



전화기에서 구성

- 설정 메뉴에서 전화기 네트워크를 수동으로 설정, 1 페이지
- Wi-Fi 네트워크에 전화기 추가, 3 페이지
- 전화기를 Cisco Unified Communications Manager로 연결, 5 페이지
- Cisco IP 전화기 관리 페이지, 6 페이지
- 무선 LAN 보안, 13 페이지
- USB 동글과 데스크탑 충전기로 전화기 설정, 16 페이지


설정 메뉴에서 전화기 네트워크를 수동으로 설정

전화기를 수동으로 설정한 경우 다음 필드를 설정해야 합니다.

- IP 주소
- 서브넷 마스크
- 기본 라우터
- DNS 서버 1
- TFTP 서버 1

네트워크 구성을 설정한 후 Wi-Fi 연결을 설정합니다.

프로시저

-
- 단계 1 설정 앱에 액세스합니다.
 - 단계 2 **Wi-Fi**를 선택합니다.
 - 단계 3 프로파일을 선택합니다.
 - 단계 4 (선택 사항) 프로파일 이름을 설정합니다.
 - a) 프로파일 이름을 선택합니다.
 - b) 프로파일 이름을 입력합니다.
 - c) 추가 를 누르고 저장을 선택합니다.

단계 5 네트워크 구성 > **IPv4** 설정을 선택합니다.

단계 6 **DHCP**를 선택하고 끄기를 누릅니다.

단계 7 전화기의 IP 주소를 입력합니다.

- a) IP 주소를 선택합니다.
- b) 탐색 링을 누르고 선택을 눌러 편집 모드로 전환합니다.
- c) IP 주소를 입력합니다.
- d) 저장을 누릅니다.

단계 8 서브넷 마스크를 입력합니다.

- a) 서브넷 마스크를 선택합니다.
- b) 탐색 링을 누르고 선택을 눌러 편집 모드로 전환합니다.
- c) 마스크를 입력합니다.
- d) 저장을 누릅니다.

단계 9 기본 라우터를 입력합니다.

- a) 서브넷 마스크를 선택합니다.
- b) 탐색 링을 누르고 선택을 눌러 편집 모드로 전환합니다.
- c) 마스크를 입력합니다.
- d) 저장을 누릅니다.

단계 10 주 DNS 서버를 입력합니다.

- a) **DNS 서버 1**을 선택합니다.
- b) 탐색 링을 누르고 선택을 눌러 편집 모드로 전환합니다.
- c) DNS 서버의 IP 주소를 입력합니다.
- d) 저장을 누릅니다.

단계 11 주 TFTP 서버를 입력합니다.

- a) **TFTP 서버 1**을 선택합니다.
- b) 탐색 링을 누르고 선택을 눌러 편집 모드로 전환합니다.
- c) Cisco Unified Communications Manager에 대한 TFTP 서버의 IP 주소를 입력합니다.
- d) 저장을 누릅니다.

단계 12 신뢰 목록 프롬프트에서 지우기를 누릅니다.

지우기를 선택하면 CTL 및 ITL 파일이 전화기에서 제거됩니다. 계속을 선택하면 파일이 유지되지만, 새로운 Cisco Unified Communications Manager에 연결하지 못하게 될 수 있습니다.

관련 항목


[네트워크 설정 재설정](#)

[설정 앱 액세스](#), 2 페이지

설정 앱 액세스

설정 앱을 사용하여 전화기를 설정, 관리 및 사용자 정의합니다.

프로시저

- 단계 1 회선 보기 화면에서 탐색 클러스터의 왼쪽 화살표를 눌러 애플리케이션이 화면을 표시합니다.
- 단계 2 애플리케이션 화면에서 탐색 클러스터의 왼쪽 화살표를 눌러 설정  을 선택합니다.

Wi-Fi 네트워크에 전화기 추가



IP 주소를 입력할 때 해당 필드로 스크롤 이동하고 선택을 누릅니다. 필드가 필드 하나에서 여러 입력 상자로 바뀝니다. 키패드를 사용하여 숫자를 입력하고 탐색 링을 사용하여 필드 사이를 이동합니다. 전화기를 구성하고 변경사항을 저장하면 전화기가 Cisco Unified Communications Manager에 연결됩니다. 연결이 설정되면 전화기에 구성 파일이 다운로드되고 필요한 경우 펌웨어를 새 펌웨어 로드로 업그레이드합니다.

시작하기 전에

Wi-Fi 네트워크에 대한 다음 정보가 필요합니다.

