Cisco IP 전화기 보안

도메인 및 인터넷 설정

제한된 액세스 도메인 구성

지정 된 서버만을 사용하여 등록, 프로비저닝, 펌웨어 업그레이드 및 보내기로 전화기를 구성할 수 있습니다. 지정된 서버를 사용하지 않는 등록, 프로비저닝, 업그레이드 및 보고서는 전화기에서 수행할 수 없습니다. 사용할 서버를 지정하는 경우 다음 필드에 입력하는 서버가 목록에 포함되어 있는지 확인합니다.

- 프로비저닝 탭의 프로파일 규칙, 프로파일 규칙 **B**, 프로파일 규칙 **C** 및 프로파일 규칙 **D**
- 프로비저닝 탭의 업그레이드 규칙과 **Cisco** 헤드셋 업그레이드 규칙
- 프로비저닝 탭의 보고서 규칙
- 프로비저닝 탭의 사용자 지정 **CA** 규칙
- 내선 번호**(n)** 탭의 프록시 및 아웃바운드 프록시

시작하기 전에

전화기 웹 인터페이스 액세스.

프로시저

단계 **1** 음성 > 시스템을 선택합니다.

단계 **2** 시스템 구성 섹션의 제한된 액세스 도메인 필드를 찾아 각 서버에 대한 정규화 도메인 이름(FQDN)을 입력합니다. FQDN을 쉼표로 구분합니다.

예제:

```
voiceip.com, voiceip1.com
```

다음 형식으로 문자열을 입력하여 구성 XML 파일(cfg.xml)에서 이 매개 변수를 구성할 수 있습니다.

```
<Restricted_Access_Domains ua="na">voiceip.com, voiceip1.com</Restricted_Access_Domains>
```

단계 **3** 모든 변경 사항 제출을 클릭합니다.

DHCP 옵션 구성

전화기에서 DHCP 옵션을 사용하는 순서를 설정할 수 있습니다. DHCP 옵션에 대한 도움말은 DHCP 옵션 지원, 3 페이지의 내용을 참조하십시오.

시작하기 전에

전화기 웹 인터페이스 액세스.

프로시저

단계 **1** 음성 > 프로비저닝을 선택합니다.

단계 **2** 구성 프로파일 섹션에서 DHCP 옵션 구성을 위한 매개 변수, 3 페이지 테이블에 설명된 대로 사용할 **DHCP** 옵션 및 사용할 **DHCPv6** 옵션 매개 변수를 설정합니다.

단계 **3** 모든 변경 사항 제출을 클릭합니다.

DHCP 옵션 구성을 위한 매개 변수

다음 표는 전화기 웹 인터페이스의 음성>프로비저닝 탭에 있는 구성 프로파일 섹션에서 DHCP 옵션 구성을 위한 매개 변수의 기능과 사용법을 정의합니다. 또한 전화기 구성 파일에 XML(cfg.xml) 코드로 추가되어 매개 변수를 구성하는 문자열 구문을 정의합니다.

표 ***1: DHCP*** 옵션 구성을 위한 매개 변수

매개 변수	설명
사용할 DHCP 옵션	쉼표로 구분되는 DHCP 옵션은 펌웨어 및 프로파일을 검색하는 데 사용됩니다. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. `<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>` • 전화기 웹 페이지에서 DHCP 옵션을 쉼표로 구분하여 입력합니다. 예: 66,160,159,150,60,43,125.... 기본값: 66,160,159,150,60,43,125
사용할 DHCPv6 옵션	쉼표로 구분되는 DHCPv6 옵션은 펌웨어 및 프로파일을 검색하는 데 사용됩니다. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. `<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>` • 전화기 웹 페이지에서 DHCP 옵션을 쉼표로 구분하여 입력합니다. 예: 17,160,159.... 기본값: 17,160,159

DHCP 옵션 지원

다음 테이블은 다중 플랫폼 전화기에서 지원되는 DHCP 옵션을 보여줍니다.

네트워크 표준	설명
DHCP 옵션 1	서브넷 마스크
DHCP 옵션 2	시간 오프셋
DHCP 옵션 3	라우터
DHCP 옵션 6	DNS(도메인 네임 서버)

네트워크 표준	설명
DHCP 옵션 15	도메인 이름
DHCP 옵션 41	IP 주소 임대 시간
DHCP 옵션 42	NTP 서버
DHCP 옵션 43	공급업체별 정보 TR.69 자동 구성 서버(ACS) 검색을 위해 사용될 수 있습니다.
DHCP 옵션 56	NTP 서버 IPv6으로 NTP 서버 구성
DHCP 옵션 60	공급업체 클래스 식별자
DHCP 옵션 66	TFTP 서버 이름
DHCP 옵션 125	공급업체 식별 공급업체별 정보 TR.69 자동 구성 서버(ACS) 검색을 위해 사용될 수 있습니다.
DHCP 옵션 150	TFTP 서버
DHCP 옵션 159	프로비저닝 서버 IP
DHCP 옵션 160	프로비저닝 URL

SIP INVITE 메시지에 대한 요구 사항 구성

전화기가 세션에 SIP INVITE(초기) 메시지를 요구하도록 설정할 수 있습니다. 요구 사항은 서비스 제공자 네트워크에서 장치와 상호 작용하도록 허용되는 SIP 서버를 제한할 수 있습니다. 이 방법은 전화기에 대한 악의적인 공격을 방지합니다. 이 기능을 활성화한 경우 SIP 프록시로부터 수신되는 최초 INVITE 요청에 대한 인증이 필요합니다.

XML(cfg.xml) 코드를 사용하여 전화기 설정 파일에서 매개 변수를 설정할 수도 있습니다.

시작하기 전에

전화기 웹 인터페이스 액세스.

프로시저

단계 **1** 음성 > 내선번호**(n)**를 선택합니다. 여기서 n은 내선 번호입니다.

단계 2 **SIP** 설정 섹션의 **INVITE** 인증 목록에서 예를 선택하여 이 기능을 활성화하거나 아니요를 선택하여 비활성화합니다.

다음 형식으로 문자열을 입력하여 구성 XML 파일(cfg.xml)에서 이 매개 변수를 구성할 수 있습니다.

```
<Auth_INVITE_1>Yes</Auth_INVITE_1_>
```

기본값: 아니요.

단계 3 모든 변경 사항 제출을 클릭합니다.

RFC-8760에 대한 지원

RFC-3261을 대체할 수 있으며 RFC-8760에 지정된 추가 인증 다이제스트 알고리즘의 지원을 추가할 수 있습니다. RFC-8760은 SHA256, SHA-512/256 및 MD5와 같은 다이제스트 알고리즘을 지정합니다. RFC-8760을 사용하면 전화기가 인증 헤더 필드 없이 SIP REGISTER 또는 INVITE 또는 SUBSCRIBE 요청을 전송합니다. SIP 서버가 www-authenticate 또는 proxy-authenticate 헤더 필드를 사용하여 401/407 상태 코드를 응답합니다. SIP 서버는 여러 개의 www-authenticate 헤더로 응답합니다. 여러 헤더가 전송되는 경우 각 헤더는 서로 다른 알고리즘을 가져야 하며 가장 선호하는 것을 먼저 사용해야 합니다. RFC-8760에 대한 지원은 RFC-3261에 비해 이점이 있으며 다음 표에 다양한 시나리오가 설명되어 있습니다.

