프로비저닝 방법

BroadSoft 서버를 사용하여 전화기 프로비저닝

BroadSoft 서버 사용자만 해당됩니다.

Cisco IP 다중 플랫폼 전화기를 BroadWorks 플랫폼에 등록할 수 있습니다.

프로시저

단계 **1** BroadSoft Xchange에서 CPE 키트를 다운로드합니다. 최신 CPE 키트를 얻으려면 URL: https://xchange.broadsoft.com으로 이동합니다.

단계 **2** 최신 DTAF 파일을 BroadWorks(시스템 수준) 서버에 업로드합니다.

자세한 내용을 보려면 URL:(https://xchange.broadsoft.com/node/1031047)로 이동합니다. *BroadSoft* 파트너 구성 가이드에 액세스하여 섹션 "*BroadWorks* 장치 프로파일 유형 구성"을 참조하십시오.

단계 **3** Broadworks 장치 프로파일 유형을 구성합니다.

장치 프로파일 유형을 구성하는 방법에 대한 자세한 내용은 다음 URL을 방문하십시오.

https://xchange.broadsoft.com/node/1031047. *BroadSoft* 파트너 구성 가이드에 액세스하고 "*Broadworks* 장치 프로파일 유형 구성" 섹션을 참조하십시오.

프로비저닝 예 개요

이 장에서는 전화기와 프로비저닝 서버 간에 구성 프로파일을 전송하는 절차의 예를 설명합니다.

구성 프로파일 생성에 대한 내용은 프로비저닝 형식를 참조하십시오.

기본 재동기화

이 섹션에서는 전화기의 기본 재동기화 기능을 보여줍니다.

Syslog를 사용하여 메시지 로깅

프로비저닝과 관련된 메시지를 포함하여 UDP를 통해 syslog 서버에 로깅 메시지를 전송하도록 전화기를 구성할 수 있습니다. 이 서버를 식별하기 위해 전화기 웹 인터페이스(전화기 웹 인터페이스 액세스 참조)에 액세스하고 음성 > 시스템을 선택한 후 선택적 네트워크 설정 섹션의 **Syslog** 서버 파라미터에서 서버를 식별할 수 있습니다. syslog 서버 IP 주소를 장치에 구성하고 나머지 절차 중에 생성되는 메시지를 확인하십시오.

이 정보를 얻으려면 전화기 웹 인터페이스에 액세스하고 **Info** > **Debug Info** > **Control Logs**를 선택하고 **messages**를 클릭하면 됩니다.

시작하기 전에

프로시저

단계 **1** 로컬 PC에 syslog 서버를 설치하고 활성화합니다.

단계 **2** PC IP 주소를 프로파일의 Syslog_Server 매개 변수로 프로그래밍하고 변경을 제출합니다.

```
<Syslog_Server>192.168.1.210</Syslog_Server>
```

단계 **3** 시스템 탭을 클릭하고 로컬 syslog 서버의 값을 Syslog_Server 매개 변수에 입력합니다.

단계 **4** TFTP 재동기화, 3 페이지에 설명된 대로 재동기화 작업을 반복합니다.

장치는 재동기화 중에 두 개의 syslog 메시지를 생성합니다. 첫 번째 메시지는 요청이 진행 중임을 나타냅니다. 두 번째 메시지는 재동기화의 성공 또는 실패를 나타냅니다.

단계 **5** syslog 서버가 다음과 비슷한 메시지가 받았는지 확인합니다.

```
CP-88xx-3PCC 00:0e:08:ab:cd:ef –- Successful resync tftp://192.168.1.200/basic.txt
```

상세 메시지는 syslog 서버의 IP 주소를 사용하여 (Syslog_Server 매개 변수 대신) Debug_Server 매개 변수를 프로그래밍하고 Debug_Level을 0 ~ 3 사이의 값(3이 가장 자세함)으로 설정하면 얻을 수 있습니다.

```
<Debug_Server>192.168.1.210</Debug_Server>
<Debug_Level>3</Debug_Level>
```

이러한 메시지의 내용은 다음 매개 변수를 사용하여 구성합니다.

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

이러한 매개 변수 중 제거된 매개 변수가 있으면, 해당하는 syslog 메시지가 생성되지 않습니다.

TFTP 재동기화

전화기는 구성 프로파일을 검색하기 위한 여러 네트워크 프로토콜을 지원합니다. 가장 기본적인 프로파일 전송 프로토콜은 TFTP(RFC1350)입니다. TFTP는 개인 LAN 네트워크 내에서 네트워크 장치를 프로비저닝하는 데 널리 사용됩니다. TFTP는 인터넷을 통한 원격 엔드포인트를 구축하는 데는 권장되지 않지만, 소규모 조직 내의 구축, 사내 프로비저닝, 개발 및 테스트 용도로 편리하게 사용할 수 있습니다. 사내 프로비저닝에 대한 자세한 내용은 사내 장치 사전 프로비저닝를 참조하십시오. 다음 절차에서 TFTP 서버에서 파일을 다운로드한 후 프로파일이 수정됩니다.

프로시저

단계 **1** LAN 환경 내에서 PC 및 전화기를 허브, 스위치 또는 소형 라우터에 연결합니다.

단계 **2** PC에서 TFTP 서버를 설치 및 활성화합니다.

단계 **3** 다음 예와 같이 텍스트 편집기를 사용해 구성 프로파일을 만들고 GPP_A의 값을 12345678로 설정합니다.

```
<flat-profile>
  <GPP_A> 12345678
  </GPP_A>
</flat-profile>
```

단계 **4** TFTP 서버의 루트 디렉터리에 `basic.txt`라는 이름으로 프로파일을 저장합니다.

TFTP 서버가 올바르게 구성되었는지 확인하려면 전화기가 아닌 TFTP 클라이언트를 사용하여 `basic.txt` 파일을 요청하면 됩니다. 가급적이면 프로비저닝 서버가 아닌 별도의 호스트에서 실행되는 TFTP 클라이언트를 사용하는 것이 좋습니다.

단계 **5** PC 웹 브라우저를 열고 관리자/고급 구성 페이지로 이동합니다. 예를 들어 전화기의 IP 주소가 192.168.1.100인 경우 다음과 같습니다.

```
http://192.168.1.100/admin/advanced
```

단계 **6** 음성 > 프로비저닝 탭을 선택하고 일반 목적 매개 변수 GPP_A ~ GPP_P의 값을 검사합니다. 비어 있을 것입니다.

단계 **7** 웹 브라우저 창에서 재동기화 URL을 열어 테스트 전화기를 `basic.txt` 구성 프로파일로 재동기화합니다.

TFTP 서버의 IP 주소가 192.168.1.200인 경우 명령은 다음의 예와 비슷합니다.

```
http://192.168.1.100/admin/resync?tftp://192.168.1.200/basic.txt
```

전화기가 이 명령을 수신하면 IP 주소 192.168.1.100에 있는 장치가 IP 주소 192.168.1.200에 있는 TFTP 서버로 `basic.txt` 파일을 요청합니다. 전화기는 다운로드한 파일을 구문 분석하고 GPP_A 매개 변수를 12345678 값으로 업데이트합니다.

단계 **8** 매개 변수가 올바르게 업데이트되었는지 확인합니다. PC 웹 브라우저의 구성 페이지를 새로 고치고 음성 > **Provisioning** 탭을 선택합니다.

이제 GPP_A 매개 변수에 12345678 값이 포함됩니다.

Syslog 서버에 메시지 로그

syslog 서버는 전화기에서 매개 변수를 사용하여 구성하며 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.

XML(cfg.xml) 코드를 사용하여 전화기 설정 파일에서 매개 변수를 설정할 수도 있습니다. 각 매개 변수를 구성하려면 시스템 로그 매개 변수, 5 페이지에서 문자열의 구문을 참조하십시오.

시작하기 전에

- Syslog 서버가 설치되고 구성되었습니다.
- 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 시스템을 클릭합니다.

단계 **2** 옵션 네트워크 구성 섹션에서 **Syslog** 서버에 서버 IP를 입력하고 선택적으로 시스템 로그 매개 변수, 5 페이지에 정된 의**Syslog** 식별자를 지정합니다 .

단계 **3** 선택적으로 시스템 로그 매개 변수, 5 페이지에 정의된 대로 로그 요청 메시지, 로그 성공 메시지 및 로그 실패 메시지를 사용하여 syslog 메시지의 내용을 정의합니다 .

syslog 메시지 콘텐츠를 정의하는 필드는 음성 > 프로비저닝 탭의 설정 프로파일 섹션에 있습니다. 메시지 내용을 지정하지 않으면 필드의 기본 설정이 사용됩니다. 필드 중 제거된 필드가 있으면, 해당하는 메시지가 생성되지 않습니다.

단계 **4** 모든 변경 사항 제출을 클릭하여 구성을 적용합니다.

단계 **5** 구성의 유효성을 확인합니다.

a) TFTP 재동기화를 수행합니다. TFTP 재동기화, 3 페이지 참조

장치는 재동기화 중에 두 개의 syslog 메시지를 생성합니다. 첫 번째 메시지는 요청이 진행 중임을 나타냅니다. 두 번째 메시지는 재동기화의 성공 또는 실패를 나타냅니다.

b) syslog 서버가 다음과 비슷한 메시지가 받았는지 확인합니다.

```
CP-78xx-3PCC 00:0e:08:ab:cd:ef –- Requesting resync tftp://192.168.1.200/basic.txt

CP-88xx-3PCC 00:0e:08:ab:cd:ef –- Successful resync tftp://192.168.1.200/basic.txt
```

시스템 로그 매개 변수

다음 테이블은 전화기 웹페이지의 음성 > 시스템 탭에 있는 선택적 네트워크 설정 섹션에서 syslog 파라미터의 기능과 사용법을 정의합니다. 또한 전화기 구성 파일(cfg.xml)에 XML 코드로 추가되어 매개 변수를 구성하는 문자열 구문을 정의합니다.