- SSID
- 보안 유형(예: WEP, EAP)
- 선택한 보안 유형에 대한 PIN 또는 패스키

프로시저

- 단계 1 설정 앱에 액세스합니다.
- 단계 2 **Wi-Fi**를 선택합니다.
- 단계 3 프로파일을 선택합니다.
- 단계 4 (선택 사항) 프로파일 이름을 설정합니다.
- a) 프로파일 이름을 선택합니다.
 - b) 키패드를 사용하여 새 이름을 입력합니다.
 - 뒤로  소프트키는 커서 왼쪽 문자를 삭제합니다.
 - 탐색 링을 사용하여 필드에서 왼쪽에서 오른쪽으로 이동합니다.
 - c) 추가  를 누르고 저장을 선택합니다.
- 단계 5 네트워크 구성 > **IPv4** 설정을 선택합니다.
- 네트워크가 DHCP를 지원하지 않으면 다음 단계를 수행하십시오.
- a) 필수: **DHCP**를 선택하고 끄기를 누릅니다.

- b) IP 주소를 선택하고 전화기의 할당된 주소를 입력합니다.
- c) 서브넷 마스크를 선택하고 필수 서브넷 마스크를 입력합니다. 예: 255.255.255.0.
- d) 기본 라우터를 선택하고 기본 라우터의 IP 주소를 입력합니다.
- e) DNS 서버 1을 선택하고 DNS 서버의 IP 주소를 입력합니다.

모든 네트워크의 경우,

- a) 대체 TFTP를 선택하고 켜기로 설정합니다.
- b) TFTP 서버 1을 선택하고 Cisco Unified Communications Manager에 대한 TFTP IP 주소를 입력합니다.
- c) 추가를 누르고 저장을 선택합니다.
- d) 신뢰 목록 창에서 다음을 누르고 지우기를 선택합니다.
- e) 뒤로를 선택한 다음 다시 뒤로를 선택합니다.

단계 6 WLAN 구성을 선택합니다.

단계 7 SSID를 선택합니다.

- a) 키패드를 사용하여 액세스 지점의 SSID를 입력합니다.
- b) 추가를 누르고 저장을 선택합니다.

단계 8 보안 모드를 선택합니다.

단계 9 액세스 지점에 필요한 보안 유형을 선택합니다.

단계 10 다음 표를 사용하여 필수 보안 필드를 설정합니다.

보안 모드	구성된 필드	설명
없음	없음	보안 모드가 없음으로 설정될 때는 다른 필수 필드는 없습니다.
WEP	WEP 키	40/104 또는 64/128 ASCII 또는 Hex WEP 키를 입력합니다.
PSK	암호구	8-63 ASCII 또는 64 Hex 암호구를 입력합니다.
EAP-FAST	사용자 ID	사용자 ID를 입력합니다.
PEAP-GTC	암호	암호를 입력합니다.
PEAP-MSCHAPV2		
EAP-TLS	사용자 인증서	인증서 유형을 선택합니다. 사용자에게 인증서를 제공해야 할 수도 있습니다. 자세한 내용은 인증서의 내용 을 참조하십시오.


단계 11 802.11 모드를 선택하고 필수 모드를 선택합니다.

모드에 따라 주파수가 결정됩니다. 모드를 자동으로 설정할 경우 전화기는 5GHz 또는 2.4GHz 주파수를 사용할 수 있으며, 선호되는 주파수는 5GHz입니다.

단계 12 통화 중 절전을 선택하고 선택을 눌러 설정을 변경합니다.

이 필드는 문제를 해결하기 위해 필요한 경우에만 사용 안 함으로 설정해야 합니다.

단계 13 추가를 누르고 저장을 선택합니다.

단계 14 전원/통화종료 를 누릅니다.

관련 항목

[설정 앱 액세스](#), 2 페이지

전화기를 Cisco Unified Communications Manager로 연결

시작하기 전에

- Cisco Unified Communications Manager TFTP 서버의 IP 주소가 필요합니다.
- 전화기를 Cisco Unified Communications Manager에서 구성해야 합니다.
- 전화기가 Wi-Fi 네트워크에 연결되어야 합니다.

프로시저

단계 1 설정 앱에 액세스합니다.


단계 2 **Wi-Fi**를 선택합니다.

단계 3 프로파일을 선택합니다.

단계 4 네트워크 구성 > **IPv4**를 선택합니다.

단계 5 대체 TFTP를 선택하고 켜기로 설정합니다.