단계	**SIP** 요청 방향	**RFC-3261**	**RFC-8760**
1단계	전화기에서 SIP로	전화기가 인증 없이 SIP 요청을 전송합니다.	전화기가 인증 없이 SIP 요청을 전송합니다.
2단계	SIP에서 전화기로	SIP 서버는 MD5 알고리즘을 사용하는 하나의 www-authenticate로 401 상태에 응답합니다.	SIP 서버는 SHA-256, SHA-512-256 및 MD5와 같은 서로 다른 알고리즘을 사용하여 하나 이상의 www-authenticates로 401 상태에 응답합니다.
3단계	전화기에서 SIP로	전화기가 요청을 보내고 MD5 알고리즘을 사용하여 인증 헤더를 추가하려고 시도합니다.	전화기가 요청을 전송하고 최상위 헤더 필드(SHA-256)를 사용하여 인증을 추가하려고 시도합니다.
4단계	SIP에서 전화기로	SIP 서버에서 인증을 확인합니다.	SIP 서버에서 인증을 확인합니다.

인증 **INVITE** 활성화 및 인증 재동기화 재부팅**(Auth Resync Reboot)**

RFC 8760을 사용해 전화 인증을 활성화할 수 있습니다.

시작하기 전에

- 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조
- **SIP** 설정 섹션. 인증 초대가 예로 설정 됩니다.

프로시저

단계 **1** 음성 > 내선번호**(n)**을 선택하되 여기서 n은 내선 번호입니다.

단계 **2** **SIP** 설정 섹션의 인증 지원 **RFC8760** 목록에서 예를 선택합니다.

예를 선택하면 전화 인증에서 RFC 8760을 지원합니다. 아니오를 선택하면 이 기능을 비활성화할 수 있습니다.

다음 형식으로 문자열을 입력하여 구성 XML 파일(cfg.xml)에서 이 매개 변수를 구성할 수 있습니다.

```
<Auth_Support_RFC8760>Yes</Auth_Support_RFC8760/>
```

기본값: 아니요

단계 **3** 모든 변경 사항 제출을 클릭합니다.

호텔 인증을 위한 추가 다이제스트 알고리즘 지원

이제 전화에서 호텔링 통신 인증을 위해 RFC 8760를 지원합니다. 이 기능을 지원하기 위해 SHA-256, SHA-512 및 SHA-256 다이제스트 알고리즘이 전화에 추가됩니다. 이전에는 전화기가 MD5 알고리즘만 지원했습니다.

TLS 최소값을 제어 합니다.

새 TLS 매개 변수를 사용하여 TLS의 전화기 최소값을 제어할 수 있습니다. 다음 표에서는 TLS 최소값 결과의 간략한 보기를 보여줍니다.

클라이언트 **TLS** 최소 버전	서버 최고 **TLS** 버전	결과
TLS 1.0	TLS 1.0	TLS 1.0
	TLS 1.1	TLS 1.1
	TLS 1.2	TLS 1.2
TLS 1.1	TLS 1.0	프로토콜 알림
	TLS 1.1	TLS 1.1
	TLS 1.2	TLS 1.2

클라이언트 TLS 최소 버전	서버 최고 TLS 버전	결과
TLS 1.2	TLS 1.0	프로토콜 알림
	TLS 1.1	프로토콜 알림
	TLS 1.2	TLS 1.2

시작하기 전에

- 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 시스템을 선택합니다.

단계 **2** 보안 설정 섹션의 **TLS** 최소 버전 목록에서 **TLS 1.1**을 선택합니다.

다음 형식으로 문자열을 입력하여 구성 XML 파일(cfg.xml)에서 이 매개 변수를 구성할 수 있습니다.

```
<TLS_Min_Version ua="na">TLS 1.1</TLS_Min_Version>
```

기본 값: **TLS 1.1**

단계 **3** 모든 변경 사항 제출을 클릭합니다.

참고 이 기능은 전화에서 시작한 대부분의 TLS 클라이언트에 적용되었습니다. (예: TLS에 대응하는 SIP, XMPP, E911 지리적 위치, Wifi)

Webex 메트릭 서비스를 제어할 수 있습니다.

메트릭 활성화를 사용해 모든 메트릭 서비스의 전화 제어를 활성화 합니다.

시작하기 전에

- 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 전화를 선택합니다.

단계 **2** **Webex** 섹션의 메트릭 활성화 목록에서 예를 선택합니다.

예 를 선택하면 전화가 모든 메트릭 메시지의 송신을 제어 합니다. 아니요 를 선택하면이 기능을 비활성화할 수 있습니다.

다음 형식으로 문자열을 입력하여 구성 XML 파일(cfg.xml)에서 이 매개 변수를 구성할 수 있습니다.

```
<Webex_Metrics_Enable ua="na">Yes</Webex_Metrics_Enable>
```

기본값: 아니요

단계 **3** 모든 변경 사항 제출을 클릭합니다.

크래시 서비스에서 PRT 업로드 제어 활성화

전화가 작동을 멈출 때 PRT 패키지를 서버에 자동으로 업로드할 것인지 여부를 지정할 수 있습니다.

시작하기 전에

- 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 프로비저닝을 선택합니다.

단계 **2** 문제 보고서 도구 섹션의 **PRT** 업로드 크래시 목록에서 예를 선택합니다.

예를 선택하면, 전화에서 프로세스 충돌을 자동 업로드 하는 것을 제어합니다. 아니요 를 선택하면이 기능을 비활성화할 수 있습니다.

다음 형식으로 문자열을 입력하여 구성 XML 파일(cfg.xml)에서 이 매개 변수를 구성할 수 있습니다.

```
<PRT_Upload_at_Crash ua="na">Yes</PRT_Upload_at_Crash>
```

기본값: 아니요

단계 **3** 모든 변경 사항 제출을 클릭합니다.

전송 레이어 보안

전송 레이어 보안(TLS)은 인터넷에서 통신을 보호 및 인증하기 위한 표준 프로토콜입니다. SIP over TLS는 서비스 제공자 SIP 프록시와 최종 사용자 사이의 SIP 신호 처리 메시지를 암호화합니다.

Cisco IP 전화기는 UDP를 표준 SIP 전송으로 사용하지만 전화기는 추가 보안을 위해 SIP over TLS도 지원합니다.

다음 표에서는 두 가지 TLS 계층에 대해 설명합니다.

표 *2: TLS* 계층

프로토콜 이름	설명
TLS 레코드 프로토콜	SIP 또는 TCH와 같은 신뢰할 수 있는 전송 프로토콜에 계층화되는 이 레이어는 대칭 데이터 암호화를 사용하여 연결이 비공개됨을 보장하고 연결을 신뢰할 수 있는지 확인합니다.
TLS 핸드셰이크 프로토콜	서버와 클라이언트를 인증하고 애플리케이션 프로토콜이 데이터를 전송하거나 수신하기 전에 암호화 알고리즘 및 암호 키를 협상합니다.

SIP Over TLS를 통한 신호 처리 암호화

TLS를 통한 SIP을 사용하여 신호 처리 메시지를 암호화하는 경우 추가 보안을 구성할 수 있습니다.

시작하기 전에

전화기 웹 인터페이스 액세스. 를 참조하십시오. 전송 레이어 보안, 8 페이지

프로시저

단계 **1** 음성 > 내선번호**(n)**를 선택합니다. 여기서 n은 내선 번호입니다.

단계 **2** **SIP** 설정 섹션의 **SIP** 전송 목록에서 **TLS**를 선택합니다.

다음 형식으로 문자열을 입력하여 구성 XML 파일(cfg.xml)에서 이 매개 변수를 구성할 수 있습니다.

```
<SIP_Transport_1_ ua="na">TLS</SIP_Transport_1_>
```

.

사용 가능한 옵션:

- UDP
- TCP
- TLS
- 자동

디폴트: **UDP**.

단계 **3** 모든 변경 사항 제출을 클릭합니다.

