을 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	MLPP(Multilevel Precedence and Preemption) 도메인 구성, 896 페이지	<p>디바이스 및 리소스를 MLPP 가입자와 연결합니다. 특정 도메인에 속하는 MLPP 가입자가 동일한 도메인에 속하는 다른 MLPP 가입자에게 우선 순위 통화를 걸 경우 MLPP 서비스는 착신 MLPP 가입자가 더 높은 우선 순위 통화를 위해 연결한 기존 통화를 선점할 수 있습니다. MLPP 서비스 가용성은 다른 도메인에 적용되지 않습니다.</p> <p>발신 사용자의 MLPP 도메인 가입에 따라 통화 및 연결의 도메인이 결정됩니다. 한 도메인에서 우선 순위가 높은 통화만 동일한 도메인의 통화가 사용 중인 연결을 선점할 수 있습니다.</p>
단계 2	리소스 우선 순위 네임스페이스 네트워크 도메인 구성, 897 페이지	SIP 트렁크를 사용하는 VoSIP(Voice over Secured IP) 네트워크에 대해 네임스페이스 도메인을 구성합니다. 시스템은 비상시 및 전화 회선, IP 대역폭, 게이트웨이 혼잡 시 SIP-지정 리소스가 가장 효과적으로 사용될 수 있도록 SIP-지정 리소스에 우선 순위를 지정합니다. 엔드포인트는 우선 순위 및 선점 정보를 수신합니다.
단계 3	리소스 우선 순위 네임스페이스 네트워크 도메인 목록 구성, 897 페이지	허용 가능한 네트워크 도메인의 목록을 구성합니다. 수신 통화는 이 목록과 비교되며, 허용되는 네트워크 도메인이 목록에 있을 경우 처리됩니다.

MLPP(Multilevel Precedence and Preemption) 도메인 구성

디바이스 및 리소스를 MLPP 가입자와 연결합니다. 특정 도메인에 속하는 MLPP 가입자가 동일한 도메인에 속하는 다른 MLPP 가입자에게 우선 순위 통화를 걸 경우 MLPP 서비스는 착신 MLPP 가입자가 더 높은 우선 순위 통화를 위해 연결한 기존 통화를 선점할 수 있습니다. MLPP 서비스 가용성은 다른 도메인에 적용되지 않습니다.

발신 사용자의 MLPP 도메인 가입에 따라 통화 및 연결의 도메인이 결정됩니다. 한 도메인에서 우선 순위가 높은 통화만 동일한 도메인의 통화가 사용 중인 연결을 선점할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > **MLPP** > 도메인 > **MLPP** 도메인을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 도메인 이름 필드에 새 MLPP 도메인에 할당할 이름을 입력합니다.

최대 50개의 영숫자와 공백, 마침표(.), 하이픈(-) 및 밑줄 문자(_)의 조합을 입력할 수 있습니다.

단계 4 도메인 ID 필드에 고유한 6자 16진수 MLPP 도메인 ID를 입력합니다.

도메인 ID는 000001 ~ FFFFFFF 범위에 속해야 합니다. 000000은 기본 MLPP 도메인 ID용으로 예약되어 있습니다.

단계 5 저장을 클릭합니다.

리소스 우선 순위 네임스페이스 네트워크 도메인 구성

SIP 트렁크를 사용하는 VoSIP(Voice over Secured IP) 네트워크에 대해 네임스페이스 도메인을 구성합니다. 시스템은 비상시 및 전화 회선, IP 대역폭, 게이트웨이 혼잡 시 SIP-지정 리소스가 가장 효과적으로 사용될 수 있도록 SIP-지정 리소스에 우선 순위를 지정합니다. 엔드포인트는 우선 순위 및 선점 정보를 수신합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > **MLPP** > 네임스페이스 > **Resource Priority Namespace Network Domain**을 선택합니다.

단계 2 정보 섹션에 리소스 우선 순위 네임스페이스 네트워크 도메인의 이름을 입력합니다. 최대 도메인 이름 수는 100개입니다.

단계 3 도메인 이름에 대한 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&) 또는 꺾쇠괄호(<>)는 사용할 수 없습니다.

단계 4 도메인 이름을 기본값으로 사용하려는 경우 이 항목을 기본 리소스 우선 순위 네임스페이스 네트워크 도메인으로 설정 확인란을 선택합니다.

단계 5 저장을 클릭합니다.

리소스 우선 순위 네임스페이스 네트워크 도메인 목록 구성

허용 가능한 네트워크 도메인의 목록을 구성합니다. 수신 통화는 이 목록과 비교되며, 허용되는 네트워크 도메인이 목록에 있을 경우 처리됩니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > **MLPP** > 네임스페이스 > 리소스 우선 순위 네임스페이스 목록을 선택합니다.

- 단계 2 리소스 우선 순위 네임스페이스 목록의 이름을 입력합니다. 최대 문자 수는 50입니다.
- 단계 3 목록에 대한 설명을 입력합니다. 설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.
- 단계 4 위쪽 및 아래쪽 화살표를 사용하여 Resource Priority Namespace Network Domain을 선택한 리소스 우선 순위 네임스페이스 필드로 이동합니다.
- 단계 5 저장을 클릭합니다.

MLPP(Multilevel Precedence and Preemption)에 대한 일반 디바이스 구성

일반 디바이스 구성에는 여러 사용자 및 해당 디바이스에 적용할 수 있는 MLPP 관련 정보가 포함됩니다. 각 디바이스가 일반 디바이스 구성과 연결되어 있는지 확인합니다. 이들 설정은 엔터프라이즈 매개 변수 설정을 무시합니다.

프로시저

- 단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 디바이스 설정 > 일반 디바이스 구성
- 단계 2 다음 작업 중 하나를 수행합니다.
- 기존 일반 디바이스 구성을 수정하려면 찾기를 클릭하고 결과 목록에서 일반 디바이스 구성을 선택합니다.
 - 새 일반 디바이스 구성을 추가하려면 새로 추가를 클릭합니다.
- 단계 3 일반 디바이스 구성 창에서 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 4 저장을 클릭합니다.

MLPP(Multilevel Precedence and Preemption)에 대한 엔터프라이즈 매개 변수 구성

엔터프라이즈 매개 변수를 설정하여 MLPP 표시 및 선점을 활성화합니다. 개별 디바이스 및 일반 디바이스 구성의 디바이스에 대한 MLPP 설정이 [기본값]인 경우 MLPP 관련 엔터프라이즈 매개 변수는 이러한 디바이스 및 일반 디바이스 구성에 적용됩니다.

프로시저

- 단계 1 시스템 > 엔터프라이즈 매개 변수를 선택합니다.
- 단계 2 엔터프라이즈 매개 변수 구성 창에서 MLPP 엔터프라이즈 매개 변수를 구성합니다. 매개 변수 및 해당 구성 옵션에 대한 자세한 내용은 관련 항목 섹션을 참조하십시오.

단계 3 저장을 클릭합니다.

MLPP(Multilevel Precedence and Preemption)에 대한 엔터프라이즈 매개 변수

표 85: MLPP(Multilevel Precedence and Preemption)에 대한 엔터프라이즈 매개 변수

매개 변수	설명
MLPP 도메인 식별자	이 매개 변수를 설정하여 도메인을 정의합니다. MLPP 서비스는 도메인에 적용되므로 Cisco Unified Communications Manager에서는 지정된 도메인의 MLPP 사용자가 건 전화에 속한 연결 및 리소스에만 우선 수준을 표시합니다. Cisco Unified Communications Manager에서는 같은 도메인의 MLPP 사용자가 건 전화 중 우선 순위가 낮은 전화만 선점할 수 있습니다. 기본값은 000000 입니다.
MLPP 표시 상태	이 매개 변수는 디바이스에서 MLPP 신호음과 특수 표시를 사용하여 MLPP 우선 순위 통화를 표시하는지 여부를 지정합니다. 기업 전체에서 MLPP 표시를 활성화하려면 이 매개 변수를 [MLPP 표시 켜짐]으로 설정합니다. 기본값은 MLPP 표시 해제 입니다.
MLPP 선점 설정	이 매개 변수는 디바이스에서 우선 순위가 높은 통화를 수용하기 위해 선점 및 선점 신호 처리(예: 선점 신호음)를 적용할지 여부를 결정합니다. 기업 전체에서 MLPP 선점을 활성화하려면 이 매개 변수를 [강제 선점]으로 설정합니다. 기본값은 선점 허용 안 됨입니다.
우선 대체 상대 시간 초과	우선 순위 통화에서 착신자가 대체 상대 전환에 가입하는 경우 이 타이머에는 착신자가 선점을 확인하지 않거나 우선 순위 통화를 받지 않는 경우 Cisco Unified Communications Manager에서 얼마 후에 통화를 대체 상대방으로 전환하는지를 나타내는 시간(초)이 표시됩니다. 기본값은 30초 입니다.
우선 순위 통화에 대해 표준 VM 처리 사용	이 매개 변수는 우선 순위 통화를 음성 메시징 시스템으로 착신 전환할지 여부를 결정합니다. 매개 변수를 [거짓]으로 설정하는 경우 우선 순위 통화가 음성 메시징 시스템으로 착신 전환되지 않습니다. 매개 변수를 [참]으로 설정하는 경우 우선 순위 통화가 음성 메시징 시스템으로 착신 전환됩니다. MLPP의 경우 이 매개 변수를 [False]로 설정하는 것이 좋습니다. 우선 순위 통화는 항상 음성 메시징 시스템이 아니라 사용자가 받아야 하기 때문입니다. 기본값은 False 입니다.

MLPP(Multilevel Precedence and Preemption)에 대한 파티션 구성

연결성 특성이 비슷한 디렉터리 번호(DN) 및 라우트 패턴의 논리적 그룹을 만들기 위해 파티션을 구성합니다. 일반적으로 파티션에 배치되는 디바이스에는 DN 및 라우트 패턴이 포함됩니다. 이러한 엔티티는 사용자가 전화를 거는 DN과 연결됩니다. 간단하게 하기 위해 파티션 이름에는 일반적으로 특성이 반영됩니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 통화 라우팅 > 제어 클래스 > 파티션.

단계 2 새로 추가를 클릭하여 새 파티션을 생성합니다.

단계 3 파티션 이름, 설명 필드에 경로 플랜에 고유한 파티션 이름을 입력합니다.

파티션 이름에는 영숫자 문자는 물론 공백, 하이픈(-) 및 밑줄(_)을 사용할 수 있습니다. 파티션 이름에 대한 지침은 온라인 도움말을 참조하십시오.

단계 4 파티션 이름 뒤에 쉼표(,)를 입력하고 동일한 줄에 파티션 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\), 꺾쇠괄호(<>) 또는 대괄호([])는 사용할 수 없습니다.

설명을 입력하지 않으면 Cisco Unified Communications Manager에서 자동으로 이 필드에 파티션 이름을 입력합니다.

단계 5 여러 파티션을 생성하려면 각 파티션 항목마다 한 행을 사용합니다.

단계 6 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.

시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성 상태로 유지됩니다.

단계 7 구성할 다음 라디오 버튼 중 하나를 선택하고 시간대를 구성합니다.

- 시작 디바이스—이 라디오 버튼을 선택하면 시스템은 발신 디바이스의 표준 시간대를 시간 일정과 비교하여 파티션을 수신 통화를 받는 데 사용할 수 있는지 여부를 확인합니다.
- 특정 표준 시간대—이 라디오 버튼을 선택한 후에 드롭다운 목록에서 표준 시간대를 선택합니다. 시스템은 선택한 표준 시간대를 시간 일정과 비교하여 수신 통화를 받는 데 파티션을 사용할 수 있는지 여부를 확인합니다.

단계 8 저장을 클릭합니다.

파티션 이름 지정 지침

발신 검색 공간의 파티션 목록에서 최대 문자 수는 1024자로 제한됩니다. 즉, CSS의 최대 파티션 수는 파티션 이름의 길이에 따라 달라집니다. 다음 표를 사용하여 파티션 이름이 고정 길이인 경우 발신 검색 공간에 추가할 수 있는 최대 파티션 수를 결정합니다.

표 86: 파티션 이름 지침

파티션 이름 길이	최대 파티션 수
2자	340
3자	256
4자	204
5자	172
...	...
10자	92
15자	64

MLPP(Multilevel Precedence and Preemption)에 대한 발신 검색 공간 구성

발신 검색 공간은 순서가 지정된 파티션 목록입니다. 발신 검색 공간은 통화를 완료하려고 시도할 때 IP 전화기, 소프트폰 및 게이트웨이를 포함한 발신 디바이스에서 검색할 수 있는 파티션을 결정합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 제어 클래스 > 발신 검색 공간.

단계 2 새로 추가를 클릭합니다.

단계 3 이름 필드에 이름을 입력합니다.

각 발신 검색 공간 이름은 시스템에 고유해야 합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.

단계 4 설명 필드에 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.

단계 5 사용 가능한 파티션 드롭다운 목록에서 다음 단계 중 하나를 수행합니다.

- 단일 파티션의 경우 해당 파티션을 선택합니다.
- 여러 파티션의 경우 컨트롤(CTRL) 키를 누른 상태에서 해당 파티션을 선택합니다.

단계 6 상자 사이에서 아래쪽 화살표를 선택하여 선택한 파티션 필드로 파티션을 이동합니다.

단계 7 (선택 사항) 선택한 파티션 상자 오른쪽의 화살표 키를 사용하여 선택한 파티션의 우선 순위를 변경합니다.

단계 8 저장을 클릭합니다.

MLPP(Multilevel Precedence and Preemption)에 대한 경로 패턴 구성

내부와 외부 모두의 통화를 라우팅하거나 차단하는 라우트 패턴을 구성합니다.

프로시저

단계 1 Cisco 통합 CM 관리에서 콜 라우팅 > 라우트/헌트 > 라우트 패턴을 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 라우트 패턴에 대한 설정을 수정하려면 검색 기준을 입력하고 찾기를 클릭하여 결과 목록에서 기존 라우트 패턴을 선택합니다.
- 새 라우트 패턴을 추가하려면 새로 추가를 클릭합니다.

단계 3 라우트 패턴 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 관련 항목 섹션을 참조하십시오.

단계 4 저장을 클릭합니다.

MLPP(Multilevel Precedence and Preemption)에 대한 경로 패턴 구성 필드

표 87: MLPP(Multilevel Precedence and Preemption)에 대한 경로 패턴 구성 필드

필드	설명
경로 패턴	공백 없이 숫자와 와일드 카드를 포함하여 라우트 패턴을 입력합니다. 예를 들어 NANP의 일반적인 로컬 액세스를 위해서는 9.@를 입력하고, 일반적인 개인 네트워크 번호 지정 플랜을 위해서는 8XXX를 입력합니다. 올바른 문자에는 대문자 A, B, C, D와 국제 이스케이프 문자 +를 나타내는 \+가 포함됩니다.

필드	설명
MLPP 우선 순위	<p>드롭다운 목록에서 이 경로 패턴에 대한 MLPP 우선 순위 설정을 선택합니다.</p> <ul style="list-style-type: none"> • 이그제큐티브 오버라이드 - MLPP 통화에 대한 가장 높은 우선 순위 설정입니다. • 플래시 오버라이드 - MLPP 통화에 대한 두 번째로 높은 우선 순위 설정입니다. • 플래시 - MLPP 통화에 대한 세 번째로 높은 우선 순위 설정입니다. • 즉시 - MLPP 통화에 대한 네 번째로 높은 우선 순위 설정입니다. • 우선 순위 - MLPP 통화에 대한 다섯 번째로 높은 우선 순위 설정입니다. • 루틴 - MLPP 통화에 대한 가장 낮은 우선 순위 설정입니다. • 기본값 - 수신 통화 우선 순위 수준을 무시하지 않으며 그 대신 변경되지 않은 상태로 통과시킵니다.
전화 차단 비율 적용	<p>DCC(Destination Code Control) 기능을 활성화하려면 이 확인란을 선택합니다. DCC를 활성화하면 대상으로 걸려온 통화 중 플래시 통화와 우선 순위 높은 통화 외의 모든 통화는 필터링되고 대상에 대해 설정된 전화 차단 비율 할당을 기준으로 허용되거나 거부됩니다. 플래시 통화와 우선 순위가 높은 통화는 항상 허용됩니다. DCC는 기본적으로 비활성화되어 있습니다.</p> <p>전화 차단 비율 적용 필드는 MLPP 수준이 즉시, 우선, 루틴 또는 기본값인 경우에만 활성화됩니다.</p>
전화 차단 비율(%)	<p>이 대상에 대해 차단할 전화의 비율을 숫자로 입력합니다. 이 값은 이 대상으로 걸린 통화 중 라우트 패턴에 의해 차단되는 우선 순위가 낮은 통화의 비율을 지정합니다. 이 비율은 우선 순위가 낮은 통화만 제한합니다. 이 대상으로 걸려온 플래시 통화와 우선 순위가 높은 통화는 항상 허용됩니다.</p> <p>전화 차단 비율(%) 필드는 전화 차단 비율 적용 확인란을 선택하는 경우에만 활성화됩니다.</p>
리소스 우선 순위 네임스페이스 네트워크 도메인	<p>드롭다운 목록에서 리소스 우선 순위 네임스페이스 네트워크 도메인을 선택합니다. 리소스 우선 순위 네임스페이스 네트워크 도메인을 구성하려면 시스템 > MLPP > 네임스페이스 > 리소스 우선 순위 네임스페이스 네트워크 도메인을 선택합니다.</p>

MLPP(Multilevel Precedence and Preemption)에 대한 변환 패턴 구성

통화를 배치한 후 라우팅하는 방법을 지정하는 변환 패턴을 구성합니다. 변환 패턴을 구성하면 시스템에서 필요에 따라 발신 번호 및 착신 번호를 조작할 수 있습니다. 시스템에서 패턴 일치 발생했음을 식별하면 시스템에서 변환 패턴에 대해 구성된 발신 검색 공간을 사용하여 후속 일치를 수행합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 통화 라우팅 > 변환 패턴을 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 변환 패턴의 설정을 수정하려면 검색 기준을 입력하고 찾기를 클릭한 다음 결과 목록에서 기존 변환 패턴을 선택합니다.
- 새 변환 패턴을 추가하려면 새로 추가를 클릭합니다.

