프로비저닝

- 프로비저닝 개요, 1 페이지
- 프로비저닝, 3 페이지
- TR69 프로비저닝, 10 페이지
- 통신 암호화, 11 페이지
- 네트워크 혼잡 시 전화기 동작, 12 페이지
- 사내 사전 프로비저닝 및 프로비저닝 서버, 12 페이지
- 서버 준비 및 소프트웨어 도구, 12 페이지
- 사내 장치 사전 프로비저닝, 14 페이지
- 프로비저닝 서버 설정, 15 페이지

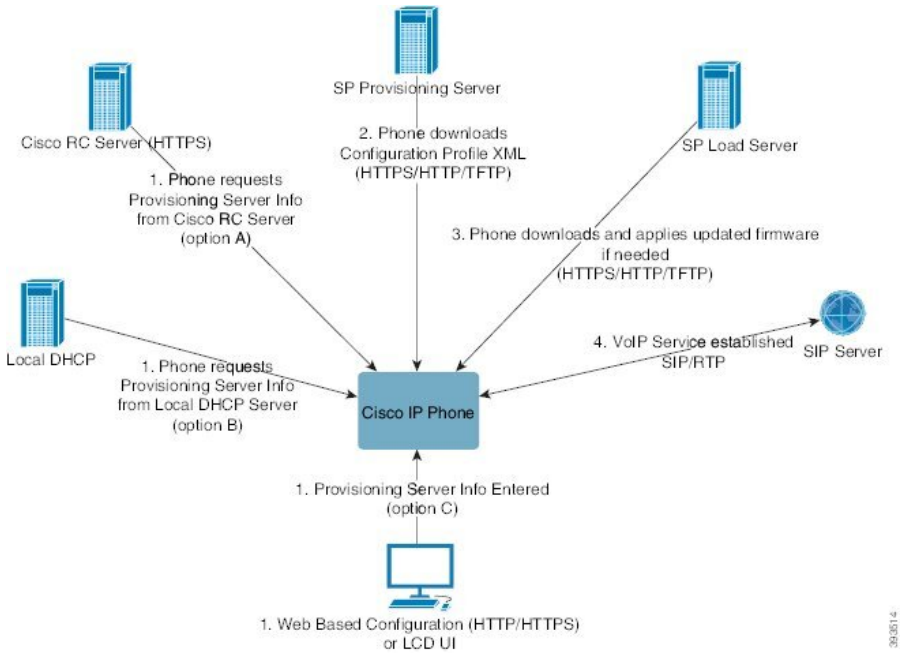
프로비저닝 개요

Cisco IP 전화기는 VoIP(Voice over IP) 서비스 제공자가 가정이나 기업, 엔터프라이즈 환경의 고객을 대상으로 대규모로 구축하기 위한 것입니다. 이를 통해 원격 관리와 구성을 사용하여 전화기를 프로비저닝하고, 고객이 있는 곳에서 전화기가 올바르게 작동하도록 합니다.

Cisco는 다음을 사용하여 전화기의 사용자 지정된, 지속적인 기능 구성을 지원합니다.

- 전화기의 신뢰할 수 있는 원격 제어
- 전화기를 제어하는 통신의 암호화
- 효율적인 전화기 계정 바인딩

전화기는 원격 서버에서 구성 프로파일이나 업데이트된 펌웨어를 다운로드하도록 프로비저닝할 수 있습니다. 전화기는 네트워크에 연결될 때, 전원을 켰을 때, 지정된 기간이 지났을 때 다운로드하도록 설정할 수 있습니다. 프로비저닝은 보통 대개 서비스 제공자가 수행하는 대규모, VoIP 구축의 일부입니다. 구성 프로파일 또는 업데이트된 펌웨어는 TFTP, HTTP 또는 HTTPS를 사용하여 장치로 전송됩니다.



간략하게 살펴보면 전화기 프로비저닝 과정은 다음과 같습니다.

1. 전화기 구성되지 않은 경우, 다음 중 하나의 옵션을 사용하여 프로비저닝 서버 정보가 전화기에 적용됩니다.
   - **A** - HTTPS, DNS SRV, GDS(활성화 코드 온보딩), EDOS 장치 활성화를 사용하여 Cisco EDOS(활성화 데이터 오케스트레이션 시스템) RC(원격 사용자 지정) 서버에서 다운로드합니다.
   - **B** - 로컬 DHCP 서버에서 쿼리합니다.
   - **C** - Cisco 전화기 웹 기반 구성 유틸리티나 전화기 UI를 사용하여 수동으로 입력합니다.
2. 전화기는 HTTPS, HTTP, TFTP 프로토콜을 사용하여 프로비저닝 서버 정보를 다운로드하고 구성 XML을 적용합니다.
3. 전화기는 필요에 따라 HTTPS, HTTP 또는 TFTP를 사용하여 업데이트된 펌웨어를 다운로드 및 적용합니다.
4. 지정된 구성 및 펌웨어를 사용하여 VoIP 서비스가 설정됩니다.

VoIP 서비스 제공자가 다수의 전화기를 주거 지역 및 소기업 고객에게 배포하려고 합니다. 기업 또는 엔터프라이즈 환경에서는 전화기를 터미널 노드로 사용할 수 있습니다. 제공자가 인터넷을 통해 이러한 장치를 광범위하게 배포하며, 장치가 고객 구내의 라우터와 방화벽을 통해 연결합니다.

전화기를 서비스 제공자 백엔드 장비의 원격 확장으로 사용할 수 있습니다. 원격 관리 및 구성은 고객 구내에서 전화기의 올바른 작동을 보장합니다.

프로비저닝

전화기는 전원을 켤 때 및 주기적으로 내부 구성 상태를 원격 프로파일과 일치하도록 재동기화할 수 있습니다. 전화기는 일반 프로비저닝 서버(NPS) 또는 액세스 제어 서버(ACS)에 연결합니다.