TLS를 통한 LDAP 구성

TLS 통해 LDAP(LDAPS)를 구성하여 서버와 특정 전화기 간의 데이터 통신에 보안을 적용할 수 있습니다.

주의 인증 방법은 기본값인 없음으로 유지하는 것이 좋습니다. 서버 필드 옆의 인증 필드에는 없음, 단순 또는 **DIGEST-MD5** 값을 사용합니다. 인증에 대한 **TLS** 값은 없습니다. 소프트웨어는 서버 문자열의 LDAP 프로토콜로 인증 방법을 결정합니다.

XML(cfg.xml) 코드를 사용하여 전화기 설정 파일에서 매개 변수를 설정할 수도 있습니다.

시작하기 전에

전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 전화를 선택합니다.

단계 **2** **LDAP** 섹션의 서버 필드에 서버 주소를 입력합니다.

다음 형식으로 문자열을 입력하여 구성 XML 파일(cfg.xml)에서 이 매개 변수를 구성할 수도 있습니다.

```
<LDAP_Server ua="na">ldaps://10.45.76.79</LDAP_Server>
```

예를 들어, `ldaps://<ldaps_server>[:port]`를 입력합니다.

여기서:

- **ldaps://**= 서버 주소 문자열의 시작입니다.
- **ldaps_server** = IP 주소 또는 도메인 이름
- 포트 = 포트 번호 기본값: 636

단계 **3** 모든 변경 사항 제출을 클릭합니다.

StartTLS 구성

전화기와 LDAP 서버 간의 통신에 대해 StartTLS(전송 계층 보안)를 활성화할 수 있습니다. 보안 및 비보안 통신 모두에 동일한 네트워크 포트(기본값 389)를 사용합니다. LDAP 서버에서 StartTLS를 지원하는 경우 TLS는 통신을 암호화합니다. 그렇지 않으면, 통신은 일반 텍스트로 보내집니다.

시작하기 전에

- 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 1 음성 > 전화를 선택합니다.

단계 2 **LDAP** 섹션의 서버 필드에 서버 주소를 입력합니다.

예를 들어, `ldap://<ldap_server>[:port]`를 입력합니다.

여기서:

- **`ldap://`** = 서버 주소 문자열(URL 체계)의 시작입니다.
- **`ldap_server`** = IP 주소 또는 도메인 이름
- **`port`** = 포트 번호

다음 형식으로 문자열을 입력하여 구성 XML 파일(cfg.xml)에서 이 매개 변수를 구성할 수도 있습니다.

```
<LDAP_Server ua="na">ldap://<ldap_server>[:port]</LDAP_Server>
```

단계 3 **StartTLS** 활성화 필드를 예로 설정합니다.

다음 형식으로 문자열을 입력하여 구성 XML 파일(cfg.xml)에서 이 매개 변수를 구성할 수도 있습니다.

```
<LDAP_StartTLS_Enable ua="na">예</LDAP_StartTLS_Enable>
```

단계 4 모든 변경 사항 제출을 클릭합니다.

관련 항목

LDAP 디렉터리에 대한 매개 변수

HTTPS 프로비저닝

전화기는 원격으로 배포된 장치를 관리할 때 보안을 향상하기 위해 HTTPS를 지원합니다. 각 전화기에는 고유한 SLL 클라이언트 인증서(및 연결된 개인 키)와 Sipura CA 서버 루트 인증서가 있습니다. 후자는 전화기가 승인된 프로비저닝 서버를 인식하고 승인되지 않은 서버를 거부하도록 해줍니다. 반면, 클라이언트 인증서는 프로비저닝 서버가 요청을 전송한 각 장치를 식별하도록 해줍니다.

서비스 제공자가 HTTPS를 사용하여 구축을 관리하려면, 전화기가 HTTPS를 사용하여 재동기화하려는 각 프로비저닝 서버를 위해 서버 인증서를 생성해야 합니다. 서버 인증서는 Cisco 서버 CA 루트 키를 사용하여 서명해야 하며, 배포된 모든 장치에 해당 인증서가 있어야 합니다. 서명된 서버 인증서를 얻으려면, 서비스 제공자가 인증서 서명 요청을 Cisco로 전달해야 하며, Cisco가 서명하고 전달한 서버 인증서를 프로비저닝 서버에 설치해야 합니다.

프로비저닝 서버 인증서는 CN(일반 이름) 필드와 해당 서버를 실행 중인 호스트의 FQDN을 주체에 포함해야 합니다. 선택적으로 슬래시 (/) 문자로 구분하고 호스트 FQDN 정보를 포함할 수 있습니다. 다음 예는 전화기에서 유효한 것으로 허용되는 CN 항목을 보여줍니다.

```
CN=sprov.callme.com
CN=pv.telco.net/mailto:admin@telco.net
CN=prof.voice.com/info@voice.com
```

전화기는 서버 인증서를 확인하는 것 외에, 서버 인증서에 지정된 서버 이름을 DNS에서 조회하고 서버 IP 주소와 비교하는 테스트를 합니다.

서명된 서버 인증서 얻기

OpenSSL 유틸리티로 인증서 서명 요청을 생성할 수 있습니다. 다음 예에서는 1024비트 RSA 공개/개인 키 쌍 및 인증서 서명 요청을 생성하는 **openssl** 명령을 보여줍니다.

```
openssl req -new -out provserver.csr
```

이 명령은 **privkey.pem**에 서버 개인 키를 생성하고 해당하는 인증서 서명 요청을 **provserver.csr**에 생성합니다. 서비스 제공자는 **privkey.pem** 비밀을 저장하고 서명을 위해 **provserver.csr**을 Cisco로 제출합니다. Cisco는 **provserver.csr**을 수신하고 서명된 서버 인증서 **provserver.crt**를 생성합니다.

프로시저

단계 **1** https://software.cisco.com/software/cda/home으로 이동하고 CCO 자격 증명을 사용하여 로그인합니다.

참고 전화기가 처음으로 네트워크에 연결되거나 공장 설정이 초기화된 후 DHCP 옵션을 설정하지 않으면 장치 활성화 서버에 연결하여 제로 터치 프로비저닝을 수행합니다. 새 전화기는 프로비저닝을 위해 “webapps.cisco.com” 대신 “activate.cisco.com”을 사용합니다. 펌웨어 릴리스가 11.2(1) 이전인 전화기는 “webapps.cisco.com”을 계속 사용합니다. 두 도메인 이름 모두 방화벽을 통과하도록 허용하는 것이 좋습니다.

단계 **2** 인증서 관리를 선택합니다.

CSR 서명 탭에서 이전 단계의 CSR이 서명을 위해 업로드됩니다.

단계 **3** 제품 선택 드롭다운 목록표에서 **SPA1xx** 펌웨어 **1.3.3** 및 최신/**SPA232D** 펌웨어 **1.3.3** 및 최신/**SPA5xx** 펌웨어 **7.5.6** 및 최신/**CP-78xx-3PCC/CP-88xx-3PCC**를 선택합니다.

단계 **4** **CSR** 파일 필드에서 찾아보기를 클릭하고 서명하려는 CSR을 선택합니다.

단계 **5** 암호화 방법을 선택합니다.

- MD5
- SHA1
- SHA256

SHA256 암호화를 선택하는 것이 좋습니다.

단계 **6** 로그인 지속 시간 드롭다운 목록표에서 적절한 기간(예: 1년)을 선택합니다.

단계 **7** 인증서 서명 요청을 클릭합니다.

단계 8 서명된 인증서를 받는 옵션으로 다음 중 하나를 선택합니다.