단계 3 MLPP 우선 순위 드롭다운 목록에서 이 변환 패턴의 다음 설정 중 하나를 선택합니다.

- 이그제큐티브 오버라이드 - MLPP 통화에 대한 가장 높은 우선 순위 설정입니다.
- 플래시 오버라이드 - MLPP 통화에 대한 두 번째로 높은 우선 순위 설정입니다.
- 플래시 - MLPP 통화에 대한 세 번째로 높은 우선 순위 설정입니다.
- 즉시 - MLPP 통화에 대한 네 번째로 높은 우선 순위 설정입니다.
- 우선 순위 - MLPP 통화에 대한 다섯 번째로 높은 우선 순위 설정입니다.
- 루틴 - MLPP 통화에 대한 가장 낮은 우선 순위 설정입니다.
- 기본값 - 수신 통화 우선 순위 수준을 무시하지 않으며 그 대신 변경되지 않은 상태로 통과시킵니다.

단계 4 리소스 우선 순위 네임스페이스 네트워크 도메인 드롭다운 목록에서 구성된 리소스 우선 순위 네임스페이스 네트워크 도메인을 선택합니다.

단계 5 발신 검색 공간 드롭다운 목록에서 구성된 발신 검색 공간을 선택합니다.

단계 6 저장을 클릭합니다.

게이트웨이에 대한 MLPP(Multilevel Precedence and Preemption) 구성

Cisco Unified Communications Manager를 사용하면 비 IP 이동통신 디바이스와 통신할 수 있습니다.

시작하기 전에

- 다음 게이트웨이 중 하나를 구성합니다.
 - Cisco Catalyst 6000 24 port FXS 게이트웨이
 - Cisco Catalyst 6000 E1 VoIP 게이트웨이
 - Cisco Catalyst 6000 T1 VoIP 게이트웨이
 - Cisco DE-30+ 게이트웨이
 - Cisco DT-24+ 게이트웨이
 - H.323 게이트웨이

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 게이트웨이에 대한 설정을 수정하려면 검색 기준을 입력하고 찾기를 클릭하여 결과 목록에서 게이트웨이를 선택합니다.
- 새 게이트웨이를 추가하려면:
 1. 새로 추가를 클릭합니다.
 2. 게이트웨이 유형 드롭다운 목록에서 지원되는 게이트웨이 모델 중 하나를 선택합니다.
 3. 다음을 클릭합니다.

단계 3 게이트웨이 구성 창에서 MLPP 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 관련 항목 섹션을 참조하십시오.

단계 4 저장을 클릭합니다.

전화기에 대한 MLPP(Multilevel Precedence and Preemption) 구성



주의 [MLPP 선점]이 [강제]로 설정되어 있는 상태에서 [MLPP 표시]를 [끄기] 또는 [기본값](기본값이 [끄기]인 경우)으로 설정하는 설정 조합으로 디바이스를 구성하지 마십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 2 검색 조건을 입력합니다.

단계 3 찾기를 클릭하고 결과 목록에서 전화기를 선택합니다.

단계 4 전화기 구성 창에서 MLPP 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 관련 항목 섹션을 참조하십시오.

전화기에 대한 MLPP(Multilevel Precedence and Preemption) 설정

표 88: 전화기에 대한 MLPP(Multilevel Precedence and Preemption) 설정

전화기에 대한 MLPP 설정 필드	설명
일반 디바이스 구성	구성한 일반 디바이스 구성을 선택합니다. 일반 디바이스 구성에는 특정 사용자와 연결된 특성(서비스 또는 기능)이 포함됩니다.
발신 검색 공간	드롭다운 목록에서 구성된 CSS(발신 검색 공간)를 선택합니다. 발신 검색 공간은 전화 건 번호를 전송하는 방법을 결정하기 위해 검색하는 파티션 모음으로 구성됩니다. 디바이스에 대한 발신 검색 공간과 디렉터리 번호에 대한 발신 검색 공간은 함께 사용됩니다. 디렉터리 번호 CSS는 디바이스 CSS보다 우선합니다.
MLPP 도메인	이 디바이스와 연결된 MLPP 도메인의 드롭다운 목록에서 MLPP 도메인을 선택합니다. 없음 값을 유지하는 경우 이 디바이스는 일반 디바이스 구성에 설정된 값에서 MLPP 도메인을 상속받습니다. 일반 디바이스 구성에 MLPP 도메인 설정이 없는 경우 이 디바이스는 MLPP 도메인 식별자(MLPP Domain Identifier) 엔터프라이즈 파라미터에 설정된 값에서 MLPP 도메인을 상속받습니다.
MLPP 표시	<p>사용 가능한 경우, 이 설정은 통화 선점이 진행 중일 수 있는 디바이스에서 MLPP 우선 순위 통화를 거는 경우 해당 기능을 사용할지 여부를 지정합니다.</p> <p>드롭다운 목록의 다음 옵션에서 이 디바이스에 할당할 설정을 선택합니다.</p> <ul style="list-style-type: none"> • 기본값 - 이 디바이스는 일반 디바이스 구성에서 MLPP 표시 설정을 상속받습니다. • 끄기 - 이 디바이스에서 MLPP 우선 순위 통화 표시를 취급하거나 처리하지 않습니다. • 켜기 - 이 디바이스에서 MLPP 우선 순위 통화 표시를 취급 및 처리합니다. <p>참고 [MLPP 선점]이 [강제]로 설정되어 있는 상태에서 [MLPP 표시]를 [끄기] 또는 [기본값](기본값이 [끄기]인 경우)으로 설정하는 설정 조합으로 디바이스를 구성하지 마십시오.</p> <p>MLPP 표시를 켜면(엔터프라이즈 파라미터 또는 디바이스 수준에서) 디바이스에서 MLPP 표시가 꺼지지(무시되지) 않는 한, 디바이스 회선에 대한 일반 벨소리 설정 동작이 비활성화됩니다.</p>

전화기에 대한 MLPP 설정 필드	설명
MLPP 선점	<p>이 설정은 일부 디바이스에서만 사용할 수 있습니다. 사용 가능한 경우, 이 설정은 통화 선점이 진행 중일 수 있는 디바이스에서 MLPP 우선 순위 통화가 걸리는 경우 해당 기능을 사용할지 여부를 지정합니다.</p> <p>드롭다운 목록의 다음 옵션에서 이 디바이스에 할당할 설정을 선택합니다.</p> <ul style="list-style-type: none"> • 기본값 이 디바이스는 일반 디바이스 구성에서 MLPP 선점 설정을 상속받습니다. • 사용 안 함 - 우선 순위가 더 높은 통화를 완료하는 데 필요한 경우 이 디바이스는 우선 순위가 낮은 통화의 선점이 발생하는 것을 허용하지 않습니다. • 강제 - 우선 순위가 더 높은 통화를 완료하는 데 필요한 경우 이 디바이스는 우선 순위가 낮은 통화가 선점하도록 허용합니다.

디렉터리 번호를 구성하여 **MLPP(Multilevel Precedence and Preemption)** 통화 설정

디바이스를 구성한 후에는 업데이트된 디바이스 구성 창에서 회선(디렉터리 번호)을 추가할 수 있습니다.

프로시저

- 단계 1** Cisco Unified CM 관리의 디바이스 구성 창에서 해당 회선에 대한 새 **DN** 추가를 클릭합니다.
- 단계 2** 대상 필드에 이 디렉터리 번호에서 우선 순위 통화를 수신하였는데 이 번호도, 이 번호의 착신 전환 대상도 우선 순위 통화를 받지 않을 때 **MLPP** 우선 순위 통화를 전환해야 하는 번호를 입력합니다.
값에는 숫자, 파운드 기호(#) 및 별표(*)가 포함될 수 있습니다.
- 단계 3** **MLPP** 발신 검색 공간 드롭다운 목록에서 **MLPP** 대체 상대 대상 번호와 연결할 발신 검색 공간을 선택합니다.
- 단계 4** **MLPP** 응답 없음 벨소리 지속 기간(초)에 이 디렉터리 번호와 해당 통화 착신 전환 대상에서 우선 순위 통화로 응답하지 않을 경우 **MLPP** 우선 순위 통화가 이 디렉터리 번호 대체 상대로 전송되기까지 대기하는 시간을 초 단위(4~60)로 입력합니다.
엔터프라이즈 매개 변수인 우선 대체 상대 시간 제한에 설정된 값을 사용하려면 이 설정을 비워 둡니다.

단계 5 저장을 클릭합니다.

다중 수준 우선 순위 및 선점에 대한 사용자 디바이스 프로파일 구성

사용자 프로파일이 전화기에 할당되면, 해당 전화기는 사용자와 연결된 CSS를 포함하여, 할당된 사용자의 구성을 상속합니다. 그러나, 전화기 CSS는 사용자 프로파일을 무시할 수 있습니다. Cisco Unified Communications Manager는 패턴 일치가 발생하면 다이얼된 패턴과 연결된 우선 순위 수준을 통화에 할당합니다. 시스템은 해당 통화 요청을 할당된 우선 순위 수준을 가진 우선 순위 통화로 설정합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 디바이스 프로파일을 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 디바이스 프로파일에 대한 설정을 수정하려면 검색 기준을 입력하고 찾기를 클릭하여 결과 목록에서 기존 디바이스 프로파일을 선택합니다.
- 새 디바이스 프로파일을 추가하려면:
 - 새로 추가를 클릭합니다.
 - 디바이스 프로파일 유형 드롭다운 목록에서 프로파일 유형을 선택합니다.
 - 다음을 클릭합니다.
 - 디바이스 프로토콜 드롭다운 목록에서 SIP 또는 SCCP를 선택합니다.

단계 3 다음을 클릭합니다.

단계 4 MLPP 도메인 드롭다운 목록에서 구성된 MLPP 도메인을 선택합니다.

단계 5 MLPP 표시 드롭다운 목록에서 다음 설정 중 하나를 선택하여 우선 순위 신호음을 재생할 수 있는 디바이스에서 MLPP 우선 순위 전화를 걸 때 해당 기능을 사용할지 여부를 지정합니다.

- 기본값 - 이 디바이스는 디바이스폴에서 MLPP 표시 설정을 상속합니다.
- 끄기 - 이 디바이스에서 MLPP 우선 순위 통화 표시를 취급하거나 처리하지 않습니다.
- 켜기 - 이 디바이스에서 MLPP 우선 순위 통화 표시를 취급 및 처리합니다.

단계 6 MLPP 선점 드롭다운 목록에서 다음 설정 중 하나를 선택하여 진행 중인 통화를 선점할 수 있는 디바이스에서 MLPP 우선 순위 전화를 걸 때 해당 기능을 사용할지 여부를 지정합니다.

- 기본값 - 이 장치는 디바이스 폴에서 MLPP 선점 설정을 상속합니다.
- 사용 안 함 - 우선 순위가 더 높은 통화를 완료하는 데 필요한 경우 이 디바이스는 우선 순위가 낮은 통화의 선점이 발생하는 것을 허용하지 않습니다.

- 강제 - 우선 순위가 더 높은 통화를 완료하는 데 필요한 경우 이 디바이스는 우선 순위가 낮은 통화가 선점하도록 허용합니다.

단계 7 저장을 클릭합니다.

다중 수준 우선 순위 및 선점에 대한 디폴트 디바이스 프로파일 구성

사용자 디바이스 프로파일이 없는 전화기 모델에 사용자가 로그인할 때마다 기본 디바이스 프로파일을 사용합니다. 기본 디바이스 프로파일은 특정 디바이스와 연결된 서비스 및 기능 세트로 구성됩니다.



주의 [MLPP 선점]이 [강제]로 설정되어 있는 상태에서 [MLPP 표시]를 [끄기] 또는 [기본값](기본값이 [끄기]인 경우)으로 설정하는 설정 조합으로 기본 디바이스 프로파일을 구성하지 마십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스설정 > 디폴트 디바이스 프로파일을 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 기존 디폴트 디바이스 프로파일에 대한 설정을 수정하려면 디바이스 프로파일 기본값 섹션에서 기존 디폴트 디바이스 프로파일을 선택합니다.
- 새 디바이스 프로파일을 추가하려면 드롭다운 목록에서 디바이스 프로파일 유형을 선택하고 다음을 클릭하고 디바이스 프로파일을 선택하고 다음을 클릭합니다.

단계 3 MLPP 도메인 드롭다운 목록에서 디바이스에 연결하도록 구성된 MLPP 도메인을 선택합니다.

단계 4 MLPP 표시 드롭다운 목록에서 다음 설정 중 하나를 선택하여 우선 순위 신호음을 재생할 수 있는 디바이스에서 MLPP 우선 순위 전화를 걸 때 해당 기능을 사용할지 여부를 지정합니다.

- 기본값 - 이 디바이스는 디바이스폴에서 MLPP 표시 설정을 상속합니다.
- 끄기 - 이 디바이스에서 MLPP 우선 순위 통화 표시를 취급하거나 처리하지 않습니다.
- 켜기 - 이 디바이스에서 MLPP 우선 순위 통화 표시를 취급 및 처리합니다.

단계 5 MLPP 선점 드롭다운 목록에서 다음 설정 중 하나를 선택하여 진행 중인 통화를 선점할 수 있는 디바이스에서 MLPP 우선 순위 전화를 걸 때 해당 기능을 사용할지 여부를 지정합니다.

- 기본값 - 이 장치는 디바이스 폴에서 MLPP 선점 설정을 상속합니다.
- 사용 안 함 - 우선 순위가 더 높은 통화를 완료하는 데 필요한 경우 이 디바이스는 우선 순위가 낮은 통화의 선점이 발생하는 것을 허용하지 않습니다.
- 강제 - 우선 순위가 더 높은 통화를 완료하는 데 필요한 경우 이 디바이스는 우선 순위가 낮은 통화가 선점하도록 허용합니다.

단계 6 저장을 클릭합니다.

MLPP(Multilevel Precedence and Preemption) 상호 작용

표 89: MLPP(Multilevel Precedence and Preemption) 상호 작용

기능	상호 작용
729 부록 A	729 Annex A가 지원됩니다.
Cisco Extension Mobility	사용자가 내선 이동을 사용하여 디바이스에 로그인하는 경우 MLPP 서비스 도메인은 사용자 디바이스 프로파일과 연결된 상태로 유지됩니다. [MLPP 표시] 및 [선점] 설정은 Extension Mobility로도 전파됩니다. 디바이스 또는 디바이스 프로파일에서 MLPP를 지원하지 않는 경우 이 설정은 전파되지 않습니다.
Cisco Unified Communications Manager Assistant	MLPP는 아래와 같이 다음 Cisco Unified Communications Manager 보조자 기능과 상호 작용합니다. <ul style="list-style-type: none"> • Cisco Unified Communications Manager Assistant에서 MLPP 우선 순위 통화를 처리하는 경우 Cisco Unified Communications Manager Assistant는 통화 우선 순위를 유지합니다. • Cisco Unified Communications Manager Assistant는 다른 모든 통화를 필터링하는 것과 같은 방식으로 MLPP 우선 순위 통화를 필터링합니다. 통화 우선 순위는 통화 필터링 여부에 영향을 미치지 않습니다. • Cisco Unified Communications Manager Assistant에서는 통화 우선 순위를 등록하지 않으므로 Attendant Console에 통화 우선 순위를 추가로 표시하지 않습니다.
지정전환	즉시 전환에서는 통화 유형(예: 우선 순위 통화)에 관계없이 통화를 음성 메시징 사서함으로 전환합니다. 대체 상대 전환(통화 우선 순위)이 활성화된 경우 CFNA(부재중 착신 전환)는 비활성화됩니다.
RSVP(Resource Reservation Protocol)	RSVP는 기본적으로 MLPP를 지원합니다. Cisco Unified Communications Manager 시스템 설명서에는 RSVP가 활성화된 경우 MLPP가 작동하는 방식이 설명되어 있습니다.
보조 서비스	MLPP는 각 서비스와의 상호 작용에 대해 설명하는 서브 섹션에 명시된 것처럼 여러 회선 표시, 호전환, 착신 전환, 3자 통화, 통화 당겨받기 및 헛트 파일럿과 상호 작용합니다.

MLPP(Multilevel Precedence and Preemption) 제한 사항

표 90: MLPP(Multilevel Precedence and Preemption) 제한 사항

제한 사항	설명
대역폭	Cisco Unified Communications Manager는 높은 우선 순위 통화를 위해 비디오 대역폭을 조정할 때 더 낮은 우선 순위 통화를 선점합니다. 대역폭이 선점하기에 충분하지 않을 경우, Cisco Unified Communications Manager는 엔드포인트에 이전에 예약한 더 낮은 비디오 대역폭을 사용하도록 지시합니다. Cisco Unified Communications Manager가 영상 통화를 선점하면, 선점된 상대방은 선점 신호음을 받게 되며, 통화가 종료됩니다.
통화 세부 정보 레코드	DRSN의 경우, CDR은 값 0, 1, 2, 3, 4를 갖는 우선 순위 수준을 나타냅니다. 여기서 0은 이그제큐티브 오버라이드를, 4는 DSN에서 사용되는 것과 같이 루틴을 나타냅니다. 따라서, CDR은 DRSN 형식을 사용하지 않습니다.
공동 네트워크 시설 선점	공동 네트워크 시설 선점 지원은 대상 VoIP(Voice over IP) 게이트웨이에 있는 T1-CAS 및 T1-PRI(복미) 인터페이스에 대해서만 존재합니다. 해당 게이트웨이는 Cisco Unified Communications Manager가 MGCP 프로토콜을 사용하여 제어하고, MLPP 선점 활성화됨으로 구성되어야 합니다.
인터클러스터 트렁크	클러스터 간 트렁크 MLPP는 다이얼된 숫자를 통해 우선 순위 정보를 전달합니다. 도메인 정보는 보존되지 않으며, 수신 통화용 트렁크별로 구성해야 합니다.