기본적으로 전화기가 유휴 상태일 때만 프로파일 재동기화를 시도합니다. 이것은 업그레이드 때문에 소프트웨어 재부팅과 통화 중단이 발생하는 것을 예방하기 위한 것이다. 이전 릴리스에서 최신 업그레이드 상태로 만들기 위해 중간 업그레이드가 필요한 경우, 업그레이드 논리로 다중 단계 업그레이드를 자동화할 수 있습니다.

일반 프로비저닝 서버

일반 프로비저닝 서버(NPS)는 TFTP, HTTP 또는 HTTPS 서버일 수 있습니다. 펌웨어에는 민감한 정보가 들어 있지 않으므로 원격 펌웨어 업그레이드는 TFTP, HTTP 또는 HTTPS를 사용하여 수행됩니다.

HTTPS가 권장되지만, 업데이트된 프로파일을 공유된 비밀 키를 사용하여 암호화할 수 있으므로, NPS와의 통신에는 보안 프로토콜을 사용할 필요가 없습니다. HTTPS를 사용하는 방법에 대한 자세한 내용은 통신 암호화, 11 페이지를 참조하십시오. 첫 번째 프로비저닝을 보호하는 데는 SSL 기능을 사용하는 메커니즘이 적용됩니다. 프로비저닝되지 않은 전화기는 해당 장치를 대상으로 하는 256비트 대칭 키로 암호화된 프로파일을 받을 수 있습니다.

전화기 프로비저닝 방식

일반적으로 Cisco IP 전화기는 처음 네트워크에 연결하면 프로비저닝하도록 구성됩니다. 또한 전화기는 서비스 제공자 또는 VAR이 전화기를 사전 프로비저닝(구성)할 때 설정한 예약 간격에 따라 프로비저닝됩니다. 서비스 제공자는 VAR 또는 고급 사용자가 전화기 키패드를 사용하여 수동으로 전화기를 프로비저닝하는 것을 승인할 수 있습니다. 전화기 웹 UI를 사용하여 프로비저닝을 구성할 수도 있습니다.

전화기 LCD UI에서 상태 > 전화기 상태 > 프로비저닝을 선택하거나 웹 기반 구성 유틸리티의 상태 탭에서 프로비저닝 상태를 선택합니다.

활성화 코드를 사용하여 전화기를 온보드

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. 새 펌웨어로 업그레이드하고 `gds://` 프로파일 규칙을 사용하여 활성화 코드 화면을 트리거하도록 전화기에 지시할 수 있습니다. 사용자는 제공된 필드에 16자리 코드를 입력하여 전화기를 자동으로 온보드합니다.

