

Cisco Meeting Server Spaces에서 DTMF 시퀀스 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1. dtmfProfile 개체를 만들고 전역으로 적용합니다.](#)

[2. DTMF 작업을 수행할 수 있는 권한을 세부적으로 조정합니다.](#)

[특정 스페이스에서만 작업 허용](#)

[비밀번호가 있는 사용자만 작업 수행 허용](#)

[관련 정보](#)

소개

이 문서에서는 사용자가 Cisco Meeting Server(CMS) 스페이스에서 작업을 수행할 수 있도록 DTMF 시퀀스를 구성하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 회의 서버
- DTMF

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 3.8을 실행하는 Cisco Meeting Server

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

CMS에서 공간 참가자가 공간과 해당 참가자에게 영향을 주는 작업을 호출하는 데 사용할 사용자 지정 DTMF 시퀀스를 정의할 수 있습니다. 예를 들어, DTMF 시퀀스를 사용하면 참가자가 자신의 오디오 음소거 전환, 모임 스트리밍 시작/중지 또는 모임 종료를 수행할 수 있습니다.

dtmfProfile은 사용 가능한 각 특정 작업을 호출하는 데 사용할 DTMF 시퀀스를 정의합니다. CMS API를 통해 시스템/프로파일에 dtmfProfile을 할당하면 DTMF 시퀀스가 전역적으로 사용 가능해집니다. DTMF 작업에 대한 제한은 각 작업에 대한 권한이 다른 callLegProfiles를 만들고 API의 다른 수준에 적용하여 세부적으로 조정할 수 있습니다.

구성

1. dtmfProfile 개체를 만들고 전역으로 적용합니다

dtmfProfile 객체를 생성하려면 다음을 수행합니다.

1. CMS 웹 관리 페이지에 로그인합니다.
2. 구성 > API로 이동합니다.
3. /api/v1/dtmfProfiles 섹션으로 이동하여 확장합니다.
4. 신규 생성을 클릭합니다.



5. 필요한 작업을 수행하는 데 사용할 DTMF 시퀀스를 정의합니다. 이 예에서는 toggleMuteSelfAudio 및 endCall 작업에 대해 DTMF 시퀀스가 정의됩니다.

- 4. dtmfProfile 설정에서 선택을 클릭하고 이전에 생성한 개체를 선택합니다.
- 5. 수정을 클릭합니다.