제한 사항	설명
회선 그룹	<p>MLPP 지원 디바이스는 회선 그룹에서 지원되지 않습니다. 다음 지침을 권장합니다.</p> <ul style="list-style-type: none"> • MLPP 지원 디바이스를 회선 그룹으로 구성해서는 안 됩니다. 그러나, 경로 그룹은 지원됩니다. 트렁크 선택 방법과 헌팅 방법이 모두 지원됩니다. • MLPP 지원 디바이스가 회선 그룹 또는 경로 그룹으로 구성될 경우, 선점 발생 시, 라우트 목록이 해당 디바이스를 추적하지 않으면, 선점된 통화가 경로/헌트 목록에 있는 다른 디바이스로 재전송될 수 있으며, 어떤 디바이스도 통화를 받을 수 없는 경우에만 선점 표시가 반환될 수 있습니다. • 라우트 목록은 우선 순위 통화에 대해 트렁크 선택 및 헌팅의 두 가지 알고리즘 중 하나를 지원하도록 구성할 수 있습니다. 방법 1에서는 선제적 검색을 직접 수행합니다. 방법 2에서는 먼저 우호적 검색을 수행합니다. 이 검색이 성공적이지 않을 경우, 선제적 검색을 수행합니다. 방법 2는 라우트 목록에서 디바이스까지 2회 반복을 필요로 합니다. 라우트 목록이 방법 2에 대해 구성된 경우, 회선 그룹이 관련된 특정 상황에서는 라우트 목록이 우선 순위 통화에 대해 디바이스까지 2회 반복하는 것처럼 보일 수 있습니다.
통화 예측	Cisco Unified Communications Manager는 LFB(통화 예측) 옵션을 지원하지 않습니다.
MLPP 알림	MLPP 표시가 활성화된 디바이스만 연결음 및 벨소리와 같은 MLPP 관련 알림을 생성합니다. MLPP 표시가 활성화되지 않은 디바이스에서 우선 순위 통화가 종료될 경우, 우선 순위 벨소리가 적용되지 않습니다. MLPP 표시가 활성화되지 않은 디바이스에서 우선 순위 통화를 걸 경우, 우선 순위 통화 연결음이 적용되지 않습니다. MLPP 표시가 활성화되지 않은 디바이스가 선점된 통화에 관련될 경우(즉, 통화의 상대방이 선점을 시작한 경우), 해당 디바이스에는 선점 연결음이 적용되지 않습니다.
전화기 및 트렁크	전화기의 경우, MLPP 표시가 비활성화된(즉, MLPP 표시가 끄기로 설정된) 디바이스는 선점될 수 없습니다. 트렁크의 경우, MLPP 표시와 선점 기능은 독립적입니다.
벨소리 설정 동작	MLPP 표시를 켜면(엔터프라이즈 매개변수, 일반 디바이스 구성 또는 디바이스 수준에서) 디바이스에 대해 MLPP 표시가 꺼지지(오버라이드되지) 않는 한, 디바이스의 회선에 대한 정상 벨소리 설정 동작이 비활성화됩니다.

제한 사항	설명
SCCP	IOS 게이트웨이는 Cisco Unified Communications Manager에 대한 SCCP 인터페이스를 지원합니다. Cisco Unified Communications Manager에 지원되는 전화기 모델로 표시되는 BRI 및 아날로그 전화기를 지원합니다. SCCP 전화기는 MLPP 기능을 지원하지하므로 특정 SIP 로드를 사용하는 전화기도 있습니다. Cisco IP 전화기 지원 정보는 관련 전화기 관리 및 사용자 설명서를 참조하십시오.
보조 서비스	<p>보조 서비스에 대한 MLPP 지원에는 다음 제한 사항이 있습니다.</p> <ul style="list-style-type: none"> • MLPP는 기본 통화 당겨받기 기능과 그룹 통화 당겨받기 기능만 지원하고 다른 그룹 당겨받기는 지원하지 않습니다. • 착신 MLPP 통화에 대한 CFA(모든 통화 착신 전환) 지원 기능은 착신자의 MLPP 대체 상대(MAP) 대상이 구성된 경우 항상 해당 대상으로 통화를 착신 전환합니다. 구성이 잘못된 경우(즉, MAP 대상이 지정되지 않은 경우), 통화가 거부되고, 발신자는 다시 걸기 신호음을 받게 됩니다. • 착신 MLPP 통화에 대한 CFNA(응답 없음 착신 전환) 지원 기능은 CFNA 대상으로 한 번 통화를 착신 전환합니다. 첫 번째 호출 후, 통화의 응답이 계속 이루어지지 않을 경우, 원래 착신자의 MAP 대상이 구성되었으면 통화가 해당 대상으로 전송됩니다. 구성이 잘못된 경우(즉, MAP 대상이 지정되지 않은 경우), 통화가 거부되고, 발신자는 다시 걸기 신호음을 받게 됩니다. • 착신 MLPP 통화에 대한 CFB(통화 중 착신 전환) 지원 기능은 착신 전환 호출에 대해 구성된 최대 숫자까지 통화를 착신 전환합니다. 최대 호출 수에 도달할 경우, 원래 착신자의 MAP 대상이 구성되었으면 해당 대상으로 통화가 전송됩니다. 구성이 잘못된 경우(즉, MAP 대상이 지정되지 않은 경우), 통화가 거부되고, 발신자는 다시 걸기 신호음을 받게 됩니다. • 헛트 파일럿 지원의 경우, 헛트 그룹 알고리즘이 최장 유희 시간, 위에서 아래로 또는 순환을 지정해야 합니다. 통화 중 취급, 응답 없음 취급, 등록되지 않음 취급에 대한 헛트 그룹 옵션이 다음 그룹으로 이동이 아니라 다음 구성원 시도로 설정되었는지 확인하십시오. 선점은 단일 헛트 그룹에서만 발생합니다.
사용자 액세스 채널	<p>사용자 액세스 채널 지원은 다음 Cisco Unified IP Phone 모델에 대해서만 존재합니다. 해당 모델은 MLPP 선점 활성화됨으로 구성되어야 합니다.</p> <ul style="list-style-type: none"> • Cisco Unified IP Phone 7960, 7962, 7965 • Cisco Unified IP Phone 7940, 7942, 7945



XVI 부

SIP 상호 운용성

- [SIP 정규화 및 투명성 구성, 917 페이지](#)
- [SDP 투명성 프로파일 구성, 923 페이지](#)
- [BFCP를 통한 프레젠테이션 공유 구성, 925 페이지](#)
- [비디오 텔레포니, 929 페이지](#)



71 장

SIP 정규화 및 투명성 구성

- [SIP 정규화 및 투명성 개요, 917 페이지](#)
- [SIP 정규화 및 투명성 사전 요건, 918 페이지](#)
- [SIP 정규화 및 투명성 구성 작업 흐름, 919 페이지](#)

SIP 정규화 및 투명성 개요

SIP 정규화 및 투명성은 SIP를 다르게 구현하는 Unified Communications Manager와 엔드포인트, 서비스 공급업체, PBX 또는 게이트웨이 간의 SIP 상호 운용성 문제를 처리하는 선택적 기능입니다. SIP 정규화 및 투명성을 구성하려면 사용자 정의 LUA 스크립트를 SIP 트렁크 또는 SIP 회선에 적용합니다. Unified Communications Manager는 SIP 트렁크 또는 SIP 회선을 통과하는 SIP 메시징에 스크립트를 적용합니다.

설치 시 Unified Communications Manager는 시스템의 SIP 트렁크 및 SIP 프로파일에 할당할 수 있는 기본 정규화 및 투명성 스크립트를 포함합니다. 사용자 정의 스크립트를 만들고 가져올 수도 있습니다.

SIP 정규화

SIP 정규화 스크립트는 수신 및 발신 SIP 메시지를 수정합니다. 예를 들어, Cisco TelePresence Video Communications Server와 Unified Communications Manager를 상호 운용하는 경우, *vcs-interop* 스크립트를 둘을 연결하는 SIP 트렁크에 적용합니다. 스크립트는 두 제품이 통신할 수 있도록 SIP 메시징의 차이점을 해결합니다.

해당 SIP 트렁크를 연결하는 엔드포인트에서 사용 중인 프로토콜에 관계 없이 모든 SIP 트렁크 연결에 정규화 스크립트를 적용할 수 있습니다.

SIP 투명성

SIP 투명성 스크립트를 사용하면 Unified Communications Manager가 한 통화 레그에서 다른 통화 레그로 SIP 정보(예: 독점적인 헤더)를 투명하게 전달할 수 있습니다. 투명성을 사용하려면 두 통화 레그 모두 SIP여야 합니다.

SIP 투명성의 또 다른 기능은 REFER 투명성이며, 이는 Unified Communications Manager가 해당 요청에 대해 작동하지 않고 REFER 요청을 전달할 수 있도록 합니다. 중앙 집중식 상담사가 통화에 응답

할 수 있는 컨택 센터 환경에서 REFER 투명성을 사용할 수 있으며 발신자와 동일한 지역에 있는 상대방에게 통화를 호 전환할 수 있습니다. REFER 투명성을 사용하면 중앙 집중식 Unified Communications Manager에서 통화를 끊고 통화 제어를 새 상대방에게 전환할 수 있습니다.

SIP 정규화 및 투명성에 대한 기본 스크립트

설치 시, Cisco Unified Communications Manager에는 SIP 정규화 및 투명성에 대한 다음과 같은 기본 스크립트가 포함되어 있습니다. 이러한 스크립트를 SIP 트렁크 또는 SIP 프로파일에 적용할 수 있지만, 이러한 스크립트는 편집할 수 없습니다. 이러한 스크립트 중 어느 것도 요구 사항에 맞지 않으면 스크립트를 직접 만들 수 있습니다.

- **cisco-meeting-server-interop** - Cisco Unified Communications Manager 및 Cisco Meeting Server(CMS) 간의 상호 운용성을 제공합니다.
- **cisco-telepresence-conductor-interop** - TelePresence Conductor에 등록된 엔드포인트에 대한 상호 운용성을 제공합니다.
- **cisco-telepresence-mcu-ts-direct-interop** - Cisco Unified Communications Manager와 Cisco TelePresence MCU 또는 Cisco telepresence Server 간의 상호 운용성을 제공합니다.
- **diversion-counter** - 전환 카운터를 조정하는 기능을 제공합니다.
- **HCS-PCV-PAI** 통과 - 엔터프라이즈 IMS와 Cisco HCS 플랫폼 통합을 제공합니다.
- **redsky-alternate-id-interop** - 아웃바운드 초대에 Redsky 헤더를 추가합니다.
- **refer-passthrough** - SIP 트렁크 간 비공개 전환으로 인해 통화에서 Cisco Unified Communications Manager를 제거합니다.
- **vcs-interop** - 이 스크립트는 Cisco TelePresence Video Communication Server(VCS)에 등록된 엔드포인트에 상호 운용성을 제공합니다.

SIP 정규화 및 투명성 사전 요건

- Cisco Unified Communications Manager는 SIP 정규화 및 투명성에 대한 기본 스크립트를 제공합니다. 기존 스크립트 및 시스템 설정을 검토하여 사용자의 요구에 맞는지 여부를 확인합니다. 사용 가능한 기본 스크립트에 대한 자세한 내용은 [SIP 정규화 및 투명성에 대한 기본 스크립트, 918 페이지](#)의 내용을 참조하십시오.
- 타사 제품에 대한 SIP 요구 사항과 함께 구축의 SIP 요구 사항을 이해해야 합니다. Cisco Unified Communications Manager의 SIP 구현에 대한 자세한 내용은 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html>의 *Cisco Unified Communications Manager*(표준 버전)용 SIP 회선 메시징 설명서를 참조하십시오.
- 사용자 정의된 SIP 정규화 스크립트를 개발하려는 경우에는 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/>

[products-programming-reference-guides-list.html](https://www.cisco.com/.../products-programming-reference-guides-list.html)의 SIP 정규화 및 투명성을 위한 개발자 설명서를 참조하십시오.

SIP 정규화 및 투명성 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 1	새 SIP 정규화 및 투명성 스크립트 만들기, 919 페이지	(선택 사항) 사전 설치된 스크립트 중 사용자의 요구 사항을 충족하지 않는 경우 이 절차를 사용하여 사용자 정의된 스크립트를 구성합니다. SIP 정규화 스크립트 구성 창에서 새 스크립트를 만들거나 사용자 정의된 스크립트를 가져올 수 있습니다.
단계 2	SIP 트렁크에 정규화 또는 투명성 스크립트 적용, 920 페이지	트렁크 구성 창에서 스크립트를 SIP 트렁크에 바로 적용합니다. Cisco Unified Communications Manager는 트렁크를 통과하는 모든 SIP 메시징에 스크립트를 적용합니다.
단계 3	SIP 디바이스에 정규화 또는 투명성 적용, 921 페이지	SIP 회선에 정규화 또는 투명성 스크립트를 적용하려면 해당 SIP 회선에 연결된 SIP 프로파일에 스크립트를 적용합니다. Cisco Unified Communications Manager는 해당 SIP 프로파일을 사용하는 모든 SIP 메시징에 스크립트를 적용합니다.

새 SIP 정규화 및 투명성 스크립트 만들기

기본 정규화 및 투명성 스크립트가 사용자의 요구를 충족하지 않는 경우 이 절차를 사용하여 새 LUA 스크립트를 만듭니다. Cisco Unified Communications Manager에 새 스크립트를 작성하거나 파일을 시스템으로 가져올 수 있습니다.



팁 만들려는 스크립트가 기본 스크립트와 매우 유사하면 **SIP** 정규화 스크립트 구성 창에서 기본 스크립트를 열고 콘텐츠 텍스트 상자를 복사합니다. 새 스크립트를 만들고 내용을 콘텐츠 텍스트 상자에 붙여 넣습니다. 그런 다음 새 스크립트에서 콘텐츠를 편집할 수 있습니다.



참고 SIP 정규화 스크립트의 메모리 사용량은 각 트렁크를 기반으로 하며 각 스크립트가 아니라 각 트렁크를 기반으로 합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 정규화 스크립트.
- 단계 2 새로 추가를 클릭합니다.
SIP 정규화 스크립트 구성 창이 표시됩니다.
- 단계 3 스크립트에 대한 이름 및 설명을 입력합니다.
- 단계 4 새 스크립트를 작성하는 경우 콘텐츠 텍스트 상자에서 스크립트를 편집합니다.
- 단계 5 (선택 사항) 가져올 외부 파일이 있는 경우 다음을 수행합니다.
- 파일 가져오기를 클릭합니다.
 - 찾아보기로 파일을 찾고 파일을 선택합니다.
 - 파일 가져오기를 클릭합니다.
- SIP** 정규화 스크립트 구성 창에는 콘텐츠 텍스트 상자에 가져온 파일의 내용이 표시됩니다.
- 단계 6 **SIP** 정규화 스크립트 구성 창에서 필드를 완성합니다. 필드 및 해당 콘텐츠에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.
- 단계 7 저장을 클릭합니다.
-

다음에 수행할 작업

스크립트를 SIP 프로파일 또는 SIP 트렁크에 할당합니다.

- [SIP 디바이스에 정규화 또는 투명성 적용, 921 페이지](#)
- [SIP 트렁크에 정규화 또는 투명성 스크립트 적용, 920 페이지](#)

SIP 트렁크에 정규화 또는 투명성 스크립트 적용

SIP 정규화 또는 투명성 스크립트를 SIP 트렁크에 적용하려면 이 절차를 사용합니다. Cisco Unified Communications Manager는 트렁크를 통과하는 모든 SIP 메시징에 스크립트를 적용합니다.

프로시저

-
- 단계 1 Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.
- 단계 2 찾기를 클릭하고 스크립트를 적용할 트렁크를 선택합니다.
- 단계 3 정규화 스크립트 드롭다운 목록에서 트렁크에 적용할 스크립트를 선택합니다.
- 단계 4 (선택 사항) SIP 메시징 내에서 특정 매개 변수를 정규화하려면 다음을 수행합니다.
- 정규화할 매개 변수 이름을 입력하고 매개 변수에 적용하려는 값의 매개 변수 값을 입력합니다.
예를 들어 위치 매개 변수와 **North Carolina**를 값으로 입력할 수 있습니다.
 - 추가 매개 변수를 추가하려면 (+)를 클릭하여 추가 매개 변수와 값을 입력할 수 있는 추가 줄을 만듭니다.

단계 5 (선택 사항) 스크립트에 대한 SDI 추적을 생성하려면 추적 활성화 확인란을 선택합니다.

참고 스크립트를 디버그하는 동안 추적을 활성화하는 것이 좋습니다.

단계 6 저장을 클릭합니다.

SIP 디바이스에 정규화 또는 투명성 적용

해당 디바이스에서 사용하는 SIP 프로파일에 스크립트를 적용하여 사용자 정의된 SIP 정규화 및 투명성 스크립트 또는 사용자 정의된 SDP 투명성 프로파일을 SIP 전화기에 적용할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 2 찾기를 클릭하고 스크립트를 적용하려는 SIP 프로파일을 선택합니다.