단계 6 TFTP 서버 1을 선택하고 Cisco Unified Communications Manager에 대한 TFTP IP 주소를 입력합니다.

단계 7 추가 를 누르고 설정을 선택합니다.

단계 8 신뢰 목록 창에서 다음을 누르고 지우기를 선택합니다.

지우기를 선택하면 CTL 및 ITL 파일이 전화기에서 제거됩니다. 계속을 선택하면 파일이 유지되지만, 새로운 Cisco Unified Communications Manager에 연결하지 못하게 될 수 있습니다.

단계 9 홈 화면으로 종료합니다.

전화기가 Cisco Unified Communications Manager로 연결합니다. 연결이 설정되면 전화기에 구성 파일이 다운로드되고 필요한 경우 펌웨어를 새 펌웨어 로드로 업그레이드합니다.

관련 항목

[설정 앱 액세스](#), 2 페이지

Cisco IP 전화기 관리 페이지

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

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

다음과 같은 방식으로 관리 페이지에 액세스할 수 있습니다.

- 무선 연결
- 직접 USB 연결
- USB 이더넷 동글

관리 페이지에서 전화기 구성

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

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

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

시작하기 전에

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

사용자 이름은 영구적으로 admin으로 설정됩니다.

프로시저

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

단계 2 전화기를 찾습니다.

단계 3 제품별 구성 레이아웃에서 웹 관리 매개 변수를 활성화로 설정합니다.

단계 4 관리자 암호 필드에 암호를 입력합니다.

단계 5 저장을 선택하고 확인을 클릭합니다.

단계 6 구성 적용을 선택하고 확인을 클릭합니다.

단계 7 전화기를 다시 시작합니다.

전화기 관리 웹 페이지 액세스

관리 웹 페이지에 액세스하려는 경우 관리 포트를 지정해야 합니다.

프로시저

단계 1 전화기의 IP 주소를 확보합니다.

- Cisco 통합 커뮤니케이션 매니저 관리에서 장치 > 전화기를 선택하고 전화기를 찾습니다. Cisco Unified Communications Manager에 등록된 전화기는 전화기 찾기 및 나열 창과 전화기 구성 창 상단에 IP 주소를 표시합니다.
- 전화기에서 설정 앱에 액세스하고 전화기 정보 > 네트워크 > IPv4를 선택한 다음 IP 주소 필드로 스크롤합니다.

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

https://<IP_address>:8443

단계 3 암호 필드에 암호를 입력합니다.

단계 4 제출을 클릭합니다.

관련 항목

[설정 앱 액세스](#), 2 페이지

관리 웹 페이지에서 전화기 설정

전화기를 원격으로 설정해야 하는 경우 관리 웹 페이지에서 전화기 파라미터를 설정할 수 있습니다. 이러한 방식으로 전화기를 설정할 때는 먼저 전화기에 대한 첫 번째 WLAN 프로파일을 설정해야 합니다.

프로시저

단계 1 전화기 관리 웹 페이지에서 **WLAN**을 선택합니다.

단계 2 프로파일 1을 클릭합니다.

단계 3 다음 표에 설명된 대로 필드를 설정합니다.

필드 이름	설명
출처	읽기 전용 필드
상태	프로파일을 활성화 또는 비활성화합니다.

필드 이름	설명
프로파일	프로필의 이름을 입력합니다.
사용자 수정 가능	사용자가 자신의 WLAN 프로파일을 활성화 또는 비활성화할 수 있도록 합니다.
WLAN 구성	
SSID	액세스 포인트의 SSID를 입력합니다.
보안 모드	보안 모드를 선택합니다.
WEP 키	보안 유형을 WEP로 설정한 경우 화면이 변경되고 WEP 키 필드가 표시됩니다. 40/104 또는 64/128 ASCII 또는 16진 WEP 키를 입력합니다.
암호구	보안 유형을 PSK로 설정한 경우 화면이 변경되고 암호구 필드가 표시됩니다. 8-63 ASCII 또는 64Hex 암호구를 입력합니다.
사용자 ID	보안 유형이 EAP-Fast, PEAP-GTC 또는 PEAP-MSCHAPV2인 경우 화면이 변경되고 사용자 ID 필드가 표시됩니다. 사용자 ID를 입력합니다.
암호	보안 유형이 EAP-Fast, PEAP-GTC 또는 PEAP-MSCHAPV2인 경우 화면이 변경되고 암호 필드가 표시됩니다. 암호를 입력합니다.
사용자 인증서	인증서 유형을 선택합니다.
802.11 모드	필요한 모드를 선택합니다.
통화 중 절전	전화기가 전원을 절약하기 위해 사용하는 절전 모드 유형을 선택합니다.
네트워크 구성	
도메인 이름	도메인 이름을 입력합니다.
IPv4 설정	
DHCP	DHCP 방식을 설정합니다. DHCP 꺼져 있는 경우 더 많은 필드를 설정해야 합니다.
IP 주소	DHCP가 해제된 경우 정적 IP 주소 할당
서브넷 마스크	DHCP가 해제된 경우 서브넷 마스크를 입력합니다.

