CHAPTER 5

Provisioning

Phones can be *provisioned* to download configuration profiles or updated firmware from a remote server when they are connected to a network, when they are powered up, and at set intervals. Provisioning is typically part of high-volume, Voice-over-IP (VoIP) deployments and limited to service providers. Configuration profiles or updated firmware are transferred to the device by using TFTP, HTTP, or HTTPS.

The conference phone accepts configuration profiles in XML format, or in a proprietary binary format generated by the SIP Profile Compiler (SPC) available from Cisco. The conference phone supports 256-bit symmetric key encryption to secure the XML content of the profiles. SPC compiled binary profiles can be encrypted when they are complied. Since firmware does not contain sensitive personal information, typically it is not encrypted.

Provisioning is described in detail in the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide*.

This chapter describes:

Redundant Provisioning Servers

The provisioning server may be specified as an IP address or as a fully qualified domain name (FQDN). The use of a FQDN facilitates the deployment of redundant provisioning servers. When the provisioning server is identified through a FQDN, the Cisco IP phone attempts to resolve the FQDN to an IP address through DNS. Only DNS A-records are supported for provisioning; DNS SRV address resolution is not available for provisioning. The Cisco conference phone continues to process A-records until the first server responds. If no server associated with the A-records responds, the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control logs an error to the syslog server.

Retail Provisioning

The conference phone includes the web-based configuration utility that displays internal configuration and accepts new configuration parameter values. The server also accepts a special URL command syntax for performing remote profile resync and firmware upgrade operations.

In a retail distribution model, a customer purchases a Cisco voice endpoint device, and subsequently subscribes to a particular service. The customer first signs on to the service and establishes a VoIP account, possibly through an online portal. Subsequently, the customer binds the particular device to the assigned service account.

To do so, the unprovisioned Cisco Unified IP Conference Phone 8831 for Third-Party Call Control is instructed to resync with a specific provisioning server through a resync URL command. The URL command typically includes an account PIN number or alphanumeric code to associate the device with the new account.

In the following example, a device at the DHCP-assigned IP address 192.168.1.102 is instructed to provision itself to the SuperVoIP service:

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/1234abcd
```

In this example, 1234abcd is the PIN number of the new account. The remote provisioning server is configured to associate the phone that is performing the resync request with the new account, based on the URL and the supplied PIN. Through this initial resync operation, the phone is configured in a single step, and is automatically directed to resync thereafter to a permanent URL on the server. For example:

```
https://prov.supervoip.com/cisco-init
```

For both initial and permanent access, the provisioning server relies on the Cisco IP phone client certificate for authentication and supplies correct configuration parameter values based on the associated service account.

Automatic In-House Preprovisioning

Using the phone web user interface and issuing a resync URL is convenient for a customer in the retail deployment model, but it is not as convenient for preprovisioning a large number of units.

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control supports a more convenient mechanism for in-house preprovisioning. With the factory default configuration, the phone automatically tries to resync to a specific file on a TFTP server, whose IP address is offered as one of the DHCP-provided parameters. This lets a service provider connect each new Cisco IP phone to a LAN environment configured to preprovision phones. Any new Cisco IP phone connected to this LAN automatically resyncs to the local TFTP server, initializing its internal state in preparation for deployment. Among other parameters, this preprovisioning step configures the URL of the Cisco IP phone provisioning server.

Subsequently, when a new customer signs up for service, the preprovisioned Cisco Unified IP Conference Phone 8831 for Third-Party Call Control can be simply bar-code scanned, to record its MAC address or serial number, before being shipped to the customer. Upon receiving the unit, the customer connects the unit to the broadband link. On power-up the Cisco IP phone already knows the server to contact for its periodic resync update.

Use HTTPS

The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control provides a reliable and secure provisioning strategy based on HTTPS requests from the phone to the provisioning server, using both server and client certificates for authenticating the client to the server and the server to the client.

To use HTTPS with the phone, you must generate a Certificate Signing Request (CSR) and submit it to Cisco. The Cisco Unified IP Conference Phone 8831 for Third-Party Call Control generates a certificate for installation on the provisioning server that is accepted by the conference phones when they seek to establish an HTTPS connection with the provisioning server.

The phone implements up to 256-bit symmetric encryption, using the American Encryption Standard (AES), in addition to 128-bit RC4. The phone supports the Rivest, Shamir, and Adelman (RSA) algorithm for public/private key cryptography.

Server Certificates

Each secure provisioning server is issued an secure sockets layer (SSL) server certificate, directly signed by Cisco. The firmware running on the Cisco IP phone clients recognizes only these certificates as valid. The clients try to authenticate the server certificate when connecting via HTTPS, and reject any server certificate not signed by Cisco.

This mechanism protects the service provider from unauthorized access to the Cisco IP phone endpoint, or any attempt to spoof the provisioning server. This might allow the attacker to reprovision the Cisco IP phone to gain configuration information, or to use a different VoIP service. Without the private key corresponding to a valid server certificate, the attacker is unable to establish communication with a Cisco IP phone.

Client Certificates

In addition to a direct attack on the phone, an attacker might attempt to contact a provisioning server using a standard web browser, or other HTTPS client, to obtain the phone configuration profile from the provisioning server. To prevent this kind of attack, each phone carries a unique client certificate, also signed by Cisco, including identifying information about each individual endpoint. A certificate authority root certificate capable of authenticating the device client certificate is given to each service provider. This authentication path allows the provisioning server to reject unauthorized requests for configuration profiles.

Obtain a Server Certificate

To obtain a server certificate:

Step 1 Contact a Cisco support person who will work with you on the certificate process. If you are not working with a specific support person, you can email your request to ciscosb-certadmin@cisco.com.)

Step 2 Generate a private key that will be used in a CSR (Certificate Signing Request). This key is private and you do not need to provide this key to Cisco support. Use open source “openssl” to generate the key. For example:

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

Step 3 Generate CSR a that contains fields that identify your organization, and location. For example:

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

You must have the following information:

- Subject field—Enter the Common Name (CN) that must be a FQDN (Fully Qualified Domain Name) syntax. During SSL authentication handshake, the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control verifies that the certificate it receives is from the machine that presented it.
- Server's hostname—For example, provserv.domain.com.
- Email address—Enter an email address so that customer support can contact you if needed. This email address is visible in the CSR.

Step 4 Email the CSR (in zip file format) to the Cisco support person or to ciscosb-certadmin@cisco.com. The certificate is signed by Cisco and given to you.

Manually Provision a Phone from the Keypad

Typically the conference phone is configured to be provisioned when first connected to the network and at configured intervals that are set when the phone is preprovisioned (configured) by the service provider or the VAR. Service providers can authorize VARs or advanced users to manually provision the phone by using the phone keypad.

The status of the provisioning process is indicated by the phone mute button blinking in the following patterns:

- Red/orange slow blink (1.0 seconds on, 1.0 seconds off): Contacting server, server not resolvable, not reachable, or down.
- Red/orange fast blink (0.2 seconds on, 0.2 seconds off, 0.2 seconds on, 1.4 seconds off): Server responded with file not found or corrupt file.

To manually provision the phone by using the keypad:

Step 1 Press **Setup**, then scroll to **Profile Rule**.

Step 2 Enter the profile rule by using the following format:

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

For example:

```
tftp://192.168.1.5/CP_8831_3PCC.cfg
```

If no protocol is specified, TFTP is assumed. If no server-name is specified, the host that requests the URL is used as the server name. If no port is specified, the default port is used (69 for TFTP, 80 for HTTP, or 443 for HTTPS).

Step 3 Press the **Resync** softkey.

Sample Configuration File

Refer to the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide*.

Update Profiles and Firmware

Cisco conference phones support secure remote provisioning (configuration) and firmware upgrades. An unprovisioned phone can receive an encrypted profile specifically targeted for that device without requiring an explicit key by using a secure first-time provisioning mechanism using SSL functionality.

User intervention is not required to initiate or complete a profile update or firmware upgrade. If intermediate upgrades are required to reach a future upgrade state from an older release, the Cisco IP phone upgrade logic is capable of automating multi-stage upgrades. A profile resync is only attempted when the Cisco IP phone is idle, because this might trigger a software reboot and disconnect a call.

General purpose parameters manage the provisioning process. Each Cisco IP phone can be configured to periodically contact a normal provisioning server (NPS). Communication with the NPS does not require the use of a secure protocol because the updated profile is encrypted by a shared secret key. The NPS can be a standard TFTP, HTTP or HTTPS server with client certificates.

The administrator can upgrade, reboot, restart, or resync Cisco IP phones by using the phone web user interface. The administrator can also perform these tasks by using a SIP notify message.

Configuration profiles are generated by using common, open-source tools that integrate with service provider provisioning systems. (Provisioning is described in detail in the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide*.)

Allow and Configure Profile Updates

The profile updates can be allowed at specified intervals. Updated profiles are sent from a server to the phone by using TFTP, HTTP, or HTTPS.

To configure a profile update:

Step 1 Click **Admin Login > advanced > Voice > Provisioning**.

Step 2 Under **Configuration Profile** in the Provision Enable field, choose **Yes**.

Step 3 Enter the parameters defined in the table:

Parameter	Description
Provision Enable	Allows or denies resync actions. Defaults to **Yes**.
Resync On Reset	The device performs a resync operation after power-up and after each upgrade attempt when set to **Yes**.
Resync Random Delay	A random delay following the boot-up sequence before performing the reset, specified in seconds. In a pool of IP Telephony devices that are scheduled to simultaneously powered up, this introduces a spread in the times at which each unit sends a resync request to the provisioning server. This feature can be useful in a large residential deployment, in the case of a regional power failures.
Resync At (HHmm)	Time in 24-hour format (hhmm) to resync the device. When this parameter is provisioned, the Resync Periodic parameter is ignored. Default is empty.

Parameter	Description
Resync At Random Delay	To avoid flooding the server with simultaneously resync requests from multiple phones set to resync at the same time, the phone triggers the resync up to ten minutes after the specified time. The input value (in seconds) is converted to minutes. The default value is 600 seconds (10 minutes). If the parameter value is set to less than 600, the default value is used.
Resync Periodic	Time in seconds between periodic resyncs. If this value is empty or zero, the device does not resync periodically.
Resync Error Retry Delay	If a resync operation fails because the IP Telephony device was unable to retrieve a profile from the server, if the downloaded file is corrupt, or an internal error occurs, the device tries to resync again after a time specified in seconds. If the delay is set to 0, the device does not try to resync again following a failed resync attempt.
Forced Resync Delay	The resync typically takes place when the voice lines are idle. When a voice line is active and a resync is due, the IP Telephony device delays the resync procedure until the line becomes idle. However, it waits no longer than the Forced Resync Delay (seconds). A resync might cause configuration parameter values to change. This causes a firmware reboot and terminates any voice connection active at the time of the resync.
Resync Fails On FNF	A resync is considered unsuccessful if a requested profile is not received from the server. This can be overridden by this parameter. When it is set to **no**, the device accepts a `file-not-found` response from the server as a successful resync.
Profile Rule Profile Rule B Profile Rule C Profile Rule D	Remote configuration profile rules evaluated in sequence. Each resync operation can retrieve multiple files, potentially managed by different servers.
Resync DHCP Option To Use	DHCP options, delimited by commas, used to retrieve firmware and profiles.
Transport Protocol	The transport protocol used to retrieve firmware and profiles. If none is selected, TFTP is assumed and the IP address of the TFTP server is obtained from the DHCP server.
Log Request Msg	The message sent to the syslog server at the start of a resync attempt. The default value is: `$PN $MAC –Requesting % $SCHEME://$SERVIP:$PORT$PATH`
Log Success Msg	The syslog message issued upon successful completion of a resync attempt. The default value is: `$PN $MAC –Successful % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
User Configurable Resync	Allows a user to resync the phone from the phone screen.

Allow and Configure Firmware Updates

The firmware updates can be allowed at specified intervals. Updated firmware is sent from a server to the phone by using a TFTP or HTTP. Security is less of an issue with a firmware upgrade, because firmware does not contain personal information.

To configure a firmware update:

Step 1 Click **Admin Login > advanced > Voice > Provisioning**.

Step 2 Under **Firmware Upgrade** in the Upgrade Enable field, choose **Yes**.

Step 3 Enter the parameters defined in the table:

Parameter	Description
Upgrade Enable	Allows firmware update operations independent of resync actions. Defaults to Yes.
Upgrade Error Retry Delay	The interval applied in the event of an upgrade failure. The firmware upgrade error timer activates after a failed firmware upgrade attempt and is initialized with this value. The next firmware upgrade attempt occurs when this timer counts down to zero. The default is 3600 seconds.
Upgrade Rule	A firmware upgrade script that defines upgrade conditions and associated firmware URLs. It uses the same syntax as Profile Rule. (See "Manually Provision a Phone from the Keypad" section on page 5-4 for the Upgrade Rule syntax.) The default is (empty).

Firmware Upgrade

The 3PCC supports single one image upgrade by tftp/http/https.

Step 1 Put the 3PCC image cp-8831-sip.9-3-3-5-3PCC.bin.sgn on the tftp/http/https download directory.

Step 2 Configure Upgrade Rule on the 'Provisioning' tab in the web page, with the valid URL format:

```
<schema>:// <server[:port]> /filepath
```

Note A device (with new base and DCU) may not be downgraded to an earlier firmware release, such as 9.3(3). For details, refer to the hardware information and the firmware/hardware compatibility information in the current *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Release Notes*.

Firmware Upgrade With a Browser Command

An upgrade command entered into the browser address bar can be used to upgrade firmware on a phone. The phone updates only when it is idle. The update is attempted automatically after the call is complete.

To upgrade the conference phone CP-8831-3PCC via URL on web browser enter this command:

```
http://<phone_ip>/admin/upgrade?<schema>://<serv_ip[:port]>/filepath
```

Configure a Custom Certificate Authority

Digital certificates can be used to authenticate network devices and users on the network. They can be used to negotiate IPSec sessions between network nodes.

A third party uses a Certificate Authority certificate to validate and authenticate two or more nodes that are attempting to communicate. Each node has a public and private key. The public key encrypts data. The private key decrypts data. Because the nodes have obtained their certificates from the same source, they are assured of their respective identities.

The device can use digital certificates provided by a third-party Certificate Authority (CA) to authenticate IPSec connections. See the *Cisco Unified IP Conference Phone 8831 for Third-Party Call Control Provisioning Guide* for more information.

The phones support a set of preloaded Root Certificate Authority embedded in the firmware:

- Cisco Small Business CA Certificate
- CyberTrust CA Certificate
- Verisign CA certificate
- Sipura Root CA Certificate
- Linksys Root CA Certificate

On the phone web user interface:

Step 1 Click **Admin Login > advanced > Voice > Info**.

Step 2 Select **Download Status** and scroll to **Custom CA Status** and see the following fields:

- Custom CA Provisioning Status—Indicates the provisioning status.
  - Last provisioning succeeded on mm/dd/yyyy HH:MM:SS; or
  - Last provisioning failed on mm/dd/yyyy HH:MM:SS
- Custom CA Info—Displays information about the custom CA.
  - Installed—Displays the "CN Value," where "CN Value" is the value of the CN parameter for the Subject field in the first certificate.
  - Not Installed—Displays if no custom CA certificate is installed.

General Purpose Parameters

The general purpose parameters GPP_* are used as free string registers when configuring the conference phone to interact with a particular provisioning server solution. The GPP_* parameters are empty by default. They can be configured to contain diverse values, including the following:

- Encryption keys
- URLs
- Multistage provisioning status information
- Post request templates
- Parameter name alias maps
- Partial string values, eventually combined into complete parameter values.

The GPP_* parameters are available for macro expansion within other provisioning parameters. For this purpose, single-letter upper-case macro names (A through P) are sufficient to identify the contents of GPP_A through GPP_P. Also, the two-letter upper-case macro names SA through SD identify GPP_SA through GPP_SD as a special case when used as arguments of the **key** URL option.

These parameters can be used as variables in provisioning and upgrade rules. They are referenced by prepending the variable name with a '$' character, such as $GPP_A.

To configure general purpose parameters, navigate to **Admin Login > advanced > Voice > Provisioning**.