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

프로시저

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

단계 **2** config.xml 파일에서 아래 예를 따라 활성화 코드 온보딩에 대한 프로파일 규칙을 설정합니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<device>
<flat-profile>
<!-- System Configuration -->
<Profile_Rule ua="na">gds://</Profile_Rule>
<!--  Firmware Upgrade  -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na">http://<server ip address>/sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>
<!-- <BACKUP_ACS_Password ua="na"/> -->
</flat-profile>
</device>
```

참고 11.2(3) SR1 이후의 펌웨어 릴리스에 대해서는 펌웨어 업그레이드 설정이 선택 사항입니다.

단계 **3** 변경 내용을 config.xml 파일에 저장합니다.

CDA 재시도를 사용한 장치 온보딩

전화기를 프로비저닝하도록 구성하기 위해 DHCP 옵션(DNS SRV, CDA 장치 활성화 또는 활성화 코드 온보딩)을 사용하여 프로비저닝 서버 정보가 전화기에 적용됩니다. 펌웨어 릴리스 12.0(3)부터 장치 온보딩 환경을 간소화하고 오류에 대한 복원력을 높이기 위해 CDA를 사용하여 프로비저닝을 다시 시도합니다. 이 과정에서 전화기가 활성화 코드 화면으로 이동하거나 전화기에 빈 화면이 표시됩니다. 재시도 프로세스는 백엔드에서 계속되지만 사용자는 이를 인식하지 못합니다. 이 기능은 처음에 CDA 서비스에 전화 MAC 주소를 추가하지 못한 경우와 전화기가 CDA 서비스에서 처음으로 구성을 가져오는 데 실패하여 나중에 MAC 주소를 추가한 경우 전화기를 원격으로 설정하는 데 도움이 됩니다. 펌웨어 릴리스 12.0(3)에서는 재시도 메커니즘이 사용되며, 전화기는 기하급수적으로 백오프 타이머로 CDA를 다시 시도합니다. CDA 서비스에 MAC 주소가 추가된 후 CDA를 다시 시도하도록 전화기를 선택적으로 재부팅할 수도 있습니다.

이 프로비저닝은 다음 조건에서 발생합니다.

- 전화기를 처음으로 꺼내고 펌웨어 버전 12.0.3 이상이 사전 설치된 경우
- 펌웨어 버전 12.0.3 이상을 실행하는 동안 전화기가 공장 초기화 재설정되는 경우

사용자는 CDA 재시도가 발생할 때 사용자 정의 상태에서 다음과 같은 변경 사항을 볼 수 있습니다.

- 사용자 지정 상태가 **GDS** 보류 중에서 보류 중으로 변경되었습니다.
- 사용자 지정 상태가 사용자 지정 보류 중에서 보류 중으로 변경됩니다.

원격 사용자 지정 프로세스가 최종 상태로 들어가고 사용자 지정 상태가 중단됨, 획득됨 또는 **GDS** 획득됨으로 설정되어 있으면 CDA 재시도가 중지됩니다.

참고 기본 시나리오에서는 **Resync_Error_Retry_Delay** 값을 변경하지 않고 유지하는 것이 좋습니다. 또한 값은 항상 60초 이상이어야 합니다.

Webex Cloud로 전화기 온보딩

전화기 온보딩은 Webex 인식 전화기를 Webex Cloud로 온보딩하는 간단하고 안전한 방식을 제공합니다. GDS(활성화 코드 온보딩) 또는 전화기 MAC 주소(EDOS 장치 활성화)를 사용하여 온보딩 프로세스를 달성할 수 있습니다.

활성화 코드를 생성하는 방법에 대한 자세한 내용은 *Cisco BroadWorks* 파트너 구성 가이드, *Cisco* 멀티 플랫폼 전화기를 참조하십시오.

Webex 인식 전화기 온보딩에 대한 자세한 내용은 *Webex for Cisco BroadWorks* 솔루션 가이드를 참조하십시오.

전화기에서 Webex Cloud에 온보딩 활성화

Webex Cloud에 전화기를 성공적으로 등록한 후에는 전화기 화면에 클라우드 기호 가 표시됩니다.

시작하기 전에

전화기 관리 웹페이지 액세스. 전화기 웹 인터페이스 액세스 참조

프로시저

단계 **1** 음성 > 전화를 선택합니다.

단계 **2** **Webex** 섹션에서 온보딩 활성화 매개 변수를 예로 설정합니다.

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

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

기본값: 예

단계 **3** 모든 변경 사항 제출을 클릭합니다.

짧은 활성화 코드를 사용하여 자동 프로비저닝 활성화

다음 단계에 따라 짧은 활성화 코드를 사용하여 자동 프로비저닝을 활성화합니다.

시작하기 전에

전화기가 펌웨어 릴리스 11.3(1) 이상으로 업데이트되었는지 확인합니다.

전화기에 대한 프록시 서버를 설정하려면 프록시 서버가 올바르게 설정되어 있는지 확인하십시오. 프록시 서버 설정 참조

리디렉션 프로파일에 대한 CDA 서버를 설정하는 방법을 검토합니다.

https://community.cisco.com/t5/collaboration-voice-and-video/cisco-multi-platform-phones-cloud-provisioning-process/ta-p/3910244

프로시저

단계 **1** 3 ~ 16(포함) 사이의 숫자를 포함하는 리디렉션 프로파일 이름을 생성합니다. 이는 나중에 활성화 코드가 됩니다. 다음 형식 중 하나를 사용합니다.

- **nnn**.
- **nnnnnnnnnnnnnnnn**
- 3 ~ 16개 사이의 숫자. 예, **123456**

단계 **2** 1단계에서 만든 프로파일 이름을 cdap-support@cisco.com의 CDA(Customer Device Activation) 지원 팀에 제공합니다.

단계 **3** 프로파일을 검색할 수 있도록 CDA 지원 팀에 요청하십시오.

단계 **4** CDA 지원 팀에서 확인을 받으면 활성화 코드를 사용자에게 배포합니다.

단계 **5** 인증 화면에서 숫자를 입력하기 전에 사용자에게 파운드(#) 키를 누르도록 알립니다.

키패드로 전화기 수동 프로비저닝

프로시저

단계 **1** 애플리케이션  을 누릅니다.

단계 **2** 장치 관리 > 프로파일 규칙을 선택합니다.

단계 **3** 다음 형식으로 프로파일 규칙을 입력합니다.

```
protocol://server[:port]/profile_pathname
```

예:

```
tftp://192.168.1.5/CP_x8xx_MPP.cfg
```

프로토콜이 지정되지 않은 경우 TFTP가 사용됩니다. 서버 이름을 지정하지 않으면 URL을 요청하는 호스트가 서버 이름으로 사용됩니다. 포트를 지정하지 않은 경우 기본 포트가 사용됩니다 (TFTP의 경우 69, HTTP의 경우 80 또는 HTTPS의 경우 443).

단계 **4** 재동기화를 누릅니다.

HTTP 프로비저닝을 위한 DNS SRV

HTTP 프로비저닝용 DNS SRV 기능을 사용하면 다중 플랫폼 전화기를 자동으로 프로비저닝할 수 있습니다. DNS SRV(Domain Name System Service) 레코드는 서비스와 호스트 이름 간의 연결을 설정합니다. 전화기가 프로비저닝 서비스의 위치를 찾을 때, 지정된 DNS SRV 도메인 이름을 먼저 쿼리한 다음 SRV 레코드를 쿼리합니다. 전화기에서 레코드의 유효성을 검사하여 서버에 액세스할 수 있는지 확인합니다. 그런 다음 실제 프로비저닝 흐름으로 계속 진행됩니다. 서비스 공급자는 이 DNS SRV 프로비저닝 흐름을 활용하여 자동 프로비저닝을 제공할 수 있습니다.

DNS SRV는 DHCP가 제공한 도메인 이름의 인증서를 기반으로 호스트 이름 검증을 수행합니다. 모든 SRV 레코드는 DHCP에서 제공한 도메인 이름이 포함된 유효한 인증서를 사용하는 것이 중요합니다.

DNS SRV 쿼리에는 다음과 같이 구성에 DHCP 도메인 이름이 포함됩니다. **_<servicename>._<transport>.<domainName>**.

예를 들어, **_ciscoprov-https._tls.example.com**은 전화기에 example.com을 조회하도록 지시합니다. 전화기는 DNS SRV 쿼리에서 검색한 호스트 이름 및 포트 번호를 사용하여 초기 구성을 다운로드하는 데 사용하는 URL을 작성합니다.

DNS SRV는 전화기에서 사용하는 여러 가지 자동 프로비저닝 메커니즘 중 하나입니다. 전화기는 다음 순서로 메커니즘을 시도합니다.

1. DHCP
2. DNS SRV
3. EDOS
4. GDS(활성화 코드 온보딩) 또는 EDOS 장치 활성화

다음 표에는 SRV 레코드 필드에 대한 설명이 나와 있습니다.

표 ***1: SRV*** 레코드 필드

필드	설명	예제
<_servicename.>	서비스 이름은 밑줄로 시작합니다. 서버 서비스는 SRV 레코드에 기호화된 이름을 사용합니다. 서비스 다음에 마침표(.)는 서비스가 설정되어 있고 다음 섹션을 시작하고 있음을 나타냅니다.	**_ciscoprov-https.** 또는 **_ciscoprov-http.** DNS SRV가 TFTP 프로토콜을 지원하지 않습니다. TFTP를 사용하는 경우 다음과 같은 오류 메시지가 나타납니다. 오류 - TFTP 체계는 SRV 조회에서 지원되지 않습니다.

필드	설명	예제
<_proto.>	전송 프로토콜은 밑줄로 시작합니다. 프로토콜 다음의 기간은 프로토콜 섹션이 종료되었음을 나타냅니다.	**_tls.** TLS와 함께 HTTPS를 사용해야 합니다. 또는 **_tcp.** TCP와 함께 HTTP를 사용해야 합니다.
<domainName>	서비스 도메인 이름은 프로토콜을 따릅니다. 호스트 이름 확인: 모든 SRV 레코드는 원래 DHCP에서 제공한 도메인 이름을 기반으로 검증됩니다. 모든 레코드는 원래 도메인 이름이 포함된 유효한 인증서를 사용하는 것이 중요합니다.	**example.com**
TTL(Time to Live)	레코드의 만료 값(초)입니다.	86400
클래스	인터넷 유형 - SRV 레코드임을 나타내는 표준 바인드 표시법입니다.	IN
<priority>	각 회선은 우선 순위 번호를 포함합니다. 번호가 작을수록 이전 전화기는 이 DNS SRV 레코드에 포함된 대상 호스트 이름 및 포트를 시도합니다.	**10**
<weight>	두 개 이상의 서비스에 동일한 우선 순위가 있는 경우 가중치 번호에 따라 첫 번째 회선이 먼저 표시됩니다. 번호가 작을수록 이전 전화기는 이 DNS SRV 레코드에 포함된 대상 호스트 이름 및 포트를 시도합니다.	**20**
<port>	선택적 포트 번호	**5060**
<target>	서비스를 제공하는 컴퓨터의 A 레코드입니다. 레코드는 가장 기본적인 DNS 레코드 유형이며 도메인 또는 하위 도메인을 IP 주소로 가리키기 위해 사용됩니다.	**pr1.example.com**

SRV 구성 예

_service._proto.name. TTL 클래스 SRV 우선 순위 가중치 포트 대상입니다.

_ciscoprov-https._tls.example.com. 86400 IN SRV 10 60 5060 pr1.example.com.

_ciscoprov-https._tls.example.com. 86400 IN SRV 10 20 5060 pr2.example.com.

_ciscoprov-http._tcp.example.com. 86400 IN SRV 10 50 5060 px1.example.com.

_ciscoprov-http._tcp.example.com. 86400 IN SRV 10 30 5060 px2.example.com.

HTTP 프로비저닝을 위한 DNS SRV 사용

새 전화기는 DNS SRV를 자동 프로비저닝의 한 가지 방법으로 사용합니다. 기존 전화기의 경우 HTTP에 대해 DNS SRV를 사용하여 설정하는 네트워크에서는 이 기능을 사용하여 전화기를 재동기화할 수 있습니다. 샘플 구성 파일:

```
<flat-profile>
<!-- System Configuration -->
<Primary_DNS ua="rw">10.89.68.150</Primary_DNS>
<Back_Light_Timer ua="rw">Always On</Back_Light_Timer>
<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>
<Profile_Authentication_Type ua="na">Basic Http Authentication </Profile_Authentication_Type>
<Proxy_1_ ua="na">example.com</Proxy_1_>
<Display_Name_1_ ua="na">4081001141</Display_Name_1_>
<User_ID_1_ ua="na">4081001141</User_ID_1_>
</flat-profile>
```

시작하기 전에

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

프로시저

다음 작업 중 하나를 수행합니다. 그런 다음 웹 페이지에서 SRV 옵션을 사용하여 프로파일 규칙 설정, 9 페이지 또는 전화기에서 SRV 옵션을 사용하여 프로파일 규칙 설정, 10 페이지

- XML 구성 파일인 $PSN.xml을 웹 서버 루트 디렉터리에 저장합니다.
- 웹 서버 루트 디렉터리/Cisco/에 XML 구성 파일, $MA.cfg를 저장합니다.

웹 페이지에서 SRV 옵션을 사용하여 프로파일 규칙 설정

SRV 옵션을 사용하여 전화기에 구성 파일을 다운로드할 수 있습니다.

시작하기 전에

전화기 웹 인터페이스 액세스

프로시저

단계 **1** 음성 > 프로비저닝을 선택합니다.

단계 **2** 프로파일 규칙 필드에 SRV 옵션을 사용하여 프로파일 규칙을 입력합니다. HTTP 및 HTTPS만 지원됩니다.

예:

```
[--srv] https://example.com/$PSN.xml
```

전화기에서 SRV 옵션을 사용하여 프로파일 규칙 설정

전화기의 SRV 옵션을 사용하여 구성 파일을 다운로드할 수 있습니다.

프로시저

단계 1 애플리케이션 을 누릅니다.

단계 2 장치 관리 > 프로파일 규칙을 선택합니다.

단계 3 **[--srv]** 매개 변수를 사용하여 프로파일 규칙을 입력합니다. HTTP 및 HTTPS만 지원됩니다.

예:

```
[--srv] https://example.com/$PSN.xml
```

단계 4 재동기화를 누릅니다.

TR69 프로비저닝

Cisco IP 전화기는 관리자가 웹 UI를 사용하여 TR69 매개 변수를 구성하도록 도와줍니다. XML 및 TR69 매개 변수의 비교를 포함하여 매개 변수와 관련된 정보는 해당 전화기 시리즈의 관리 가이드를 참조하십시오.

전화기는 DHCP 옵션 43, 60, 125에서 ACS(Auto Configuration Server) 검색을 지원합니다.

- 옵션 43 - ACS URL에 대한 공급업체별 정보.
- 옵션 60 - 전화기가 `dslforum.org`를 사용하여 ACS에 대해 자신을 식별하기 위한 공급업체 클래스 식별자.
- 옵션 125 - 게이트웨이 연결을 위한 공급업체별 정보.

TR69 RPC Methods

지원되는 RPC 메서드

전화기는 다음과 같이 제한된 RPC(Remote Procedure Call) 메서드 집합을 지원합니다.

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes

- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: Download RPC 메서드, 다음 파일 형식이 지원됩니다.
  - 펌웨어 업그레이드 이미지
  - 구성업체 구성 파일
  - 사용자 지정 CA(Certificate Authority) 파일
- Transfer Complete

지원되는 이벤트 유형

전화기는 지원되는 기능 및 방식에 따라 이벤트 유형을 지원합니다. 다음 이벤트 유형만 지원됩니다.

- 부트스트랩
- 부팅
- 값 변경
- 연결 요청
- 주기적
- Transfer Complete
- M 다운로드
- M 재부팅

통신 암호화

장치에 전달되는 구성 매개 변수에는 시스템을 무단 액세스로부터 보호하는 인증 코드나 기타 정보가 포함될 수 있습니다. 인증되지 않은 고객 활동을 방지하는 것은 서비스 제공자의 책임이며, 계정의 무단 사용을 방지하는 것은 고객의 책임입니다. 서비스 제공자는 관리 웹 서버로의 액세스를 제한하는 것 외에 프로비저닝 서버와 장치 사이의 구성 프로파일 통신을 암호화할 수도 있습니다.

네트워크 혼잡 시 전화기 동작

네트워크 성능을 저하시키는 것이라면 무엇이나 전화기 오디오에 영향을 미칠 수 있고, 어떤 경우에는 통화가 끊어지게 만들 수도 있습니다. 네트워크 저하의 근원에는 다음과 같은 활동이 포함되며 이에 국한되는 것은 아닙니다.

- 관리자 작업(예: 내부 포트 스캔 또는 보안 스캔)
- 네트워크에 발생한 공격(예: DoS(서비스 거부) 공격 등)

사내 사전 프로비저닝 및 프로비저닝 서버

서비스 제공자는 프로파일로 TC 단위가 아닌 전화기를 프로비저닝합니다. 프로비전 프로파일은 전화기를 재동기화하는 제한된 매개 변수 집합으로 구성될 수 있습니다. 프로파일은 원격 서버가 전달하는 매개 변수의 완전한 집합을 구성할 수도 있습니다. 기본적으로 전화기는 전원을 켤 때 및 프로파일에 구성된 간격에 따라 재동기화합니다. 사용자가 전화기를 고객 구내에 연결하면 장치가 업데이트된 프로파일 및 모든 펌웨어 업데이트를 다운로드합니다.

사전 프로비저닝, 구축 및 원격 프로비저닝하는 과정은 여러 가지 방법으로 수행할 수 있습니다.

서버 준비 및 소프트웨어 도구

이 장에서 예에서는 서버를 하나 이상 사용할 수 있어야 합니다. 로컬 PC에 다음과 같은 서버를 설치 및 실행할 수 있습니다.

- TFTP(UDP 포트 69)
- syslog(UDP 포트 514)
- HTTP(TCP 포트 80)
- HTTPS(TCP 포트 443).

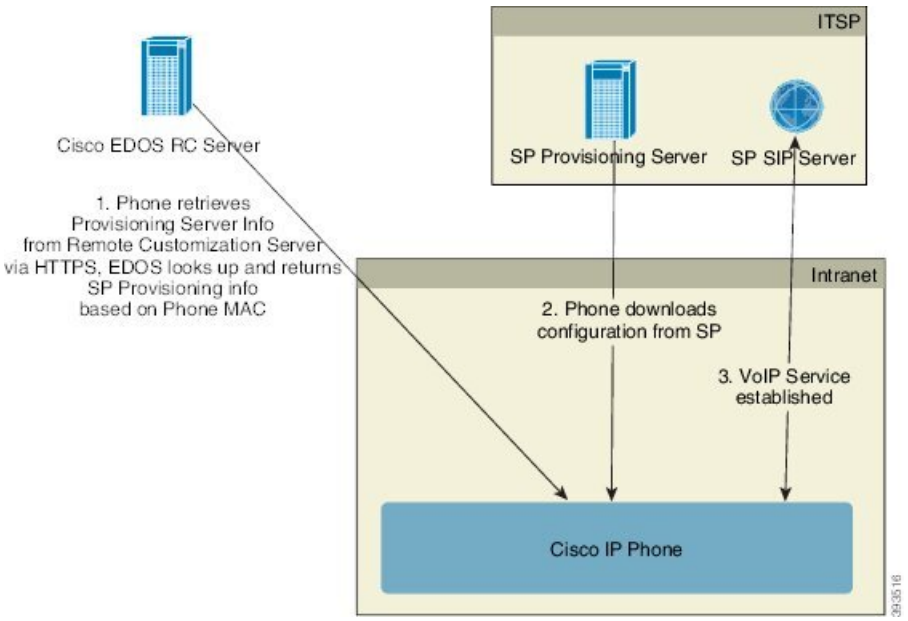
서버 구성 문제를 해결하려면 각 서버 유형별 클라이언트를 별도의 서버 시스템에 설치하는 것이 좋습니다. 이 방법을 사용하면 전화기와의 상호 작용에 관계없이 적절한 서버 작업이 설정됩니다.

또한 다음과 같은 소프트웨어 도구를 설치하는 것이 좋습니다.

- 구성 프로파일을 생성하려면 오픈소스 gzip 압축 유틸리티를 설치합니다.
- 프로파일 암호화 및 HTTPS 작업을 위해 오픈소스 OpenSSL 소프트웨어 패키지를 설치합니다.
- 동적 프로파일 생성 및 HTTPS를 사용한 1단계 원격 프로비저닝 테스트를 위해 CGI 스크립팅 지원을 사용하여 스크립팅 언어를 설치하는 것이 좋습니다. 오픈소스 Perl 언어 도구는 이러한 스크립팅 언어의 예입니다.