단계 3 **SDP** 정보 영역의 **SDP** 투명성 프로파일 드롭다운 목록에서 프로파일을 선택합니다.

단계 4 정규화 스크립트 드롭다운 목록에서 트렁크에 적용할 스크립트를 선택합니다.

단계 5 (선택 사항) SIP 메시징 내에서 특정 매개 변수를 정규화하려면 다음을 수행합니다.

- a) 정규화할 매개 변수 이름을 입력하고 매개 변수에 적용하려는 값의 매개 변수 값을 입력합니다.
예를 들어 위치 매개 변수와 **North Carolina**를 값으로 입력할 수 있습니다.
- b) 추가 매개 변수를 추가하려면 (+)를 클릭하여 추가 매개 변수와 값을 입력할 수 있는 추가 줄을 만듭니다.

단계 6 (선택 사항) 스크립트에 대한 SDI 추적을 생성하려면 추적 활성화 확인란을 선택합니다.

참고 스크립트를 디버그하는 동안 추적을 활성화하는 것이 좋습니다.

단계 7 저장을 클릭합니다.



72 장

SDP 투명성 프로파일 구성

- SDP 투명성 프로파일 개요, 923 페이지
- SDP 투명성 프로파일 제한 사항, 923 페이지
- SDP 투명성 프로파일 사전 요건, 924 페이지
- SDP 투명성 프로파일 구성, 924 페이지

SDP 투명성 프로파일 개요

SDP 투명성 프로파일에는 시스템이 Unified Communications Manager에서 송신 통화 레그로의 수신에서 기본적으로 지원하지 않는 선언적 속성을 통과할 수 있는 선언적 SDP 속성에 대한 규칙 집합이 포함되어 있습니다. SDP 투명성 프로파일이 없으면 Unified Communications Manager에서 지원되지 않는 SDP 속성을 삭제합니다.

여러 개의 규칙을 사용하여 SDP 투명성 프로파일을 구성하고 SIP 프로파일을 통해 SIP 디바이스에 적용할 수 있습니다. SDP 투명성 프로파일을 적용하려면 두 통화 레그 모두 SIP여야 합니다. SDP 속성에 대해 다음과 같은 유형의 규칙을 구성할 수 있습니다.

- 특성 - 특성 속성에 대해 규칙이 구성된 경우에는 Unified Communications Manager가 해당 특성에 값이 없는 경우 SDP 속성을 통과합니다.
- 임의 값 - 임의 값에 대해 규칙이 구성된 경우에는 하나 이상의 공백이 아닌 문자로 구성된 값이 있는 경우 SDP 속성을 통과합니다.
- 목록의 값 - 이 옵션을 사용하여 규칙이 구성된 경우, SDP 속성은 지정된 값 중 하나와 일치하는 경우에만 통과합니다. 최대 5개의 가능한 값을 구성할 수 있습니다.

SDP 투명성 프로파일 제한 사항

SDP 투명성 프로파일에는 다음과 같은 제한 사항이 적용됩니다. 송신 통화 레그에서 이러한 상황이 발생하는 경우 Cisco Unified Communications Manager는 선언적인 SDP 속성을 통과하지 않습니다.

- 통과를 지원하지 않는 하나 이상의 미디어 터미네이션 포인트(MTP) 또는 Trusted Relay Point(TRP)가 할당됨
- SIP 트렁크에 대해 미디어 터미네이션 포인트 필요 확인란이 선택되어 있음

- 트랜스코더가 사용 중임
- RSVP가 사용 중임
- 수신 통화 레그는 Delayed Offer를 사용 중이고 송신 통화 레그는 Early Offer를 사용 중임
- 미디어 회선이 거부되었음(포트 = 0).
- 통화 레그 중 하나가 SIP 이외의 프로토콜을 사용 중임

SDP 투명성 프로파일 사전 요건

타사 SIP 제품을 구축하려는 경우에는 제품이 SDP(Session Description Protocol)를 구현하는 방법을 이해해야 합니다.

SDP 투명성 프로파일 구성

Cisco Unified Communications Manager에서 기본적으로 지원하지 않는 선언적 SDP 특성에 대한 일련의 규칙을 사용하여 사용자 정의된 SDP 투명성 프로파일을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SDP** 투명성 프로파일을 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 이름과 설명을 입력합니다.

단계 4 속성 정보 창에서 통과시키려는 SDP 속성에 대한 규칙을 생성합니다.

- 속성 속성을 전달하려면 이름 텍스트 상자에 속성(예: a=recvonly)을 입력하고 유형 드롭다운 목록에서 속성을 선택합니다.
- 값 속성을 전달하려면 이름 텍스트 상자에 속성(예: a=rtpmap)을 입력하고 유형 드롭다운 목록 상자에서 값을 선택합니다.
- 값 속성을 최대 5개의 값으로 전달하려면 이름 필드에 속성(예: a=rtpmap)을 입력하고 유형 드롭다운 목록에서 값을 선택합니다. 결과 값 텍스트 상자에 속성 값을 입력합니다. +를 클릭하여 이 속성에 가능한 값을 최대 5개까지 추가할 수 있습니다.

단계 5 (+)를 클릭하여 이 투명성 프로파일에 대한 추가 SDP 속성을 입력할 수 있는 새 줄을 만듭니다.

단계 6 저장을 클릭합니다.

참고 SIP 프로파일을 사용하는 디바이스에서 SDP 투명성 프로파일을 사용할 수 있도록 이 프로파일을 SIP 프로파일에 적용해야 합니다.



73 장

BFCP를 통한 프레젠테이션 공유 구성

- [Binary Floor Control Protocol 개요, 925 페이지](#)
- [BFCP 사전 요건을 사용하여 프레젠테이션 공유, 927 페이지](#)
- [BFCP 구성 작업 흐름을 사용하여 프레젠테이션 공유, 927 페이지](#)

Binary Floor Control Protocol 개요

Unified Communications Manager는 지원되는 Cisco 엔드포인트 및 타사 비디오 엔드포인트에 대한 BFCP(Binary Floor Control Protocol)를 사용하여 프레젠테이션 공유를 지원합니다. 이 기능을 사용하면 사용자가 진행 중인 오디오 또는 비디오 대화 내에서 프레젠테이션을 공유할 수 있습니다.

다음 예에서는 BFCP를 사용하여 프레젠테이션 공유를 작동하는 방법을 설명합니다.

- 두 비디오 전화기 사이에 진행 중인 비디오 대화가 있습니다. 사용자 A는 대화 중에 사용자 B와 콘텐츠를 공유하기로 결정합니다. 사용자 A에게 전체 화면을 공유하거나 특정 애플리케이션을 공유할 수 있는 옵션이 있습니다.
- BFCP 스트림을 사용하여 사용자 B가 사용자 A의 공유 콘텐츠를 볼 수 있습니다.

콘텐츠 공유를 사용하는 오디오 영상 통화에는 최소 4개의 채널(오디오, 기본 비디오, 두 번째 비디오 및 BFCP 제어 채널)이 필요합니다. 비디오 회의를 걸고 두 번째 비디오 채널에서 프레젠테이션을 공유할 수 있습니다. 통화 당사자가 FECC(Far Camera Control)를 사용할 수 있는 경우에는 다섯 번째 채널을 설정해야 합니다.

BFCP를 사용한 프레젠테이션 공유

Unified Communications Manager 등록된 SIP 엔드포인트의 경우 12.5(1)SU3부터는 다음과 같은 경우에 BFCP가 작동합니다.

- 오디오 전용 모드에서 대화를 시작하는 비디오 지원 엔드포인트 두 개는 BFCP 지원을 사용하여 통화 중에 콘텐츠를 공유합니다.
- 통화 중에 TRP가 할당됩니다.

BFCP 아키텍처

BFCP를 사용한 프레젠테이션 공유는 BFCP가 활성화된 SIP 네트워크에서만 지원됩니다. 엔드포인트 디바이스 및 트렁크를 포함한 전체 네트워크는 SIP여야 합니다.

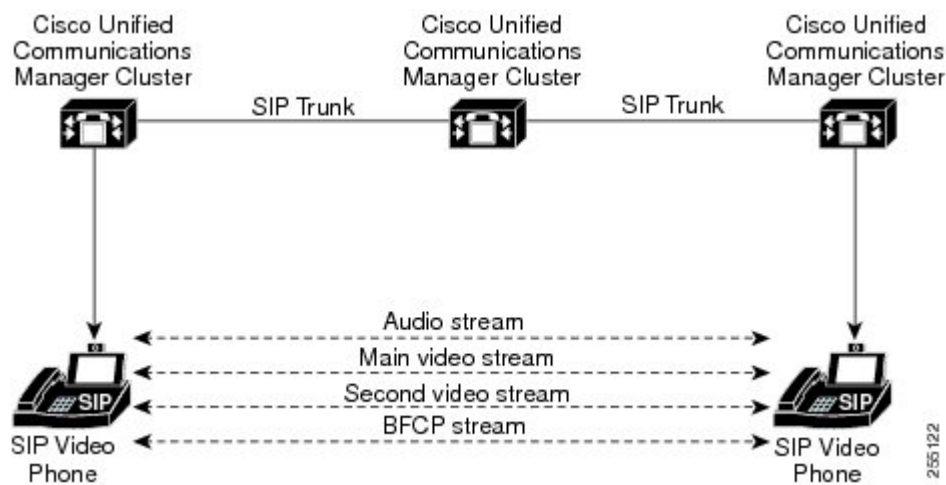
Unified Communications Manager는 두 엔드포인트 간에 SIP 메시지를 릴레이하여 BFCP 스트림의 협상을 지원합니다.

이 협상에는 공유 리소스에 액세스하기 위한 임시 권한인 층 설정이 포함됩니다.

BFCP 스트림은 엔드포인트 간의 포인트-투-포인트 스트림입니다. Unified Communications Manager는 BFCP 스트림의 대상이 아닙니다.

다음 그림은 여러 개의 Unified Communications Manager 클러스터를 포함하는 복잡 한 비디오 네트워크의 예를 제공합니다. BFCP는 디바이스를 연결하는 모든 트렁크 및 회선에서 활성화되어야 합니다. 이 네트워크의 경우, BFCP 4개의 SIP 트렁크와 엔드포인트를 연결하는 두 개의 SIP 회선에서 활성화되어야 합니다.

그림 14: 여러 개의 **Cisco Unified Communications Manager** 클러스터가 있는 비디오 네트워크



BFCP 제한 사항

Unified Communications Manager는 다음과 같은 시나리오에서 BFCP 스트림을 거부합니다.

- SIP 프로파일 페이지의 **BFCP**를 통한 프레젠테이션 공유 허용 확인란은 네트워크의 SIP 회선 또는 트렁크 중 하나에 대해 선택되지 않았습니다.
- 한 엔드포인트는 BFCP를 제공하지만 다른 엔드포인트는 제공하지 않습니다.
- SIP 회선 또는 SIP 트렁크가 MTP(비 통과 모드) 또는 트랜스코더를 사용하는 경우



참고 BFCP 제어 채널은 항상 암호화되지 않습니다. 그러나, 두 전화기가 모두 암호화된 경우에는 프레젠테이션 채널이 암호화됩니다.

BFCP 사전 요건을 사용하여 프레젠테이션 공유

- 통화 흐름의 모든 엔드포인트 및 트렁크에서 SIP 프로파일을 실행하고 있는지 확인합니다.
- 전화 지원 절차를 확인하고 기능 **BFCP** 지원에 대한 보고서를 생성하여 BFCP를 사용하여 프레젠테이션 공유를 지원하는 Cisco 엔드포인트 목록을 얻습니다. 이러한 엔드포인트의 경우 기본적으로 BFCP 지원이 활성화됩니다. BFCP를 지원하기 위해 전화기에 추가 구성을 수행할 필요가 없습니다. 자세한 내용은 [전화기 기능 목록 생성, 7 페이지](#)의 내용을 참조하십시오.

BFCP 구성 작업 흐름을 사용하여 프레젠테이션 공유

BFCP(Binary Floor Control Protocol)를 사용하여 프레젠테이션 공유를 활성화하려면 다음 작업을 완료합니다.

프로시저

	명령 또는 동작	목적
단계 1	SIP 트렁크에 대한 BFCP 지원 활성화, 927 페이지	통화 흐름의 모든 SIP 트렁크에서 BFCP 지원을 활성화합니다.
단계 2	타사 전화기에 대해 BFCP를 사용하여 프레젠테이션 공유 활성화, 928 페이지	타사 SIP 엔드포인트를 사용하는 경우 타사 전화기 구성에서 BFCP 지원을 활성화합니다.

SIP 트렁크에 대한 BFCP 지원 활성화

BFCP와 프리젠테이션 공유를 사용하는 경우, 이 기능은 메시지 또는 통화 흐름의 모든 트렁크에서 사용되는 SIP 프로파일에서 활성화되어야 합니다. BFCP 스트림은 프레젠테이션 공유를 지원하지 않는 트렁크에 의해 거부됩니다.

프로시저

단계 1 SIP 트렁크에서 사용하는 SIP 프로파일 내에서 BFCP 지원을 활성화합니다.

- Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.
- 다음 단계 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 SIP 프로파일을 선택합니다.
- 새로 추가를 클릭하여 새 SIP 프로파일을 만듭니다.

- SDP** 정보 섹션에서 **BFCP**를 통한 프레젠테이션 공유 허용 확인란을 선택하여 Unified Communications Manager에서 BFCP를 활성화합니다.

기본적으로 이 확인란은 선택되어 있지 않습니다. 프레젠테이션 공유의 경우, Unified CM 클러스터 간의 모든 SIP 트렁크에 대해 BFCP를 활성화해야 합니다.

- d) **SIP** 프로파일 구성 창의 다른 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.
- e) 저장을 클릭합니다.

단계 2 BFCP 활성화된 SIP 프로파일을 SIP 트렁크에 연결합니다.

- a) Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.
- b) 찾기를 클릭하고 기존 SIP 트렁크를 선택합니다.
- c) **SIP** 정보 섹션의 **SIP** 프로파일 드롭다운 목록에서 클러스터 간 통화의 프레젠테이션을 공유하도록 BFCP를 활성화한 SIP 프로파일을 선택합니다.
- d) 저장을 클릭합니다.
- e) BFCP 세션의 통화 흐름에 해당하는 모든 SIP 트렁크에 대해 이 단계를 반복합니다.

타사 전화기에 대해 BFCP를 사용하여 프레젠테이션 공유 활성화

타사 SIP 전화기와 BFCP를 사용하여 프레젠테이션 공유를 사용하려면 해당 기능이 엔드포인트에 대해 활성화되어 있는지 확인해야 합니다. 이 기능은 다음 타사 전화기 유형에 지원됩니다.

- 타사 SIP 디바이스(고급)
- 타사 AS-SIP 엔드포인트

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 2 찾기를 클릭하고 기존 타사 SIP 전화기를 선택합니다.

단계 3 BFCP를 통한 프레젠테이션 공유 허용 확인란을 선택합니다.

단계 4 저장을 클릭합니다.



74 장

비디오 텔레포니

- 비디오 전화 통신 개요, 929 페이지
- 비디오 전화 통신 지원, 930 페이지
- 비디오 네트워크, 933 페이지
- 비디오 전화 통신 구성 작업 흐름, 935 페이지
- H.323 비디오, 935 페이지
- 비디오 지원, 940 페이지
- 비디오 기능, 944 페이지
- 비디오 네트워크에 대한 QoS, 946 페이지

비디오 전화 통신 개요

Unified Communications Manager는 비디오 전화 통신을 지원하므로 음성 및 영상 통화 환경을 통합합니다. 비디오 엔드포인트는 Unified CM 통화 처리 기능을 사용하고 영상 통화에 전화를 걸고 연결하기 위해 통합 음성 및 비디오 솔루션에 액세스합니다.

Unified Communications Manager 비디오 전화 통신 솔루션은 다음 기능을 제공합니다.

- FECC(원거리 카메라 제어)와 같은 비디오 및 비디오 관련 기능을 지원합니다.
- 비디오 스트림 전송을 허용하는 데 필요한 다중 논리적 채널을 지원합니다.
- 통화 중 비디오에 필요한 미디어 관련 메시지(즉, 영상 통화에 필요한, 명령 또는 표시를 전송)를 전송합니다.
- H.323, SCCP(Skinny Call Control Protocol) 또는 SIP(Session Initiation Protocol)를 지원합니다.
- 대역폭 관리를 제공하기 위해 위치 및 지역을 개선합니다.
- 영상 통화에 대한 CDR(통화 세부 정보 레코드) 같은 서비스 가용성 정보를 제공합니다.

비디오 전화 통신 지원

다음 섹션에서는 Unified Communications Manager 환경에서 비디오 전화 통신의 세부 정보에 대해 논의합니다.

영상 통화

일반적인 영상 통화에는 각 방향에 2개 또는 3개의 RTP(실시간 프로토콜) 스트림이 포함됩니다(즉, 4개 또는 6개 스트림). 통화는 다음과 같은 스트림 유형을 포함할 수 있습니다.

- 비디오(H.261, H.263, H.263+, H.264-SVC, X-H.264UC, H.264-AVC, H.265, AV1 및 VT 카메라 와이드밴드 비디오 코덱)
- FECC(Far End Camera Control) - 선택 사항
- BFCP(Binary Floor Control Protocols)



참고 영상 통화에 대한 통화 제어는 다른 모든 통화를 제어하는 통화 제어와 동일한 방식으로 작동합니다. 자세한 내용은 [시스템 구성 설명서](#)의 미디어 리소스 구성 장을 참조하십시오. Unified Communications Manager가 자동으로 비디오 컨퍼런스 브리지를 할당하는 방법에 대한 자세한 내용은 [시스템 구성 설명서](#)에서 전화 회의 브리지 장을 참조하십시오.

