Cisco IP 전화회의 전화기 보안

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 전화회의 전화기 8832는 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 전화기의 상태 메시지에 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

LSC(Locally Significant Certificate) 설정, 6 페이지
Cisco Unified Communications Manager 설명서

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 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.

지원 보안 기능

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

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

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

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

Cisco Unified Communications Manager 시스템에 보안을 구현하면 전화기 및 Cisco Unified Communications Manager 서버의 ID 도난을 방지하고, 데이터 변조를 방지하고, 통화 시그널링 및 미디어 스트림 변조를 방지합니다.

이러한 위협을 완화하기 위해 Cisco IP 텔레포니 네트워크는 전화기와 서버 간에 보안(암호화된) 통신 스트림을 설정하고 유지 보수하고, 파일이 전화기로 전송되기 전에 파일에 디지털로 서명하고, Cisco IP 전화기 간에 미디어 스트림 및 통화 시그널링을 암호화합니다.

LSC(Locally Significant Certificate)는 CAPF(Certificate Authority Proxy Function)와 관련된 필수 작업을 수행한 후 전화기에 설치됩니다. Cisco Unified Communications Manager Administration을 사용하여

Cisco Unified Communications Manager 보안 설명서에 설명된 대로, LSC를 구성할 수 있습니다. 또는 전화기의 [보안 설정] 메뉴에서 LSC 설치를 시작할 수도 있습니다. 이 메뉴에서는 LSC를 업데이트하거나 삭제할 수도 있습니다.

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

전화기는 장치가 비보안인지 보안인지를 정의하는 전화기 보안 프로파일을 사용합니다. 전화기에 보안 프로파일을 적용하는 작업에 관한 자세한 내용은 특정 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

Cisco Unified Communications Manager Administration에서 보안 관련 설정을 구성할 경우 전화기 구성 파일은 중요한 정보를 포함합니다. 구성 파일의 프라이버시를 보장하려면 암호화에 대한 설정을 구성해야 합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

Cisco Unified Communications Manager 시스템에 보안을 구현하면 전화기 및 Cisco Unified Communications Manager 서버의 ID 도난을 방지하고, 데이터 변조를 방지하고, 통화 시그널링 및 미디어 스트림 변조를 방지합니다.

다음 표에는 Cisco IP 전화회의 전화기 8832에서 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 인증 프로세스에 실패하여 새 이미지를 거부합니다.
고객측 인증서 설치	각 전화기에는 장치 인증을 위한 고유 인증서가 필요합니다(만, 추가 보안을 위해 Cisco Unified Communications Manage 증서를 설치한다고 명시할 수 있습니다. 또는 전화기의 보니다.
장치 인증	각 개체가 다른 개체의 인증서를 수락할 때는 Cisco Unified와 Cisco Unified Communications Manager 간에 보안 연결을 간에 안전한 시그널링 경로를 구축합니다. Cisco Unified C증할 수 없는 경우만 아니라면 전화기를 등록하지 않을 것
파일 인증	전화기에서 다운로드한 디지털 서명 파일을 확인합니다. 을 확인하기 위해 서명을 확인합니다. 인증에 실패한 파일의 경우 추가 처리 없이 거부합니다.
신호 처리 인증	TLS 프로토콜을 사용해 전송되는 동안 시그널링 패킷에
MIC(Manufacturing Installed Certificate)	각 전화기에는 장치 인증에 사용할 고유한 MIC(Manufactu명하는 고유한 영구 증명서로, Cisco Unified Communicatio