- 프로비저닝 서버와 전화기 간의 보안 통신을 확인하려면 이더넷 패킷 스니퍼(예: 무료로 다운로드할 수 있는 Ethereal/Wireshark)를 설치합니다. 전화기와 프로비저닝 서버 간의 상호 작용에 대한 이더넷 패킷 추적을 캡처합니다. 이렇게 하려면 포트 미러링이 활성화된 스위치에 연결된 PC에서 패킷 스니퍼를 실행합니다. HTTPS 트랜잭션의 경우 ssldump 유틸리티를 사용할 수 있습니다.

원격 사용자 지정(RC) 배포



모든 전화기는 처음 프로비저닝되기 전까지 Cisco EDOS RC Server로 연결합니다.

RC 배포 모델에서는 고객이 Cisco EDOS RC Server의 특정 서비스 제공자와 이미 연결된 전화기를 구매합니다. ITSP(Internet Telephony Service Provider)는 프로비저닝 서버를 설정 및 유지 관리하고 해당 프로비저닝 서버 정보를 Cisco EDOS RC Server에 등록합니다.

인터넷에 연결된 전화기의 전원이 켜지면 프로비저닝되지 않은 전화기의 사용자 지정 상태는 열림입니다. 전화기는 먼저 로컬 DHCP 서버에 프로비저닝 서버 정보를 쿼리하고 전화기의 사용자 지정 상태를 설정합니다. DHCP 쿼리가 성공한 경우 사용자 지정 상태가 중단됨으로 설정되며 필요한 프로비저닝 서버 정보를 DHCP가 제공하므로 RC를 시도하지 않습니다.

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.com을 계속 사용합니다. 두 도메인 이름 모두 방화벽을 통과하도록 허용하는 것이 좋습니다.

DHCP 서버가 프로비저닝 서버 정보를 제공하지 않은 경우, 전화기는 해당 MAC 주소와 모델을 제공하고 Cisco EDOS RC Server를 쿼리하며 사용자 지정 상태를 보류 중으로 설정합니다. Cisco EDOS Server는 프로비저닝 서버 URL을 비롯한 연결된 서비스 제공자의 프로비저닝 서버 정보를 제공하고 전화기의 사용자 지정 상태를 사용자 지정 보류 중으로 설정합니다. 전화기는 이어 재동기화 URL 명

령을 수행하여 서비스 제공자의 구성을 검색하며, 성공할 경우 사용자 지정 상태를 취득으로 설정합니다.

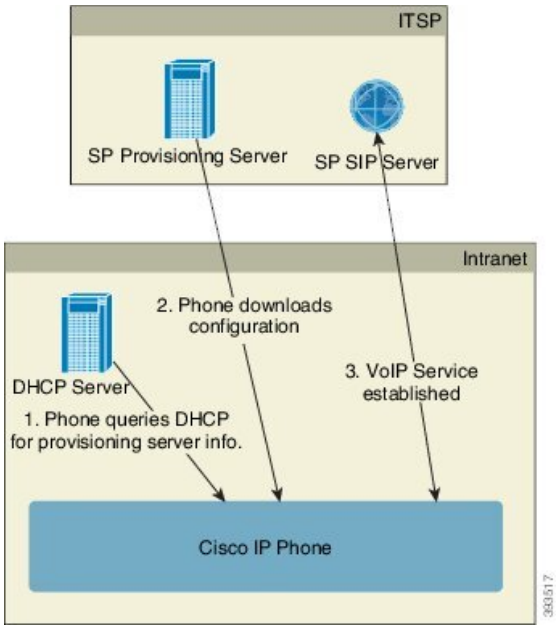
DHCP 서버 프로비저닝이 실패하는 경우, 전화기는 해당 MAC 주소와 모델을 제공하고 Cisco EDOS RC Server를 쿼리하며 사용자 지정 상태를 보류 중으로 설정합니다. Cisco EDOS Server는 프로비저닝 서버 URL을 비롯한 연결된 서비스 제공자의 프로비저닝 서버 정보를 제공하고 전화기의 사용자 지정 상태를 사용자 지정 보류 중으로 설정합니다. 전화기는 이어 재동기화 URL 명령을 수행하여 서비스 제공자의 구성을 검색하며, 성공할 경우 사용자 지정 상태를 취득으로 설정합니다. 로컬 DHCP 서버 또는 EDOS 서버에 대한 쿼리가 프로비저닝에 실패하는 경우 DHCP 및 EDOS를 통해 온보드로 전화를 다시 시도합니다.

Cisco EDOS RC Server에 전화기와 연결된 서비스 제공자가 없는 경우 전화기의 사용자 지정 상태가 사용할 수 없음으로 설정됩니다. 전화기는 수동으로 구성하거나 전화기와 서비스 제공자의 연결을 Cisco EDOS Server로 추가할 수 있습니다.

사용자 지정 상태가 취득이 되기 전에 전화기를 LCD 또는 웹 구성 유틸리티를 통해 프로비저닝한 경우, 사용자 지정 상태가 중단됨으로 설정되며 전화기를 팩토리 설정하기 전에는 Cisco EDOS Server가 쿼리되지 않습니다.

전화기를 프로비저닝한 후에는 전화기를 팩토리 설정하기 전까지 Cisco EDOS RC Server가 사용되지 않습니다.

사내 장치 사전 프로비저닝



Cisco 공장 기본값 구성에서, 전화기는 자동으로 TFTP 서버의 프로파일로 재동기화를 시도합니다. LAN 상의 관리되는 DHCP 서버는 장치의 사전 프로비전닝을 위해 구성된 TFTP 서버와 프로파일에 대한 정보를 제공합니다. 서비스 제공자가 각 새 전화기를 LAN에 연결합니다. 전화기는 자동으로 로컬 TFTP 서버로 재동기화하며 구축 준비를 위한 내부 상태를 초기화합니다. 이 사전 프로비저닝 프

로파일은 일반적으로 원격 프로비저닝 서버의 URL을 포함합니다. 프로비저닝 서버는 장치가 배포되고 고객 네트워크에 연결된 후 장치를 업데이트 상태로 유지합니다.

전화기를 고객에게 배송하기 전에, 사전 프로비저닝된 장치 바코드를 스캔하여 MAC 주소 또는 일련 번호를 기록할 수 있습니다. 이 정보는 전화기를 재동기화하는 프로파일을 생성하는 데 사용할 수 있습니다.

고객은 전화기를 받으면 광대역 링크에 연결합니다. 전화기 전원을 켜면 사전 프로비저닝을 통해 구성된 URL을 통해 프로비저닝 서버로 연결합니다. 전화기는 이제 필요에 따라 재동기화 및 펌웨어 업데이트를 할 수 있습니다.