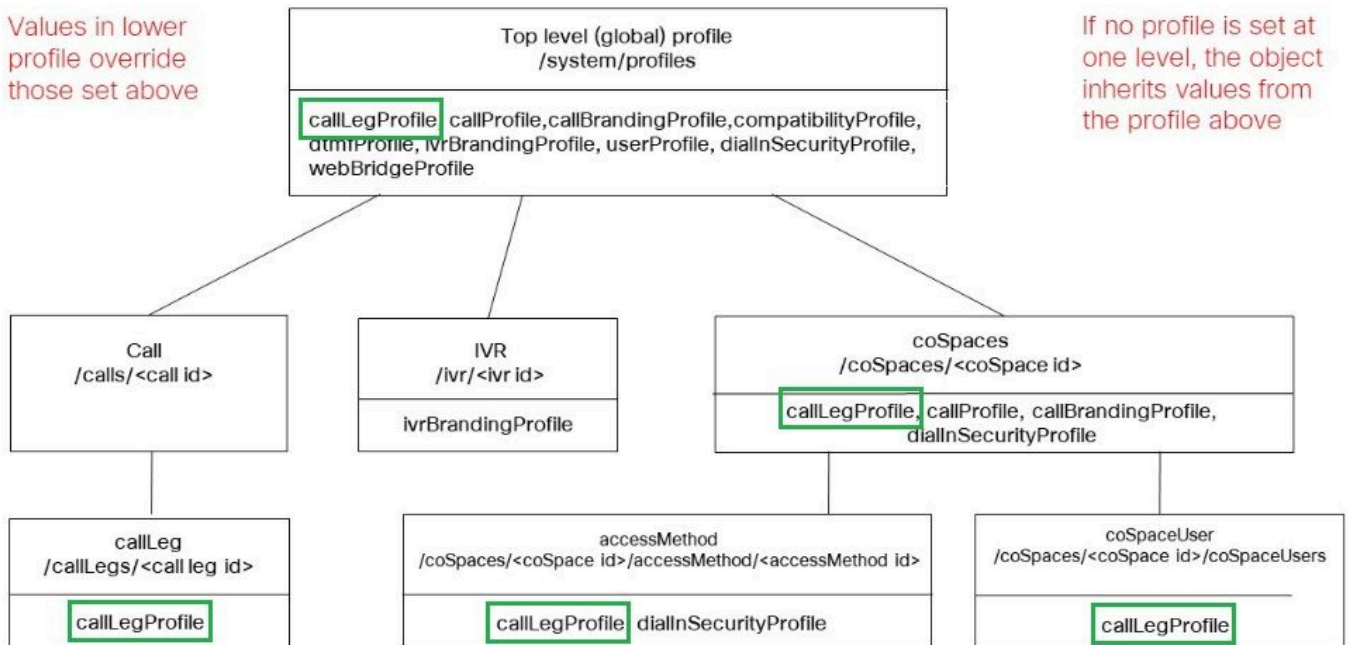
/api/v1/system/profiles

callLegProfile	<input type="checkbox"/>	<input type="text"/>	Choose
callProfile	<input type="checkbox"/>	<input type="text"/>	Choose
dtmfProfile	<input checked="" type="checkbox"/>	85e509af-bab5-4ff4-bbe1-94cb99ac80cf	Choose
userProfile	<input type="checkbox"/>	<input type="text"/>	Choose
ivrBrandingProfile	<input type="checkbox"/>	<input type="text"/>	Choose
callBrandingProfile	<input type="checkbox"/>	<input type="text"/>	Choose
compatibilityProfile	<input type="checkbox"/>	<input type="text"/>	Choose
dialInSecurityProfile	<input type="checkbox"/>	<input type="text"/>	Choose
lobbyProfile	<input type="checkbox"/>	<input type="text"/>	Choose
webBridgeProfile	<input type="checkbox"/>	<input type="text"/>	Choose

Modify

2. DTMF 작업을 수행할 수 있는 권한을 세부적으로 조정합니다.

DTMF 작업을 실행하기 위한 권한을 세부적으로 제어할 수 있습니다. callLegProfiles를 구성하면 됩니다. 이 프로파일은 API의 여러 레벨에 적용할 수 있습니다. 이 다이어그램은 가능한 모든 레벨을 보여줍니다.



callLegProfile이 적용되는 수준에 따라 범위가 결정됩니다. 더 낮은 레벨에서 할당된 프로파일은 위에 설정된 프로파일을 재정의합니다. 이러한 예는 이 원리를 사용하여 특정 스페이스 또는 사용자에게만 DTMF 작업을 호출하는 것을 허용하는 방법을 보여줍니다.

특정 스페이스에서만 작업 허용

DTMF 작업을 실행하기 위한 권한을 무효화하는 callLegProfile을 /시스템/프로필 수준에서 만들고 적용할 수 있습니다. 그런 다음 작업을 허용하는 다른 callLegProfile을 coSpace 수준에서 만들고 적용할 수 있으므로 권한 범위가 특정 coSpace(또는 coSpaces 집합(여러 개에 적용되는 경우)로 제한됩니다.

1. 구성 > API로 이동합니다.
2. /api/v1/callLegProfiles 섹션으로 이동하여 확장합니다.
3. 새로 만들기를 클릭합니다.