기능	설명
안전한 SRST 참조	보안을 위해 SRST 참조를 구성하고 Cisco Unified Com 서버에서 전화기의 cnf.xml 파일에 SRST 인증서를 추가 SRST 활성화 라우터와 상호 작용하는 데 TLS 연결을 사
미디어 암호화	SRTP를 사용하면 지원 장치들 간의 미디어 스트림이 안 수 있습니다. 여기에는 장치를 위해 미디어 기본 키 한 안전하게 보호하는 일도 포함됩니다.
CAPF(Certificate Authority Proxy Function)	지나치게 프로세싱 집약적인 인증서 생성 절차의 일부를 는 전화기를 대신해 고객이 지정한 인증 기관에 인증서 도 있습니다.
보안 프로파일	전화기의 비보안, 인증, 암호화 여부를 정의합니다.
암호화된 구성 파일	전화기 구성 파일의 프라이버시를 보장할 수 있습니다
전화기용 웹 서버 기능의 선택적 비활성화	전화기에 관한 다양한 사용 통계를 보여주는 전화기 웹
전화기 강화	Cisco Unified Communications Manager Administration에 • 전화기 웹 페이지 액세스 비활성화 참고 전화기 구성 메뉴를 보면 GARP 활성화 및
802.1X 인증	전화기는 네트워크에 액세스 권한을 요청하고 확보하
AES 256 암호화	Cisco Unified Communications Manager 릴리스 10.5(2) 및 TLS 및 SIP를 위한 AES 256 암호화 지원을 지원합니다 FIPS(Federal Information Processing Standards)를 준수하 다. 다음은 새 암호입니다. • TLS 연결용: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH • sRTP용: • AEAD_AES_256_GCM • AEAD_AES_128_GCM 자세한 내용은 Cisco Unified Communications Manager 릴
ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서	Cisco Unified Communications Manager는 CC(공통 평가 Unified Communications Manager 11.5 이상 버전의 모든

관련 항목

Cisco Unified Communications Manager 설명서

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 설정을 선택합니다.

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 매개변수). 서버를 선택하고, Unified Communications Manager 서비스를 선택합니다. [서비스 매개변수 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

개시자 전화기 보안 수준	사용되는기능	참가자 보안 수준	동작 결과
비보안	회의개설	최소 보안 수준이 암호화되어 있습니다.	개시자는 보안 수준을 충족하지 않아 부되었습니다라는 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.

참여를 위한 암호화 제공

Cisco Unified Communications Manager는 전화회의가 설정되면 전화기 보안 상태를 확인하고 전화회의에 대한 보안 표시를 변경하거나 통화 완료를 차단하여 시스템의 무결성 및 보안을 유지합니다.

참여에 사용되는 전화기가 암호화에 대해 구성되지 않은 경우, 사용자는 암호화된 통화에 참여할 수 없습니다. 이 경우 참여가 실패하면 사용자가 참여를 개시한 전화기에서 다시 걸기(빠른 통화 중) 신호음이 재생됩니다.

개시자 전화기가 암호화에 대해 구성된 경우, 참여 개시자는 암호화된 전화기에서 발신된 비보안 통화에 참여할 수 있습니다. 참여가 발생하면 Cisco Unified Communications Manager는 통화를 비보안으로 분류합니다.

개시자 전화기가 암호화에 대해 구성된 경우, 참여 개시자는 암호화된 통화에 참여할 수 있으며 전화기에 통화가 암호화되었음이 표시됩니다.

WLAN 보안

범위 내에 있는 모든 WLAN 장치는 기타 모든 WLAN 트래픽을 수신할 수 있으므로, 음성 통신 보안이 WLAN에서 중요합니다. 침입자가 음성 트래픽을 조작하거나 가로채지 않도록 하기 위해 Cisco SAFE 보안 아키텍처는 Cisco IP 전화기 및 Cisco Aironet AP를 지원합니다. 네트워크의 보안에 대한 자세한 내용은 http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html을 참조하십시오.

Cisco Wireless IP 텔레포니 솔루션은 무선 Cisco IP 전화기가 지원하는 다음 인증 방법을 사용하여 인증되지 않은 로그인 및 통신 저하를 방지하는 무선 네트워크 보안을 제공합니다.

- 개방형 인증: 무선 장치가 개방형 시스템에서 인증을 요청할 수 있습니다. 요청을 수신하는 AP는 요청자에게 또는 사용자 목록에 있는 요청자에게만 인증을 허가할 수 있습니다. 무선 장치와 AP 간 통신은 암호화되지 않을 수 있거나 장치가 WEP(Wired Equivalent Privacy) 키를 사용하여 보안을 제공할 수 있습니다. WEP를 사용하는 장치만 WEP를 사용 중인 AP로 인증을 시도합니다.

- EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) 인증: 이 클라이언트 서버 보안 아키텍처는 AP와 Cisco ACS(Access Control Server)와 같은 RADIUS 서버 간 TLS(Transport Level Security) 터널 내에서 EAP 트랜잭션을 암호화합니다.

  TLS 터널은 클라이언트(전화기)와 RADIUS 서버 간 인증을 위해 PAC(Protected Access Credential)를 사용합니다. 서버가 AID(Authority ID)를 클라이언트(전화기)로 보내면, 거기서 해당 PAC를 선택합니다. 클라이언트(전화기)는 PAC-Opaque를 RADIUS 서버로 반환합니다. 서버는 기본 키로 PAC를 해독합니다. 이제 두 엔드포인트에는 PAC 키가 있고 TLS 터널이 생성됩니다. EAP-FAST는 자동 PAC 구축을 지원하지만, RADIUS 서버에서 이것을 활성화해야 합니다.

참고 Cisco ACS에서는 기본적으로 PAC가 1주일 후 만료됩니다. 전화기에 만료된 PAC가 있는 경우, 전화기가 새 PAC를 가져오는 동안 RADIUS 서버에서 인증 시간이 더 오래 걸립니다. PAC 구축 지연을 피하기 위해 PAC 만료 기간을 ACS 또는 RADIUS 서버에서 90일 이상으로 설정하십시오.

- 확장 가능 인증 프로토콜 - 전송 계층 보안 EAP-TLS) 인증: EAP-TLS에는 인증 및 네트워크 액세스를 위한 클라이언트 인증서가 필요합니다. 유선 EAP-TLS의 경우, 클라이언트 인증서는 전화기의 MIC 또는 LSC 중 하나가 될 수 있습니다. LSC는 유선 EAP-TLS에 권장되는 클라이언트 인증 인증서입니다.
- PEAP(Protected Extensible Authentication Protocol): 클라이언트(전화기)와 RADIUS 간 Cisco의 독점적 암호 기반 상호 인증 체계입니다. Cisco IP 전화기는 무선 네트워크에서 인증을 위해 PEAP를 사용할 수 있습니다. PEAP-MSCHAPV2만 지원됩니다. PEAP-GTC는 지원되지 않습니다.

다음 인증 체계는 RADIUS 서버를 사용하여 인증 키를 관리합니다.

- WPA/WPA2: RADIUS 서버 정보를 사용하여 인증을 위한 고유 키를 생성합니다. 이러한 키는 중앙 집중식 RADIUS 서버에서 생성되므로, WPA/WPA2는 AP 및 전화기에 저장된 WAP 사전 공유 키보다 더 강화된 보안을 제공합니다.
- 고속 보안 로밍: RADIUS 서버와 무선 도메인 서버(WDS) 정보를 사용하여 키를 관리하고 인증합니다. WDS는 빠르고 안전한 재인증을 위해 CCKM 사용 가능 클라이언트 장치에 대한 보안 자격 증명 캐시를 만듭니다. Cisco IP 전화기 8800 시리즈는 802.11r(FT)을 지원합니다. 11r(FT)와 CCKM 모두 고속 보안 로밍이 가능하도록 지원됩니다. 그러나 Cisco는 802.11r (FT) over air 방식을 활용할 것을 적극 권장합니다.

WPA/WPA2 및 CCKM을 사용할 때, 암호화 키는 전화기에 입력되지 않지만 AP와 전화기 간에 자동으로 파생됩니다. 그러나 인증을 위해 사용되는 EAP 사용자 이름과 암호는 각 전화기에 입력해야 합니다.

음성 트래픽이 보안되도록 하기 위해 Cisco IP 전화기는 암호화를 위해 WEP, TKIP 및 AES(Advanced Encryption Standards)를 지원합니다. 암호화를 위해 이러한 메커니즘이 사용될 때 시그널링 SIP 패킷과 음성 RTP(Real-Time Transport Protocol) 패킷은 모두 AP와 Cisco IP 전화기 사이에서 암호화됩니다.