- 수신자의 이메일 주소 입력 - 이메일을 통해 인증서를 받으려면 이 필드에 이메일 주소를 입력합니다.
- 다운로드 - 서명된 인증서를 다운로드하려면 이 옵션을 선택합니다.

단계 9 제출을 클릭합니다.

서명된 서버 인증서를 지정한 이메일 주소로 받거나 다운로드할 수 있습니다.

다중 플랫폼 전화기 CA 클라이언트 루트 인증서

Cisco는 다중 플랫폼 전화기 클라이언트 루트 인증서를 서비스 제공자에게 제공합니다. 이 루트 인증서는 각 전화기가 가진 클라이언트 인증서의 신뢰성을 인증합니다. 다중 플랫폼 전화기는 Verisign, Cybertrust 등의 타사에서 제공한 타사 서명 인증서도 지원합니다.

전화기가 개별 인증서를 가지고 있는지 확인하려면 $CCERT 프로비저닝 매크로 변수를 사용합니다. 이 변수는 고유 클라이언트 인증서의 존재 유무에 따라 Installed 또는 Not Installed로 확장됩니다. 일반 인증서의 경우 HTTP 요청 헤더의 사용자 에이전트 필드에서 장치의 일련 번호를 얻을 수 있습니다.

HTTPS 서버가 연결하는 클라이언트에서 SSL 인증서를 요청하도록 구성할 수 있습니다. 활성화된 경우, 서버는 Cisco가 제공하는 다중 플랫폼 전화기 클라이언트 루트 인증서를 사용해 클라이언트 인증서를 확인할 수 있습니다. 그런 다음 서버는 인증서 정보를 CGI로 전달해 추가로 처리할 수 있습니다.

인증서 저장소의 위치는 달라질 수 있습니다. 예를 들어 Apache 설치의 경우, 프로비저닝 서버 서명 인증서, 이와 연결된 개인 키, 다중 플랫폼 전화기 CA 클라이언트 루트 인증서의 저장소에 대한 파일 경로는 다음과 같습니다.

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

구체적인 정보는 HTTPS 서버의 설명서를 참조하십시오.

Cisco 클라이언트 인증서 루트 인증 기관은 각 고유 인증서를 서명합니다. 서비스 제공자는 클라이언트 인증을 위해 해당 루트 인증서를 사용합니다.

중복 프로비저닝 서버

프로비저닝 서버는 IP 주소 또는 FQDN(Fully Qualified Domain Name)으로 지정할 수 있습니다. FQDN을 사용하면 중복 프로비저닝 서버를 구축하는 데 용이합니다. 프로비저닝 서버를 FQDN을 통해 식

별하는 경우, 전화기는 DNS를 통해 FQDN을 IP 주소로 확인하려고 시도합니다. 프로비저닝에 대해서는 DNS A-레코드만 지원되며, DNS SRV 주소 확인은 사용할 수 없습니다. 전화기는 서버가 응답할 때까지 A-레코드를 계속 처리합니다. A-레코드 응답과 연결된 서버가 없는 경우 전화기는 syslog 서버에 오류를 기록합니다.

Syslog 서버

전화기에서 <Syslog Server> 파라미터를 사용하여 syslog 서버를 설정하는 경우, 재동기화 및 업그레이드 작업을 수행하면 syslog 서버로 메시지가 전송됩니다. 메시지는 원격 파일 요청의 시작 시(구성 프로파일 또는 펌웨어 로드) 및 작업 완료 시(성공 또는 실패를 나타냄) 생성될 수 있습니다.

로깅되는 메시지는 다음 매개 변수에서 구성되며 매크로는 실제 syslog 메시지로 확장됩니다.

방화벽 활성화

운영 체제를 강화하여 전화기 보안이 향상되었습니다. 보안 강화를 사용하면 전화기에서 방화벽을 사용하여 악의적인 수신 트래픽으로부터 보호할 수 있습니다. 방화벽은 수신 및 발신 데이터용 포트를 추적합니다. 예기치 않은 소스에서 수신 트래픽이 감지되면 액세스를 차단합니다. 방화벽은 모든 발신 트래픽을 허용합니다.

방화벽은 정상적으로 차단된 포트를 동적으로 차단 해제할 수 있습니다. 발신 TCP 연결 또는 UDP 흐름은 반환 및 지속적인 트래픽을 위해 포트를 차단 해제합니다. 흐름을 활성화한 상태에서 포트는 차단 해제된 상태로 유지됩니다. 흐름이 종료되거나 만료되면 포트가 차단됨 상태로 복귀됩니다.

레거시 설정, IPv6 멀티캐스트 Ping 음성 > 시스템 > **IPv6** 설정 > 브로드캐스트 에코는 새 방화벽 설정과 관계없이 계속 작동합니다.

일반적으로 방화벽 구성 변경으로 인해 전화기가 다시 시작되지 않습니다. 일반적으로 전화기 소프트 재시작은 방화벽 작동에 영향을 미치지 않습니다.

방화벽은 기본적으로 활성화되어 있습니다. 비활성화된 경우 전화기 웹 페이지에서 활성화할 수 있습니다.

시작하기 전에

전화기 웹 인터페이스 액세스

프로시저

단계 **1** 음성 > 시스템 > 보안 설정을 선택합니다.

단계 **2** 방화벽 드롭다운 목록에서 활성화를 선택합니다.

다음 형식으로 문자열을 입력하여 구성 파일(cfg.xml)에서 이 매개 변수를 구성할 수도 있습니다.

```
<Firewall ua="na">Enabled</Firewall>
```

허용되는 값은 비활성화|활성화입니다. 기본값은 활성화 상태입니다.

단계 **3** 모든 변경 사항 제출을 클릭합니다.
이렇게 하면 방화벽에서 기본 개방형 UDP 및 TCP 포트를 사용할 수 있습니다.

단계 **4** 네트워크를 이전 동작으로 되돌리려면 비활성화를 선택하여 방화벽을 비활성화합니다.

다음 표에서는 기본 개방형 UDP 포트에 대해 설명합니다.

표 ***3:*** 방화벽 기본 개방형 ***UDP*** 포트

기본 개방형 **UDP** 포트	설명
DHCP/DHCPv6	DHCP 클라이언트 포트 68 DHCPv6 클라이언트 포트 546
SIP/UDP	회선 활성화가 예로 설정되고 **SIP** 전송이 **UDP** 또는 자동으로 설정되면 음성 > 내선번호<**n**> > **SIP** 설정 > **SIP** 포트(예: 5060)에서 포트를 설정합니다.
RTP/RTCP	UDP 포트 범위: **RTP** 포트 최소 ~ **RTP** 포트 최대**+1**
PFS(피어 펌웨어 공유)	포트 4051, 업그레이드 활성화 및 피어 펌웨어 공유를 예로 설정하는 경우
TFTP 클라이언트	포트 53240-53245. 원격 서버가 표준 TFTP 포트 69 이외의 포트를 사용하는 경우, 이 포트 범위가 필요합니다. 서버가 표준 포트 69를 사용하는 경우 이 기능을 끌 수 있습니다. 추가 옵션을 사용하여 방화벽 구성, 16 페이지을 참조하세요.
TR-069	UDP/STUN 포트 7999, **TR-069** 활성화가 예로 설정된 경우.

다음 표에서는 기본 개방형 TCP 포트에 대해 설명합니다.

표 ***4:*** 방화벽 기본 개방형 ***TCP*** 포트

기본 개방형 **TCP** 포트	설명
웹 서버	웹 서버 포트를 통해 구성된 포트(기본값 80), 웹 서버 활성화는 예로 설정 되어 있습니다.
PFS(피어 펌웨어 공유)	포트 4051 및 6970, 업그레이드 활성화 및 피어 펌웨어 공유를 모두 예로 설정하는 경우
TR-069	TR-069 연결 요청 URL에서 HTTP/SOAP 포트, **TR-069** 활성화가 예로 설정된 경우. 포트는 8000-9999 범위에서 임의로 선택됩니다.

