Deployment and Provisioning

Cisco IP Telephony devices are intended for high-volume deployments by VoIP service providers to residential and small business customers. In business or enterprise environments, IP Telephony devices can serve as terminal nodes. These devices are widely distributed across the Internet, connected through routers and firewalls at the customer premises.

The IP Telephony device can be used as a remote extension of the service provider back-end equipment. Remote management and configuration ensures the proper operation of the IP Telephony device at the customer premises.

This customized, ongoing configuration is supported by the following features:

- Reliable remote control of the endpoint
- Encryption of the communication controlling the endpoint
- Streamlined endpoint account binding

This chapter describes the features and functionality available when provisioning the Cisco Small Business IP Telephony devices and explains the setup required:

- Deployment, page 1-1
- Provisioning Overview, page 1-3

Deployment

Cisco IP Telephony devices provide convenient mechanisms for provisioning, based on two deployment models:

- Bulk distribution—The service provider acquires IP Telephony devices in bulk quantity and either preprovisions them in-house or purchases RC units from Cisco. The devices are then issued to the customers as part of a VoIP service contract.
- Retail distribution—The customer purchases the IP Telephony device from a retail outlet and requests VoIP service from the service provider. The service provider must then support the secure remote configuration of the device.

Bulk Distribution

In this model, the service provider issues IP Telephony devices to its customers as part of a VoIP service contract. The devices are either RC units or preprovisioned in-house.

RC units are preprovisioned by Cisco to resynchronize with a Cisco server that downloads the device profile and firmware updates.

A service provider can preprovision IP Telephony devices with the desired parameters, including the parameters that control resynchronization, through various methods: in-house by using DHCP and TFTP; remotely by using TFTP, HTTP, or HTTPS; or a combination of in-house and remote provisioning.

RC Unit Deployment

RC units eliminate in-house preprovisioning of IP Telephony devices and reduce the need for the service provider to physically handle the devices prior to shipping them to end customers. This approach also discourages the use of IP Telephony devices with an inappropriate service provider.

A RC unit is preprovisioned by Cisco with the connection information for the provisioning servers. These servers are maintained by Cisco Systems, Inc. for the service provider that purchased the units. The MAC address of each RC unit is associated with a customizable profile on the Cisco provisioning servers. When the RC unit is connected to the broadband link, it contacts the Cisco provisioning server and downloads its customized profile.

The service provider works with a Cisco sales engineer to develop a simple provisioning profile. The profile contains minimal information that redirects the device to the service provider provisioning server. This profile is placed on the Cisco RC server by the Cisco Voice Team.

RC Unit Status

The status of an RC unit can be determined by viewing the Info > Product Information page, Customization section, on the administration web server. An RC unit that has not been provisioned displays **Pending**. An RC unit that has been provisioned displays the name of the company that owns the unit. If the unit is not an RC unit, the page displays **Open**.

Below is a sample template for an RC unit to be preprovisioned by Cisco with the connection information:

```
Restricted Access Domains "domain.com, domain1.com, domain2.com";
Primary_DNS               * "x.y.w.z";
Secondary_DNS             * "a.b.c.d";
Provision_Enable          * "Yes";
Resync_Periodic           * "30";
Resync_Error_Retry_Delay  * "30";
Profile_Rule  * "http://prov.domain.com/sipura/profile?id=$MA";
```

The `Restricted Access Domains` parameter is configured with the actual domain names of up to a maximum of five domains. The Primary_DNS and Secondary_DNS parameters are configured with the actual domain names or IP addresses of the DNS servers available to the RC unit.

Retail Distribution

In a retail distribution model, a customer purchases a Cisco IP Telephony device and subscribes to a particular service. The Internet Telephony Service Provider (ITSP) sets up and maintains a provisioning server, and preprovisions the phone to resynchronize with the service provider server. See the "In-House Device Preprovisioning" section on page 3-2 for more information.

The customer signs on to the service and establishes a VoIP account, possibly through an online portal, and binds the device to the assigned service account. When the device is powered up or a specified time elapses, the IP Telephony device resynchronizes, downloading the latest parameters. These parameters can address goals such as setting up a hunt group, setting speed dial numbers, and limiting the features that a user can modify.

Resynchronization Process

The firmware for each IP Telephony device includes an administration web server that accepts new configuration parameter values. The IP Telephony device is instructed to resync with a specified provisioning server through a resync URL command in the device profile. The URL command typically includes an account PIN number or alphanumeric code to associate the device with the new account. For example:

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

In this example, a device at the DHCP-assigned IP address 192.168.1.102 is instructed to provision itself to the SuperVoIP service at `prov.supervoip.com`. The PIN number for the new account is 1234abcd. The remote provisioning server is configured to associate the IP Telephony device that is performing the resync request with the new account, based on the URL and PIN.