WEP

WEP가 무선 네트워크에서 사용될 때, 인증은 개방형 또는 공유 키 인증을 사용하여 AP에서 수행됩니다. 전화기에 설정된 WEP 키는 성공적인 연결을 위해 AP에서 구성된 WEP 키와 일치해야 합니다. Cisco IP 전화기는 40비트 암호화 또는 128비트 암호화를 사용하고 전화기와 AP에서 정적 상태로 있는 WEP 키를 지원합니다.

EAP 및 CCKM 인증은 암호화를 위해 WEP 키를 사용할 수 있습니다. RADIUS 서버는 WEP 키를 관리하고 모든 음성 패킷을 암호화하기 위해 인증 후 AP로 고유 키를 전달합니다. 따라서 이러한 WEP 키는 각 인증과 함께 변경될 수 있습니다.

TKIP

WPA 및 CCKM은 WEP 상에서 여러 번 향상된 TKIP 암호화를 사용합니다. TKIP는 암호화를 강화하는 패킷당 키 암호화 또는 더 긴 초기화 벡터(IV)를 제공합니다. 뿐만 아니라, MIC(Message Integrity Check)가 암호화된 패킷을 변경하고 있지 않음을 확인합니다. TKIP는 침입자가 WEP 키를 해독하는 데 도움을 주는 WEP의 예측 가능성을 제거합니다.

AES

WPA2 인증을 위해 사용되는 암호화 방법입니다. 이 암호화 국가 표준은 암호화 및 암호 해독에 동일한 키를 가지는 대칭 알고리즘을 사용합니다. AES는 128비트 크기의 CBC(Cipher Blocking

Chain) 암호화를 최소값으로 사용하는데, CBC 암호화는 128, 192 및 256비트의 키 크기를 지원합니다. Cisco IP 전화기는 256비트의 키 크기를 지원합니다.

참고 Cisco IP 전화기는 CMIC와 함께 CKIP(Cisco Key Integrity Protocol)를 지원하지 않습니다.

인증 및 암호화 체계는 무선 LAN 내에서 설정됩니다. VLAN은 네트워크 및 AP에서 구성되고 다른 인증과 암호화의 조합을 지정합니다. SSID는 VLAN과 특정 인증 및 암호화 체계와 연결됩니다. 무선 클라이언트 장치가 성공적으로 인증하기 위해서는 AP 및 Cisco IP 전화기에 해당 인증 및 암호화 체계를 포함하는 동일한 SSID를 구성해야 합니다.

일부 인증 체계에서는 특정 유형의 암호화가 필요합니다. 개방형 인증을 사용하면 보안 강화를 위해 암호화에 대해 정적 WEP를 사용할 수 있습니다. 그러나 공유 키 인증을 사용 중이면 암호화를 위해 정적 WEP를 설정하고, 전화기에 WEP 키를 구성해야 합니다.

참고
- WPA 사전 공유 키 또는 WPA2 사전 공유 키를 사용할 때 사전 공유 키가 정적으로 전화기에 설정되어야 합니다. 이러한 키는 AP에 있는 키와 일치해야 합니다.
- Cisco IP 전화기는 자동 EAP 협상을 지원하지 않습니다. EAP-FAST 모드를 사용하려면 이 기능을 지정해야 합니다.

다음 표에서는 Cisco IP 전화기가 지원하는 Cisco Aironet AP에 구성되는 인증 및 암호화 체계의 목록을 제공합니다. 표는 AP 구성에 상응하는 전화기의 네트워크 구성 옵션을 나타냅니다.

표 ***3:*** 인증 및 암호화 체계

Cisco IP 전화기 구성	**AP** 구성			
보안 모드	보안	키 관리	암호화	고속 로밍
없음	없음	없음	없음	해당 없음
WEP	정적 WEP	정적	WEP	해당 없음
PSK	PSK	WPA	TKIP	없음
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

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

AP에서 인증 및 암호화 체계 구성에 대한 자세한 내용은 다음 URL 아래에서 해당 모델 및 릴리스에 대한 *Cisco Aironet* 구성 설명서를 참조하십시오.

