Cisco IP 전화기 보안

- Cisco IP 전화기 보안 개요, 1 페이지
- 전화기 네트워크의 보안 강화, 2 페이지
- 전화기의 현재 보안 기능 확인, 3 페이지
- 보안 프로파일 확인, 3 페이지
- 지원 보안 기능, 4 페이지

Cisco IP 전화기 보안 개요

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

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

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

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

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

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

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

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

Cisco IP 전화기 7800 시리즈는 FIPS(Federal Information Processing Standard)를 준수합니다. 올바르게 작동하려면 FIPS 모드는 2048비트 이상의 RSA 키 크기가 필요합니다. RSA 서버 인증서가 2048비트 이상이 아닌 경우 전화기가 Cisco Unified Communications Manager에 등록되지 않고 전화기 등록에 실패합니다. 인증서의 키 크기가 FIPS와 호환되지 않습니다. 가 전화기에 표시됩니다.

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

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

관련 항목

Cisco Unified Communications Manager 설명서

LSC(Locally Significant Certificate) 설정, 7 페이지

전화기 네트워크의 보안 강화

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

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

향상된 보안 환경에는 다음과 같은 기능이 포함됩니다.

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

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

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

보안에 대한 자세한 내용은 다음 내용을 참조하십시오.

- *Cisco Unified Communications Manager*용 시스템 구성 설명서, 릴리스 14.0(1) 이상 (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).
- *Cisco IP* 전화기 *7800* 및 *8800* 시리즈 보안 개요(https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html)
- *Cisco Unified Communications Manager* 보안 설명서(https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)
- SIP OAuth: *Cisco Unified Communications Manager* 기능 구성 설명서(https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)

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

전화기의 현재 보안 기능 확인

보안 기능과 Cisco Unified Communications Manager 및 Cisco IP 전화기 보안에 대한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

프로시저

단계 **1** 애플리케이션  을 누릅니다.

단계 **2** 관리 설정 > 보안 설정을 선택합니다.

전화기에 CTL(Certificate Trust List)이 설치되어 있으면 대부분의 보안 기능이 제공됩니다.

관련 항목

Cisco Unified Communications Manager 설명서

보안 프로파일 확인

Cisco Unified Communications Manager를 지원하는 모든 Cisco IP 전화기는 전화기의 비보안, 인증 또는 암호화 여부를 정의하는 보안 프로파일을 사용합니다. 보안 프로파일 구성 및 전화기에 해당 프로파일을 적용하는 작업에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

프로시저

단계 **1** Cisco Unified Communications Manager Administration에서 시스템 > 보안 > 전화기 보안 프로파일을 선택합니다.

단계 **2** [보안 모드] 설정을 확인합니다.

관련 항목

Cisco Unified Communications Manager 설명서

지원 보안 기능

다음 표에는 Cisco IP 전화기 7800 시리즈에서 지원하는 보안 기능에 대한 개요가 나와 있습니다. Cisco Unified Communications Manager 및 Cisco IP 전화기 보안에 대한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

표 *1:* 보안 기능 개요

기능	설명
이미지 인증	서명된 이진 파일(확장자 .sbn)이 펌웨어 이미지를 전화기에 로드하기 전 함부로 변경할 수 없게 합니다. 이미지를 함부로 변경하면 인증 프로세스에 실패하여 새 이미지를 거부합니다.
고객측 인증서 설치	각 Cisco IP 전화기에는 장치 인증을 위한 고유 인증서가 필요합니다. 전화기에는 MIC(Manufacturing Installed Certificate)가 포함되어 있지만, 추가 보안을 위해 Cisco Unified Communications Manager Administration에 CAPF(Certificate Authority Proxy Function)를 사용해 인증서를 설치한다고 명시할 수 있습니다. 또는 전화기의 보안 구성 메뉴에서 LSC(Locally Significant Certificate)를 설치할 수도 있습니다.
장치 인증	각 개체가 다른 개체의 인증서를 수락할 때는 Cisco Unified Communications Manager 서버와 전화기 사이에서 이루어집니다. 전화기와 Cisco Unified Communications Manager 간에 보안 연결을 시행할 것인지를 결정하고 필요할 경우, TLS 프로토콜을 사용해 개체 간에 안전한 시그널링 경로를 구축합니다. Cisco Unified Communications Manager는 Cisco Unified Communications Manager에서 인증할 수 없는 경우만 아니라면 전화기를 등록하지 않을 것입니다.