표 ***1: Syslog*** 매개 변수

매개 변수명	설명과 기본값
Syslog 서버	전화기 시스템 정보 및 주요 이벤트를 로깅하는 서버를 지정합니다. 디버그 서버 및 syslog 서버가 모두 지정된 경우 syslog 메시지도 디버그 서버에 로그됩니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Syslog_Server ua="na">10.74.30.84</Syslog_Server>` • 전화기 웹 페이지에서 Syslog 서버를 지정합니다.

매개 변수명	설명과 기본값
Syslog 식별자	syslog 서버에 업로드되는 syslog 메시지에 포함할 장치 식별자를 선택합니다. 장치 식별자는 각 메시지의 타임스탬프 뒤에 나타납니다. 식별자에 대한 옵션은 다음과 같습니다. • 없음: 장치 식별자가 없습니다. • $MA: 연속 소문자와 숫자로 표시되는 전화기의 MAC 주소입니다. 예: `c4b9cd811e29` • $MAU: 연속 대문자와 숫자로 표시되는 전화기의 MAC 주소입니다. 예: `C4B9CD811E29` • $MAC: 표준 쉼표로 구분된 형식으로 된 전화기의 MAC 주소입니다. 예: `c4:b9:cd:81:1e:29` • $SN: 전화기의 제품 일련 번호입니다. • **XML(cfg.xml)**이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. `<Syslog_Identifier ua="na">$MAC</Syslog_Identifier>` • 전화기 웹 페이지의 목록에서 식별자를 선택합니다. 기본값: 없음
로그 요청 메시지	재동기화 시도 시작 시 syslog 서버로 전송되는 메시지입니다. 값을 지정하지 않으면 syslog 메시지가 생성되지 않습니다. 기본값은 `$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH`입니다. • **XML(cfg.xml)**이 있는 전화 구성 파일에서, 다음 형식으로 문자열을 입력합니다. `<Log_Request_Msg ua="na">$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH</Log_Request_Msg>`
로그 성공 메시지	재동기화 시도가 성공적으로 완료되면 전송되는 syslog 메시지입니다. 값을 지정하지 않으면 syslog 메시지가 생성되지 않습니다. **XML(cfg.xml)**이 있는 전화 설정 파일에서 문자열을 다음 형식으로 입력합니다. `<Log_Success_Msg ua="na">$PN $MAC -- Successful resync $SCHEME://$SERVIP:$PORT$PATH</Log_Success_Msg>`

매개 변수명	설명과 기본값
로그 실패 메시지	실패한 재동기화 시도 이후 전송되는 syslog 메시지입니다. 값을 지정하지 않으면 syslog 메시지가 생성되지 않습니다. 디폴트 값은 `$PN $MAC -- Resync failed: $ERR`입니다. **XML(cfg.xml)**을 사용하는 전화기 설정 파일에서 문자열을 `<Log_Failure_Msg ua="na">$PN $MAC -- Resync failed: $ERR</Log_Failure_Msg>` 형식으로 입력합니다.

고유한 프로파일, 매크로 확장 및 HTTP

각 전화기의 사용자 ID 또는 표시 이름과 같은 일부 매개 변수를 고유한 값으로 구성해야 하는 구축의 경우, 서비스 제공자가 배포된 각 장치를 위한 고유한 프로파일을 생성하고 프로비저닝 서버에서 이러한 프로파일을 호스팅할 수 있습니다. 각 전화기는 미리 결정된 프로파일 명명 규칙에 따라 자체 프로파일로 재동기화하도록 구성되어야 합니다.

프로파일 URL 구문은 기본 제공 변수의 매크로 확장을 사용하여 MAC 주소나 일련 번호와 같은 각 전화기별 식별 정보를 포함할 수 있습니다. 매크로 확장을 사용하면 각 프로파일의 여러 위치에 이러한 값을 지정할 필요가 없습니다.

프로파일 규칙은 규칙을 전화기에 적용하기 전에 매크로 확장을 거칩니다. 매크로 확장은 다음과 같이 값의 수를 제어합니다.

- $MA는 장치의 12자 MAC 주소(소문자 16진 숫자 사용)로 확장됩니다. 예: 000e08abcdef.
- $SN은 장치의 일련 번호로 확장됩니다. 예: 88012BA01234

다른 값도 모든 일반 목적 매개 변수(GPP_A ~ GPP_P)를 포함하여 같은 방법으로 확장할 수 있습니다. TFTP 재동기화, 3 페이지에서 이 프로세스의 예를 볼 수 있습니다. 매크로 확장은 URL 파일 이름에 제한되지 않으며, 프로파일 규칙 매개 변수의 모든 부분에 적용할 수 있습니다. 이러한 파라미터는 $A ~ $P로 참조합니다. 매크로 확장에 사용할 수 있는 전체 변수 목록은 매크로 확장 변수를 참조하십시오.

이 연습에서는 한 전화기의 전용 프로파일이 TFTP 서버에서 프로비저닝됩니다.

TFTP 서버에서 특정 IP 전화기 프로파일 프로비저닝

프로시저

단계 **1** 전화기의 제품 레이블에서 MAC 주소를 얻습니다. (MAC 주소는 숫자와 소문자 16진수를 사용하는 숫자입니다(예 000e08aabbcc).

단계 2 basic.txt 구성 파일(TFTP 재동기화, 3 페이지 참조)을 새 파일 이름 CP-xxxx-3PCC macaddress.cfg로(xxxx는 모델 번호로 바꿈, macaddress는 전화기의 MAC 주소로 바꿈) 복사합니다.

단계 3 TFTP 서버의 가상 루트 디렉터리로 새 파일을 이동합니다.

단계 4 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

단계 5 음성 > 프로비저닝을 선택합니다.

단계 6 프로파일 규칙 필드에 tftp://192.168.1.200/CP-8841-3PCC$MA.cfg를 입력합니다.

```
<Profile_Rule>
  tftp://192.168.1.200/CP-8841-3PCC$MA.cfg
</Profile_Rule>
```

단계 7 모든 변경 사항 제출을 클릭합니다. 이렇게 하면 즉시 재부팅되고 재동기화됩니다.

다음 재동기화가 발생하면 전화기는 $MA 매크로 식을 확장하여 MAC 주소를 얻고 새 파일을 검색합니다.

HTTP GET 재동기화

HTTP는 TCP 연결을 사용하는 반면, TFTP는 덜 안정적인 UDP를 사용하므로, HTTP가 TFTP보다 안정적인 재동기화 메커니즘을 제공합니다. 뿐만 아니라, HTTP 서버는 TFTP 서버보다 향상된 필터링 및 로깅 기능을 제공합니다.

클라이언트 측에서, 전화기는 서버 측에 특수한 구성 설정 없이도 HTTP를 사용하여 재동기화할 수 있습니다. GET 방식과 HTTP를 사용하는 Profile_Rule 매개 변수 구문은 TFTP에 대해 사용하는 구문과 비슷합니다. 표준 웹 브라우저가 HTTP 서버에서 프로파일을 검색할 수 있다면, 전화기도 검색할 수 있습니다.

HTTP GET을 사용하여 재동기화

프로시저

단계 1 로컬 PC 또는 이용 가능한 다른 호스트에 HTTP 서버를 설치합니다.

오픈소스 Apache 서버는 인터넷에서 다운로드할 수 있습니다.

단계 2 basic.txt 구성 프로파일(TFTP 재동기화, 3 페이지 참조)을 설치된 서버의 가상 루트 디렉터리로 복사합니다.

단계 3 서버 설치와 basic.txt 파일 액세스가 올바른지 확인하기 위해 웹 브라우저로 프로파일에 액세스합니다.

단계 4 해당 프로파일을 주기적으로 다운로드하도록, 테스트 전화기의 Profile_Rule을 수정하여 TFTP 서버 대신 HTTP 서버를 가리키도록 합니다.

예를 들어 HTTP 서버가 192.168.1.300에 있는 경우 다음 값을 입력합니다.

```
<Profile_Rule>
http://192.168.1.200/basic.txt
</Profile_Rule>
```

단계 **5** 모든 변경 사항 제출을 클릭합니다. 이렇게 하면 즉시 재부팅되고 재동기화됩니다.

단계 **6** 전화기가 전송하는 syslog 메시지를 확인합니다. 이제 주기적 재동기화를 할 때 HTTP 서버에서 프로파일을 얻습니다.

단계 **7** HTTP 서버 로그에서 테스트 전화기를 식별하는 정보가 사용자 에이전트의 로그에 어떻게 표시되는지 확인합니다.

이 정보에는 제조업체, 제품 이름, 현재 펌웨어 버전 및 일련 번호가 포함됩니다.

Cisco XML을 통한 프로비저닝

여기에서 xxxx로 지정된 각 전화기를 Cisco XML 기능을 통해 프로비저닝할 수 있습니다.

SIP 통지 패킷을 통해 XML 개체를 전화기로 전송하거나 HTTP Post를 전화기의 CGI 인터페이스(`http://IPAddressPhone/CGI/Execute`)로 전송할 수 있습니다.