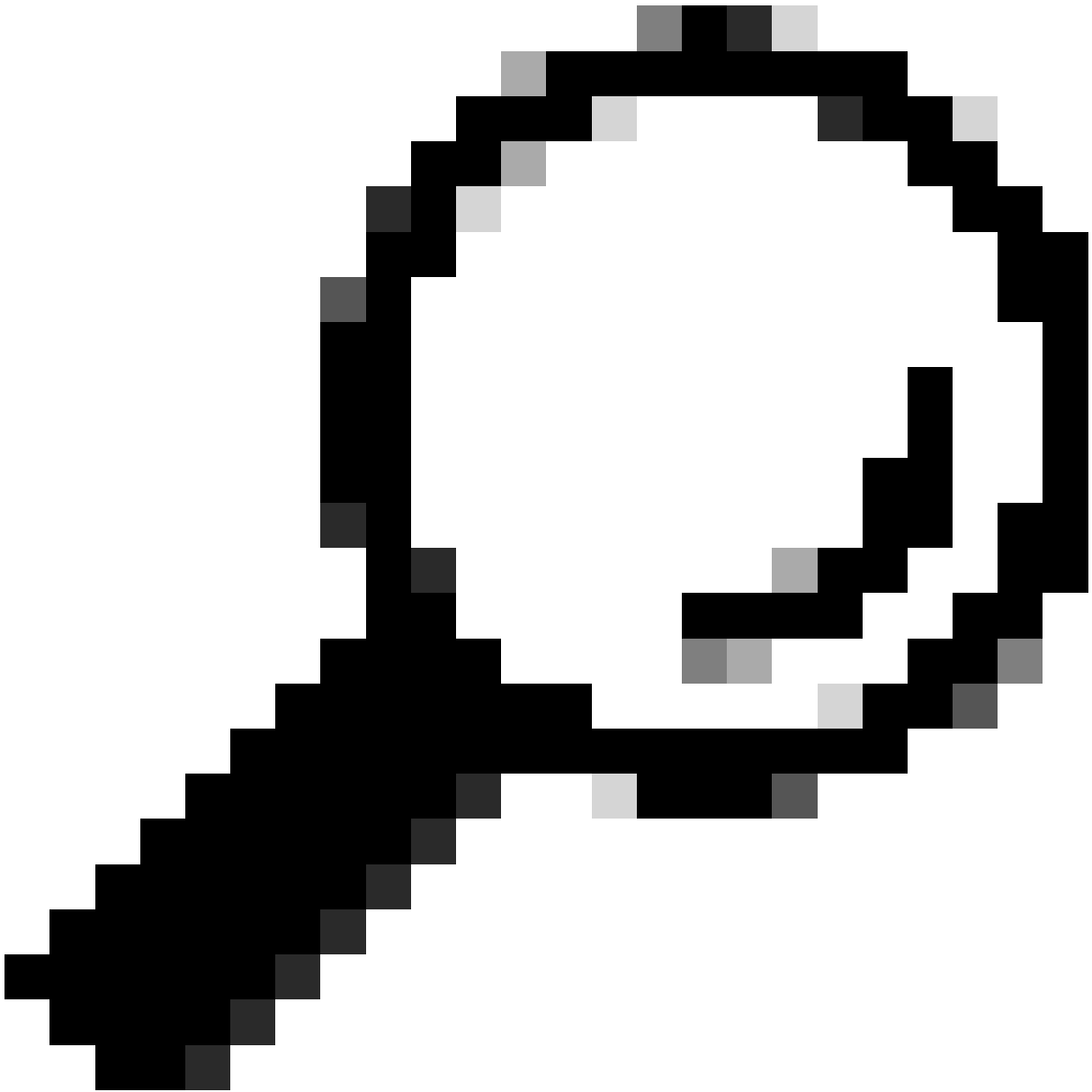


4. 허용되지 않아야 할 조치를 탐색하고 이를 거짓으로 설정합니다.
5. 생성을 클릭합니다.

이 예에서는 endCallAllowed를 false로 설정하여 회의 종료를 허용하지 않도록 callLegProfile을 만들었습니다.