필드 이름	설명
기본 라우터	DHCP가 해제된 경우 라우터의 IP 주소를 입력합니다.
DNS 서버 1 DNS 서버 2 DNS 서버 3	DHCP가 해제된 경우 DNS 서버의 IP 주소를 하나 이상 입력합니다.
대체 TFTP	Cisco Unified Communications Manager와 연결된 다른 TFTP 서버를 사용하는 경우 이 필드를 설정합니다.
TFTP 서버 1 TFTP 서버 2	Cisco Unified Communications Manager TFTP 서버의 IP 주소를 입력합니다(주 서버 및 사용 가능한 경우 보조 서버).
IPv6	현재 지원되지 않습니다.

단계 4 저장을 클릭합니다.

전화기 관리 웹 페이지에서 백업 설정 구성

전화기 관리 웹 페이지를 사용하여 전화기 구성을 백업 및 복원할 수 있습니다.

프로시저

단계 1 전화기 관리 웹 페이지에서 설정 백업을 선택합니다.

단계 2 다음 옵션 중 하나를 수행합니다.

- 백업 파일을 가져옵니다. 컴퓨터에서 파일을 찾고, 암호화 키를 입력한 후 가져오기를 클릭합니다.
- 백업 파일을 내보냅니다. 암호화 키를 입력하고 내보내기를 클릭합니다. 이 키는 파일을 가져올 때 필요합니다.

전화기 날짜 및 시간 직접 설정

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

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

프로시저

단계 1 전화기 관리 웹 페이지에서 날짜 및 시간으로 스크롤합니다.

단계 2 다음 옵션 중 하나를 수행합니다.

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

전화기 관리 페이지에서 로컬 연락처 관리

전화기 관리 웹 페이지에서 수행할 수 있는 작업:

- 연락처의 CSV(쉼표로 구분된 값) 파일을 사용자의 전화기로 가져옵니다.
- 사용자의 로컬 연락처 목록을 CSV 파일로 내보냅니다.
- 사용자의 전화기에서 모든 로컬 연락처를 삭제합니다.

가져오기 및 내보내기 기능은 초기 전화기 설정에 유용할 수 있습니다. 조직에서 자주 사용하는 전화 번호의 목록을 한 전화기에 설정할 수 있습니다. 그런 다음 해당 목록을 내보내고 다른 전화기에서 가져올 수 있습니다.

사용자가 전화기 관리 페이지에 액세스하도록 허용한 경우 로컬 연락처 가져오기와 내보내기에 대한 지침을 제공하십시오.

초기 로컬 연락처 목록에 대한 권장되는 방법

여러 전화기로 가져올 목록을 만드는 경우 권장되는 방법:

1. 한 전화기에서 로컬 연락처 목록에 한 항목을 만듭니다.
2. 전화기에서 목록을 내보냅니다.
3. 목록에서 편집하여 항목을 추가합니다.

텍스트 편집기를 사용하여 목록을 편집할 수 있습니다.

다른 도구(예: 워드프로세서 또는 스프레드시트)를 사용하는 경우 다음 중 한 가지 형식으로 목록을 저장해야 합니다.

- CSV UTF-8
- 표준 CSV

4. 목록을 전화기로 가져옵니다.

- 5. 목록을 다른 전화기로 가져오기 전에 목록이 올바르게 표시되는지 확인합니다.

사용자의 로컬 연락처 가져오기

CSV 파일을 사용자의 전화기로 가져올 수 있습니다. 텍스트 편집기를 사용하여 이 CSV 파일을 생성하거나 한 전화기에서 목록을 만들고 내보낼 수 있습니다([사용자의 로컬 연락처 내보내기](#), 12 페이지 참조).

최대 200개의 로컬 연락처를 추가할 수 있습니다. 전화기에 로컬 연락처 목록이 이미 있으면 전화기의 CSV 파일의 항목 수가 200개를 초과할 수 있으며 가져오기가 실패합니다.