CP-xxxx-3PCC는 Cisco XML 기능을 확장하여 XML 개체를 통한 프로비저닝을 지원합니다.

```
<CP-xxxx-3PCCExecute>
        <ExecuteItem URL=Resync:[profile-rule]/>
</CP-xxxx-3PCCExecute>
```

전화기는 XML 개체를 수신한 후 [profile-rule]에서 프로비저닝 파일을 다운로드합니다. 이 규칙은 XML 서비스 애플리케이션의 개발을 간소화하기 위해 매크로를 사용합니다.

매크로 확장과 URL 확인

서버에 다수의 프로파일과 하위 디렉터리를 구성하면 다수의 배포된 장치를 편리하게 관리할 수 있습니다. 프로파일 URL은 다음 항목을 포함할 수 있습니다.

- 프로비저닝 서버 이름 또는 명시적 IP 주소. 프로파일이 프로비저닝 서버를 이름으로 식별하는 경우 전화기는 DNS 조회를 수행하여 이름을 확인합니다.
- 서버 이름 뒤에 표준 구문 `:port`를 사용하여 URL에 지정된 비표준 서버 포트.
- 표준 URL 표기법을 사용하여 지정하고 매크로 확장을 사용하여 관리하는 프로파일이 저장된 서버 가상 루트 디렉터리의 하위 디렉터리

예를 들어 다음 Profile_Rule은 포트 6900에서 연결을 수신하는 prov.telco.com 호스트에서 실행 중인 TFTP 서버에서 `/cisco/config` 서버 하위 디렉터리에 있는 프로파일 파일($PN.cfg)을 요청합니다.

```
<Profile_Rule>
tftp://prov.telco.com:6900/cisco/config/$PN.cfg
```

```
</Profile_Rule>
```

각 전화기의 프로파일은 일반 목적 매개 변수로 식별할 수 있으며, 해당 값은 일반 프로파일 규칙 내에서 매크로 확장을 사용하여 참조됩니다.

예를 들어 GPP_B가 `Dj6Lmp23Q`로 정의되었다고 가정합니다.

Profile_Rule은 다음 값을 가집니다.

```
tftp://prov.telco.com/cisco/$B/$MA.cfg
```

장치가 재동기화하고 매크로가 확장되면 MAC 주소가 000e08012345인 전화기는 다음 URL로 장치 MAC 주소를 포함하는 이름의 프로파일을 요청합니다.

```
tftp://prov.telco.com/cisco/Dj6Lmp23Q/000e08012345.cfg
```

장치를 자동으로 재동기화

장치를 주기적으로 프로비저닝 서버로 재동기화하면, (명시적인 재동기화 요청을 엔드포인트로 전송하는 대신) 서버에 적용한 프로파일 변경 사항을 엔드포인트 장치로 전파할 수 있습니다.

전화기를 주기적으로 서버로 재동기화하려면, Profile_Rule 매개 변수를 사용하여 구성 프로파일 URL을 정의하고, Resync_Periodic 매개 변수를 사용하여 재동기화 주기를 정의합니다.

시작하기 전에

전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 프로비저닝을 선택합니다.

단계 **2** Profile_Rule 매개 변수를 정의합니다. 이 예에서는 TFTP 서버의 IP 주소가 192.168.1.200이라고 가정합니다.

단계 **3** 주기적 재동기화 필드에 테스트를 위한 작은 값(예 **30** 초)을 입력합니다.

단계 **4** 모든 변경 사항 제출을 클릭합니다.

이제 전화기가 새로운 매개 변수 설정으로 URL이 지정하는 구성 파일로 1분당 두 번 재동기화합니다.

단계 **5** syslog 추적에서 결과 메시지를 검사합니다(Syslog를 사용하여 메시지 로깅, 2 페이지 섹션 참조).

단계 **6** 초기화 시 재동기화 필드가 예로 설정되었는지 확인합니다.

```
<Resync_On_Reset>Yes</Resync_On_Reset>
```

단계 **7** 프로비저닝 서버로 재동기화하도록 전화기를 껐다가 켭니다.

서버가 응답하지 않는 등의 이유로 재동기화 작업이 실패한 경우 장치는 재동기화를 다시 시도하기 전에 (재동기화 오류 재시도 지연에 지정된 초만큼) 대기합니다. 재동기화 오류 재시도 지연이 0인 경우 전화기는 재동기화 시도가 실패해도 재동기화를 시도하지 않습니다.

단계 **8** (선택 사항) 재동기화 오류 재시도 지연 필드를 작은 수(예 **30**)로 설정합니다.

```
<Resync_Error_Retry_Delay>30</Resync_Error_Retry_Delay>
```

단계 **9** TFTP 서버를 비활성화하고 syslog 출력에서 결과를 확인합니다.

프로파일 재동기화 매개 변수

다음 테이블에서는 전화기 웹페이지의 음성 > 프로비저닝 탭에 있는 설정 프로파일 섹션에서 프로파일 재동기화 파라미터의 기능과 사용법을 정의합니다. 또한 전화기 구성 파일(cfg.xml)에 XML 코드로 추가되어 매개 변수를 구성하는 문자열 구문을 정의합니다.

매개 변수	설명
프로비저닝 활성화	구성 프로파일 재동기화 작업을 허용하거나 거부합니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Provision_Enable ua="na">예</Provision_Enable>` • 전화기 웹 페이지에서 이 필드를 예로 설정하여 재동기화 작업을 허용하거나 아니요로 설정하여 재동기화 작업을 차단합니다. 기본값: 예
초기화 시 동기화	전원 공급 후 업그레이드 시도가 끝난 후 전화기에서 프로비저닝 서버와의 구성을 재동기화 할지 여부를 지정합니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Resync_On_Reset ua="na">예</Resync_On_Reset>` • 전화기 웹 페이지에서 이 필드를 예로 설정하여 전원 공급이나 재설정 시 재동기화 작업을 허용하거나 아니요로 설정하여 전원 공급이나 재설정 시 재동기화 작업을 차단합니다. 기본값: 예

매개 변수	설명
임의 지연 재동기화	많은 수의 장치가 동시에 켜지고 초기 구성을 시도할 경우 프로비저닝 서버의 과부하를 방지합니다. 이 지연은 장치 전원 켜기 또는 재설정에 따라 초기 구성 시도에서만 유효합니다. 이 매개 변수는 장치가 프로비저닝 서버에 연결하기 전에 대기하는 최대 시간 간격입니다. 실제 지연은 0과 이 값 사이의 의사 난수입니다. 이 매개 변수는 20초 단위로 되어 있습니다. 유효한 값의 범위는 0 - 65535 사이입니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Resync_Random_Delay ua="na">2</Resync_Random_Delay>` • 전화기 웹 페이지에서 전원 공급이나 재설정 후에 전화기에서 재동기화를 지연하도록 단위 수(초)를 지정합니다. 기본값은 2(40초)입니다.
(HHmm)에 재동기화	전화기가 프로비저닝 서버와 재동기화하는 시간(HHmm)입니다. 이 필드의 값은 HHmm 형식으로 시간을 나타내기 위해 0000 - 2400 사이의 네 자리 숫자여야 합니다. 예를 들어 0959는 09:59를 나타냅니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Resync_At__HHmm_ ua="na">0959</Resync_At__HHmm_>` • 전화기 웹 페이지에서 전화기가 재동기화를 시작하는 데 사용할 HHMM 형식의 시간을 지정합니다. 기본값은 비어 있습니다. 값 유효하지 않을 경우 매개 변수가 무시됩니다. 이 매개 변수가 유효한 값으로 설정되면 주기적 재동기화 매개 변수가 무시됩니다.

매개 변수	설명
임의 지연 시 재동기화	많은 수의 장치가 동시에 켜질 경우 프로비저닝 서버의 과부하를 방지합니다. 여러 전화기로부터 재동기화 요청이 서버로 쇄도하는 것을 방지하기 위해, 전화기는 일정한 시간 및 분 범위에 임의의 지연 시간 및 분을 더한 시점에 재동기화합니다(hhmm, hhmm+random_delay) 예를 들어, 임의 지연 = (임의 지연 시 재동기화 + 30)/60분인 경우 입력된 값(초)은 분으로 변환되고 다음 분으로 반올림되어 최종 random_delay 간격을 계산하는 데 사용됩니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Resync_At_Random_Delay ua="na">600</Resync_At_Random_Delay>` • 전화기 웹 페이지에서 시간 기간(초)을 지정합니다. 유효한 값의 범위는 600 - 65535 사이입니다. 값이 600보다 작으면 내부 임의 지연은 0과 600 사이입니다. 기본값은 600초(10분)입니다.
주기적 재동기화	프로비저닝 서버와 주기적으로 재동기화하는 시간 간격입니다. 연결된 재동기화 타이머는 서버와 첫 번째 동기화가 성공해야 활성화됩니다. 올바른 형식은 다음과 같습니다. • 한 정수 예: 입력 **3000**은 3000초 내에 다음 재동기화가 발생함을 나타냅니다. • 여러 정수 예: 입력 **600,1200,300**은 첫 번째 재동기화가 600초 내에 발생하고 두 번째 재동기화가 첫 번째 재동기화 후 1200초 내에 발생하고 세 번째 재동기화가 두 번째 재동기화 후 300초 내에 발생함을 나타냅니다. • 시간 범위 예를 들어, 입력 **2400 + 30**은 성공적인 재동기화 후 2400에서 2430초 사이에 다음 재동기화가 발생함을 나타냅니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Resync_Periodic ua="na">3600</Resync_Periodic>` • 전화기 웹 페이지에서 시간 기간(초)을 지정합니다. 주기적 재동기화를 비활성화 이 매개 변수를 0으로 설정합니다. 기본값은 3600초입니다.