MTP 토폴로지에서 실시간 전송 제어 프로토콜 통과

15.2(2)T 이전의 IOS 미디어 종료 포인트(MTP)는 실시간 전송 제어 프로토콜(RTCP) 패킷을 통과할 수 없으며, 따라서 RTP(실시간 프로토콜) 피드백 데이터를 교환하여 RTP 전송을 개선할 수 없습니다. RTCP의 기본 기능은 스트리밍 멀티미디어 세션의 참가자에게 주기적으로 통계를 전송하여 미디어 배포에 대한 피드백을 제공하는 것입니다. RTCP는 미디어 연결에 대한 통계 및 전송된 옥텟 및 패킷 수, 손실된 패킷 수, 지터, 왕복 지연 시간 등의 정보를 수집합니다. 애플리케이션은 이 정보를 사용하여 흐름을 제한하거나 다른 코덱을 사용하여 서비스의 품질 매개 변수를 제어할 수 있습니다.

IOS MTP 버전 15.2(2)T 이상에서 RTCP 통과 기능을 지원하므로 MTP가 있는 통화의 엔드포인트는 여전히 RTP 전송에 대한 피드백 및 상태를 제공할 수 있습니다. RTCP 통과 기능은 미디어 채널에 적용됩니다.

RTCP 통과 기능은 특정 통화 신호 처리 프로토콜로 제한되지 않습니다. 예를 들어, SIP-SIP, SIP-nonSIP 또는 nonSIP-nonSIP일 수 있습니다.

Unified CM에서 RTCP 통과 지원 MTP를 명시적으로 할당하려면 통화에서 다음 조건을 충족해야 합니다.

- MTP가 미디어 통과 모드에 있어야 하는 기능에 대해 MTP가 요청됩니다. 예를 들어, TRP, DTMF 변환, IP 주소 V4/V6 변환 등이 있습니다. RTCP 통과는 미디어가 통과 모드에 있는 경우에만 적용됩니다.

- RTCP 통과 MTP는 MTP를 후원하는 엔드포인트의 미디어 리소스 그룹 목록(MRGL)에 포함되어야 합니다. RSVP, TRP, DTMF 불일치로 인해 MTP가 삽입될 수 있습니다.
- 통화에서 비디오 채널을 설정할 수 있는 경우에는 Unified CM이 RTCP 통과 가능 MTP를 검색하려고 시도합니다. 예를 들어, Unified CM은 MRGL에서 지원되지 않는 다른 위치에서 RTCP 통과 가능 MTP를 선택합니다. RTCP 통과 지원 MTP를 사용할 수 없는 경우에는 Unified CM이 여전히 통화해 MTP를 할당합니다.
- 통화에서 오디오 채널만 설정할 수 있는 경우에는 Unified CM이 비 영상 통화해 대해 RTCP 통과 가능 MTP를 사용할 수 있는 RTCP 통과를 의도적으로 요청하지 않습니다. 그러나 MRGL에 RTC 통과 가능 MTP가 포함되어 있는 경우에는 Unified CM이 오디오 통화해 해당 중 하나를 삽입합니다.
- 이 통화는 RTCP 통과 가능 MTP를 갖도록 영상 통화해 대한 현재 CAC 대역폭을 충족해야 합니다.



참고

통화해 처음으로 RTCP 통과 가능 MTP(버전 15.2(2)T)가 설치되어 있고 통화해 비디오 가능 통화해 에스컬레이션 되는 경우, Unified CM은 RTCP 통과 가능 MTP에 다시 할당되지 않습니다. 이 경우 통화해 영상 통화해 에스컬레이션 된 경우에도 기존 MTP에서는 RTCP 패킷이 전달될 수 없습니다.

비디오 코덱

일반적인 비디오 코덱에는 이전 비디오 코덱인 H.261, IP(인터넷 프로토콜) 비디오를 제공하는 데 사용되는 최신 코덱인 H.263 및 고품질 코덱인 H.264 등이 포함됩니다. 시스템은 발신 및 종료 엔드포인트에서만 SCCP(Skinny Client Control Protocol), H.323 및 SIP를 사용하는 통화해 대해 H.264를 지원합니다. 시스템은 지역 및 위치도 지원합니다.

가능하면 Unified Communications Manager는 응답을 할 때 제공자의 비디오 코덱 순서 기본 설정을 유지합니다. H.265는 기본 비디오 코덱을 엔드포인트에서 사용할 수 있으며, 그렇지 않은 경우에는 Unified Communications Manager가 다음 코덱 기본 설정 순서를 따릅니다.

기본 설정 순서	코덱	설명
1	H.265(HEVC)	낮은 대역폭을 사용하여 더 높은 품질의 비디오를 제공합니다.
2	H.264(SVC)	수신된 패킷의 하위 집합을 무시하여 동일한 미디어 스트림에서 가변 품질 비디오를 렌더링할 수 있습니다. 참고 H.264 SVC는 H.264-AVC 비디오 압축 표준에 대한 새로운 부록입니다. 이는 H.264-AVC 위에 있는 향상된 기능입니다. 이는 한 컨테이너의 다양한 프레임 속도 및 해상도에서 여러 비디오 스트림을 캡슐화하는 기능을 제공합니다.
3	X-H.264UC(Lync)	Microsoft 독점 변형

기본 설정 순서	코덱	설명
4	H.264(AVC)	고급 비디오 코딩
5	H.263	H.263 및 H.261 코덱에는 다음과 같은 매개 변수와 일반적인 값이 나타납니다. <ul style="list-style-type: none"> • 비트 속도 범위는 64kb/s에서 몇 mb/s까지입니다. 이러한 비트 속도는 100 b/s의 배수로 존재할 수 있습니다. H.261 및 H.263이 64 kb/s보다 낮은 비트 전송률로 작동할 수 있지만, 이러한 경우에는 비디오 품질이 저하됩니다. • 1/4 일반 교환 형식(QCIF) (해상도는 176x144) • 일반 교환 형식(CIF) (해상도는 352x288) • 4CIF(해상도는 704x576) • Sub QCIF(SQCIF)(해상도는 128x96) • 16CIF(해상도는 1408x1152) • 사용자 정의 사진 형식 • 해상도: • 프레임 속도: 초당 15 프레임(fps), 30fps • 부록: F, D, I, J, K, L, P, T, N
6	H.261	

영상 통화의 대역폭은 오디오 대역폭과 비디오 대역폭의 합과 같습니다. 총 대역폭에는 오버헤드가 포함되지 않습니다.

384 kb/s 영상 통화는 64 kb/s(오디오용)와 320 kb/s(비디오용)로 G.711을 구성할 수 있습니다. 이 합계에는 오버헤드가 포함되지 않습니다. 화상 통화에 대한 오디오 코덱이 G.729(24 kb/s)인 경우 비디오 속도가 증가하여 384 kb/s의 총 대역폭을 유지합니다. 통화는 H.323 엔드포인트가 포함되는 경우에는 H.323 엔드포인트에서 사용 가능한 총 비디오 대역폭 보다 낮은 값을 사용할 수 있습니다. 프로토콜과 상관 없이 엔드포인트는 항상 통화의 경우 최대 비트 속도 미만으로 전송하도록 선택할 수 있습니다.

AV1 코덱 지원

AV1은 오픈 미디어 연합(Alliance for Open Media)에 의해 개발된 차세대 비디오 코덱입니다. AV1의 이점은 다음과 같습니다.

- 다른 비디오 인코딩과 비교하여 더 나은 압축 효율을 활용하여 대역폭 사용량과 향상된 시각적 품질 감소
- 매우 낮은 대역폭 네트워크에서 사용자를 위해 비디오 활성화

- 다른 코덱에 비해 상당한 화면 공유 효율성 향상

Unified Communications Manager는 엔드포인트에서 AV1 코덱을 지원하는 경우 미디어를 설정하기 위해 AV1 코덱의 협상을 지원합니다.

두 엔드포인트 모두 응답에서 여러 코덱을 지원할 경우, Unified CM은 수신되는 기본 설정 순서를 기반으로 AV1를 포함하여 일치하는 모든 코덱을 협상합니다. 그러면 엔드포인트는 미디어 스트리밍을 위해 협상된 코덱 목록에 있는 코덱 중 하나를 사용합니다. 낮은 대역폭 환경에서는 AV1 코덱이 협상된 목록에 있는 다른 코덱보다 엔드포인트에 의해 선호됩니다.

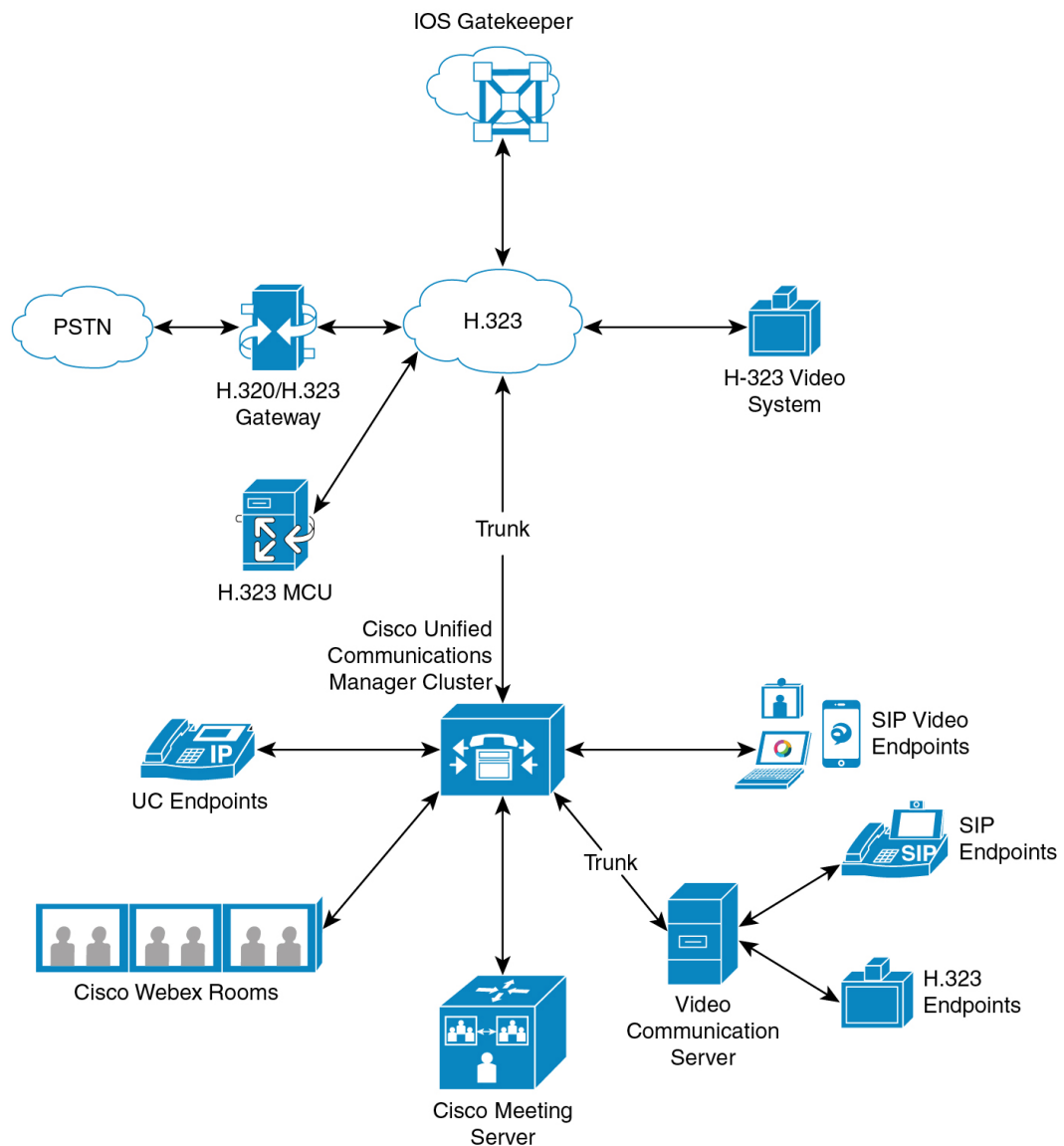
통화에 관련된 두 엔드포인트 모두 응답에 여러 코덱을 지원하지 않으며 AV1이 다른 코덱에 비해 선호되는 코덱인 경우에는 Unified CM은 협상된 코덱으로 AV1를 선택합니다.



참고 AV1는 Webex DeskPro, Room Kit Pro 및 Room Panorama와 같은 엔드포인트에서 지원됩니다.

비디오 네트워크

다음 그림은 단일 Unified Communications Manager 클러스터를 사용하는 비디오 네트워크의 예를 제공합니다. 성공적인 비디오 네트워크에서 모든 엔드포인트는 다른 엔드포인트를 호출할 수 있습니다. 두 엔드포인트 모두 비디오를 사용할 수 있는 경우에만 비디오 사용 가능 여부가 존재합니다. 비디오 기능은 트렁크 간에 확장됩니다.



455693

Cisco 화상 회의 포트폴리오는 다음과 같은 비디오 브리지로 구성됩니다.

- Cisco TelePresence MCU 시리즈
- Webex Meeting Server

Cisco UC 엔드포인트 포트폴리오는 비디오를 지원하는 다음 엔드포인트로 구성됩니다.

비디오를 지원하는 Cisco UC 엔드포인트 포트폴리오에 대한 자세한 내용은 [호환성 매트릭스](#)를 참조하십시오.



참고 타사 SIP 비디오 엔드포인트는 Cisco Unified Communications Manager를 회선 측 디바이스로 또는 트렁크 측 디바이스로 연결할 수 있습니다. 자세한 내용은 타사 SIP 엔드포인트를 참조하십시오.

비디오 전화 통신 구성 작업 흐름

Cisco Unified Communications Manager 관리에서 비디오 전화 통신을 구성하려면 다음 단계를 수행합니다.

프로시저

- 단계 1 통화 허용 제어에 지역을 사용하는 경우 영상 통화 대역폭에 대한 영역을 구성합니다.
참고 모든 디바이스에는 기본적으로 비디오에 대한 384 kb/s가 지정되어 있습니다. 지역 구성의 대역폭 설정을 원하는 해상도에 맞게 충분히 높게 설정할 수 있습니다(예: 고화질 영상 통화의 경우 2Mb/s로 증가).
- 단계 2 콜수락 제어(CAC)에 대한 위치를 사용하는 경우 영상 통화 대역폭의 위치를 구성합니다.
- 단계 3 (선택 사항) SIP 영상 통화의 대역폭 관리를 위해 RSVP를 사용하는 경우 RSVP 서비스 매개 변수를 구성하거나 위치 구성 창에서 RSVP 정책을 설정합니다.
- 단계 4 네트워크에서 Cisco 화상 회의 브리지를 사용하도록 적절한 전화회의 브리지를 구성합니다.
- 단계 5 사용자가 다른 전화회의 브리지를 사용하는 대신 화상 회의 브리지를 사용하도록 구성하려면 그에 따라 사용자에게 대한 미디어 리소스 그룹 및 미디어 리소스 그룹 목록을 구성합니다.
- 단계 6 영상 통화를 음성 통화로 다시 시도하거나 (기본 동작) AAR 그룹 및 경로/헌트 목록을 구성하여 연결되지 않는 영상 통화에 대해 대체 라우팅을 사용하도록 시스템에서 H.323 트렁크를 구성합니다.
- 단계 7 영상 통화를 음성 통화로 다시 시도하거나 (기본 동작) AAR 그룹 및 경로/헌트 목록을 구성하여 연결되지 않는 영상 통화에 대해 대체 라우팅을 사용하도록 시스템에서 H.323 게이트웨이를 구성합니다. 비디오 기능에 대해 활성화를 선택합니다.
- 단계 8 영상 통화를 음성 통화로 다시 시도하거나 (기본 동작) AAR 그룹 및 경로/헌트 목록을 구성하여 연결되지 않는 영상 통화에 대해 대체 라우팅을 사용하도록 시스템에서 H.323 트렁크를 구성합니다.
- 단계 9 비디오를 지원할 Cisco Unified IP Phone을 구성합니다.
- 단계 10 비디오를 지원할 타사 SIP 엔드포인트를 구성합니다.
- 단계 11 영상 통화를 음성 통화로 다시 시도하도록 시스템의 SIP 트렁크를 구성합니다(기본 동작).

H.323 비디오

H.323 비디오는 다음과 같은 특성을 보입니다.

- H.323 엔드포인트는 H.323 전화기, H.323 게이트웨이 또는 H.323 트렁크로 구성될 수 있습니다.
- 착신 전환, 다이얼 플랜 및 기타 통화 라우팅 관련 기능은 H.323 엔드포인트에서 작동합니다.
- H.323 비디오 엔드포인트는 보류, 재시작, 호 전환, 지정 보류 및 기타 유사한 기능을 시작할 수 없습니다.
- H.323 엔드포인트에서 ECS(빈 기능 집합)을 지원하는 경우 엔드포인트는 보류, 지정 보류 등이 될 수 있습니다.
- 일부 공급업체는 통화가 호 전환되거나 재전송될 때 통화의 대역폭을 늘릴 수 없는 방식으로 통화 설정을 구현합니다. 이러한 경우, 초기 통화가 오디오인 경우 비디오 엔드포인트로 전송할 때 비디오를 수신하지 못할 수 있습니다.
- 현재 MTP(비디오 미디어 터미네이션 포인트) 또는 비디오 트랜스코더가 없습니다. 오디오 트랜스코더 또는 MTP가 통화로 삽입되는 경우 해당 통화는 오디오 전용입니다. 이것은 IPVC 오디오 트랜스코딩 기능이 사용되지 않는 경우에 적용됩니다. IPVC 트랜스코더를 사용하는 경우 오디오를 트랜스코딩하고 비디오를 주고 받을 수 있습니다.
- H.323 영상 통화의 경우 사용자가 영상 통화 대역폭을 지정해야 합니다.