추가 옵션을 사용하여 방화벽 구성

방화벽 옵션 필드에서 추가 옵션을 구성할 수 있습니다. 필드에 각 옵션에 대한 키워드를 입력하고 키워드를 쉼표(,)로 구분합니다. 일부 키워드에는 값이 있습니다. 콜론(:)을 기준으로 값을 구분합니다.

시작하기 전에

전화기 웹 인터페이스 액세스

프로시저

단계 **1** 음성 > 시스템 > 보안 설정으로 이동합니다.

단계 **2** 방화벽 필드에 대해 활성화됨을 선택합니다.

단계 **3** 방화벽 옵션 필드에 키워드를 입력합니다. 포트 목록은 IPv4 및 IPv6 프로토콜 모두에 적용됩니다.

키워드를 입력할 때

- 키워드를 쉼표(,)로 구분합니다.
- 키워드 값은 콜론(:)으로 구분합니다.

표 *5:* 방화벽 옵션 설정

방화벽 옵션 키워드	설명
필드가 비어 있습니다.	방화벽은 기본 열린 포트를 사용하여 실행됩니다.
NO_ICMP_PING	방화벽은 수신 ICMP/ICMPv6 에코 요청(Ping)을 차단합니다. 이 옵션은 전화기에 대한 일부 유형의 트레이스라우트(traceroute) 요청을 중단할 수 있습니다. Windows **tracert**가 하나의 예입니다. 옵션 조합이 있는 방화벽 옵션 항목의 예: NO_ICMP_PING,TCP:12000,UDP:8000:8010 방화벽은 기본 설정과 다음 추가 옵션을 사용하여 실행됩니다. • 수신 ICMP/ICMPv6 에코(Ping) 요청을 삭제합니다. • 수신 연결을 위해 TCP 포트 12000(IPv4 및 IPv6)을 엽니다. • 수신 요청을 위해 UDP 포트 범위 8000-8010(IPv4 및 IPv6)을 엽니다.

방화벽 옵션 키워드	설명
NO_ICMP_UNREACHABLE	전화기가 UDP 포트에 대해 ICMP/ICMPv6 연결할 수 없는 대상을 전송하지 않습니다. 참고 예외는 항상 RTP 포트 범위에 있는 포트에 대해 연결할 수 없는 대상을 전송하는 것입니다. 이 옵션은 장치에 대한 일부 유형의 **traceroute** 요청을 중단할 수 있습니다. 예를 들어, **Linux** traceroute이 중단될 수 있습니다.
NO_CISCO_TFTP	• 전화기에서 TFTP 클라이언트 포트 범위(UDP 53240:53245)를 열지 않습니다. • 비표준(비 69) TFTP 서버 포트에 대한 요청이 실패합니다. • 표준 TFTP 서버 포트 69에 대한 요청이 작동합니다.
전화기에서 수신 요청을 처리하는 사용자 지정 앱을 실행하는 경우 다음 키워드 및 옵션이 적용됩니다.	
UDP:<xxx>	UDP 포트 <xxx>를 엽니다.
UDP:<xxx:yyy>	UDP 포트 범위 <xxx to yyy>를 엽니다. UDP 포트 옵션(단일 포트 및 포트 범위)을 5개까지 가질 수 있습니다. 예를 들어, 3 UDP:<xxx>과 2 UDP:<xxx:yyy>를 가질 수 있습니다.
TCP:<xxx>	TCP 포트 <xxx>를 엽니다.
TCP:<xxx:yyy>	TCP 포트 범위 <xxx to yyy>를 엽니다. TCP 포트 옵션(단일 포트 및 포트 범위)을 5개까지 가질 수 있습니다. 예를 들어, 4 TCP:<xxx>과 1 TCP:<xxx:yyy>를 가질 수 있습니다.

다음 형식으로 문자열을 입력하여 구성 파일(cfg.xml)에서 이 매개 변수를 구성할 수도 있습니다.

```
<Firewall_Config ua="na">NO_ICMP_PING</Firewall_Config>
```

단계 **4** 모든 변경 사항 제출을 클릭합니다.

암호화 목록 구성

전화기 TLS 애플리케이션에 사용되는 암호 그룹을 지정할 수 있습니다. 지정된 암호화 목록은 TLS 프로토콜을 사용하는모든 애플리케이션에 적용됩니다. 전화기의 TLS 애플리케이션에는 다음이 포함됩니다.

- 고객 CA 프로비저닝
- E911 지리위치
- 펌웨어/Cisco 헤드셋 업그레이드
- LDAPS
- LDAP(StartTLS)
- 사진 다운로드
- 로고 다운로드
- 사전 다운로드
- 프로비저닝
- 보고서 업로드
- PRT 업로드
- TLS를 통한 SIP
- TR-069
- WebSocket API
- XML 서비스
- XSI 서비스

TR-069 매개 변수(`Device.X_CISCO_SecuritySettings.TLSCipherList`) 또는 구성 파일(cfg.xml)을 사용하여 암호 그룹을 지정할 수도 있습니다. 구성 파일에서 다음 형식으로 문자열을 입력합니다.

```
<TLS_Cipher_List ua="na">RSA:!aNULL:!eNULL</TLS_Cipher_List>
```

시작하기 전에

전화기 관리 웹 페이지 액세스는 전화기 웹 인터페이스 액세스의 내용을 참조하십시오.

프로시저

단계 **1** 음성 > 시스템을 선택합니다.

단계 **2** 보안 설정 섹션에서 **TLS** 암호화 목록 필드에 암호 그룹 또는 암호 그룹 조합을 입력합니다.

예:

```
RSA:!aNULL:!eNULL
```

RSA 인증을 사용하는 이러한 암호 그룹을 지원하지만 암호화 및 인증을 제공하지 않는 암호화 그룹은 제외됩니다.

참고 유효한 암호화 목록은 https://www.openssl.org/docs/man1.1.1/man1/ciphers.html에 정의된 형식을 따라야 합니다. 전화기에서 OpenSSL 웹 페이지에 나열된 암호화 문자열을 모두 지원하지는 않습니다. 지원되는 문자열에 대해서는 지원되는 암호화 문자열, 20 페이지의 내용을 참조하십시오.

TLS 암호화 목록 필드에 공백 또는 잘못된 값이 있는 경우 사용되는 암호 그룹은 애플리케이션에 따라 달라집니다. 이 필드에 공백 또는 잘못된 값이 있는 경우 애플리케이션에서 사용하는 그룹은 다음 목록을 참조하십시오.