매개 변수	설명
재동기화 오류 재시도 지연	전화기가 서버에서 프로파일을 검색할 수 없어 재동기화 작업이 실패하거나 다운로드한 파일이 충돌하거나 내부 오류가 발생한 경우 전화기는 초 단위로 지정된 시간 이후에 재동기화를 다시 시도합니다. 올바른 형식은 다음과 같습니다. • 한 정수 예: 입력 **300**은 300초 내에 다음 재동기화를 위한 재시도가 발생함을 나타냅니다. • 여러 정수 예: 입력 **600,1200,300**은 첫 번째 재시도가 실패 후 600초 내에 발생하고 두 번째 재시도가 첫 번째 재시도 실패 후 1200초 내에 발생하고 세 번째 재시도가 두 번째 재시도 실패 후 300초 내에 발생함을 나타냅니다. • 시간 범위 예를 들어, 입력 **2400 + 30**은 성공적인 재동기화 실패 후 2400에서 2430초 사이에 다음 재시도가 발생함을 나타냅니다. 지연이 0으로 설정된 경우 장치는 실패한 재동기화 시도 이후에 재동기화를 다시 시도하지 않습니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Resync_Error_Retry_Delay ua="na">60,120,240,480,960,1920,3840,7680,15360,30720,61440,86400</Resync_Error_Retry_Delay>` • 전화기 웹 페이지에서 시간 기간(초)을 지정합니다. 기본값: 60,120,240,480,960,1920,3840,7680,15360,30720,61440,86400

매개 변수	설명
강제 재동기화 지연	전화기가 재동기화를 수행하기 전에 대기하는 최대 지연 시간(초). 장치는 전화 회선 중 하나가 활성화된 동안 재동기화되지 않습니다. 재동기화는 몇 초가 걸릴 수 있으므로, 장치가 재동기화하기 전에 어느 정도 기간 동안 유휴 상태로 유지될 때까지 대기하는 것이 좋습니다. 그러면 사용자가 중단 없이 연속으로 전화를 걸 수 있습니다. 장치에는 해당 회선이 모두 유휴 상태가 되면 카운트다운을 시작하는 타이머가 있습니다. 이 매개 변수는 카운터의 초기 값입니다. 재동기화 이벤트는 이 카운터가 0으로 감소할 때까지 지연됩니다. 유효한 값의 범위는 0 - 65535 사이입니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Forced_Resync_Delay ua="na">14400</Forced_Resync_Delay>` • 전화기 웹 페이지에서 시간 기간(초)을 지정합니다. 기본값은 14,400초입니다.
SIP에서 재동기화	서비스 제공자 프록시 서버에서 전화기로 전송된 SIP NOTIFY 이벤트를 통해 재동기화 작업을 위한 요청을 제어합니다. 활성화된 경우 프록시는 이벤트: 장치로 헤더 재동기화를 포함하는 SIP NOTIFY를 전송하여 재동기화를 요청할 수 있습니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Resync_From_SIP ua="na">예</Resync_From_SIP>` • 전화기 웹 페이지에서예를 선택하여 이 기능을 활성화하거나 아니요를 선택하여 이 기능을 비활성화합니다. 기본값: 예

업그레이드 시도 이후에 재동기화	업그레이드 수행 이후에 재동기화 작업을 활성화하거나 비활성화합니다. 예를 선택하면 펌웨어 업그레이드 후에 동기화가 트리거됩니다.
	• **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다.
	`<Resync_After_Upgrade_Attempt ua="na">예`
	`</Resync_After_Upgrade_Attempt>`
	• 전화기 웹 페이지에서예를 선택하여 펌웨어 업그레이드 후 재동기화를 트리거하거나 아니요를 선택하여 재동기화하지 않습니다.
	기본값: 예

매개 변수	설명

재동기화 트리거 1
재동기화 트리거 2
	이 매개변수에서의 논리 수식이 FALSE로 평가되면 초기화 시 재동기화가 TRUE로 설정된 경우에도 초기화 시 동기화가 **TRUE**로 설정됩니다. 직접 작업 URL 및 SIP 통지를 통한 재동기화만 이러한 재동기화 트리거를 무시합니다.
	매개 변수는 매크로 확장을 거치는 조건식으로 프로그래밍할 수 있습니다. 유효한 매크로 확장에 대해서는 매크로 확장 변수의 내용을 참조하십시오.
	• **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다.
	`<Resync_Trigger_1 ua="na">$UPGTMR gt 300 and $PRVTMR ge 600</Resync_Trigger_1>`
	`<Resync_Trigger_2 ua="na"/>`
	• 전화기 웹 페이지에서 트리거를 지정합니다.
	기본값: 공백

사용자 구성 가능 재동기화	사용자가 전화기 화면 메뉴에서 전화기 재동기화를 수행하도록 허용합니다. 예로 설정하면 사용자는 전화기에서 프로파일 규칙을 입력하여 전화기 구성을 재동기화 할 수 있습니다. 아니요로 설정하면 프로파일 규칙 매개 변수가 전화기 화면 메뉴에 표시되지 않습니다. 프로파일 규칙 매개 변수는 애플리케이션 > 장치 관리 아래에 있습니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<User_Configurable_Resync ua="na">예</User_Configurable_Resync>` • 전화기 웹 페이지에서예를 선택하여 전화기 메뉴에서 프로파일 규칙 매개 변수를 표시하거나 아니요를 선택하여 이 매개 변수를 숨깁니다. 기본값: 예
FNF 시 재동기화 실패	일반적으로 요청된 프로파일을 서버에서 가져올 수 없으면 재동기화가 실패한 것으로 간주합니다. 이 매개 변수는 이 동작을 무시합니다. 아니요로 설정된 경우 서버로부터 `파일을 찾을 수 없음` 응답을 받아도 성공적인 재동기화로 간주합니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Resync_Fails_On_FNF ua="na">예</Resync_Fails_On_FNF>` • 전화기 웹 페이지에서예를 선택하여 `파일을 찾을 수 없음` 응답을 실패한 재동기화로 간주하거나 아니요를 선택하여 `파일을 찾을 수 없음` 응답을 성공한 재동기화로 간주합니다. 기본값: 예

매개 변수	설명
프로파일 인증 유형	프로 파일 계정 인증에 사용할 자격 증명을 지정합니다. 사용 가능한 옵션은 다음과 같습니다. • 비활성화됨: 프로파일 계정 기능을 비활성화합니다. 이 기능이 비활성화되면 프로파일 계정 설정 메뉴가 전화기 화면에 표시되지 않습니다. • 기본 **HTTP** 인증: HTTP 로그인 자격 증명이 프로파일 계정 인증에 사용됩니다. • **XSI** 인증: XSI 로그인 자격 증명 또는 XSI SIP 자격 증명이 프로파일 계정 인증에 사용됩니다. 인증 자격 증명은 전화기의 **XSI** 인증 유형에 따라 달라집니다. • 전화기의 **XSI** 인증 유형이 로그인 자격 증명으로 설정되면 XSI 로그인 자격 증명이 사용됩니다. • 전화기의 **XSI** 인증 유형이 **SIP** 자격 증명으로 설정되면 XSI SIP 자격 증명이 사용됩니다. • **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다. `<Profile_Authentication_Type ua="na">기본 Http 인증 </Profile_Authentication_Type>` • 전화기 웹 페이지의 목록에서 프로파일 재동기화를 인증할 옵션을 선택합니다. 기본값: 기본 HTTP 인증

매개 변수	설명

프로파일 규칙
프로파일 규칙 B
프로파일 규칙 C
프로파일 규칙 D
	각 프로파일 규칙은 전화기에 프로파일을 가져올 소스(구성 파일)를 알려줍니다. 재동기화 작업 시 전화기는 모든 프로파일을 순서대로 적용합니다.
	구성 파일에 AES-256-CBC 암호화를 적용하는 경우 다음과 같이 **--key** 키워드를 사용하여 암호화 키를 지정하십시오.
	[--key <encryption key>]
	선택적으로 암호화 키를 큰따옴표(")로 묶을 수 있습니다.
	• **XML**이 있는 전화기 구성 파일**(cfg.xml)**에서, 다음 형식으로 문자열을 입력합니다.
	`<Profile_Rule ua="na">/$PSN.xml</Profile_Rule>`
	`<Profile_Rule_B ua="na"/>`
	`<Profile_Rule_C ua="na"/>`
	`<Profile_Rule_D ua="na"/>`
	• 전화기 웹 페이지에서 프로파일 규칙을 지정합니다.
	디폴트: **/$PSN.xml**

사용할 DHCP 옵션	쉼표로 구분되는 DHCP 옵션은 펌웨어 및 프로파일을 검색하는 데 사용됩니다. 기본값: 66,160,159,150,60,43,125
사용할 DHCPv6 옵션	쉼표로 구분되는 DHCP 옵션은 펌웨어 및 프로파일을 검색하는 데 사용됩니다. 기본값: 17,160,159

활성화 코드 온보딩에 대한 전화기 설정

네트워크가 활성화 코드 온보딩을 위해 구성된 경우, 새 전화기를 설정하여 안전한 방식으로 자동으로 등록할 수 있습니다. 고유한 16자리 활성화 코드를 생성하여 각 사용자에게 제공합니다. 사용자가 활성화 코드를 입력하면 전화기가 자동으로 등록됩니다. 이 기능은 사용자가 유효한 활성화 코드를 입력할 때까지 전화기가 등록되지 않으므로 네트워크 보안을 유지합니다.

활성화 코드는 한 번만 사용할 수 있고 만료 날짜가 있습니다. 사용자가 만료된 코드를 입력하면 전화기의 화면에 잘못된 활성화 코드가 표시됩니다. 이 경우 사용자에 게 새 코드를 제공합니다.