즐거찾기 목록에서 첫 번째 항목은 음성 메일로 예약되어 있으므로 49개 항목만 즐겨찾기로 표시할 수 있습니다. 전화기에 즐겨찾기 목록이 이미 있는 경우 CSV 파일에 즐겨찾기로 표시된 번호 항목과 휴대폰에 있는 항목이 49개를 초과하면 가져오기가 실패합니다.

가져오기는 전화기에 특정 항목이 이미 있는지 확인하지 않으므로 중복 항목이 발생할 수 있습니다. 중복된 항목은 수동으로 삭제해야 합니다.

시작하기 전에

다음 형식으로 CSV 파일을 생성합니다.

샘플 CSV 파일

```
First name, Last name, Nickname, Company, Work number, Home number, Mobile number, Email address, Work primary, Home primary, Mobile primary, Work favorite, Home favorite, Mobile favorite
Michael,G,,Sample Company,1000,12345678,,test@test.com,true,false,false,2,3,
```

여기서:

필드 이름	설명	샘플 항목
이름	이름(문자열)	Michael
성	성(문자열) 또는 비워둠	G
Nickname	간단한 이름(문자열) 또는 비워둠	(비어 있음)
회사	회사 이름을 문자열로 지정하거나 비워둡니다. 참고 문자열에 쉼표를 포함할 수 없습니다.	샘플 회사
직장 전화 번호	전화기에서 걸어야 하는 정확한 번호입니다.	1000
집 전화 번호	전화기에서 걸어야 하는 정확한 번호입니다.	12345678

필드 이름	설명	샘플 항목
휴대폰 번호	전화기에서 걸어야 하는 정확한 번호입니다.	(비어 있음)
전자 메일 주소	이메일 주소 또는 비워둠	test@test.com
주 직장 주 집 주 휴대폰	값—true, false 이러한 값 중 하나만 true로 구성하며 나머지 두 항목은 false로 구성됩니다.	주 직장—true 주 집—false 주 휴대폰—false
직장 즐겨찾기 집 즐겨찾기 휴대폰 즐겨찾기	즐겨찾기로 추가할 숫자를 지정하여 즐겨찾기 슬롯 번호를 구성합니다. 예를 들어 직장 즐겨찾기에 2를 입력하면 직장 번호를 즐겨찾기 슬롯 2와 매핑합니다. 참고 즐겨찾기 슬롯 1은 음성 메일에 예약되어 있습니다.	직장 즐겨찾기—2 집 즐겨찾기—3 휴대폰 즐겨찾기—(비워둠)

프로시저

- 단계 1 전화기 관리 웹 페이지에서 로컬 연락처를 선택합니다.
- 단계 2 로컬 연락처 가져오기 아래에서 찾아보기를 클릭합니다.
- 단계 3 CSV 파일로 이동하여 클릭한 다음 확인을 클릭합니다.
- 단계 4 업로드를 클릭합니다.
- 단계 5 전화기에서 목록이 제대로 표시되는지 확인합니다.

사용자의 로컬 연락처 내보내기

전화기의 로컬 연락처 목록을 CSV 파일로 내보낼 수 있습니다.

프로시저

- 단계 1 전화기 관리 웹 페이지에서 로컬 연락처를 선택합니다.
- 단계 2 로컬 연락처 내보내기 아래의 내보내기를 클릭합니다.
- 단계 3 파일을 컴퓨터에 저장합니다.

사용자의 로컬 연락처 삭제하기

전화기에서 전체 로컬 연락처 목록을 삭제할 수 있습니다. 예를 들어 다른 사용자에게 전화를 넘겨주기 전에 이렇게 할 수 있습니다.

프로시저

-
- 단계 1 전화기 관리 웹 페이지에서 로컬 연락처를 선택합니다.
 - 단계 2 모든 로컬 연락처 삭제 아래의 삭제를 클릭합니다.
 - 단계 3 팝업 창에서 삭제를 확인합니다.
 - 단계 4 전화기에서 로컬 연락처 목록이 비어 있는지 확인합니다.
-

무선 LAN 보안

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

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

전화기 관리 웹 페이지에서 사용자 인증서 설치

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

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

사용자 인증서 설치 후 RADIUS 서버 신뢰 목록에 추가해야 합니다.

시작하기 전에

전화기에 대한 사용자 인증서를 설치하기 전에 다음을 확인해야 합니다.