- 웹 서버(HTTPS) 애플리케이션은 다음 암호화 그룹을 사용합니다.
  - **ECDHE-RSA-AES256-GCM-SHA384**
  - **ECDHE-RSA-AES128-GCM-SHA256**
  - **AES256-SHA**
  - **AES128-SHA**
  - **DES-CBC3-SHA**
- XMPP는 암호화 목록 **HIGH:MEDIUM:AES:@STRENGTH**을 사용합니다.
- curl 라이브러리를 사용하는 SIP, TR-069 및 기타 애플리케이션은 기본 암호 문자열을 사용합니다. 기본 암호 문자열에는 전화기가 지원하는 다음 암호화 그룹이 포함됩니다.

```
DEFAULT Cipher Suites (28 suites):
        ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        ECDHE_RSA_WITH_AES_256_GCM_SHA384
        DHE_RSA_WITH_AES_256_GCM_SHA384
        ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        ECDHE_RSA_WITH_AES_128_GCM_SHA256
        DHE_RSA_WITH_AES_128_GCM_SHA256
        ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
        ECDHE_RSA_WITH_AES_256_CBC_SHA384
        DHE_RSA_WITH_AES_256_CBC_SHA256
        ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        ECDHE_RSA_WITH_AES_128_CBC_SHA256
        DHE_RSA_WITH_AES_128_CBC_SHA256
        ECDHE_ECDSA_WITH_AES_256_CBC_SHA
        ECDHE_RSA_WITH_AES_256_CBC_SHA
        DHE_RSA_WITH_AES_256_CBC_SHA
        ECDHE_ECDSA_WITH_AES_128_CBC_SHA
        ECDHE_RSA_WITH_AES_128_CBC_SHA
        DHE_RSA_WITH_AES_128_CBC_SHA
        RSA_WITH_AES_256_GCM_SHA384
        RSA_WITH_AES_128_GCM_SHA256
        RSA_WITH_AES_256_CBC_SHA256
        RSA_WITH_AES_128_CBC_SHA256
```

```
RSA_WITH_AES_256_CBC_SHA
RSA_WITH_AES_128_CBC_SHA
EMPTY_RENEGOTIATION_INFO_SCSV
```

단계 **3** 모든 변경 사항 제출을 클릭합니다.

지원되는 암호화 문자열

다음에 나열된 지원되는 암호화 문자열은 OpenSSL 1.1.1d 표준을 기반으로 합니다.

표 ***6:*** 지원되는 암호화 문자열***(OpenSSL 1.1.1d)***

문자열	문자열	문자열
DEFAULT	kECDHE, EECDH	CAMELLIA128, CAMELLIA256, CAMELLIA
COMPLEMENTOFDEFAULT	kECDHE, EECDH	CHACHA20
ALL	ECDH	SEED
COMPLEMENTOFALL	AECDH	MD5
HIGH	aRSA	SHA1, SHA
Medium	aDSS, DSS	SHA256, SHA384
eNULL, NULL	aECDSA, ECDSA	SUITEB128, SUITEB128ONLY, SUITEB192
aNULL	TLSv1.2, TLSv1, SSLv3	
kRSA, RSA	AES128, AES256, AES	
kDHE, kEDH, DH	AESGCM	
DHE, EDH	AESCCM, AESCCM8	
ADH	ARIA128, ARIA256, ARIA	

TLS를 통한 SIP에 대한 호스트 이름 확인 활성화

TLS를 사용하는 경우 전화 회선에서 전화기 보안을 강화할 수 있습니다. 전화기 회선에서 호스트 이름을 확인하여 연결이 안전한지 확인할 수 있습니다.

TLS 연결을 통해 전화기에서 호스트 이름을 확인하여 서버 ID를 확인할 수 있습니다. 전화기에서 두 개의 SAN(주체 대체 이름)과 CN(주체 일반 이름)을 모두 확인할 수 있습니다. 유효한 인증서의 호스트 이름이 서버와 통신하는 데 사용되는 호스트 이름과 일치하는 경우 TLS 연결이 설정됩니다. 그렇지 않으면 TLS 연결이 실패합니다.

전화기는 항상 다음 애플리케이션에 대한 호스트 이름을 확인합니다.

- LDAPS
- LDAP(StartTLS)
- XMPP
- HTTPS를 통한 이미지 업그레이드
- HTTPS를 통한 XSI
- HTTPS를 통한 파일 다운로드
- TR-069

전화선이 TLS를 통해 SIP 메시지를 전송하는 경우, 내선 번호**(n)** 탭의 **TLS** 이름 확인 필드를 사용하여 호스트네임 확인을 활성화하거나 무시하도록 회선을 설정할 수 있습니다.

시작하기 전에

- 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조
- 내선 번호**(n)**) 탭에서 **SIP** 전송을 **TLS**로 설정합니다.

프로시저

단계 **1** 음성 > 내선 번호**(n)**로 이동합니다.

단계 **2** 프록시 및 등록 섹션에서 호스트 이름 확인을 활성화하려면 **TLS** 이름 확인 필드를 예로 설정하고 호스트 이름 확인을 사용하지 않으려면 아니요로 설정합니다.

다음 형식으로 문자열을 입력하여 구성 파일(cfg.xml)에서 이 매개 변수를 구성할 수도 있습니다.

```
<TLS_Name_Validate_1_ ua="na">Yes</TLS_Name_Validate_1_>
```

허용되는 값은 예 또는 아니요입니다. 기본 설정은 예입니다.

단계 **3** 모든 변경 사항 제출을 클릭합니다.

미디어 평면 보안 협상을 위해 클라이언트 시작 모드 활성화

미디어 세션을 보호하기 위해 전화기에서 서버와 미디어 평면 보안 협상을 시작하도록 구성할 수 있습니다. 보안 메커니즘은 RFC 3329에 언급된 표준과 내선 번호 드래프트 미디어를 위한 보안 메커니즘 이름을 따릅니다(https://tools.ietf.org/html/draft-dawes-sipcore-mediasec-parameter-08#ref-2 참조). 전화기와 서버 간의 협상 전송은 UDP, TCP 및 TLS를 통해 SIP 프로토콜을 사용할 수 있습니다. 신호 처리 전송 프로토콜이 TLS 인 경우에만 미디어 평면 보안 협상이 적용되도록 제한할 수 있습니다.

설정 파일(cfg.xml)에서 이 매개 변수를 설정할 수도 있습니다. 각 매개 변수를 구성하려면 미디어 평면 보안 협상을 위한 매개 변수, 22 페이지에서 문자열의 구문을 참조하십시오.

시작하기 전에

전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 내선 번호**(n)**를 선택합니다.

단계 **2** **SIP** 설정 섹션에서 미디어 평면 보안 협상을 위한 매개 변수, 22 페이지에 정의된 대로 **MediaSec** 요청 및 **MediaSec Over TLS**만 해당 필드를 설정합니다.

단계 **3** 모든 변경 사항 제출을 클릭합니다.

미디어 평면 보안 협상을 위한 매개 변수

다음 테이블에서는 전화기 웹 인터페이스의 음성 > 내선 번호**(n)** 탭에 있는 **SIP** 설정 섹션에서 미디어 평면 보안 협상에 대한 파라미터의 기능과 사용법을 정의합니다. 또한 전화기 구성 파일(cfg.xml)에 XML 코드로 추가되어 매개 변수를 구성하는 문자열 구문을 정의합니다.

표 *7:* 미디어 평면 보안 협상을 위한 매개 변수

매개 변수	설명
MediaSec 요청	전화기가 서버와의 미디어 평면 보안 협상을 시작하는지 여부를 지정합니다. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. `<MediaSec_Request_1_ ua="na">Yes</MediaSec_Request_1_>` • 전화기 웹 인터페이스에서 이 필드를 **Yes** 또는 **No**로 설정합니다. 허용되는 값: 예|아니요 • 예 - 클라이언트 시작 모드입니다. 전화기가 미디어 평면 보안 협상을 시작합니다. • 아니요 - 서버 시작 모드입니다. 서버가 미디어 평면 보안 협상을 시작합니다. 전화기에서 협상을 시작하지는 않지만 서버에서 협상 요청을 처리하여 보안 통화를 설정할 수 있습니다. 기본값: 아니요