프로비저닝 서버 설정

이 섹션에서는 다양한 서버와 여러 시나리오를 사용하여 전화기 프로비저닝하는 설정 요구 사항에 대해 설명합니다. 이 설명서의 설명과 테스트를 위해, 프로비저닝 서버는 로컬 PC에 설치 및 실행합니다. 또한, 전화기를 프로비저닝하는 데는 쉽게 구할 수 있는 소프트웨어 도구가 유용합니다.

TFTP 프로비저닝

전화기는 프로비저닝 재동기화 및 펌웨어 업그레이드 작업에 TFTP를 지원합니다. 장치가 원격으로 배포되는 경우 HTTPS가 권장되지만, HTTP와 TFTP도 사용할 수 있습니다. 그런 다음 프로비저닝 파일 암호화를 요구하여 NAT와 라우터 보호 메커니즘을 기반으로 안정성을 향상시켜서 보안 수준을 높일 수 있습니다. TFTP는 프로비저닝되지 않은 다수의 장치를 사내에서 사전 프로비저닝하는 데 유용합니다.

전화기는 DHCP 옵션 66을 통해 DHCP 서버에서 TFTP 서버 IP 주소를 직접 얻을 수 있습니다. Profile_Rule이 해당 TFTP 서버의 파일 경로를 사용하여 설정된 경우, 장치는 TFTP 서버에서 해당 프로파일을 다운로드합니다. 다운로드는 장치가 LAN에 연결되고 전원이 켜질 때 수행됩니다.

공장 기본값 구성의 Profile_Rule은 *&PN*.cfg이며, 여기에서 *&PN*은 전화기 모델 이름입니다.

예를 들어 CP-7841-3PCC의 경우, 파일 이름은 CP-7841-3PCC.cfg입니다. CP-7832-3PCC의 경우, 파일 이름은 CP-7832-3PCC.cfg입니다.

예를 들어 CP-8841-3PCC의 경우, 파일 이름은 CP-8841-3PCC.cfg입니다.

예를 들어 CP-6841-3PCC의 경우, 파일 이름은 CP-6841-3PCC.cfg입니다.

장치 프로파일이 공장 기본값인 경우 장치를 켜면 DHCP 옵션 66이 지정하는 로컬 TFTP 서버의 이 파일로 재동기화를 수행합니다. 파일 경로는 TFTP 서버 가상 루트 디렉터리에 상대적입니다.

원격 엔드포인트 제어 및 **NAT**

전화기는 라우터를 통해 인터넷에 액세스하기 위해 NAT(Network Address Translation)와 호환됩니다. 라우터는 보안 강화를 위해 인터넷에서 보안 네트워크로 들어오는 패킷을 강력하게 제한하는 패킷 필터링 전략인 대칭 NAT를 구현하여 무단 수신 패킷을 차단하려고 할 수 있습니다. 따라서 TFTP를 사용한 원격 프로비저닝은 권장되지 않습니다.

VoIP는 일부 형식의 NAT 통과가 허용되는 경우에만 NAT와 공존할 수 있습니다. STUN(Simple Traversal of UDP)을 구성합니다. 이 옵션을 사용하려면 사용자에게 다음 항목이 있어야 합니다.

- 서비스의 동적 외부(공개) IP 주소
- STUN 서버 소프트웨어를 실행하는 컴퓨터
- 비대칭 NAT 메커니즘을 사용하는 최종 장치

HTTP 프로비저닝

전화기에서 원격 인터넷 사이트에서 웹 페이지를 요청하는 브라우저처럼 작동합니다. 이를 통해 고객 라우터가 동기 NAT 또는 다른 보호 메커니즘을 구현하더라도 프로비저닝 서버에 연결할 수 있는 안정적인 수단을 제공합니다. HTTP와 HTTPS는 원격 구축에서 TFTP보다 안정적이며, 특히 배포된 장치가 거주 방화벽 또는 NAT 지원 라우터에 연결된 경우 더 안정적입니다. HTTP와 HTTPS 다음 요청 유형 설명에서 같은 의미로 사용됩니다.

기본 HTTP 기반 프로비저닝은 구성 프로파일을 검색하기 위해 HTTP GET 방식을 사용합니다. 일반적으로 구성 파일은 배포된 각 전화기를 위해 생성되며, HTTP 서버 디렉터리 안에 저장됩니다. 서버가 GET 요청을 받으면 GET 요청 헤더에 지정된 파일을 반환합니다.

정적 프로파일을 제공하는 대신, 고객 데이터베이스를 쿼리하고 동적으로 즉석에서 구성 프로파일을 생성할 수도 있습니다.

전화기가 재동기화를 요청할 때는 HTTP POST 방식을 사용해 재동기화 구성 데이터를 요청할 수 있습니다. 장치는 HTTP POST 요청의 본체 내에서 특정 상태와 식별 정보를 서버로 전달하도록 구성할 수 있습니다. 서버는 이 정보를 사용하여 필요한 응답 구성 프로파일을 생성하거나 이후 분석과 추적을 위해 상태 정보를 저장합니다.

전화기는 GET과 POST 요청의 일부로서 자동으로 기본 식별 정보를 요청 헤더의 User-Agent 필드에 포함합니다. 이 정보에는 제조업체, 제품 이름, 현재 펌웨어 버전 및 장비의 제품 일련 번호가 포함됩니다.

다음 예는 CP-8841-3PC의 User-Agent 요청 필드입니다.