기능	설명
파일 인증	전화기에서 다운로드한 디지털 서명 파일을 확인합니다. 전화기는 파일이 작성된 후에 부당한 파일 변경이 일어나지 않았다는 것을 확인하기 위해 서명을 확인합니다. 인증에 실패한 파일은 전화기의 플래시 메모리에 기록되지 않습니다. 전화기는 그러한 파일의 경우 추가 처리 없이 거부합니다.
신호 처리 인증	TLS 프로토콜을 사용해 전송되는 동안 시그널링 패킷에 변조되지 않았는지를 확인합니다.
MIC(Manufacturing Installed Certificate)	각 Cisco IP 전화기에는 장치 인증에 사용할 고유한 MIC(Manufacturing Installed Certificate)가 포함되어 있습니다. MIC은 전화기의 ID를 증명하는 고유한 영구 증명서로, Cisco Unified Communications Manager는 이를 사용해 전화기를 인증합니다.
안전한 SRST 참조	보안을 위해 SRST 참조를 구성하고 Cisco Unified Communications Manager Administration에서 종속 장치를 재설정하고 나면, TFTP 서버에서 전화기의 cnf.xml 파일에 SRST 인증서를 추가하고 전화기에 해당 파일을 전송합니다. 그럼 보안이 이루어진 전화기는 SRST 활성화 라우터와 상호 작용하는 데 TLS 연결을 사용합니다.
미디어 암호화	SRTP를 사용하면 지원 장치들 간의 미디어 스트림이 안전하다는 것을 증명하고, 오직 의도한 장치에서만 데이터를 주고 받도록 할 수 있습니다. 여기에는 장치를 위해 미디어 기본 키 한 쌍을 생성하고, 장치에 이 키를 전달하며, 키가 전송되는 동안 키의 전달을 안전하게 보호하는 일도 포함됩니다.
CAPF(Certificate Authority Proxy Function)	지나치게 프로세싱 집약적인 인증서 생성 절차의 일부를 수행하고, 키 생성 및 인증서 설치를 위해 전화기와 상호 작용합니다. CAPF는 전화기를 대신해 고객이 지정한 인증 기관에 인증서를 요청하도록 구성할 수도 있고, 로컬에서 인증서를 생성하도록 구성할 수도 있습니다.
보안 프로파일	전화기의 보안 또는 암호화 여부를 정의합니다.
암호화된 구성 파일	전화기 구성 파일의 프라이버시를 보장할 수 있습니다.

기능	설명
전화기용 웹 서버 기능의 선택적 비활성화	전화기에 관한 다양한 사용 통계를 보여주는 전화기 웹 페이지에 액세스하지 못하게 할 수 있습니다.
전화기 강화	Cisco Unified Communications Manager Administration에서 제어하는 추가 보안 옵션: • PC 포트 비활성화 • PC 음성 VLAN 액세스 비활성화 • 전화기 웹 페이지 액세스 비활성화 참고 전화기 구성 메뉴를 보면 PC 포트 비활성화, GARP 활성화 및 음성 VLAN 활성화 옵션에 관한 현재 설정을 확인할 수 있습니다.
802.1X 인증	Cisco IP 전화기는 네트워크에 액세스 권한을 요청하고 확보하는 데 802.1X 인증을 사용할 수 있습니다.
AES 256 암호화	Cisco Unified Communications Manager 릴리스 10.5(2) 또는 그 이후 버전에 연결하면, 전화기는 시그널링 및 미디어 암호화를 위해 TLS 및 SIP를 위한 AES 256 암호화 지원을 지원합니다. 이렇게 하면 전화기에서 SHA-2(Secure Hash Algorithm) 표준을 따르고 FIPS(Federal Information Processing Standards)를 준수하는 AES-256 기반 암호를 사용해 TLS 1.2 연결을 시작하고 지원할 수 있습니다. 다음은 새 암호입니다. • TLS 연결용: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • sRTP용: • AEAD_AES_256_GCM • AEAD_AES_128_GCM 자세한 내용은 Cisco Unified Communications Manager 문서를 참조하십시오.

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

관련 항목

Cisco Unified Communications Manager 설명서
전화기 통화 보안, 8 페이지
802.1x 인증, 11 페이지
보안 프로파일 확인, 3 페이지

LSC(Locally Significant Certificate) 설정

이 작업은 인증 문자열 방법으로 LSC를 설정하는 작업에 적용됩니다.

시작하기 전에

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

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

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

프로시저

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

단계 **2** 전화기에서 애플리케이션 을 누릅니다.