이 기능은 펌웨어 릴리스 11-3MSR1, BroadWorks 애플리케이션 서버 릴리스 22.0(패치 AP.as.22.0.1123.ap368163 및 해당 종속성)에서 사용할 수 있습니다. 그러나 이전 펌웨어가 있는 전화기를 변경하여 이 기능을 사용할 수 있습니다. 이렇게 하려면 다음 절차를 사용하십시오.

시작하기 전에

방화벽을 통해 activation.webex.com 서비스에서 활성화 코드를 통해 온보딩을 지원하도록 허용해야 합니다.

온보딩을 위한 프록시 서버를 설정하려면 프록시 서버가 올바르게 설정되어 있는지 확인하십시오. 프록시 서버 설정 참조

전화기 웹페이지에 액세스합니다. 전화기 웹 인터페이스 액세스

프로시저

단계 **1** 전화기를 초기 설정으로 재설정합니다.

단계 **2** 음성 > 프로비저닝 > 구성 프로파일을 선택합니다.

단계 **3** 활성화 코드 프로비저닝 매개 변수, 19 페이지 테이블에 설명된 대로 프로파일 규칙 필드에 프로파일 규칙을 입력합니다.

단계 **4** (선택 사항) 펌웨어 업그레이드 섹션에서 활성화 코드 프로비저닝 매개 변수, 19 페이지 테이블에 설명된 대로 업그레이드 규칙 필드에 업그레이드 규칙을 입력합니다.

단계 **5** 모든 변경 사항을 제출합니다.

활성화 코드 프로비저닝 매개 변수

다음 테이블에서는 전화기 웹페이지의 음성 > 프로비저닝 탭에 있는 설정 프로파일 섹션에서 활성화 코드 파라미터의 기능과 사용법을 정의합니다. 또한 전화기 구성 파일(cfg.xml)에 XML 코드로 추가되어 매개 변수를 구성하는 문자열 구문을 정의합니다.

매개 변수	설명

프로파일 규칙
프로파일 규칙 B
프로파일 규칙 C
프로파일 규칙 D
	순서에 따라 평가되는 원격 구성 프로파일 규칙입니다. 각 재동기화 작업은 여러 파일을 검색할 수 있고 이러한 파일은 다른 서버에서 관리되는 것일 수 있습니다.
	다음 중 하나를 수행합니다.
	• 전화기 구성 파일(cfg.xml)에서, 다음 형식으로 문자열을 입력합니다.
	`<Profile_Rule ua="na">gds://</Profile_Rule>`
	• 전화기 웹 인터페이스에서 다음 형식으로 문자열을 입력합니다.
	`gds://`
	기본값: /$PSN.xml

매개 변수	설명

업그레이드 규칙	업그레이드 조건 및 관련 펌웨어 URL을 정의하는 펌웨어 업그레이드 스크립트를 지정합니다. 프로파일 규칙과 동일한 구문을 사용합니다.
	다음 중 하나를 수행합니다.
	• 전화기 구성 파일(cfg.xml)에서, 다음 형식으로 문자열을 입력합니다.
	`<Upgrade_Rule ua="na">http://<server ip address>/ sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>`
	• 전화기 웹 인터페이스에서 업그레이드 규칙을 입력합니다.
	`protocol://server[:port]/profile_pathname`
	예:
	`tftp://192.168.1.5/image/sip88xx.11-2-3MSR1-1.loads`
	프로토콜이 지정되지 않은 경우 TFTP가 사용됩니다. 서버 이름이 지정되지 않은 경우 URL을 요청한 호스트가 서버 이름으로 사용됩니다. 포트가 지정되지 않은 경우 기본 포트가 사용됩니다(TFTP의 경우 69, HTTP의 경우 80 또는 HTTPS의 경우 443).
	기본값: 공백

전화기를 엔터프라이즈 전화기로 직접 마이그레이션

이제 전환 펌웨어 로드를 사용하지 않고도 한 번에 간편하게 전화기를 엔터프라이즈 전화기로 마이그레이션할 수 있습니다.

시작하기 전에

전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 프로비저닝을 선택합니다.

단계 **2** 업그레이드 규칙 필드에서 펌웨어 업그레이드 스크립트를 입력하여 업그레이드 규칙 매개 변수를 설정합니다. 구문 세부 정보는 업그레이드 조건 및 관련 펌웨어 URL을 정의하는 항목을 참조하십시오. 프로파일 규칙과 동일한 구문을 사용합니다. 스크립트를 입력하고 다음 형식을 사용하여 업그레이드 규칙 입력:

`<tftp|http|https>://<ipaddress>/image/<load name>`

예:

`tftp://192.168.1.5/image/sip78xx.14-1-1MN-366.loads`

단계 **3** 서버에서 라이센스를 가져오고 승인할 값을 입력하여 전환 인증 규칙 매개 변수를 구성합니다.

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

```
<Trans_Auth_Rule ua="na">http://10.74.51.81/prov/migration/E2312.lic</Trans_Auth_Rule>
```

단계 **4** 전환 인증 유형 매개 변수에서 라이센스 유형을 클래식으로 설정합니다.

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

```
<Trans_Auth_Type ua="na">Classic</Trans_Auth_Type>
```

단계 **5** 모든 변경 사항 제출을 클릭합니다.

보안 **HTTPS** 재동기화

전화기에서 보안 통신 프로세스를 통해 재동기화하는 데 사용할 수 있는 메커니즘은 다음과 같습니다.

- 기본 HTTPS 재동기화
- HTTPS로 클라이언트 인증서 인증
- HTTPS 클라이언트 필터링 및 동적 콘텐츠

기본 **HTTPS** 재동기화

HTTPS는 다음과 같은 원격 프로비저닝을 위해 SSL을 HTTP에 추가합니다.

- 전화기가 프로비저닝 서버를 인증할 수 있습니다.
- 프로비저닝 서버가 전화기를 인증할 수 있습니다.
- 프로비저닝 서버와 전화기 간의 정보 교환에 기밀성을 보장합니다.

SSL은 전화기와 프로비저닝 서버에 사전 설치된 공개/개인 키 쌍을 사용하여 전화기와 서버 간의 각 연결에 대해 비밀(대칭) 키를 생성하고 교환합니다.

클라이언트 측에서, 전화기는 서버 측에 특수한 구성 설정 없이도 HTTPS를 사용하여 재동기화할 수 있습니다. GET 방식과 HTTPS를 사용하는 Profile_Rule 매개 변수 구문은 HTTP 또는 TFTP에 대해 사용하는 구문과 비슷합니다. 표준 웹 브라우저가 HTTPS 서버에서 프로파일을 검색할 수 있다면, 전화기도 검색할 수 있습니다.

HTTPS 서버를 설치하는 것 외에도, Cisco가 서명한 SSQL 서버 인증서를 프로비저닝 서버에 설치해야 합니다. HTTPS를 사용하는 서버가 Cisco 서명 서버 인증서를 제공하지 않으면 장치가 해당 서버로 재동기화할 수 없습니다. 음성 제품을 위해 서명된 SSL 인증서를 만드는 방법에 대한 지침은 https://supportforums.cisco.com/docs/DOC-9852에 있습니다.

기본 HTTPS 재동기화를 사용하여 인증

프로시저

단계 1 일반 호스트 이름 변환을 통해 네트워크 DNS 서버에 IP 주소가 알려진 호스트에 HTTPS 서버를 설치합니다.

오픈소스 Apache 서버는 오픈소스 mod_ssl 패키지를 함께 설치하면 HTTPS 서버로 작동하도록 구성할 수 있습니다.

단계 2 서버에 대한 서버 인증서 서명 요청을 생성합니다. 이 단계에서 오픈소스 OpenSSL 패키지나 이와 동등한 소프트웨어를 설치해야 할 수 있습니다. OpenSSL을 사용하는 경우 기본 CSR 파일을 생성하는 명령은 다음과 같습니다.

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

이 명령은 `privkey.pem` 파일에 저장되는 공개/개인 키 쌍을 생성합니다.

단계 3 CSR 파일(provserver.csr)을 Cisco로 제출하여 서명을 받습니다.

서명된 서버 인증서(provserver.cert)는 Sipura CA 클라이언트 루트 인증서 spacroot.cert와 함께 반환됩니다.

자세한 내용은 https://supportforums.cisco.com/docs/DOC-9852을 참고하십시오.

단계 4 서명된 서버 인증서, 개인 키 쌍 파일, 클라이언트 루트 인증서를 서버의 적절한 위치에 저장합니다.

Linux 상의 Apache 설치의 경우 이 위치는 일반적으로 다음과 같습니다.

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.cert
# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/pivkey.pem
# Certificate Authority:
SSLCACertificateFile /etc/httpd/conf/spacroot.cert
```

단계 5 서비스를 재시작합니다.

단계 6 `basic.txt` 구성 파일(TFTP 재동기화, 3 페이지 참조)을 HTTPS 서버의 가상 루트 디렉터리로 복사합니다.

단계 7 로컬 PC에서 표준 브라우저를 사용해 HTTPS 서버에서 `basic.txt`를 다운로드하여 서버가 올바르게 작동하는지 확인합니다.

단계 8 서버가 제공한 서버 인증서를 검사합니다.

Cisco를 루트 CA로 인식하도록 브라우저를 사전 구성하지 않았다면 브라우저가 인증서를 유효한 인증서로 인식하지 않을 것입니다. 하지만, 전화기는 이러한 방식으로 서명된 인증서를 인식합니다.

테스트 장치의 Profile_Rule을 수정해 다음과 같이 HTTPS 서버에 대한 참조를 포함하도록 합니다.