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

무선 LAN 보안

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

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

Cisco IP 전화기 관리 페이지

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

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

관리 페이지에서 전화기 구성

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

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

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

시작하기 전에

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

사용자 이름은 영구적으로 admin으로 설정됩니다.

프로시저

단계 1 Cisco 통합 커뮤니케이션 매니저 관리에서 장치 > 전화기를 선택합니다.
단계 2 전화기를 찾습니다.
단계 3 제품별 구성 레이아웃 섹션에서 웹 관리를 활성화됨으로 설정합니다.
단계 4 관리자 암호 필드에 암호를 입력합니다.
단계 5 저장을 선택하고 확인을 클릭합니다.
단계 6 구성 적용을 선택하고 확인을 클릭합니다.
단계 7 전화기를 다시 시작합니다.

전화기 관리 웹 페이지 액세스

관리 웹 페이지에 액세스하려는 경우 관리 포트를 지정해야 합니다.

프로시저

단계 1 전화기의 IP 주소를 확보합니다.

- Cisco 통합 커뮤니케이션 매니저 관리에서 장치 > 전화기를 선택하고 전화기를 찾습니다. Cisco Unified Communications Manager에 등록한 전화기는 전화기 찾기 및 나열 창과 전화기 구성 창 상단에 IP 주소를 표시합니다.

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

```
https://<IP_address>:8443
```

단계 3 암호 필드에 암호를 입력합니다.
단계 4 제출을 클릭합니다.

전화기 관리 웹 페이지에서 사용자 인증서 설치

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

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

사용자 인증서 설치 후 RADIUS 서버 신뢰 목록에 추가해야 합니다.

시작하기 전에

전화기에 대한 사용자 인증서를 설치하기 전에 다음을 확인해야 합니다.

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

• 인증서의 추출 암호입니다.

프로시저

단계 **1** 전화기 관리 웹 페이지에서 인증서를 선택합니다.
단계 **2** PC에서 인증서를 찾습니다.
단계 **3** 추출 암호 필드에 인증서 추출 암호를 입력합니다.
단계 **4** 업로드를 클릭합니다.
단계 **5** 업로드가 완료된 후 전화기를 다시 시작합니다.

전화기 관리 웹 페이지에서 인증 서버 인증서를 설치

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

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

시작하기 전에

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

프로시저

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

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

전화기 관리 웹에서 보안 인증서를 수동으로 제거

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

프로시저

단계 **1** 전화기 관리 웹 페이지에서 인증서를 선택합니다.

단계 2 인증서 페이지에서 인증서를 찾습니다.

단계 3 삭제를 클릭합니다.

단계 4 삭제 프로세스를 완료한 후 전화기를 다시 시작합니다.

전화기 날짜 및 시간 직접 설정

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

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

프로시저

단계 1 전화기 관리 웹 페이지에서 날짜 및 시간으로 스크롤합니다.

단계 2 다음 옵션 중 하나를 수행합니다.

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

SCEP 설정

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

SCEP 제품 특정 구성 매개변수 구성

전화기 웹 페이지에서 다음과 같은 SCEP 매개변수를 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 매개변수를 사용합니다. 매개변수를 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 매개변수를 활성화합니다.

단계 5 **WLAN Root CA Fingerprint (SHA256 or SHA1)** 확인란을 선택하여 SCEP QED 매개변수를 활성화합니다.

Simple Certificate Enrollment Protocol 서버 지원

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

- PKI 신뢰 포인트로 사용
- PKI RA로 사용
- RADIUS 서버를 사용하여 장치 인증 수행

자세한 내용을 보려면 SCEP 서버 문서를 참조하십시오.

802.1x 인증

Cisco IP 전화기는 802.1X 인증을 지원합니다.

Cisco IP 전화기와 Cisco Catalyst 스위치는 일반적으로 CDP(Cisco Discovery Protocol)를 사용해 서로를 식별하고 VLAN 할당 및 인라인 전력 요구 사항 같은 매개 변수를 결정합니다.

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.
- 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