Through this initial resync operation, the IP Telephony device is configured in a single step, and is automatically directed to resync thereafter to a permanent URL on the server.

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

Provisioning Overview

An IP Telephony device can be configured to resynchronize its internal configuration state to match a remote profile periodically and on power up by contacting a normal provisioning server (NPS) or an access control server (ACS).

By default, a profile resync is only attempted when the IP Telephony device is idle, because the upgrade might trigger a software reboot interrupting a call. If intermediate upgrades are required to reach a current upgrade state from an older release, the upgrade logic is capable of automating multi-stage upgrades.

NPS

The NPS can be a TFTP, HTTP, or HTTPS server. A remote firmware upgrade is achieved by using TFTP or HTTP, but not by using HTTPS because the firmware does not contain sensitive information.

Communication with the NPS does not require the use of a secure protocol because the updated profile can be encrypted by a shared secret key. Secure first-time provisioning is provided through a mechanism that uses SSL functionality. An unprovisioned IP Telephony device can receive a 256-bit symmetric key encrypted profile specifically targeted for that device.

Provisioning States

The provisioning process involves these provisioning states.

State	Description
MFG-RESET **Manufacturing Reset**	The device returns to a fully unprovisioned state; all configurable parameters regain their default values. On phones that do not support IVR, perform the factory reset through LCD **Setup** menu. Allowing the end user to perform a manufacturing reset guarantees that the device can always be returned to an accessible state.
SP-CUST **Service Provider Customization**	The Profile_Rule parameter points to a device-specific configuration profile by using a provisioning server that is specific to the service provider. The methods for initiating resynchronization are: • Auto-configuration by using a local DHCP server. A TFTP server name or IPv4 address is specified by DHCP. The TFTP server includes the Profile_Rule parameter in the configuration file. • Entering a resync URL. The URL starts a web browser and requests a resync to a specific TFTP server by entering the URL syntax: http://*x.x.x.x*/admin/resync?*prvserv*/*device.cfg*, where: *x.x.x.x* is the IP address of the IP Telephony device, *prvserv* is the target TFTP server, and *device.cfg* is the name of the configuration file on the server. • Editing the Profile_Rule parameter by opening the provisioning pane on the web interface and entering the TFTP URL in the Profile_Rule parameter. For example, *prserv*/spa962.cfg. • Modifying the configuration file Profile_Rule and to contact a specific TFTP server and request a configuration file identified by the MAC-address. For example, this entry contacts a provisioning server, requesting a profile unique to the device with a MAC address identified by the `$MA` parameter: `Profile_Rule tftp.callme.com/profile/$MA/spa962.cfg;`

State	Description

SEC-PRV-1 Secure Provisioning—Initial Configuration	An initial, device-unique CFG file is targeted to a IP Telephony device by compiling the CFG file with the SPC --target option. This provides an encryption that does not require the exchange of keys.
	
	The initial, device-unique CFG file reconfigures the device profile to enable stronger encryption by programming a 256-bit encryption key and pointing to a randomly-generated TFTP directory. For example, the CFG file might contain:
	
	`Profile_Rule [--key $A] tftp.callme.com/profile/$B/spa962.cfg;`
	`GPP_A 8e4ca259…;  # 256 bit key`
	`GPP_B Gp3sqLn…;  # random CFG file path directory`

SEC-PRV-2 Secure Provisioning—Full Configuration	Profile resync operations subsequent to the initial SEC-PRV-1 provisioning retrieve the 256-bit encrypted CFG files that maintain the IP Telephony device in a state synchronized to the provisioning server. The profile parameters are reconfigured and maintained through this strongly encrypted profile. The encryption key and random directory location in the SEC-PRV-2 configuration can be changed periodically for extra security.

Configuration Access Control

The IP Telephony device firmware provides mechanisms for restricting end-user access to some parameters. The firmware provides specific privileges for login to an **Admin** account or a **User** account. Each can be independently password protected.:

- Admin Account—Allows the service provider full access to all administration web server parameters.
- User Account—Allows the user to configure a subset of the administration web server parameters.

The service provider can restrict the user account in the provisioning profile in the following ways:

- Indicate which configuration parameters are available to the User account when creating the configuration. (Described in the "Element Tags" section on page 2-2.)
- Disable user access to the administration web server.
- Disable user access for LCD GUI. (Described in the "Access Control for LCD GUI" section on page 2-4.)
- Disable the factory reset control by using the IVR.
- Restrict the Internet domains accessed by the device for resync, upgrades, or SIP registration for Line 1.

Communication Encryption

The configuration parameters communicated to the device can contain authorization codes or other information that protect the system from unauthorized access. It is in the service provider's interest to prevent unauthorized activity by the customer, and it is in the customer's interest to prevent the unauthorized use of the account. The service provider can encrypt the configuration profile communication between the provisioning server and the device, in addition to restricting access to the administration web server.