```
User-Agent: Cisco-CP-8841-3PCC/11.0 (00562b043615)
```

다음 예는 CP-6841-3PC의 User-Agent 요청 필드입니다.

```
User-Agent: Cisco-CP-6841-3PCC/11.0 (00562b043615)
```

사용자 에이전트를 구성할 수 있으며, 구성하지 않은 경우에는 전화기에서 이 값을 사용합니다(기본값).

전화기가 HTTP를 사용하여 구성 프로파일로 재동기화하도록 구성된 경우 HTTPS를 사용하거나 프로파일을 암호화해 기밀 정보를 보호하는 것이 좋습니다. 전화기가 HTTP를 사용하여 암호화된 프로파일을 다운로드하면 구성 프로파일에 포함된 기밀 정보의 노출 위험이 방지됩니다. 이 재동기화 모드는 HTTPS를 사용하는 방법보다 프로비저닝 서버에 대한 컴퓨팅 부하가 낮습니다.

전화기는 다음 암호화 방법 중 하나로 암호화된 프로파일의 암호를 해독할 수 있습니다.

- AES-256-CBC 암호화
- AES-128-GCM 암호화를 사용한 RFC-8188 기반 암호화

참고 전화기는 HTTP 버전 1.0과 HTTP 버전 1.1을 지원하며 협상된 전송 프로토콜이 HTTP 버전 1.1일 경우 청크 인코딩을 지원합니다.

재동기화 및 업그레이드에서 **HTTP** 상태 코드 처리

전화기는 원격 프로비저닝(재동기화)을 위한 HTTP 응답을 지원합니다. 현재 전화기 동작은 세 가지 방법으로 분류됩니다.

- A - 성공, "주기적 재동기화" 및 "임의 지연 재동기화" 값이 후속 요청을 결정합니다.
- B - 파일이 발견되지 않거나 프로파일이 손상되어 실패. "재동기화 오류 재시도 지연" 값이 후속 요청을 결정합니다.
- C - 잘못된 URL 또는 IP 주소 때문에 연결 오류가 발생하는 다른 실패. "재동기화 오류 재시도 지연" 값이 후속 요청을 결정합니다.

표 ***2: HTTP*** 응답에 대한 전화기 동작

HTTP 상태 코드	설명	전화기 동작
301 Moved Permanently	이 요청과 향후 요청을 새로운 위치로 전달해야 합니다.	즉시 새로운 위치로 요청을 재시도합니다.
302 Found	일시적으로 이동됨이라고 합니다.	즉시 새로운 위치로 요청을 재시도합니다.
3xx	다른 3xx 응답은 처리되지 않습니다.	C
400 Bad Request	잘못된 구문 때문에 요청을 수행할 수 없습니다.	C
401 Unauthorized	기본 또는 다이제스트 액세스 인증 응답입니다.	인증 자격 증명으로 즉시 요청을 재시도합니다. 최대 2번 재시도합니다. 실패 시 전화기 동작은 C입니다.
403 Forbidden	서버에서 응답을 거부합니다.	C
404 Not Found	요청된 리소스를 찾을 수 없습니다. 클라이언트의 후속 요청은 허용됩니다.	B

HTTP 상태 코드	설명	전화기 동작
407 Proxy Authentication Required	기본 또는 다이제스트 액세스 인증 응답입니다.	인증 자격 증명으로 즉시 요청을 재시도합니다. 최대 두 번 재시도합니다. 실패 시 전화기 동작은 C입니다.
4xx	다른 클라이언트 오류 상태 코드는 처리되지 않습니다.	C
500 Internal Server Error	일반 오류 메시지입니다.	전화기 동작은 C입니다.
501 Not Implemented	서버가 요청 방법을 인식하지 못하거나 요청을 처리할 수 없습니다.	전화기 동작은 C입니다.
502 Bad Gateway	서버가 게이트웨이 또는 프록시로 작동하며 업스트림 서버에서 잘못된 응답을 수신했습니다.	전화기 동작은 C입니다.
503 Service Unavailable	현재 서버를 사용할 수 없습니다(과부하 상태 또는 유지 관리를 위해 중단된 상태). 일시적인 상태입니다.	전화기 동작은 C입니다.
504 Gateway Timeout	서버가 게이트웨이 또는 프록시로 작동하며 업스트림 서버에서 시기적절하게 응답을 수신하지 못했습니다.	C
5xx	다른 서버 오류	C