단계 **3** 관리자 설정 > 보안 설정을 선택합니다.

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

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

전화기에 인증 문자열이 표시됩니다.

단계 **5** 인증 코드를 입력하고 제출을 누릅니다.

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

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

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

관련 항목

Cisco Unified Communications Manager 설명서

FIPS 모드 활성화

프로시저

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

단계 **2** [제품별 구성] 영역으로 이동합니다.

단계 **3** **FIPS** 모드 필드를 [활성화]로 설정합니다.

단계 **4** 구성 적용을 선택합니다.

단계 **5** 저장을 선택합니다.

단계 **6** 전화기를 다시 시작합니다.

전화기 통화 보안

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

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

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

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

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

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

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

보안 컨퍼런스 식별

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

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

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

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

표 *2:* 전화회의를 통한 보안 제한

개시자 전화기 보안 수준	사용되는 기능	참가자 보안 수준	동작 결과
비보안	전화회의	보안	비보안 컨퍼런스 브리지 비보안 전화회의
보안	전화회의	최소 1명의 구성원이 비보안 상태입니다.	보안 컨퍼런스 브리지 비보안 전화회의
보안	전화회의	보안	보안 컨퍼런스 브리지 보안 암호화 수준 전화회의
비보안	회의개설	최소 보안 수준이 암호화되어 있습니다.	개시자는 보안 수준을 충족하지 않아 통화가 거부되었습니다라는 메시지를 받습니다.
보안	회의개설	최소 보안 수준이 비보안 상태입니다.	보안 컨퍼런스 브리지 전화회의에서 모든 통화를 수용합니다.

보안 전화기 통화 식별

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

보안 통화는 다음과 같은 프로세스를 사용해 이루어집니다.

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

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

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

보호된 전화기는 다음 상황에서 표시음을 재생하거나 재생하지 않습니다.

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

[보안 표시음 재생] 옵션이 비활성화되면 표시음이 재생되지 않습니다.

802.1x 인증

Cisco IP 전화기는 802.1X 인증을 지원합니다.

Cisco IP 전화기와 Cisco Catalyst 스위치는 일반적으로 CDP(Cisco Discovery Protocol)를 사용해 서로를 식별하고 VLAN 할당 및 인라인 전력 요구 사항 같은 매개 변수를 결정합니다. CDP는 로컬로 연결된 워크스테이션은 식별하지 않습니다. Cisco IP 전화기는 EAPOL 패스스루 메커니즘을 제공합니다. 이 메커니즘을 통해 Cisco IP 전화기에 연결된 워크스테이션은 LAN 스위치의 802.1X 인증자에게 EAPOL 메시지를 전달합니다. 패스스루 메커니즘은 네트워크에 접속하기 전 데이터 엔드포인트를 인증하기 위해 IP 전화기가 LAN 스위치로 작동하지 않도록 합니다.

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

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

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

802.1X를 구성하려면 다음과 같은 작업을 수행해야 합니다.

- 전화기에서 802.1X 인증을 활성화하기 전에, 먼저 다른 구성 요소를 구성합니다.
- PC 포트 구성—802.1X 표준은 VLAN을 고려하지 않기 때문에 특정 스위치 포트에서 단일 장치만 인증하도록 권장합니다. 그러나 일부 스위치(Cisco Catalyst 스위치 포함)는 멀티도메인 인증

을 지원합니다. PC를 전화기의 PC 포트에 연결할 수 있는지 여부는 스위치 구성에서 결정합니다.

- 활성화됨—멀티도메인 인증을 지원하는 스위치를 사용 중이면, PC 포트를 활성화하고 여기에 PC를 연결할 수 있습니다. 이 경우 Cisco IP 전화기는 스위치와 연결된 PC 간의 인증 교환을 모니터링하기 위해 프록시 EAPOL 로그오프를 지원합니다. Cisco Catalyst 스위치의 IEEE 802.1X 지원에 관한 자세한 내용은 Cisco Catalyst 스위치 구성 설명서를 참조하십시오.

  http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

- 비활성화됨—스위치가 같은 포트에서 여러 개의 802.1X 준수 장치를 지원하지 않는다면, 802.1X 인증이 활성화될 때 PC 포트를 비활성화해야 합니다. 이 포트를 비활성화지 않은 상태에서 나중에 PC와 연결하려고 하면, 스위치에서 전화기와 PC 모두에 대한 네트워크 액세스를 거부합니다.

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

관련 항목

Cisco Unified Communications Manager 설명서