/api/v1/callLegProfiles

needsActivation	<input type="checkbox"/>	<unset> ▼
defaultLayout	<input type="checkbox"/>	<unset> ▼
participantLabels	<input type="checkbox"/>	<unset> ▼
presentationDisplayMode	<input type="checkbox"/>	<unset> ▼
presentationContributionAllowed	<input type="checkbox"/>	<unset> ▼
presentationViewingAllowed	<input type="checkbox"/>	<unset> ▼
endCallAllowed	<input checked="" type="checkbox"/>	false ▼
disconnectOthersAllowed	<input type="checkbox"/>	<unset> ▼



팁: 적합한 callLegProfile이 이미 있는 경우 새 callLegProfile을 만드는 대신 수정할 수 있습니다.

6. 작업을 전역적으로 허용하지 않도록 시스템/프로필에 할당합니다.

/api/v1/system/profiles

callLegProfile	<input checked="" type="checkbox"/>	e3aad583-491f-4c32-8d77-aa479388fc89	Choose
callProfile	<input type="checkbox"/>		Choose

7. 새 callLegProfile을 생성합니다. 이번에는 작업을 허용합니다. 이 예에서는 endCallAllowed가 true로 설정된 callLegProfile이 생성되었습니다.

/api/v1/callLegProfiles

needsActivation	<input type="checkbox"/>	<unset> ▼
defaultLayout	<input type="checkbox"/>	<unset> ▼
participantLabels	<input type="checkbox"/>	<unset> ▼
presentationDisplayMode	<input type="checkbox"/>	<unset> ▼
presentationContributionAllowed	<input type="checkbox"/>	<unset> ▼
presentationViewingAllowed	<input type="checkbox"/>	<unset> ▼
endCallAllowed	<input checked="" type="checkbox"/>	true ▼
disconnectOthersAllowed	<input type="checkbox"/>	<unset> ▼

8. Configuration(컨피그레이션) > API > /api/v1/coSpaces로 이동하여 확장합니다.

9. 할당할 coSpace를 찾은 다음 callLegProfile 아래에서 작업을 허용하기 위해 생성한 CoSpace를 선택합니다.

/api/v1/coSpaces/01d4b658-ccf3-48d2-b079-34c81c1e9791

userProvisionedCoSpace	<input type="checkbox"/>		GUID (none available)
name	<input type="checkbox"/>	Test space	- present
uri	<input type="checkbox"/>	2000	(URI user part) - present
secondaryUri	<input type="checkbox"/>		(URI user part)
callId	<input type="checkbox"/>	2000	- present
cdrTag	<input type="checkbox"/>		
passcode	<input type="checkbox"/>		
defaultLayout	<input type="checkbox"/>	<unset> ▼	
tenant	<input type="checkbox"/>		Choose
callLegProfile	<input checked="" type="checkbox"/>	ed1a5d12-796b-4bb4-b81e-f50812548d3b	Choose
callProfile	<input type="checkbox"/>		Choose

이 callLegProfile은 더 낮은 API 레벨에서 적용되므로 /시스템/프로필에 이전에 적용된 callLegProfile을 재정의하므로, 이 특정 coSpace에서만 DTMF 작업을 호출할 수 있습니다.

비밀번호가 있는 사용자만 작업 수행 허용

권한 범위는 비디오 사업자와 같이 특수한 권한을 요구하는 사용자 그룹으로 좁힐 수 있다. DTMF 작업을 허용하는 특정 callLegProfile이 적용된 coSpace에 액세스하기 위해 자체 디렉토리 번호로 accessMethod를 만들 수 있습니다.

1. Configuration(컨피그레이션) > API > /api/v1/coSpaces로 이동하여 확장합니다.

2. 목록에서 accessMethod를 만들 coSpace를 선택합니다.