매개 변수	설명
MediaSec Over TLS만 해당	미디어 평면 보안 협상이 적용되는 신호 처리 전송 프로토콜을 지정합니다. 이 필드를 예로 설정하기 전에 신호 처리 전송 프로토콜이 TLS인지 확인하십시오. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. `<MediaSec_Over_TLS_Only_1_ ua="na">No</MediaSec_Over_TLS_Only_1_>` • 전화기 웹 인터페이스에서 이 필드를 **Yes** 또는 **No**로 설정합니다. 허용되는 값: 예|아니요 • 예 - 신호 처리 전송 프로토콜이 TLS인 경우에만 전화기에서 미디어 평면 보안 협상을 시작하거나 처리합니다. • 아니요 - 신호 처리 전송 프로토콜에 관계없이 전화기에서 미디어 평면 보안 협상을 시작하고 처리합니다. 기본값: 아니요

802.1X 인증

Cisco IP 전화기s use Cisco Discovery Protocol (CDP) to identify the LAN switch and determine parameters such as VLAN allocation and inline power requirements. 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. Cisco IP 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 Secure Access Control Server(ACS)(또는 기타 타사 인증 서버): 인증 서버와 전화기가 모두 전화기를 인증하는 공유 비밀로 구성되어야 합니다.
- 802.1X를 지원하는 LAN: 스위치는 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 스위치는 멀티도메인 인증을 지원합니다. PC를 전화기의 PC 포트에 연결할 수 있는지 여부는 스위치 구성에서 결정합니다.
  - 예: 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.
  - 아니요: 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.

802.1X 인증 활성화

전화기에서 802.1 X 인증을 활성화할 수 있습니다. 802.1 X 인증이 활성화되면 전화기는 802.1 X 인증을 사용하여 네트워크 액세스를 요청합니다. 802.1 X 인증을 끄면 전화기에서 CDP를 사용하여 VLAN 및 네트워크 액세스를 취득합니다. 전화기 화면 메뉴에서 트랜잭션 상태를 볼 수도 있습니다.

프로시저

단계 **1** 802.1 X 인증을 활성화하려면 다음 작업 중 하나를 수행하십시오.

- 전화기 웹 인터페이스에서 **Voice** > **System**을 선택하고 **Enable 802.1X Authentication** 필드를 **Yes**로 설정합니다. 그런 다음 모든 변경 사항 제출을 클릭합니다.
- 구성 파일(cfg.xml)에서 다음 형식으로 문자열을 입력합니다.

```
<Enable_802.1X_Authentication ua="rw">Yes</Enable_802.1X_Authentication>
```

- 전화기에서 애플리케이션 > 네트워크 구성 > 이더넷 구성 > **802.1X** 인증을 누릅니다. 그런 다음, 선택 버튼을 사용하여 장치 인증 필드를 켜기로 전환하고 제출을 누릅니다.

단계 **2** (선택 사항) 트랜잭션 상태를 선택하여 다음 항목을 봅니다.

- 트랜잭션 상태: 802.1x 인증의 상태를 표시합니다. 상태는 다음이 될 수 있습니다.
  - 인증 중: 인증 프로세스가 진행 중임을 나타냅니다.
  - 인증됨: 전화기가 인증되었음을 나타냅니다.
  - 비활성화됨: 802.1x 인증이 전화기에서 활성화되지 않았음을 나타냅니다.
- 프로토콜: 802.1x 인증에 사용되는 EAP 메서드를 표시합니다. 프로토콜은 EAP-FAST 또는 EAP-TLS일 수 있습니다.

단계 **3** 뒤로를 누르면 메뉴를 종료합니다.

프록시 서버 설정

프록시 서버를 사용하여 보안을 향상하도록 전화기를 설정할 수 있습니다. 프록시 서버는 전화기와 인터넷 사이에서 방화벽 역할을 합니다. 설정이 성공적으로 완료되면 전화기는 사이버 공격으로부터 전화기를 보호하는 프록시 서버를 통해 인터넷에 연결됩니다.

자동 설정 스크립트를 사용하거나 호스트 서버(호스트네임 또는 IP 주소)와 프록시 서버의 포트를 수동으로 설정하여 프록시 서버를 설정할 수 있습니다.

설정이 완료되면 HTTP 프록시 기능은 HTTP 프로토콜을 사용하는 모든 애플리케이션에 적용됩니다. 애플리케이션에는 다음이 포함됩니다.

- GDS(활성화 코드 온보딩)
- EDOS 장치 활성화
- (EDOS 및 GDS를 통한) Webex Cloud로 온보딩
- 인증서 인증
- 프로비저닝
- 펌웨어 업그레이드
- 전화기 상태 보고서
- PRT 업로드
- XSI 서비스
- Webex 서비스

시작하기 전에

전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 시스템을 선택합니다.

단계 **2** **HTTP** 프록시 설정 섹션에서 요구 사항에 따라 프록시 모드 파라미터와 기타 파라미터를 설정합니다. 세부 절차는 다음 단계에서 제공합니다.

단계 **3** 다음 작업 중 하나를 수행합니다.

- 프록시 모드가 자동:
  - 자동 검색 사용**(WPAD)**이 예인 경우, 추가 작업이 필요하지 않습니다. 전화기는 WPAD(웹 프록시 자동 검색) 프로토콜에 의해 PAC(프록시 자동 설정) 파일을 자동으로 검색합니다.
  - 자동 검색 사용**(WPAD)**이 아니요인 경우, **PAC URL**에 유효한 URL을 입력합니다.
- 프록시 모드가 수동:
  - 프록시 서버에 인증 필요가 아니요인 경우, 프록시 호스트에 프록시 서버를 입력하고 프록시 포트에 프록시 포트를 입력합니다.
  - 프록시 서버에 인증 필요가 예인 경우, 프록시 호스트에 프록시 서버를 입력하고 프록시 포트에 프록시 포트를 입력합니다. 사용자 이름에 사용자 이름을 입력하고 암호에 암호를 입력합니다.
- 프록시 모드가 끄기**(Off)** 상태이며 전화기에서 HTTP 프록시 기능을 사용할 수 없습니다.

전화기 설정 파일(cfg.xml)에서 이 매개 변수를 설정할 수도 있습니다. 각 파라미터를 설정하려면 HTTP 프록시 설정을 위한 파라미터, 26 페이지에서 문자열의 구문을 참조하십시오.

단계 **4** 모든 변경 사항 제출을 클릭합니다.

HTTP 프록시 설정을 위한 파라미터

다음 테이블에서는 전화기 웹 인터페이스의 음성 > 시스템 탭에 있는 **HTTP** 프록시 설정 섹션에서 HTTP 프록시 파라미터의 기능과 사용법을 정의합니다. 또한 전화기 구성 파일(cfg.xml)에 XML 코드로 추가되어 매개 변수를 구성하는 문자열 구문을 정의합니다.

표 *8: HTTP* 프록시 설정을 위한 파라미터

매개 변수	설명과 기본값
프록시 모드	전화기에서 사용 하는 HTTP 프록시 모드를 지정하거나 HTTP 프록시 기능을 비활성화합니다. • 자동 전화기에서 PAC(프록시 자동 설정) 파일을 자동으로 검색하여 프록시 서버를 선택합니다. 이 모드에서는 WPAD(웹 프록시 자동 검색) 프로토콜을 사용하여 PAC 파일을 검색할지 아니면 PAC 파일의 유효한 URL을 수동으로 입력할지 여부를 결정할 수 있습니다. 파라미터에 관한 자세한 내용은 자동 검색(WPAD) 및 PAC URL 사용을 참조하세요. • 수동 서버(호스트네임 또는 IP 주소)와 프록시 서버의 포트를 수동으로 지정해야 합니다. 파라미터에 관한 자세한 내용은 프록시 호스트 및 프록시 포트를 참조하십시오. • 끄기 전화기에서 HTTP 프록시 기능을 비활성화합니다. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. `<Proxy_Mode ua="rw">Off</Proxy_Mode>` • 전화기 웹 인터페이스에서 프록시 모드를 선택하거나 기능을 비활성화합니다. 허용되는 값: 자동, 수동 및 끄기 기본값: 끄기