H.323 통화의 H.239 확장 비디오 채널

확장된 비디오 채널 기능은 H.239 프로토콜을 통해 작동하며 여러 비디오 채널을 지원할 수 있습니다. Cisco Unified Communications Manager는 직접 포인트 간 H.323 통화에서 H.239 프로토콜을 사용하여 확장된 비디오 채널의 협상을 지원합니다. 여기에는 H.323 인터클러스터 트렁크에 걸친 통화도 포함됩니다.

Cisco Unified Communications Manager는 H.239 권장 사항에 지정된 모든 H.239와 관련된 지원 신호 및 명령을 지원합니다.

다음 섹션에서는 확장 비디오 채널 기능에 적용되는 특징에 대해 설명합니다.

타사 H.323 디바이스에 대한 지원

확장된 비디오 채널 기능은 타사 비디오 엔드포인트 및 Cisco Unified 음성 회의 중에 H.239 상호 운용성을 지원합니다. Cisco Unified Communications Manager를 사용하면 프레젠테이션 및 라이브 미팅 전송에 확장 비디오 채널을 사용할 수 있습니다. 이 기능은 H.245 신호 처리를 통해 여러 비디오 채널 지원에 중점을 둡니다. 다음은 이 다중 채널 지원에 대한 기초를 제공하는 프레젠테이션 애플리케이션입니다.

- 타사 공급업체 비디오 엔드포인트에 의한 기본 프레젠테이션 패키지
- 타사 공급업체 Polycom에 의한 사용자 + 콘텐츠

기본 프레젠테이션 패키지 및 사용자 + 콘텐츠는 모두 H.239 프로토콜을 사용하여 기능을 협상하고 추가 비디오 채널의 역할을 정의합니다.



참고 비디오 엔드포인트 및 Polycom에 의한 기본 프레젠테이션 패키지는 프레젠테이션 모드에 대해서만 H.239만 지원합니다.

비디오 엔드포인트 및 Polycom 제공되는 프레젠테이션 애플리케이션은 선택적 기능입니다. 두 번째 비디오 채널을 협상하려면 이러한 옵션 중 하나와 발신자 및 수신자 엔드포인트 모두에서 H.239를 활성화 해야 합니다. 그렇지 않으면 통화가 단일 비디오 채널로 제한됩니다.

H.323 디바이스에서 프레젠테이션 기능 호출

Cisco 및 Polycom 비디오 엔드포인트를 사용하면 다양한 구성 요소(예: VCR, 프로젝터, PC 등)의 프레젠테이션 자료를 공유할 수 있습니다. 구성 요소는 엔드포인트와 물리적으로 연결할 수 있으며, PC는 공급업체에서 제공하는 프레젠테이션 애플리케이션을 실행하여 프레젠테이션 이미지를 전송할 수 있습니다. 프레젠테이션 소스와 비디오 엔드포인트와의 구성 요소 연결은 H.239를 사용하여 비디오 채널을 설정 하는 메커니즘과 관련이 없습니다.



참고 프레젠테이션 소스 설정에 대한 자세한 내용은 비디오 엔드포인트 사용 설명서를 참조하십시오.

두 개의 H.239를 사용하는 엔드포인트에서 영상 통화를 설정하려고 하면 두 번째 비디오 채널에 대해 미팅 참가자의 기본 비디오 채널 및 해당 확장 비디오 기능(H.239 기능)에 대한 비디오 기능을 선언합니다. 다음 내용은 H.239 기능 신호를 구성합니다.

1. 엔드포인트는 디바이스에서 H.239를 지원한다는 것을 나타내기 위해 신호를 보냅니다. 또한 연결된 명령과 두 번째 비디오 채널 관리를 위한 표시 신호를 전송합니다. 이렇게 하면 두 엔드포인트 모두 통화에서 여러 비디오 채널을 열 수 있음을 인식할 수 있습니다.
2. 엔드포인트는 하나 이상의 확장된 비디오 코덱 기능을 전송하여 두 번째 채널에 대한 비디오 코덱 기능을 표현합니다. 엔드포인트는 두 번째 비디오 채널의 역할을 지정해야 합니다. 정의된 역할 레이블은 다음과 같을 수 있습니다.
 - 라이브 비디오 - 이 채널은 정상적으로 처리되고 사용자의 라이브 비디오에 적합합니다.
 - 프레젠테이션 - 이 채널은 디바이스에 배포되는 토큰 관리 프레젠테이션을 릴레이합니다.

기능을 교환한 후에는 두 엔드포인트 모두 일반 영상 통화에서처럼 양방향 오디오 채널 및 기본 비디오 채널을 즉시 엽니다.

두 번째 비디오 채널 열기

타사 엔드포인트 구현에 따라 두 번째 비디오 채널은 공급업체 간에 서로 다르게 처리됩니다.

Tandberg의 기본 프레젠테이션 패키지

비디오 엔드포인트는 요청 시 두 번째 비디오 채널을 시작합니다. 비디오 엔드포인트 디바이스는 기본 비디오 채널이 설정된 후에 두 번째 비디오 채널을 즉시 열지 않습니다. 두 번째 채널은 발신자 중

한 명(발표자)이 프레젠테이션 소스를 지정하고 프레젠테이션을 시작하기 위한 명령을 호출하면 열립니다.

비디오 엔드포인트 사용자가 프레젠테이션 공유를 시작하기로 결정하면 비디오 엔드포인트는 다른 통화 상대방에게 프레젠테이션 이미지를 받기 위해 확장된 비디오 채널을 열도록 요청합니다. 따라서 비디오 엔드포인트-비디오 엔드포인트 통화에는 단방향 두 번째 비디오 채널만 있습니다.

Polycom의 사용자 + 콘텐츠

비디오 엔드포인트와 달리 Polycom 비디오 엔드포인트는 두 번째 비디오 엔드포인트를 기본 메커니즘의 일부로 즉시 시작하여 두 당사자가 추가 비디오 채널을 지원할 수 있음을 확인했습니다.



참고 두 당사자가 모두 H.239를 지원하고 확장된 비디오 채널 기능이 활성화된 경우 채널이 자동으로 설정됩니다. 그러나 추가 채널은 프레젠테이션 공유를 시작할 때까지 아무 것도 표시하지 않습니다.

Polycom은 두 번째 비디오 채널의 사용과 관계 없이 다른 통화 상대방에게 두 번째 비디오 채널에 대한 요청을 시작합니다. 따라서 Polycom 간의 통화 중 하나에만 프레젠테이션 이미지/비디오를 전송하는 경우에도 디바이스 간에 양방향 비디오 채널이 열립니다.

이 구현에서는 통화 상대방이 토큰을 사용하여 무언가를 표시하는 경우 두 통화 당사자 모두 전송할 준비가 된 두 번째 비디오 채널을 가질 수 있습니다. 두 비디오 채널 중 하나가 유휴 상태로 유지되지만(아무 것도 전송하지 않음) Polycom 디바이스는 로드 효율성을 보장하기 위해 대역폭을 제어합니다.

두 번째 비디오 채널을 처리할 때의 이러한 차이는 H.239의 구현에 영향을 미치지 않습니다. Unified Communications Manager에서는 H.323 통화에서 수신 채널 요청을 시작하지 않습니다. Unified Communications Manager에서는 한 터미널에서 다른 터미널로 모든 채널 요청을 릴레이하기만 합니다.

Unified Communications Manager에서는 H.239 프로토콜에서 요구 사항을 나타내지 않으므로 두 번째 비디오 채널 세트에 대해 양방향 전송을 시행하지 않습니다.

두 번째 비디오 채널의 CAC(Call Admission Control)

두 번째 비디오 채널에 적용되는 Cisco Unified Communications Manager의 콜수락 제어(CAC) 정책은 다음과 같습니다.

Cisco Unified Communications Manager에서는 위치 구성을 기준으로 두 번째 비디오 채널에서 대역폭 사용량을 제한합니다. 두 번째 비디오 채널이 설정되면 Cisco Unified Communications Manager는 위치 풀 내에서 충분한 비디오 대역폭을 유지하고 그에 따라 대역폭을 예약합니다. 필요한 대역폭을 사용할 수 없는 경우 Cisco Unified Communications Manager에서 채널에 지시하여 사용 가능한 대역폭을 0으로 줄입니다.

두 번째 비디오 채널을 지원하기 위해 지역 구성에서 변경 사항이 발생하지 않습니다.

일반적으로 Cisco Unified Communications Manager 지역 정책은 단일 비디오 채널을 사용하는 통화만 지원하며 이 통화의 총 대역폭 사용량은 지역 구성에서 지정하는 것보다 커지지 않습니다.

관리자가 H.239 통화에 대한 유한 지역 비디오 대역폭 제한을 설정하는 경우 지역 값이 각 비디오 채널에 대해 개별적으로 요청된 대역폭에 대해 사용되므로 Cisco Unified Communications Manager 지역 정책을 위반하게 됩니다.

예제

지역 비디오 대역폭이 384Kbps로 설정되고 오디오 채널에서 64Kb/s가 사용되는 경우 각 비디오 채널에 허용되는 최대 대역폭은 $(384\text{Kb/s} - 64\text{Kb}) = 320\text{Kb/s}$ 입니다. 즉, H.239 통화에 사용할 최대 대역폭은 $(\text{오디오 bw} + 2 * (384 - \text{오디오 bw})) = 704\text{Kb/s}$ 이며 지역이 지정하는 384Kb/s 대역폭을 초과합니다.



참고 H.239 통화에 대해 지역 및 위치 대역폭 제한을 모두 해제하는 것을 고려해야 합니다. 따라서 H.239 디바이스는 Cisco Unified Communications Manager 개입 없이 두 비디오 채널 모두에 대한 로드를 다시 조정하고 균형을 조정할 수 있습니다.

허용되는 비디오 채널 수

Unified Communications Manager은 다음 이유로 인해 최대 2개의 비디오 채널만 지원합니다.

- Cisco와 Polycom은 모두 메인 비디오에 대해 두 개의 비디오 채널만 지원하고 다른 하나는 표시를 위한 것입니다.
- H.239는 표시 목적으로 기존 H.320 비디오 채널을 파티션하는 데 사용되는 AMC(추가 미디어 채널)만 정의합니다.

H.239 명령 및 표시 메시지

명령 및 표시(C&I) 메시지는 프레젠테이션 및 라이브 역할에 대한 토큰을 관리하고 디바이스에서 비디오 흐름 제어의 릴리스를 요청하여 추가 미디어 채널의 작동을 활성화하는 데 사용됩니다. Cisco Unified Communications Manager에서는 모든 C&I 메시지를 지원합니다. Cisco Unified Communications Manager에서 C&I 메시지를 받을 때마다 그에 따라 통화 상대방에게 해당 메시지를 릴레이합니다.

흐름 제어 해제 요청 및 응답 메시지를 사용하여 상대방 해제 흐름 제어를 요청할 수 있으므로 엔드 포인트는 지정된 비트 속도에 따라 지정된 채널을 보낼 수 있습니다.



참고 통화 당사자가 흐름 제어 해제 응답으로 표시된 것처럼 요청을 받거나 받지 못할 수 있습니다.

프레젠테이션 역할 토큰 메시지를 사용하여 H.239 디바이스에서 프레젠테이션을 위한 토큰을 얻을 수 있습니다. 통화 당사자는 요청을 수락 또는 거부할 수 있습니다. 프레젠테이션 디바이스는 더 이상 필요하지 않을 때 토큰 해제 메시지를 전송합니다.

토폴로지 및 프로토콜 상호 운용성 제한 사항

Cisco Unified Communications Manager는 H.323에서 H.323 통화에서 H.239만 지원합니다. Cisco Unified Communications Manager는 H.323 인터클러스터 트렁크 또는 다중 노드를 통해 H.239 통화를 설정할 수 있습니다. H.239 지원 디바이스에서 비 H.323 종료를 사용하여 전화를 걸려면 H.239 기능이 무시되고 통화가 Cisco Unified Communications Manager에서 지원하는 기존 영상 통화와 같은 방식으로 수행됩니다.

Cisco Unified Communications Manager는 미디어 터미네이션 포인트나 트랜스코더가 통화로 삽입될 때 두 번째 비디오 채널을 지원하지 않습니다. 문제가 발생하는 경우 통화가 일반 영상 통화로 대체됩니다.

통화 중 기능 제한

Cisco Unified Communications Manager는 H.323 통화에 대해 직접 H.323의 두 번째 비디오 채널 열기만 지원합니다.



주의 통화 호 전환 또는 보류/재시작 작업과 같은 통화 중 기능을 호출하지 마십시오. 이렇게 하면 문제가 발생할 수 있고 두 번째 비디오 채널의 연결이 끊어질 수 있습니다.

비디오 지원

Unified Communications Manager은 H.323, SCCP 및 SIP 프로토콜을 통해 비디오를 지원합니다.

스키니 클라이언트 제어 프로토콜 비디오

SCCP(Skinny Client Control Protocol) 비디오는 다음과 같은 특성을 보여줍니다.

- SCCP(Skinny Client Control Protocol)를 실행하는 전화기에서 비디오 기능을 보고하는 경우 다른 쪽이 비디오 채널을 지원하면 Cisco Unified Communications Manager가 비디오 채널을 자동으로 엽니다.
- SCCP(Skinny Client Control Protocol) 영상 통화의 경우 시스템 관리에서 지역을 사용하여 영상 통화 대역폭을 결정합니다. 시스템에서 사용자에게 비트 속도를 요청하지 않습니다.

SIP 비디오

SIP 비디오는 SSI(SIP 시그널링 인터페이스)를 사용하여 다음과 같은 영상 통화를 지원합니다.

- SIP에서 SIP로
- SIP에서 H.323으로
- SIP에서 SCCP로

- SIP 인터클러스터 트렁크
- H.323 트렁크
- SIP 및 H.323 트렁크의 조합

SIP 영상 통화는 비디오 회의를 위한 미디어 제어 기능도 제공합니다.

Unified Communications Manager 비디오는 비디오 시그널링을 지원하는 SIP 트렁크와 회선 모두에서 SIP를 지원합니다. SIP는 H.261, H.263+, H.264(AVC), H.264(SVC), X-H.264UC(Lync), 및 AV1 비디오 코덱(VTA가 사용하는 광대역 비디오 코덱은 지원하지 않음)을 지원합니다.



참고 엔드포인트 중 일부만 AV1 코덱을 지원합니다. 자세한 내용은 [호환성 매트릭스](#)를 참조하십시오.

영상 통화에 대한 SIP 디바이스 구성

SIP 디바이스에서 영상 통화를 활성화하려면 다음 단계를 수행합니다.

SIP 트렁크

- 비디오 연결을 사용할 수 없을 때 통화에 오디오를 사용하려면 Unified Communications Manager의 트렁크 구성 창에서 오디오로 영상 통화 재시도 확인란을 선택합니다.
- 트렁크를 재설정합니다.

타사 SIP 엔드포인트

- 비디오 연결을 사용할 수 없을 때 통화에 오디오를 사용하려면 Cisco 통합 커뮤니케이션 매니저 관리의 전화기 구성 창에서 오디오로 영상 통화 재시도 확인란을 선택합니다.
- 엔드포인트를 재설정합니다.

Cisco 화상 회의 브리지

Unified Communications Manager는 화상 회의를 위한 다양한 솔루션을 지원합니다. 다음 화상 회의 브리지는 임시 및 회의개설 화상 회의를 지원합니다.

- Cisco TelePresence MCU
- Cisco TelePresence Conductor
- Cisco Meeting Server

Cisco Telepresence MCU 화상 회의 브리지

Cisco TelePresence MCU는 Cisco Unified Communications Manager의 하드웨어 전화회의 브리지 세트입니다.

Cisco TelePresence MCU는 HD(High-Definition) 멀티포인트 비디오 컨퍼런스 브리지입니다. 초당 30 프레임, 모든 전화회의에 대한 완벽한 연속 프레즌스, 전체 트랜스코딩으로 최대 1080p를 제공하며, 혼합 HD 엔드포인트 환경에 가장 적합합니다. Cisco TelePresence MCU에는 신호 처리 통화 제어 프로토콜로 SIP가 지원됩니다. 시스템 및 전화회의의 전체 구성, 제어 및 모니터링을 수행할 수 있는 내장 웹 서버에 있습니다. Cisco TelePresence MCU는 HTTP를 통한 XML 관리 API를 제공합니다.

Cisco TelePresence MCU에서는 즉석 및 회의개설 음성/비디오 전화회의를 모두 수행할 수 있습니다. 각 컨퍼런스 브리지는 여러 개의 동시 다자간 전화회의를 호스팅할 수 있습니다. Cisco TelePresence MCU는 포트 예약 모드로 구성해야만 합니다.

Cisco TelePresence Conductor 화상 회의 브리지

Cisco TelePresence Conductor는 인텔리전트 전화회의 관리 제어 기능을 제공하며 확장 가능하므로 여러 MCU 간 로드 밸런싱 및 복수 디바이스 가용성을 위한 디바이스 클러스터링을 지원할 수 있습니다. 관리자는 Cisco UCS(Cisco Unified Computing System) 플랫폼 또는 타사 기반 플랫폼을 지원하는 VMware에 Cisco TelePresence Conductor를 어플라이언스 또는 가상화된 애플리케이션으로 구현할 수 있습니다. 동적 양방향 및 3방향 전화회의가 허용되는 다방향 전화회의도 지원됩니다.