3. Related objects(관련 객체) 목록에서 /api/v1/coSpaces/<coSpace ID>/accessMethods 링크를 클릭합니다.

Related objects: </api/v1/coSpaces>

</api/v1/coSpaces/56e3aa90-93e4-4189-9882-0aa02d60d59c/accessMethods>

</api/v1/coSpaces/56e3aa90-93e4-4189-9882-0aa02d60d59c/coSpaceUsers>

4. uri 필드에 권한이 있는 사용자가 이 스페이스로 다이얼할 번호를 입력합니다.
5. 암호를 만듭니다. 권한이 있는 사용자가 accessMethod 번호로 전화를 걸면 이 코드를 입력하고 # 기호를 입력하여 미팅에 참여해야 합니다.
6. callLegProfile 아래에서 통화를 종료할 수 있는 항목을 선택합니다.
7. 선택적으로, API 탐색기에서 accessMethod를 쉽게 인식할 수 있도록 이름을 입력합니다.

이 예에서는 coSpace에 참가할 때 비디오 운영자가 사용할 수 있도록 번호 3001의 accessMethod가 생성됩니다(디렉토리 번호 3000이 coSpace에 할당되었으며, 일반 사용자는 이 번호로 전화를 걸어 이 스페이스에서 회의에 참가합니다). 비밀번호로 보호되며, 통화를 종료할 수 있는 callLegProfile이 해당 비밀번호에만 할당됩니다.

</api/v1/coSpaces/56e3aa90-93e4-4189-9882-0aa02d60d59c/accessMethods/a410d047-cd33-43d8-8db2-0c377d19351c>

uri	<input type="checkbox"/>	<input type="text" value="3001"/>	(URI user part) - present
callId	<input type="checkbox"/>	<input type="text" value="3001"/>	- present
passcode	<input type="checkbox"/>	<input type="text" value="1234"/>	- present
name	<input type="checkbox"/>	<input type="text" value="Video operator"/>	- present
callLegProfile	<input type="checkbox"/>	<input type="text" value="ed1a5d12-796b-4bb4-b81e-f50812548d3b"/> <input type="button" value="Choose"/>	- present
secret	<input type="checkbox"/>	<input type="text" value="djJv.8wVpDbteNCNDqskFQ"/>	- present

8. 작업을 허용하지 않는 callLegProfile을 시스템/프로필에 할당하여 전역적으로 적용합니다.

이 예에서는 coSpace 자체에 callLegProfile을 할당할 필요가 없습니다. 전역적으로 적용되는 프로필을 상속하므로 coSpace 번호(3000)에 전화를 걸어 모임에 참가하는 사용자는 DTMF를 통해 통화를 종료할 권한이 없습니다.

</api/v1/coSpaces/56e3aa90-93e4-4189-9882-0aa02d60d59c>

userProvisionedCoSpace	<input type="checkbox"/>	<input type="text"/>	GUID (none available)
name	<input type="checkbox"/>	<input type="text" value="Test space 2"/>	- present
uri	<input type="checkbox"/>	<input type="text" value="3000"/>	(URI user part) - present
secondaryUri	<input type="checkbox"/>	<input type="text"/>	(URI user part)
callId	<input type="checkbox"/>	<input type="text" value="3000"/>	- present
cdrTag	<input type="checkbox"/>	<input type="text"/>	
passcode	<input type="checkbox"/>	<input type="text"/>	
defaultLayout	<input type="checkbox"/>	<input type="text" value="<unset>"/>	
tenant	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Choose"/>	
callLegProfile	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Choose"/>	
callProfile	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Choose"/>	

이 컨피그레이션의 결과, 비디오 운영자는 coSpace 번호(3000) 대신 accessMethod 번호(3001)로 전화를 걸어 회의에 참가할 수 있습니다. 통화 레그는 작업을 적용할 수 있는 callLegProfile을 사용하므로 정의된 DTMF 시퀀스를 사용하여 통화를 종료할 수만 있습니다.

관련 정보

[CMS 3.8 API 참조 설명서](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.