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

펌웨어 릴리스 11.0(6) 이상을 실행하는 전화기의 경우 이 암호는 최대 16자까지 가능합니다. 이전 릴리스의 경우 암호는 최대 12자까지 가능합니다.

프로시저

- 단계 1 전화기 관리 웹 페이지에서 인증서를 선택합니다.
 - 단계 2 사용자 설치됨 필드를 찾아 설치를 클릭합니다.
 - 단계 3 PC에서 인증서를 찾습니다.
 - 단계 4 추출 암호 필드에 인증서 추출 암호를 입력합니다.
 - 단계 5 업로드를 클릭합니다.
 - 단계 6 업로드가 완료된 후 전화기를 다시 시작합니다.
-

전화기 관리 웹 페이지에서 인증 서버 인증서를 설치

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

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

시작하기 전에

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

프로시저

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

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

전화기 관리 웹에서 보안 인증서를 수동으로 제거

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

프로시저

- 단계 1 전화기 관리 웹 페이지에서 인증서를 선택합니다.
- 단계 2 인증서 페이지에서 인증서를 찾습니다.
- 단계 3 삭제를 클릭합니다.
- 단계 4 삭제 프로세스를 완료한 후 전화기를 다시 시작합니다.

SCEP 설정

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

SCEP 제품 특정 구성 매개 변수 구성

전화기 웹 페이지에서 다음과 같은 SCEP 매개 변수를 구성해야 합니다.

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

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

프로시저

- 단계 1 Cisco 통합 커뮤니케이션 매니저 관리에서 장치 > 전화기를 선택합니다.
- 단계 2 전화기를 찾습니다.
- 단계 3 제품별 구성 레이아웃 영역으로 스크롤합니다.
- 단계 4 **WLAN SCEP** 서버 확인란을 선택하여 SCEP 매개 변수를 활성화합니다.
- 단계 5 **WLAN Root CA Fingerprint (SHA256 or SHA1)** 확인란을 선택하여 SCEP QED 매개 변수를 활성화합니다.

Simple Certificate Enrollment Protocol 서버 지원

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

- PKI 신뢰 포인트로 사용
- PKI RA로 사용

- RADIUS 서버를 사용하여 장치 인증 수행

자세한 내용을 보려면 SCEP 서버 문서를 참조하십시오.

USB 동글과 데스크탑 충전기로 전화기 설정

USB-이더넷 어댑터(동글)을 데스크탑 충전기로 삽입하면 자동 Wi-Fi 프로파일 프로비저닝과 인증서 등록을 위해서만 이더넷 네트워크에 연결할 수 있습니다. 이더넷 네트워크를 통한 음성 통화는 지원되지 않습니다.



참고 USB 동글은 일반적인 용도로 데스크탑 충전기에 연결하기 위한 것은 아닙니다. 초기 프로비저닝 용도를 위한 것입니다.

프로비저닝에 사용할 스위치 포트의 기본 VLAN은 Cisco Unified Communications Manager에 연결할 수 있어야 하며 Cisco Unified Communications Manager를 가리키는 DHCP 옵션 150을 제공해야 합니다.

지원되는 USB-이더넷 어댑터:

- Apple USB 2.0 이더넷 어댑터
- Belkin B2B048 USB 3.0 기가비트 이더넷 어댑터
- D-Link DUB-E100 USB 2.0 고속 이더넷 어댑터
- Linksys USB300M USB 2.0 이더넷 어댑터
- Linksys USB3GIG USB 3.0 기가비트 이더넷 어댑터

시작하기 전에

USB-이더넷 어댑터(동글)가 필요합니다.

데스크탑 충전기를 전원 어댑터를 통해 전원에 연결해야 합니다.

프로시저

- 단계 1** Cisco 통합 커뮤니케이션 매니저 관리에서 생성한 WLAN 프로파일이 올바른 CUCM 장치 풀(시스템 > 장치 풀)과 연결되거나 무선 전화기(장치 > 전화기)와 연결되어 있는지 확인합니다.
- 단계 2** 동글의 한쪽 끝을 데스크탑 충전기와 연결하고 다른쪽 끝을 네트워크 스위치와 연결된 RJ-45 케이블과 연결합니다.
- 단계 3** 전화기를 데스크탑 충전기에 꽂고 프로파일을 다운로드하는 동안 기다립니다.
- 단계 4** 전화기가 Cisco Unified Communications Manager에 등록되는지 확인합니다
- 단계 5** 전화기를 데스크탑 충전기에서 제거합니다.

단계 6 동글을 데스크탑 충전기에서 분리합니다.

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.