```
<Profile_Rule>
```

```
https://my.server.com/basic.txt
</Profile_Rule>
```

이 예에서 HTTPS 서버 이름은 **my.server.com**이라고 가정합니다.

단계 **9** 모든 변경 사항 제출을 클릭합니다.

단계 **10** 전화기가 전송하는 syslog 추적을 확인합니다.

syslog 메시지를 보면 재동기화가 HTTPS 서버에서 프로파일을 얻은 것을 알 수 있습니다.

단계 **11** (선택 사항) 이더넷 프로토콜 분석기를 전화기 서브넷에 대해 사용하여 패킷이 암호화되었는지 확인합니다.

이 연습에서는 클라이언트 인증서 확인이 활성화되지 않았습니다. 전화기와 서버 간의 연결이 암호화됩니다. 그러나 파일 이름과 디렉터리 위치를 알고 있으면 어떤 클라이언트라도 서버에 연결하고 파일을 요청할 수 있으므로 전송은 안전하지 않습니다. 보안 재동기화를 위해서는 HTTPS로 클라이언트 인증서 인증, 23 페이지의 연습에 나온 것처럼 서버가 클라이언트를 인증해야 합니다.

HTTPS로 클라이언트 인증서 인증

초기 기본 구성에서 서버는 클라이언트에게 SSL 클라이언트 인증서를 요청하지 않습니다. 모든 클라이언트가 서버에 연결하여 프로파일을 요청할 수 있으므로 프로파일의 전송은 안전하지 않습니다. 클라이언트 인증을 활성화하기 위해 구성을 편집할 수 있습니다. 이렇게 하면 서버는 연결 요청을 수락하기 전에 전화기 인증을 위해 클라이언트 인증서를 요청합니다.

이 요구 사항으로 인해 적절한 인증서가 없는 브라우저로는 재동기화 작업을 독립적으로 테스트할 수 없습니다. 테스트 전화기와 서버 사이의 HTTPS 연결 내에서 SSL 키의 교환은 ssldump 유틸리티로 관찰할 수 있습니다. 유틸리티 추적으로 클라이언트와 서버 간의 상호 작용을 볼 수 있습니다.

클라이언트 인증서로 HTTPS 인증

프로시저

단계 **1** HTTPS 서버에서 클라이언트 인증서 인증을 활성화합니다.

단계 **2** Apache(v.2)의 서버 구성 파일에서 다음 항목을 설정합니다.

```
SSLVerifyClient  require
```

또한 기본 HTTPS 재동기화, 21 페이지 연습에 나온 것처럼 spacroot.cert가 저장되었는지 확인합니다.

단계 **3** HTTPS 서버를 재시작하고 전화기에서 전송한 syslog 추적을 검사합니다.

이제 서버에 대한 각 재동기화에 대칭 인증이 수행되며, 프로파일을 전송하기 전에 서버 인증서와 클라이언트 인증서를 모두 확인합니다.

단계 **4** ssldump를 사용해 전화기와 HTTPS 서버 간의 재동기화 연결을 캡처합니다.

서버에서 클라이언트 인증서 확인이 올바르게 활성화된 경우, 프로파일을 포함하는 암호화된 패킷을 전송하기 전에 대칭 인증서 교환(먼저 서버에서 클라이언트로, 그런 다음 클라이언트에서 서버로)이 수행되는 것을 ssldump 추적에서 볼 수 있습니다.

클라이언트 인증이 활성화된 경우 유효한 클라이언트 인증서와 MAC 주소가 일치하는 전화기만 프로비저닝 서버에서 프로파일을 요청할 수 있습니다. 일반적인 브라우저 또는 다른 승인되지 않은 장치의 요청은 서버가 거부합니다.

클라이언트 필터링 및 동적 콘텐츠를 위해 **HTTPS** 서버 구성

HTTPS 서버는 클라이언트 인증서를 요구하도록 구성된 경우, 재동기화하는 전화기를 식별하고 올바른 구성 정보를 제공하기 위해 인증서의 정보를 사용합니다.

HTTPS 서버는 재동기화 요청의 일부로 호출되는 CGI 스크립트(또는 컴파일된 CGI 프로그램)로 인증서 정보를 제공합니다. 이 연습에서는 설명을 위해 오픈소스 Perl 스크립팅 언어를 사용하며 Apache(v.2)를 HTTPS 서버로 사용한다고 가정합니다.

프로시저

단계 **1** HTTPS 서버를 실행하는 호스트에 Perl을 설치합니다.

단계 **2** 다음과 같은 Perl 리플렉터 스크립트를 작성합니다.

```
#!/usr/bin/perl -wT
use strict;
print “Content-Type: text/plain\n\n”;
print “<flat-profile><GPP_D>”;

print “OU=$ENV{‘SSL_CLIENT_I_DN_OU’},\n”;
print “L=$ENV{‘SSL_CLIENT_I_DN_L’},\n”;
print “S=$ENV{‘SSL_CLIENT_I_DN_S’}\n”;
print “</GPP_D></flat-profile>”;
```

단계 **3** 이 파일을 파일 이름 `reflect.pl`로 HTTPS 서버의 CGI 스크립트 디렉터리에 저장하고 실행 권한(Linux의 경우 chmod 755)을 설정합니다.

단계 **4** 서버에서 CGI 스크립트에 액세스할 수 있는지 확인합니다(즉, `cgi-bin /... /`).

단계 **5** 다음 예와 같이 테스트 장치에서 리플렉터 스크립트로 재동기화하도록 Profile_Rule을 수정합니다.

```
https://prov.server.com/cgi-bin/reflect.pl?
```

단계 **6** 모든 변경 사항 제출을 클릭합니다.

단계 **7** 성공적으로 재동기화되는지 syslog 추적을 확인합니다.

단계 **8** 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

단계 **9** 음성 > 프로비저닝을 선택합니다.

단계 **10** GPP_D 매개 변수는 스크립트가 캡처한 정보를 포함합니다.

테스트 장치에 제조업체의 고유 인증서가 있는 경우, 포함되는 정보는 제품 이름, MAC 주소 및 일련 번호입니다. 장치가 펌웨어 릴리스 2.0 이전에 제조된 경우 정보에 일반 문자열이 포함됩니다.

비슷한 스크립트를 사용하여 재동기화 장치에 대한 정보를 확인하고 적절한 구성 매개 변수 값을 장치로 제공할 수 있습니다.

HTTPS 인증서

전화기는 장치에서 프로비저닝 서버로의 HTTPS 요청을 바탕으로 안전하고 신뢰성 있는 프로비저닝 전략을 제공합니다. 서버 인증서와 클라이언트 인증서를 사용해 전화기를 서버에 대해 인증하고, 서버를 전화기에 대해 인증합니다.

Cisco 발급된 인증 외에도 전화기는 일반적으로 사용되는 SSL 인증서 공급자 집합에서 서버 인증서를 받습니다.

HTTPS를 전화기에서 사용하려면 인증서 서명 요청(CSR)을 생성하고 Cisco로 제출해야 합니다. 전화기는 프로비저닝 서버에서 설치를 위한 인증서를 생성합니다. 전화기는 프로비저닝 서버와 HTTPS 연결을 수행하려고 시도할 때 인증서를 수락합니다.

HTTPS 방법론

HTTPS는 클라이언트와 서버 간의 통신을 암호화하여 메시지 내용을 다른 네트워크 장치로부터 보호합니다. 클라이언트와 서버 간 통신의 본문을 암호화하는 방법은 대칭 키 암호화에 기반을 둡니다. 대칭 키 암호화에서 클라이언트와 서버는 보안 채널을 통해 공개/개인 키 암호화로 보호되는 단일 비밀 키를 공유합니다.

비밀 키로 암호화된 메시지는 동일한 키를 사용해야 해독할 수 있습니다. HTTPS는 광범위한 대칭 암호화 알고리즘을 지원합니다. 전화기는 AES(American Encryption Standard)와 128비트 RC4를 사용하며 최대 256비트 대칭 암호화를 구현합니다.

HTTPS는 보안 트랜잭션에 참여한 서버와 클라이언트의 인증도 제공합니다. 이 기능은 프로비저닝 서버와 각 클라이언트를 네트워크의 다른 장치에서 스푸핑할 수 없도록 보장합니다. 이 기능은 원격 엔드포인트 프로비저닝 환경에 필수적입니다.

서버와 클라이언트 인증은 공개 키를 포함하는 인증서와 공개/개인 키 암호화를 사용하여 수행됩니다 공개 키를 사용하여 암호화한 텍스트는 해당하는 개인 키가 있어야 해독할 수 있습니다(반대의 경우도 동일). 전화기는 공개/개인 키 암호화를 위해 RSA(Rivest-Shamir-Adleman) 알고리즘을 지원합니다.

SSL 서버 인증서

각 보안 프로비저닝 서버는 Cisco가 직접 서명한 SSL(Secure Sockets Layer) 인증서를 발급합니다. 전화기에서 실행되는 펌웨어는 Cisco 인증서만 유효한 것으로 인식합니다. 클라이언트는 HTTPS를 사용하여 서버로 연결할 때 Cisco가 서명하지 않은 서버 인증서를 모두 거부합니다.

이 메커니즘은 전화기에 대한 무단 액세스 또는 프로비저닝 서버를 스푸핑하려는 시도로부터 서비스 제공자를 보호합니다. 이러한 보호 수단이 없으면 공격자가 전화기를 다시 프로비저닝하여 구성 정보를 탈취하거나 다른 VoIP 서비스를 사용하도록 할 수 있습니다. 공격자는 유효한 서버 인증서에 해당하는 개인 키가 없는 이상, 전화기와 연결할 수 없습니다.

서버 인증서 얻기

프로시저

단계 **1** 인증서 프로세스를 지원할 Cisco 담당자에게 문의합니다. 특정한 지원 담당자가 없는 경우 ciscosb-certadmin@cisco.com으로 요청 이메일을 보냅니다.

단계 **2** 인증서 서명 요청(CSR)에 사용할 개인 키를 생성합니다. 이 키는 개인 키이며 Cisco 담당자에게 제출할 필요가 없습니다. 오픈소스 "openssl"을 열고 키를 생성합니다. 예:

```
openssl genrsa -out <file.key> 1024
```

단계 **3** 조직 및 위치를 식별하는 필드를 포함하는 CSR을 생성합니다. 예:

```
openssl req -new -key <file.key> -out <file.csr>
```

다음과 같은 정보가 필요합니다.

- 주체 필드 - FQDN(Fully Qualified Domain Name) 구문으로 일반 이름(CN)을 입력합니다. 전화기는 SSL 인증 핸드셰이크가 진행되는 동안 받은 인증서가 실제 보낸 시스템에서 온 것인지 확인합니다.
- 서버 호스트 이름 - 예: provserv.domain.com.
- 이메일 주소 - 고객이 지원이 필요한 경우 연락할 수 있도록 이메일 주소를 입력합니다. 이 이메일 주소는 CSR에서 볼 수 있습니다.

단계 **4** CSR을 (zip 파일 형식으로) Cisco 지원 담당자에게 보내거나 ciscosb-certadmin@cisco.com으로 제출합니다. Cisco가 인증서를 서명합니다. Cisco가 시스템에 설치할 인증서를 보냅니다.

클라이언트 인증서

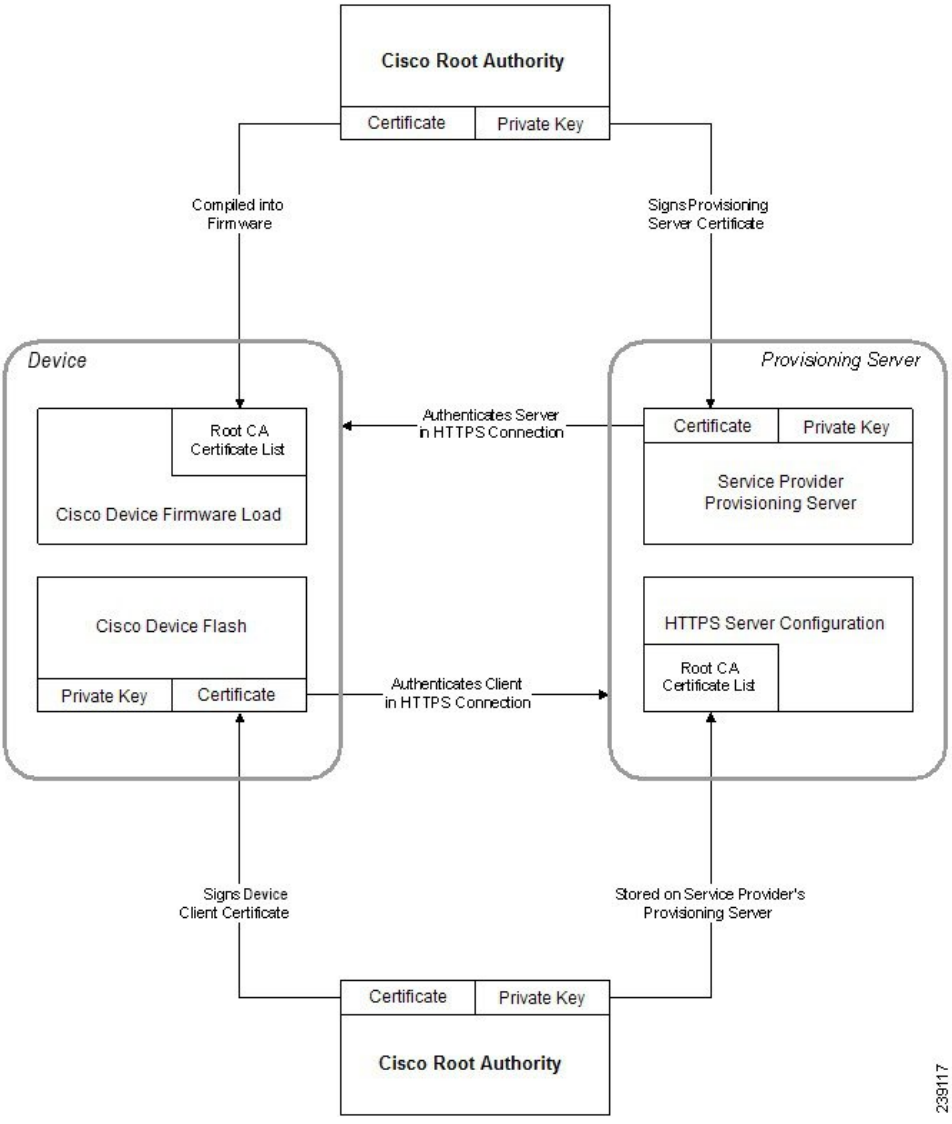
공격자는 전화기에 대한 직접 공격 외에도 표준 웹 브라우저나 다른 HTTPS 클라이언트를 이용해 프로비저닝 서버에 연결하고 구성 프로파일을 얻으려고 시도할 수 있습니다. 이러한 종류의 공격을 방지하기 위해 각 전화기는 Cisco가 서명한 고유한 클라이언트 인증서를 보유하며, 여기에는 개별 엔드포인트에 대한 식별 정보가 들어 있습니다. 인증 기관(CA) 루트 인증서는 각 서비스 제공자에 제공된 장치 클라이언트 인증서를 인증할 수 있습니다. 이 인증 경로는 프로비저닝 서버가 구성 프로파일에 대한 승인되지 않은 요청을 거부할 수 있게 해줍니다.

인증서 구조

서버 인증서와 클라이언트 인증서를 함께 사용하여 원격 전화기와 해당 프로비저닝 서버 간의 통신을 보호할 수 있습니다. 아래 그림은 Cisco 클라이언트, 프로비저닝 서버, 인증 기관 사이에서 인증서, 공개/개인 키 쌍, 서명 루트 기관의 관계와 위치를 보여줍니다.

다이어그램의 위쪽 상단은 개별 프로비저닝 서버 인증서를 서명하는 데 사용되는 프로비저닝 서버 루트 인증 기관을 보여줍니다. 해당 루트 인증서는 펌웨어로 컴파일되며 전화기가 승인된 프로비저닝 서버를 인증하는 데 사용됩니다.

그림 ***1: CA(Certificate Authority)*** 흐름



사용자 지정 **Certificate Authority** 구성

디지털 인증서는 네트워크 상에서 네트워크 장치 및 사용자를 인증하는 데 사용할 수 있습니다. 네트워크 노드 간에 IPSec 세션을 협상하는 데 사용할 수 있습니다.

타사는 서로 통신하려는 둘 이상의 노드를 확인 및 인증하기 위해 Certificate Authority 인증서를 사용합니다. 각 노드에는 공용 키와 개인 키가 있습니다. 공개 키는 데이터를 암호화합니다. 개인 키는 데이터를 해독합니다. 노드는 동일한 출처에서 해당 인증서를 얻으므로 해당하는 신원을 확신할 수 있습니다.

장치는 타사 CA(Certificate Authority)가 제공한 디지털 인증서를 사용해 IPSec 연결을 인증할 수 있습니다.

전화기는 펌웨어에 내장된 사전에 로드된 루트 Certificate Authority의 집합을 지원합니다.

- Cisco 중소기업 CA 인증서
- CyberTrust CA 인증서
- Verisign CA 인증서
- Sipura 루트 CA 인증서
- Linksys 루트 CA 인증서

시작하기 전에

전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 정보 > 상태를 선택합니다.

단계 **2** 스크롤하여 사용자 지정 **CA** 상태로 스크롤하고 다음 필드를 확인합니다.

- 사용자 지정 CA 프로비저닝 상태 - 프로비저닝 상태를 나타냅니다.
  - mm/dd/yyyy HH:MM:SS에 성공한 마지막 프로비저닝 또는
  - mm/dd/yyyy HH:MM:SS에 실패한 마지막 프로비저닝
- 사용자 지정 CA 정보 - 사용자 지정 CA에 대한 정보를 표시합니다.
  - 설치 - "CN 값"을 표시합니다. 여기에서, "CN 값"은 첫 번째 인증서의 제목 필드에 대한 CN 매개 변수의 값입니다.
  - 설치 되지 않음 - 사용자 지정 CA 인증서가 설치되지 않은 경우 표시됩니다.

프로파일 관리

이 섹션에서는 다운로드를 준비하기 위한 구성 프로파일의 구조를 보여줍니다. 기능을 설명하기 위해, 재동기화 방법을 TFTP에서 로컬 PC를 선택했지만 HTTP 또는 HTTPS도 사용할 수 있습니다.

Gzip으로 공개 프로파일 압축

프로파일에서 모든 매개 변수를 개별적으로 지정하는 경우 XML 형식의 구성 파일은 아주 커질 수 있습니다. 프로비저닝 서버에서 부하를 줄이기 위해, 전화기는 gzip 유틸리티(RFC 1951)가 지원하는 deflate 압축 형식으로 XML 파일을 압축할 수 있습니다.

참고 압축되고 암호화된 XML 프로파일을 전화기에서 인식하려면 암호화 전에 압축해야 합니다.

사용자 지정 백엔드 프로비저닝 서버 솔루션과 통합하려면 표준 gzip 유틸리티 대신 오픈소스 zlib 압축 라이브러리를 사용하여 프로파일 압축을 수행할 수 있습니다. 전화기는 파일에 유효한 gzip 헤더가 포함된다고 가정합니다.

프로시저

단계 **1** 로컬 PC에 gzip을 설치합니다.

단계 **2** 명령줄에서 gzip을 호출하여 `basic.txt` 구성 파일을 압축합니다(TFTP 재동기화, 3 페이지 참조)

```
gzip basic.txt
```

그러면 압축 파일 `basic.txt.gz`가 생성됩니다.

단계 **3** `basic.txt.gz` 파일을 TFTP 서버의 가상 루트 디렉터리에 저장합니다.

단계 **4** 다음 예에 나온 것처럼, 원래 XML 파일 대신 압축된 파일로 재동기화하도록 테스트 장치의 Profile_Rule을 수정합니다.