매개 변수	설명과 기본값
자동 검색(WPAD) 사용	전화기에서 WPAD(웹 프록시 자동 검색) 프로토콜을 사용하여 PAC 파일을 검색할지 여부를 결정합니다. WPAD 프로토콜은 DHCP 또는 DNS를 사용하거나 두 네트워크 프로토콜을 모두 사용하여 PAC(프록시 자동 설정) 파일을 자동으로 찾습니다. PAC 파일은 지정된 URL에 대한 프록시 서버를 선택하는 데 사용됩니다. 이 파일은 로컬 또는 네트워크에서 호스팅할 수 있습니다. • 프록시 모드가 자동으로 설정된 경우에는 파라미터 설정이 적용됩니다. • 파라미터를 아니요로 설정하는 경우, PAC URL을 지정해야 합니다. 파라미터에 관한 자세한 내용은 PAC URL을 참조하세요. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. <Use_Auto_Discovery__WPAD_ ua="rw">Yes</Use_Auto_Discovery__WPAD_> • 전화기 웹 인터페이스에서 필요에 따라 예 또는 아니요를 선택합니다. 허용되는 값: 예 및 아니요 기본값: 예
PAC URL	PAC 파일의 URL입니다. 예를 들면 http://proxy.department.branch.example.com이 있습니다. TFTP, HTTP, HTTPS가 지원됩니다. 프록시 모드를 자동으로 설정하고 자동 검색**(WPAD)** 사용을 아니요로 사용하는 경우, 이 파라미터를 설정해야 합니다. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. <PAC_URL ua="rw">http://proxy.department.branch.example.com/pac</PAC_URL> • 전화기 웹 인터페이스에서 PAC 파일을 찾는 유효한 URL을 입력합니다. 기본값: 비어 있음

매개 변수	설명과 기본값

프록시 호스트	전화기에서 액세스할 프록시 호스트 서버의 IP 주소 또는 호스트네임입니다.
	예:
	`proxy.example.com`
	체계(`http://` 또는 `https://`)는 필요하지 않습니다.
	프록시 모드를 수동으로 설정한 경우에는 이 파라미터를 설정해야 합니다.
	다음 중 하나를 수행합니다.
	• XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다.
	`<Proxy_Host ua="rw">proxy.example.com</Proxy_Host>`
	• 전화기 웹 인터페이스에서 프록시 서버의 IP 주소 또는 호스트네임을 입력합니다.
	기본값: 비어 있음

프록시 포트	프록시 호스트 서버의 포트 번호입니다. 프록시 모드를 수동으로 설정한 경우에는 이 파라미터를 설정해야 합니다. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. `<Proxy_Port ua="rw">3128</Proxy_Port>` • 전화기 웹 인터페이스에서 서버 포트를 입력합니다. 기본값: 3128

매개 변수	설명과 기본값
프록시 서버에 인증 필요	사용자가 프록시 서버에 필요한 인증 자격 증명(사용자 이름 및 암호)을 제공해야 하는지 여부를 결정합니다. 이 파라미터는 프록시 서버의 실제 동작에 따라 설정됩니다. 파라미터를 예로 설정하는 경우 사용자 이름과 암호를 설정해야 합니다. 파라미터에 관한 자세한 내용은 사용자 이름 및 암호를 참조하세요. 프록시 모드가 수동으로 설정된 경우에는 파라미터 설정이 적용됩니다. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. `<Proxy_Server_Requires_Authentication ua="rw">No</Proxy_Server_Requires_Authentication>` • 전화기 웹 인터페이스에서 이 필드를 필요에 따라 예 또는 아니요로 설정합니다. 허용되는 값: 예 및 아니요 기본값: 아니요
사용자 이름	프록시 서버의 자격 증명 사용자에 대한 사용자 이름입니다. 프록시 모드가 수동으로 설정되어 있고 프록시 서버에 인증 필요가 예로 설정되어 있는 경우에는 파라미터를 설정해야 합니다. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. `<Proxy_Username ua="rw">Example</Proxy_Username>` • 전화기 웹 인터페이스에서 사용자 이름을 입력합니다. 기본값: 비어 있음

매개 변수	설명과 기본값
암호	프록시 인증 목적으로 지정된 사용자 이름의 암호. 프록시 모드가 수동으로 설정되어 있고 프록시 서버에 인증 필요가 예로 설정되어 있는 경우에는 파라미터를 설정해야 합니다. 다음 중 하나를 수행합니다. • XML(cfg.xml)이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. <Proxy_Password ua="rw">Example</Proxy_Password> • 전화기 웹 인터페이스에서 사용자의 프록시 인증에 대해 유효한 암호를 입력합니다. 기본값: 비어 있음

FIPS 모드 활성화

전화기를 FIPS(Federal Information Processing Standards)를 준수하도록 만들 수 있습니다.

FIPS는 비군사 정부 및 정부 계약자 및 기관과 협력하는 공급업체에서 사용하기 위한 문서 처리, 암호화 알고리즘 및 기타 정보 기술 표준을 설명하는 표준 집합입니다. OpenSSL FOM(FIPS Object Module)은 신중하게 정의된 소프트웨어 구성 요소이며 OpenSSL 라이브러리와의 호환성을 위해 설계되었으므로 OpenSSL 라이브러리와 API를 사용하는 제품은 최소한의 노력으로 FIPS 140-2 유효성이 검증된 암호화를 사용하도록 변환할 수 있습니다.

FIPS 모드에는 다음 제한 사항이 있습니다.

- TR069가 비활성화됨
- HTTP 다이제스트 인증이 비활성화됨

시작하기 전에

- 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 시스템을 선택합니다.

단계 **2** 보안 설정 섹션의 **FIPS** 모드 매개 변수에서 예 또는 아니요를 선택합니다.

FIPS 모드를 활성화하는 데 실패하면 전화기에 보안 오류 메시지가 표시되고 전화기를 다시 시작해야 합니다.

또한 FIPS 모드 활성화가 실패하면 전화기에서 상태 메시지 화면에 FIPS 관련 오류 메시지가 표시됩니다.

단계 3 모든 변경 사항 제출을 클릭합니다.
FIPS를 활성화하면 전화기에서 다음 기능이 원활하게 작동합니다.

이미지 인증	PRT 업로드	하나의 버튼으로 참가(OBTJ)
보안 저장소	펌웨어 업그레이드	TLS를 통한 SIP
구성 파일 암호화	프로필 재동기화	SRTP
802.1x	온보드 서비스	SIP 다이제스트(RFC 8760)
HTTP 서버	Webex 온보딩, Webex 통화 로그, Webex 디렉터리	Http 프록시

Cisco 제품 보안 개요

이 제품은 암호화 기능을 포함하고 있으며 수입, 수출, 운송 및 사용을 규제하는 미국 및 현지 법규의 적용을 받습니다. Cisco 암호화 제품을 제공하는 것은 제3자에게 이 암호화의 수입, 수출, 유통 또는 사용 권한을 부여하는 것을 의미하는 것이 아닙니다. 수입자, 수출자, 유통업자 및 사용자는 미국과 현지 법규를 준수할 책임이 있습니다. 이 제품을 사용하면 해당 법률 및 규정을 준수하기로 동의하는 것입니다. 미국 및 현지 법규를 준수할 수 없는 경우 이 제품을 즉시 반품하십시오.

미국 수출 규정과 관련한 자세한 내용은 웹 사이트(https://www.bis.doc.gov/policiesandregulations/ear/index.htm)를 참조하십시오.