Cisco TelePresence Conductor는 즉석 및 회의개설 음성/비디오 전화회의를 모두 지원합니다. Cisco TelePresence Conductor는 각각의 새로운 전화회의에 가장 적합한 Cisco TelePresence 리소스를 동적으로 선택합니다. 애드-혹, "미팅 시작" 및 예약된 음성 및 비디오 전화회의가 역동적으로 성장하여 개별 MCU의 용량을 초과할 수 있습니다. One Cisco TelePresence Conductor 어플라이언스 또는 Cisco TelePresence Conductor 클러스터의 시스템 용량은 30 MCU 또는 2400 MCU 포트에 달합니다. Cisco TelePresence Conductor 어플라이언스 또는 가상화된 애플리케이션은 탁월한 복원력을 제공하도록 최대 3개까지 클러스터링할 수 있습니다.

Cisco Meeting Server

이 전화회의 브리지 솔루션을 사용하면 임시, 지금 미팅, Conference Now 및 랑데부 전화회의가 가능합니다. 이 전화회의 브리지는 프레임스 기반 오디오, 비디오 및 웹 컨퍼런싱 기능을 제공하며 타사 온프레미스 인프라에서도 작동합니다. 소규모 또는 대규모 구축에 맞추어 크기가 조정됩니다. 필요에 따라 용량을 점증적으로 추가하여 조직의 현재 및 향후 요구를 지원할 수 있도록 보장할 수 있습니다. 이 전화회의 브리지는 고급 상호운용성을 제공합니다. 참가자 수에 상관 없이 다음에서 미팅을 생성하고 참여할 수 있습니다.

- Cisco 또는 타사 회의실 또는 데스크톱 비디오 시스템
- Cisco Jabber Client
- Cisco Meeting App(기본 사용 또는 WebRTC 호환 브라우저 사용 가능)
- Skype for Business

Cisco Meeting Server 2.0의 최소 릴리스에서는 Cisco Meeting Server 전화회의 브리지를 사용해야 합니다.

Cisco Meeting Server는 신호 처리 통화 제어 프로토콜로 SIP를 지원합니다. 시스템 및 전화회의의 전체 구성, 제어 및 모니터링을 수행할 수 있는 내장 웹 서버에 있습니다. Cisco Meeting Server는 HTTP를 통한 XML 관리 API를 제공합니다.



참고 Cisco Meeting Server 는 AV1 코덱을 지원하도록 향상되었으며, H.265 비디오 코덱 및 FECC(Far End Camera Control)를 지원하지 않습니다.

비디오 암호화

Unified Communications Manager는 통신에 관련된 개별 엔드포인트에서도 암호화를 지원하는 경우 오디오, 비디오 및 기타 미디어 스트림의 암호화를 지원합니다. Unified CM은 SRTP(안전한 실시간 전송 프로토콜)를 사용하여 미디어 스트림을 암호화합니다. 일부 기능은 다음과 같습니다.

- SIP 및 H.323 엔드포인트에 대한 지원
- MTP(미디어 터미네이션 포인트) 통과 모드에서 작동하는 동안 기본 오디오 및 영상 회선 암호화 지원
- 다중 암호화 방법 지원
- RFC 4568에 따라 SDP(Session Description Protocol) 암호화 제품군 세션 매개 변수에 대한 지원

암호화된 통신을 제공하기 위해 SIP 통화 설정 중에 엔드포인트와 Unified Communications Manager 간에 암호화 키가 교환됩니다. 이러한 이유로 SIP 신호 처리는 TLS를 사용하여 암호화되어야 합니다. 초기 통화 설정 중에 비디오 엔드포인트는 지원되는 암호화 방법 목록을 교환하고 두 엔드포인트에서 지원하는 암호화 그룹을 선택하고 암호화 키를 교환합니다. 엔드포인트에서 일반 암호화 그룹에 동의할 수 없는 경우, 미디어 스트림은 RTP(실시간 전송 프로토콜)를 사용하여 암호화되지 않고 전송됩니다.



참고 개별 엔드포인트에서 암호화를 지원하지 않는 경우 RTP를 사용하여 통신을 수행합니다.

VCS를 사용하여 상호 운용성 구성

Cisco VCS에 Unified Communications Manager를 연결하는 SIP 트렁크에서 다음 단계를 수행하여 Unified CM이 CISCO VCS와 상호 작용할 수 있도록 합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 트렁크.

단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 트렁크를 선택합니다.
- 새로 추가를 클릭하여 새 트렁크를 구성합니다.

단계 3 트렁크 구성 창에서 Cisco VCS에 Unified Communications Manager를 연결하는 트렁크 유형, 디바이스 프로토콜, 트렁크 서비스 유형을 선택하고 다음을 클릭합니다.

단계 4 SIP 프로파일 드롭다운 목록에서 **VCS**에 대한 표준 SIP 프로파일을 선택합니다.

단계 5 정규화 스크립트 드롭다운 목록에서 **vcs-interop**를 선택합니다.

단계 6 정규화 스크립트 영역에서 매개 변수 이름 및 매개 변수 값 필드를 비워 둡니다. 이러한 필드에 값이 채워져 있으면 필드의 내용을 삭제합니다.

단계 7 저장을 클릭합니다.

비디오 기능

SIP 비디오 네트워크에서는 다음과 같은 비디오 관련 기능이 지원됩니다.

- BFCP(Binary Floor Control Protocol)
- 암호화된 iX 채널
- FECC(Far End Camera Control)

Binary Floor Control Protocol에 대한 엔드포인트 지원

Unified Communications Manager 특정 Cisco 및 타사 비디오 엔드포인트에 대한 BFCP(Binary Floor Control Protocol)에 대한 지원을 제공합니다. BFCP를 사용하면 사용자가 진행 중인 비디오 대화 내에서 프레젠테이션을 공유할 수 있습니다.

자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서](#)에서 BFCP를 사용하여 프레젠테이션 공유 구성 장을 참조하십시오.

암호화된 iX 채널

Unified Communications Manager에서는 암호화된 iX 채널을 지원합니다. iX 채널은 비디오 전화회의에서 SIP 전화기 간의 멀티플렉싱 애플리케이션 미디어에 대한 신뢰할 수 있는 채널을 제공합니다. 암호화된 iX 채널은 DTLS를 사용하여 구축에 보안을 추가하고, 애플리케이션 미디어가 iX 채널을 통해 전송되도록 하고, 미디어를 가로채려고 시도하는 중간 상대방이 볼 수 없도록 합니다.

통과 모드의 IOS MTP 및 RSVP 에이전트에서도 암호화된 iX 채널을 지원합니다.

구성

Unified Communications Manager에서 암호화된 iX 채널을 활성화하려면 다음을 수행해야 합니다.

- 모든 중간 SIP 트렁크에서 사용하는 SIP 프로파일 구성에서 **IX** 애플리케이션 미디어 허용 확인란을 선택합니다. 이 설정은 iX 채널 협상을 켭니다.
- 보안 잠금 아이콘을 활성화하려면 보안 통화 아이콘 표시 정책 서비스 매개 변수를 구성합니다. 기본적으로 이 설정은 **BFCP** 및 **IX** 전송을 제외한 모든 미디어를 암호화 해야 합니다.

암호화 모드

SDP(Session Description Protocol)는 두 가지 유형의 세션 설명 프로토콜로, Unified Communications Manager 암호화된 전화에 대한 iX 채널 암호화를 지원합니다. 이 암호화 유형은 엔드포인트에서 지원하는 항목에 따라 결정되며 Unified Communications Manager에서 구성할 수 있는 항목은 아닙니다.

- 모범 사례 암호화 — SDP 오픈은 암호화된 iX 채널을 위한 것이지만 SIP 피어가 지원하지 않으면 암호화되지 않은 iX 채널로 폴백합니다. 이 방법은 솔루션에서 암호화가 필수가 아닌 경우에 사용할 수 있습니다.

예를 들어, 암호화는 클라우드 내에서 필수이며 단일 엔터프라이즈가 아닙니다.

최선의 노력 iX 암호화

```
m=application 12345 UDP/UDT/iX *
```

```
a=setup:actpass
```

```
a=fingerprint: SHA-1 <key>
```

- 강제 암호화 — SDP 제공은 암호화된 iX 채널만을 위한 것입니다. SIP 피어에서 iX 채널 암호화를 지원하지 않는 경우에는 이 제공이 거부됩니다. 이 방법은 엔드포인트 간에 암호화가 필수적인 구축에 사용될 수 있습니다.

예를 들어, 두 SIP 디바이스 간에 암호화가 필수적입니다.

강제 iX 암호화

```
m=application 12345 UDP/DTLS/UDT/iX *
```

```
a=setup:actpass
```

```
a=fingerprint: SHA-1 <key>
```

기본적으로 모든 Cisco IP 전화기는 최상의 iX 암호화를 제공하도록 설정됩니다. 그러나 Cisco TelePresence 엔드포인트의 제품별 구성 내에서 암호화 모드를 켜기로 설정하거나 Cisco Meeting 서버의 설정을 재구성하여 이를 강제 암호화로 재설정할 수 있습니다.

비 암호화 모드

Unified Communications Manager에서는 엔드포인트를 완전 보안 모드로 구축하지 않을 수 있는 경우 미팅의 엔드포인트에서 미디어 경로에 있는 보안 활성 제어 메시지를 협상할 수 있습니다. 예를 들어, 엔드포인트는 오프 넷이고 모바일 및 원격 액세스 모드에서 Unified CM에 등록되어 있습니다.

사전 요구 사항

이 기능을 사용하기 전에 다음 사항을 확인하십시오.

- 시스템이 수출 규정 준수 요구 사항을 준수하는지 여부
- 전화회의 브리지에 대한 SIP 트렁크 보안

Unified CM은 비보안 엔드포인트 또는 스마트폰에 대해 보안 활성 제어 메시지의 DTLS 정보를 협상하고 다음 방법으로 메시지를 받을 수 있습니다.

- 온프레미스 등록 엔드포인트 또는 스마트폰에 대한 최고의 암호화 **iX**
- 오프프레미스 등록 엔드포인트 또는 스마트폰에 대한 강제 **iX** 암호화

중단 카메라 제어 프로토콜 지원

FECC(Far End Camera Control) 프로토콜을 사용하면 원격 카메라를 제어할 수 있습니다. 영상 통화 내에서 FECC는 통화의 한 상대방이 다른 상대방의 카메라를 제어하는 것을 허용합니다. 이 컨트롤에는 카메라를 한 쪽에서 다른 쪽으로 이동하거나, 카메라를 기울이거나, 확대/축소하는 기능이 포함될 수 있습니다. 여러 카메라를 사용하는 화상 회의의 경우 FECC를 사용하여 한 카메라에서 다른 카메라로 전환할 수 있습니다.

Unified Communications Manager는 FECC를 지원하는 비디오 엔드포인트에 대한 FECC 프로토콜을 지원합니다. Cisco Unified Communications Manager는 SIP-SIP 통화 또는 H.323-H.323 통화에 대한 FECC를 지원 하지만 SIP-H.323 통화에 대한 FECC는 지원하지 않습니다. FECC를 지원하려면 Unified Communications Manager는 SIP 또는 H.323 신호 처리를 통해 애플리케이션 미디어 채널을 설정합니다. 미디어 채널이 설정되면 개별 엔드포인트에서 FECC 신호 처리를 전달할 수 있습니다.

비디오 네트워크에 대한 QoS

Cisco Unified Communications Manager에는 비디오 네트워크에 대한 QoS(서비스 품질)를 관리하기 위한 여러 가지 관리 도구가 포함되어 있습니다.

- 대역폭 관리 — 특정 지역 및 위치에 대한 대역폭 할당을 관리합니다.
- 고급 위치 기반 통화 허용 제어
- 세션 수준 대역폭 한정자
- 유연한 DSCP 표시
- 대체 라우팅

대역폭 관리

음성 및 영상 통화에 대한 대역폭 할당은 Cisco Unified Communications Manager 관리에서 구성하는 지역 및 위치를 통해 관리됩니다.

특정 통화에 사용할 수 있는 대역폭의 양은 음성, 비디오, 신호 처리 및 BFCP 프레젠테이션과 같은 추가 미디어를 포함하여 세션과 연결된 모든 미디어 스트림의 조합을 관리할 수 있어야 합니다. Cisco Unified Communications Manager는 대역폭을 관리할 수 있는 기능을 포함합니다.

고급 위치 기반 통화 허용 제어

향상된 위치 CAC(Call Admission Control)를 사용하면 해당 링크에서 동시에 허용되는 통화 수를 제한함으로써 광역(IP WAN) 링크를 지나는 통화의 오디오와 비디오 품질을 제어할 수 있습니다. 예를

들어, 통화 허용 제어를 사용하여 기본 캠퍼스와 원격 사이트를 연결하는 56 kb/s 프레임 릴레이 회선의 음성 품질을 조정할 수 있습니다.

CAC는 통화를 완료하는 데 충분한 대역폭을 사용할 수 있는지 확인합니다. CAC는 대역폭이 부족하여 통화를 거부할 수 있습니다.

Unified Communications Manager에서 위치 기반 통화 콜수락 제어(CAC)는 지역과 함께 작동하여 네트워크 링크의 특성을 정의합니다. 지역 및 위치는 다음과 같은 방식으로 작동합니다.

- 지역을 통해 영상 통화의 대역폭을 설정할 수 있습니다. 지역에서 오디오를 제한하면 더 높은 비트 속도로 코덱을 필터링할 수 있습니다. 그러나 영상 통화의 경우 비디오를 제한하면 비디오의 품질(해상도 및 전송률)이 제약을 받습니다.
- 위치는 해당 링크의 모든 통화에 사용할 수 있는 총 대역폭의 양을 정의합니다. 링크에서 전화를 건 경우, 해당 링크에 허용되는 총 대역폭에서 해당 통화에 대한 지역 값을 빼야 합니다.

콜수락 제어(CAC)에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 '향상된 위치 콜수락 제어(CAC) 구성'을 참조하십시오.

세션 수준 대역폭 한정자

Unified Communications Manager는 세션 수준 대역폭 한정자를 처리하기 위한 위치 통화 허용 제어 지원을 제공합니다. 세션 수준 대역폭 한정자는 초기 SIP 신호 처리의 SDP 부분에 있는 매개 변수의 일부로 전달됩니다. 이러한 매개 변수는 각 엔드포인트에서 해당 통화 유형에 대해 지원하는 최대 대역폭 양을 나타냅니다. 이러한 매개 변수는 지역 및 위치 설정과 함께 사용되어 각 통화에 대한 대역폭을 설정합니다.

초기 통화 설정 중에 두 상대방이 통화 허용되는 최대 대역폭으로 Unified Communications Manager와 통신합니다. Unified Communications Manager가 통신을 다른 엔드포인트에 전달하지만 엔드포인트에서 지정하는 대역폭이 지역 설정보다 큰 경우에는 Unified Communications Manager가 해당 값을 지역 대역폭 값으로 대체합니다.

Unified Communications Manager에서는 특정 통화에 할당할 대역폭의 양을 결정하는 데 다음 규칙을 사용합니다.

- Unified Communications Manager가 엔드포인트에서 제공 또는 응답을 수신하는 경우 SDP에 세션 수준 대역폭 한정자가 있는지 확인합니다.
 - 세션 수준 대역폭 한정자가 있는 경우 Unified Communications Manager는 한정자에서 대역폭 값을 검색합니다. 둘 이상의 한정자 형식이 있는 경우, 기본 설정 순서인 TIAS(Transport Independent Application Specific), AS(Application Specific) 및 CT(Conference Total) 순으로 한정자를 검색합니다.
 - 세션 수준 대역폭 한정자가 없는 경우 Unified Communications Manager는 미디어 수준 대역폭 한정자의 합계에서 대역폭 값을 검색합니다.
- 할당된 대역폭은 두 엔드포인트가 최대 지역 설정 값까지 원하는 최대값입니다. 할당된 대역폭은 지역 설정을 초과할 수 없습니다.

Unified Communications Manager 엔드포인트와 통신할 때 다음 논리를 사용합니다.

- 둘 이상의 세션 수준 대역폭 한정자 유형(TIAS, AS, CT)을 포함하는 엔드포인트에 대한 Answer, Early Offer 또는 Re-Invite Offer를 생성할 때 Unified Communications Manager는 각각에 대해 동일한 대역폭 값을 사용합니다.
- 응답을 생성할 때 Unified Communications Manager는 초기 오퍼에서 수신된 것과 동일한 세션 수준 대역폭 한정자 유형(TIAS, CT, AS)을 사용합니다.
- 이전 버전과의 호환성을 위해, Unified Communications Manager는 영상 통화가 보류 중으로 설정되고 MOH(대기 중 음악)가 삽입되면 이전에 세션 수준 대역폭 한정자를 표시하지 않습니다.

SIP 전화기에 대한 비디오 해상도 지원

Cisco Unified Communications Manager는 고해상도 영상 통화를 위해 SIP 헤더의 SDP 부분에서 imageattr 회선을 지원합니다. 9951, 9971 및 8961과 같은 w360p(640 x 360)를 지원하는 Cisco SIP 전화기는 다음 기준에 따라 자동으로 영상 통화에 대한 최적 해상도를 선택합니다.

- 세션 수준 대역폭이 800Kb/s보다 크고, imageattr[640 x 480] 회선이 SDP에 있는 경우 VGA가 사용됩니다.
- 세션 수준 대역폭이 800Kb/s보다 크고 imageattr[640 x 480] 회선이 SDP에 없는 경우 w360p가 사용됩니다.
- 세션 수준 대역폭이 800Kb/s 미만이지만 초당 480비트 보다 크고 imageattr[640 x 480] 회선이 있는 경우에는 초당 VGA 15 프레임이 사용됩니다.