```
tftp://192.168.1.200/basic.txt.gz
```

단계 **5** 모든 변경 사항 제출을 클릭합니다.

단계 **6** 전화기에서 syslog 추적을 확인합니다.

재동기화 시, 전화기는 새 파일을 다운로드 및 사용하여 해당 매개 변수를 업데이트합니다.

OpenSSL로 프로파일 암호화

압축되거나 압축을 푼 프로파일을 암호화할 수 있습니다(암호화하려면 파일을 먼저 압축해야 합니다). 암호화는 전화기와 프로비저닝 서버 간의 통신에 TFTP 또는 HTTP를 사용할 때와 같이 프로파일 정보에 대한 기밀이 특히 중요한 경우 유용합니다.

전화기는 256비트 AES 알고리즘을 사용하는 대칭 키 암호화를 지원합니다. 이 암호화는 오픈소스 OpenSSL 패키지를 사용하여 수행할 수 있습니다.

프로시저

단계 **1** 로컬 PC에 OpenSSL을 설치합니다. AES를 활성화하려면 OpenSSL 애플리케이션을 재컴파일해야 할 수 있습니다.

단계 **2** `basic.txt` 구성 파일(TFTP 재동기화, 3 페이지 참조)을 사용하여 다음 명령으로 암호화된 파일을 생성합니다.

```
>openssl enc –aes-256-cbc –k MyOwnSecret –in basic.txt –out basic.cfg
```

XML 프로파일은 압축 및 암호화를 모두 할 수 있으므로 Gzip으로 공개 프로파일 압축, 29 페이지에서 만든 압축된 `basic.txt.gz` 파일도 사용할 수 있습니다.

단계 **3** 암호화된 `basic.cfg` 파일을 TFTP 서버 가상 루트 디렉터리에 저장합니다.

단계 **4** 테스트 장치에서 Profile_Rule을 수정해 원래 XML 파일 대신 암호화된 파일로 재동기화합니다. 암호화 키는 다음 URL 옵션으로 전화기에 전달됩니다.

```
[--key MyOwnSecret ] tftp://192.168.1.200/basic.cfg
```

단계 **5** 모든 변경 사항 제출을 클릭합니다.

단계 **6** 전화기에서 syslog 추적을 확인합니다.

재동기화 시, 전화기는 새 파일을 다운로드 및 사용하여 해당 매개 변수를 업데이트합니다.

분할된 프로파일 생성

전화기는 재동기화할 때마다 여러 분리된 프로파일을 다운로드합니다. 이 방법으로 다른 종류의 프로파일 정보를 별도의 서버에서 관리하고 계정별 값과 분리된 공통 구성 매개 변수 값을 유지 관리할 수 있습니다.

프로시저

단계 **1** 이전의 연습과 다른 매개 변수 값을 지정하는 새 XML 프로파일 `basic2.txt`를 생성합니다. 예를 들어 `basic.txt` 프로파일에 다음 항목을 추가합니다.

```
<GPP_B>ABCD</GPP_B>
```

단계 **2** `basic2.txt` 프로파일을 TFTP 서버의 가상 루트 디렉터리에 저장합니다.

단계 **3** 폴더에서 이전 연습의 첫 번째 프로파일 규칙은 그대로 두고, 두 번째 프로파일 규칙(Profile_Rule_B)은 새 파일을 가리키도록 구성합니다.

```
<Profile_Rule_B>tftp://192.168.1.200/basic2.txt
</Profile_Rule_B>
```

단계 **4** 모든 변경 사항 제출을 클릭합니다.

이제 전화기는 재동기화 작업 시간이 되면 첫 번째와 두 번째 프로파일에 대해 차례대로 재동기화합니다.

단계 **5** 예상대로 작동하는지 syslog 추적을 확인합니다.

전화기 프라이버시 헤더 설정

SIP 메시지의 사용자 프라이버시 헤더는 신뢰할 수 있는 네트워크에서 사용자 프라이버시 요구를 설정합니다.

`config.xml` 파일의 XML 태그를 사용하여 각 회선 내선 번호에 대한 사용자 프라이버시 헤더 값을 설정할 수 있습니다.

프라이버시 헤더 옵션은 다음과 같습니다.

- 비활성화됨(기본값)
- 없음 - 사용자는 프라이버시 서비스가 이 SIP 메시지에 프라이버시 기능을 적용하지 않도록 요청합니다.
- 헤더 - 사용자는 식별 정보를 삭제할 수 없는 헤더를 숨기려면 프라이버시 서비스가 필요합니다.
- 세션 - 사용자는 프라이버시 서비스가 세션에 대해 익명성을 제공할 것을 요청합니다.
- 사용자 - 사용자는 중개자에 의해서만 프라이버시 레벨을 요청합니다.
- id - 사용자는 시스템이 IP 주소나 호스트 이름을 표시하지 않는 ID를 대체하도록 요청합니다.

프로시저

단계 **1** 텍스트 또는 XML 편집기에서 전화기 `config.xml` 파일을 편집합니다.

단계 **2** **<Privacy_Header_N_ ua="na">**값**</Privacy_Header_N_>** 태그를 삽입합니다. 여기서 N은 회선 내선 번호(1~10)이며 다음 값 중 하나를 사용합니다.

- 기본값: 비활성화됨
- **none**
- 헤더
- 세션
- 사용자
- **id**

단계 **3** (선택 사항) 필요한 회선 내선 번호와 동일한 태그를 사용하여 추가 회선 내선 번호를 프로비저닝합니다.

단계 **4** 변경 내용을 `config.xml` 파일에 저장합니다.

MIC 인증서 갱신

MIC(Manufacture Installed Certificate)를 지정된 또는 기본 SUDI(Secure Unique Device Identifier) 서비스로 갱신할 수 있습니다. MIC 인증서가 만료되면 SSL/TLS를 사용하는 기능이 작동하지 않습니다.

시작하기 전에

- 방화벽을 통해 `sudirenewal.cisco.com` 서비스(포트 80)가 MIC 인증서 갱신을 지원할 수 있도록 해야 합니다.
- 전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 프로비저닝을 선택합니다.

단계 **2** **MIC** 인증서 설정 섹션에서 SUDI 서비스에 의한 MIC 인증서 갱신에 대한 매개 변수, 32 페이지에 정의된 대로 매개 변수를 설정합니다.

단계 **3** 모든 변경 사항 제출을 클릭합니다.
인증서 갱신이 성공적으로 완료되면 전화기가 재부팅됩니다.

단계 **4** (선택 사항) 정보 > 다운로드 상태의 **MIC** 인증서 새로 고침 상태 섹션에서 MIC 인증서 갱신의 최신 상태를 확인합니다.

참고 전화기를 출고 시 설정으로 복원해도 전화기는 갱신된 인증서를 사용합니다.

SUDI 서비스에 의한 MIC 인증서 갱신에 대한 매개 변수

다음 테이블에서는 음성 > 프로비저닝탭의 **MIC** 인증 설정 섹션에 있는 각 파라미터의 기능과 사용법이 정의되어 있습니다.

표 2: SUDI 서비스에 의한 MIC 인증서 갱신에 대한 매개 변수

매개 변수명	설명과 기본값
MIC 인증서 새로 고침 활성화	기본적으로 MIC(Manufacture Installed Certificate) 갱신 또는 지정된 SUDI(Secure Unique Device Identifier) 서비스를 활성화할지 여부를 제어합니다. 다음 중 하나를 수행합니다. • 전화기 구성 파일(cfg.xml)에서, 다음 형식으로 문자열을 입력합니다. `<MIC_Cert_Refresh_Enable ua="na">Yes</MIC_Cert_Refresh_Enable>` • 전화기 웹 인터페이스에서 예 또는 아니요를 선택하여 MIC 인증서 갱신을 활성화하거나 비활성화합니다. 유효한 값: 예 및 아니요 기본값: 아니요

MIC 인증서 새로 고침 규칙	갱신된 MIC 인증서를 제공하는 SUDI 서비스의 HTTP URL을 입력합니다. 예를 들어,
	`http://sudirenewal.cisco.com/`
	참고 URL을 변경하지 않습니다. MIC 인증서 갱신에는 기본 URL만 지원됩니다.
	다음 중 하나를 수행합니다.
	• 전화기 구성 파일(cfg.xml)에서, 다음 형식으로 문자열을 입력합니다.
	`<MIC_Cert_Refresh_Rule ua="na">http://sudirenewal.cisco.com/</MIC_Cert_Refresh_Rule>`
	• 전화기 웹 인터페이스에서 사용할 HTTP URL을 입력합니다.
	허용되는 값: 1024자를 초과하지 않는 유효한 URL
	기본값: `http://sudirenewal.cisco.com/`