참고 현재 Cisco IP 전화기 모델 9951, 9971 또는 8961을 w360p(640 x 360) 비디오 해상도를 지원하고 Cisco Unified Communications Manager 릴리스 8.5(1) 이상으로 업그레이드하는 경우에는 영상 통화 해상도가 변경될 수 있습니다. W360p 해상도는 전화기 로드 9.2(1)에서 도입되었습니다.

다음 영상 통화 흐름은 imageattr 회선 지원 없이 2개의 9951 전화기(전화기 A와 전화기 B) 사이에 있습니다(예: Cisco Unified Communications Manager 릴리스 8.0(1) 및 이전 버전 사용).

1. 전화기 A가 SDP에서 imageattr 회선을 사용하여 SIP 메시지를 보냅니다.
2. Cisco Unified Communications Manager는 SDP에서 imageattr 회선을 삭제한 다음 수정된 SIP 메시지를 전화기 B로 보냅니다.
3. SIP 헤더의 SDP 부분에 imageattr 회선이 없으므로 전화기 B가 w360p 해상도로 비디오를 보내려고 시도합니다.

다음 영상 통화 흐름은 imageattr 회선 지원 없이 2개의 9951 전화기(전화기 A와 전화기 B) 사이에 있습니다(예: Cisco Unified Communications Manager 릴리스 8.5(1) 이상).

1. 전화기 A에서 imageattr 회선을 사용하여 SIP 메시지를 SDP에 보냅니다.

2. Cisco Unified Communications Manager는 imageattr 회선을 삭제하지 않고 SIP 메시지를 전화기 B로 보냅니다.
3. 전화기 B가 VGA 해상도로 비디오를 보내려고 시도합니다.

대체 라우팅

엔드포인트에서 영상 통화에 필요한 대역폭을 가져올 수 없는 경우 영상 통화는 기본 동작에 대한 오디오 통화로 다시 시도됩니다. 라우트/헌트 목록 또는 AAR(자동 대체 라우팅) 그룹을 사용하여 이러한 영상 통화에 대해 다른 경로를 시도하려면 해당하는 게이트웨이, 트렁크 및 전화기에 대한 구성 설정에서 음성으로 영상 통화 재시도 설정을 선택 취소합니다.

자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서](#)의 통화 라우팅 구성 장 아래에 있는 AAR 그룹 구성 섹션을 참조하십시오.

유연한 DSCP 표시

DSCP(Differentiated Services Code Point) 패킷 표시는 각 패킷에 대한 서비스 클래스를 지정하는 데 사용됩니다. DSCP 표시를 사용하면 다른 유형보다 특정 유형의 통화 또는 미디어에 높은 우선 순위를 지정할 수 있습니다. 예를 들어, 네트워크 대역폭 문제가 발생하더라도 오디오 통화는 대역폭 문제가 발생하지 않도록 비디오보다 오디오에 높은 우선 순위를 지정할 수 있습니다.

다음 방법 중 하나를 수행하여 DSCP 표시를 사용자 정의할 수 있습니다.

- 클러스터 수준 서비스 매개 변수를 구성하여 클러스터에 대한 기본 DSCP 설정을 설정합니다.
- (선택 사항) DSCP 범주의 하위 집합인 경우 SIP 프로파일을 통해 디바이스에 사용자 정의된 DSCP 설정을 할당할 수 있습니다. 프로파일을 사용하는 디바이스의 경우 사용자 정의된 설정이 서비스 매개 변수 기본값보다 우선합니다.

DSCP 표시를 구성하는 방법에 대한 자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서](#)의 '유연한 DSCP 표시 및 비디오 프로모션 구성' 장을 참조하십시오.

영상 통화에 대한 전화기 구성

비디오 사용 디바이스에 대한 다음 설정은 영상 통화에 영향을 미칩니다.

- 영상 통화를 음성으로 재시도 - 기본적으로 이 확인란은 선택된 상태로 유지됩니다. 따라서 엔드포인트(전화기, 게이트웨이, 트렁크)에서 영상 통화에 필요한 대역폭을 가져올 수 없는 경우 통화 제어는 통화를 음성 통화로 재시도합니다. 이 설정은 영상 통화의 대상 디바이스에 적용됩니다.
- 비디오 기능 활성화됨/비활성화됨 - 이 드롭다운 목록 상자는 비디오 기능을 설정 및 해제합니다.

화상 회의를 위한 전화회의 제어

Unified Communications Manager 는 다음과 같은 전화회의 제어 기능을 지원합니다.

- 등록 명부/참석자 목록
- 참가자 삭제
- 전화회의 종료
- 전화회의 사회자/컨트롤러 표시
- 연속 참가

Unified Communications Manager 에서는 다음과 같은 SCCP(Skinny Client Control Protocol) 전화기용 화상 회의 기능도 지원합니다.

- 화상 회의를 위한 컨트롤을 표시합니다. SCCP 전화기에서는 연속 참가 또는 음성 활성화 모드를 사용하여 화상 회의를 볼 수 있습니다. 모드를 선택하면 브리지로 메시지가 전송되어 비디오 채널에서 사용할 모드를 표시합니다. 모드 간 전환을 위해 미디어를 재협상할 필요가 없습니다.
- 비디오 스트림의 사용자 이름과 같은 참가자 정보를 표시합니다. 시스템은 등록 명부와 같은 다른 전화회의 기능에 참가자 정보를 사용할 수 있습니다.

자세한 내용은 [Cisco 통합 커뮤니케이션 매니저 보안 설명서](#)의 '암호화된 iX 채널' 장을 참조하십시오.

비디오 전화 통신 및 Cisco 통합 서비스 가용성

Cisco 통합 서비스 가용성은 성능 모니터링 카운터, 비디오 브리지 카운터 및 CDR(통화 세부 정보 레코드)를 업데이트하여 영상 통화 및 전화회의를 추적합니다.

성능 카운터

비디오 전화 통신 이벤트는 다음과 같은 Cisco 통합 서비스 가용성 성능 모니터링 카운터를 업데이트합니다.

Cisco CallManager

- VCBConferenceActive
- VCBConferenceCompleted
- VCBConferenceTotal
- VCBOutOfConferences
- VCBOutOfResources
- VCBResourceActive
- VCBResourceAvailable

- VideoCallsActive
- VideoCallsCompleted
- VideoOutOfResources

Gatekeeper

- VideoOutOfResources

CiscoH.323

- VideoCallsActive
- VideoCallsCompleted

Cisco 위치

- RSVP VideoCallsFailed
- RSVP VideoReservationErrorCounts
- VideoBandwidthAvailable
- VideoBandwidthMaximum
- VideoOutOfResources

Cisco SIP

- VideoCallsActive
- VideoCallsCompleted

Cisco 화상 회의 브리지

- ConferencesActive
- ConferencesAvailable
- ConferencesCompleted
- ConferencesTotal
- OutOfConferences
- OutOfResources
- ResourceActive
- ResourceAvailable
- ResourceTotal

비디오 브리지 카운터

화상 회의 이벤트로 인해 다음 Cisco 화상 회의 브리지 성능 모니터링 카운터가 업데이트됩니다.

- ConferencesActive
- ConferencesAvailable
- ConferencesCompleted
- ConferencesTotal
- OutOfConferences
- OutOfResources
- ResourceActive
- ResourceAvailable
- ResourceTotal

이러한 카운터는 VCB 접두사를 사용하여 Cisco Unified Communications Manager 개체에 표시됩니다.

CDR(Call Detail Record)

비디오 전화 통신 이벤트가 발생하면 Cisco 통합 서비스 가용성에서 CDR(통화 세부 정보 레코드)이 업데이트됩니다. 이러한 CMR에는 다음 정보가 포함됩니다.

- origVideoCap_Codec
- origVideoCap_Bandwidth
- origVideoCap_Resolution
- origVideoTransportAddress_IP
- origVideoTransportAddress_Port
- destVideoCap_Codec
- destVideoCap_Bandwidth
- destVideoCap_Resolution
- destVideoTransportAddress_IP
- destVideoTransportAddress_Port
- origRSVPStat
- destRSVPVideoStat
- origVideoCap_Codec_Channel2
- origVideoCap_Bandwidth_Channel2

- origVideoCap_Resolution_Channel2
- origVideoTransportAddress_IP_Channel2
- origVideoTransportAddress_Port_Channel2
- origVideoChannel_Role_Channel2
- destVideoCap_Codec_Channel2
- destVideoCap_Bandwidth_Channel2
- destVideoCap_Resolution_Channel2
- destVideoTransportAddress_IP_Channel2
- destVideoTransportAddress_Port_Channel2
- destVideoChannel_Role_Channel2

통화 관리 기록(CMR)

비디오 전화 통신 이벤트는 Cisco 통합 서비스 가용성에서 CMR(통화 관리 레코드)에 대한 업데이트를 발생시킵니다. 이러한 CMR에는 다음 정보가 포함됩니다.

- videoContentType 텍스트 문자열
- videoDuration 정수
- numberVideoPacketsSent 정수
- numberVideoOctetsSent 정수
- numberVideoPacketsReceived 정수
- numberVideoOctetsReceived 정수
- numberVideoPacketsLost 정수
- videoAverageJitter 정수
- videoRoundTripTime
- videoOneWayDelay
- videoTransmissionMetrics



XVII 부

비상 통화 라우팅 규정

- [미국 연방 통신 위원회\(FCC\) 비상 통화 라우팅 규정, 957 페이지](#)



75 장

미국 연방 통신 위원회(FCC) 비상 통화 라우팅 규정

- 비상 통화 라우팅 규정 개요, 957 페이지
- 비상 통화 라우팅 규정 구성, 959 페이지

비상 통화 라우팅 규정 개요

비상 통화 라우팅 규정은 긴급 통화(911)가 미국 및 비 미국 시간대에서 구성되고 라우팅되는 방법에 대한 미국 FCC 법규를 준수하는 정보를 제공합니다.

미국 FCC는 긴급 서비스를 위한 전국적이고 원활한 통신 인프라의 신속한 배치를 장려하고 가능하게 함으로써 공공 안전을 완화하기 위해 다음 법률에 서명했습니다.

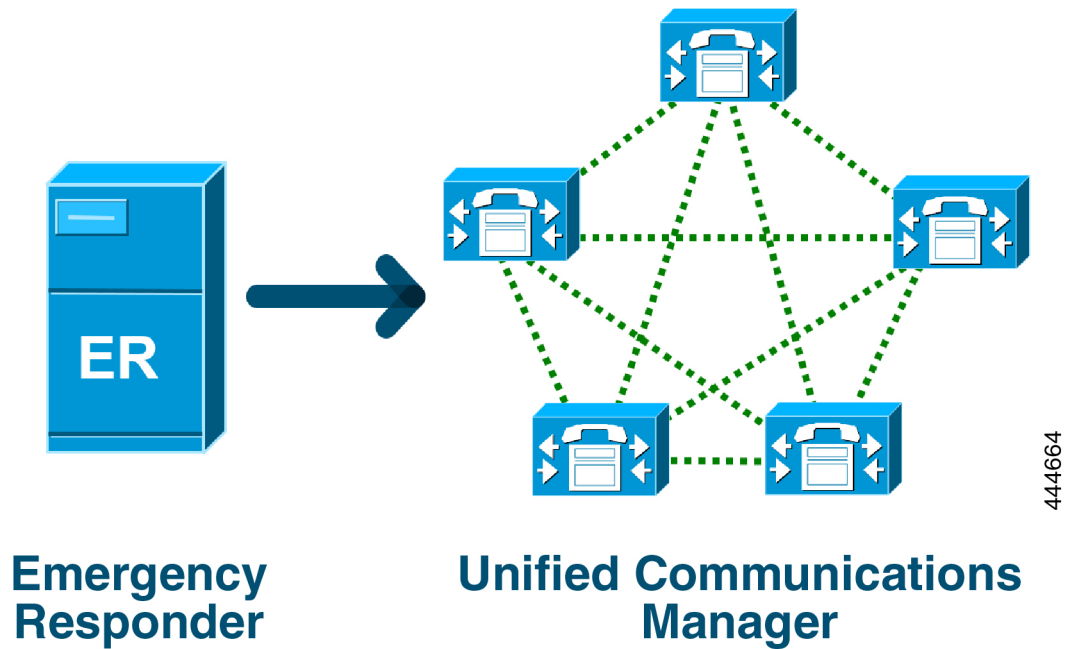
미국 FCC는 긴급 통화(911) 라우팅에 대한 다음 법률에 서명했습니다.

- Kari 법 —이 법률은 사무실 건물, 캠퍼스 및 호텔과 같은 환경에서 사용자에게 서비스를 제공하는 MLTS(다중 회선 전화 시스템)에 적용됩니다. FCC는 MLTS가 사용자가 긴급 전화가 이루어질 때 전화 번호 외부 회선에 도달하고 프런트 데스크나 보안 사무소에 통보하지 않고 911에 직접 전화할 수 있도록 할 것을 요구합니다.
- Ray Baum 법 —Ray Baum 법 506조에 따라 911 콜센터가 발신자의 위치를 자동으로 수신하고 구조원을 더 빨리 보낼 수 있도록 사용하는 기술 플랫폼에 관계 없이 긴급 호출과 함께 위치 정보(거리 주소, 건물 번호, 층 번호, 객실 번호)를 발송합니다.

FCC 법률에 대한 자세한 내용은 <https://www.fcc.gov/mlts-911-requirements>의 내용을 참조하십시오.

긴급 구조원은 지역 조례에 따라 모든 비상 통화를 대응하고 처리하기 위해 전화 네트워크의 통화를 효과적으로 관리합니다. 또한 위치 정보를 전송하고 Unified Communications Manager에게 알람을 전송합니다.

다음 그림은 긴급 구조원과 Unified Communications Manager 간의 연결을 보여줍니다.

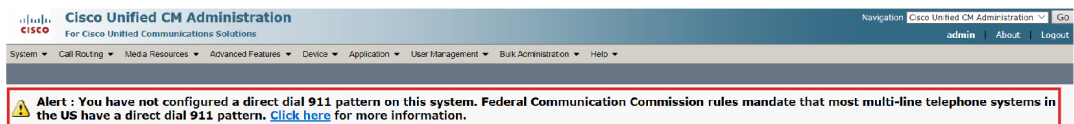


Cisco Emergency Responder에 대한 자세한 내용은 [Cisco Emergency Responder 관리 지침서](#)의 내용을 참조하십시오.

MLTS로서의 Unified Communications Manager

Cisco Unified Communications Manager 관리는 미국 표준 시간대에 설치된 시스템에 대한 직접 911 다이얼 패턴이 없음을 감지하는 소프트웨어가 내장된 MLTS입니다.

911 라우트 패턴이 활성화되지 않은 경우 Cisco Unified CM 관리 홈 페이지에 경고 메시지가 표시됩니다. 이 시스템에서 직접 다이얼 **911** 패턴을 구성하지 않았습니다. 연방 통신위원회 규정에 따르면 미국의 대부분의 다중 회선 전화 시스템은 직통 **911** 패턴을 사용합니다.



FCC 법률이 적용되지 않는 미국 이외의 시간대에 시스템이 설치된 경우 Unified Communications Manager에서 긴급 통화 라우팅 규정 구성 페이지가 비활성화됩니다.



참고 사용자는 법률 고문과 함께 FCC 법률의 적용 가능성에 대해 논의하고 시스템에서 확인해야 합니다.

비상 통화 라우팅 규정 구성

이 법률을 준수하는 직통 911 라우트 패턴을 승인하고 구성하기 위해 Unified Communications Manager에 구성된 비상 통화 라우팅 규정입니다.

시작하기 전에

향후 참조를 위해 FCC 법률을 수락 및 구성한 후에는 반드시 백업해야 합니다.

프로시저

단계 1 비상 통화 라우팅 규정 창에 액세스하려면 다음 중 하나를 수행합니다.

- Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 고급 기능 > 비상 통화 라우팅 규정
- 알림에서 사용할 수 있는 링크를 클릭하여 홈 페이지에 911 라우트 패턴을 구성합니다.

단계 2 상기 알림을 읽었으며 법률 고문과 논의해 제게 적용되는 의무를 확인했습니다 확인란을 선택하여 알림을 승인합니다.

단계 3 **911** 구성 페이지로 이동 확인란을 선택하고 제출을 클릭하여 FCC 법률을 적용할 수 있는 경우 직접 911 알림을 설정합니다. 라우트 패턴 구성 창으로 이동하면 기본적으로 패턴 정의 섹션에 911 패턴이 구성되어 있습니다.

단계 4 구성된 패턴에 대한 게이트웨이/라우트 목록 드롭다운 목록에서 적절한 게이트웨이, 라우트 또는 트링크를 선택합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

참고 FCC 법률이 적용되지 않는 미국 표준 시간대에 시스템을 설치한 경우에는 법률을 확인하고 비상 통화 라우팅 규정 창에서 **911** 의무에 관한 추가 알림 비활성화 확인란을 선택하고 제출을 클릭하여 911 알림을 비활성화합니다.

법률이 적용되지 않는 경우 관리자는 향후 업그레이드 및 911 라우트 패턴의 새 설치에 대한 알림을 포기합니다.

구성된 설정은 향후 업그레이드를 위해 보존됩니다. 홈 페이지에서 알림이 사라지고 비상 통화 라우팅 규정 창이 비활성화됩니다.

업그레이드 중에 시스템에서 이미 911 라우트 패턴을 생성했거나 표준 시간대가 미국 이외의 시간대로 변경되면 승인 페이지가 회색으로 표시됩니다.

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.