Deployment and Provisioning

- Provisioning Overview, page 1
- Phone Behavior During Times of Network Congestion, page 4
- Deployment, page 4
- Provisioning, page 6

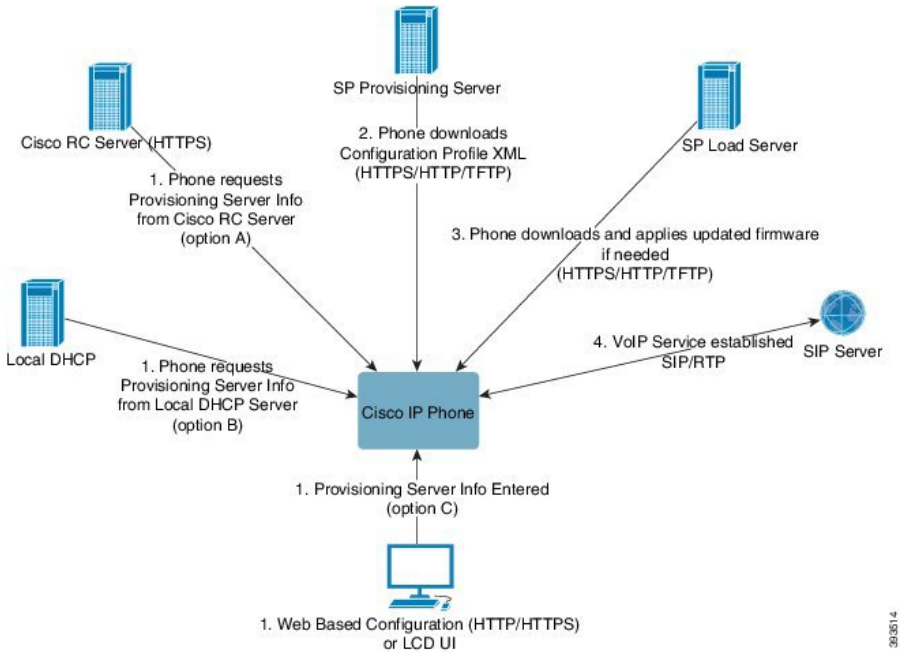
Provisioning Overview

Cisco IP Phones are intended for high-volume deployments by VoIP service providers to customers in home, business, or enterprise environments. Hence, provisioning the Cisco IP Phone via remote management and configuration ensures the proper operation of the phone at the customer site.

The following features support this customized, ongoing configuration:

- Reliable remote control of the Cisco IP Phone
- Encryption of the communication that controls the Cisco IP Phone
- Streamlined endpoint account binding

Phones can be provisioned to download configuration profiles or updated firmware from a remote server. Downloads can happen when the phones 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 common to service providers. Configuration profiles or updated firmware are transferred to the device using TFTP, HTTP, or HTTPS.



At a high level, the phone provisioning process is as follows:

1. If phone is not yet configured, provisioning server information is applied to phone via one of the following options:
    1. Downloaded from Cisco EDOS RC server via HTTPS.
    2. Queried from local DHCP server.
    3. Entered via Cisco phone web based configuration utility or Phone UI.
2. Phone downloads and applies configuration XML via HTTPS, HTTP, or TFTP using provisioning server information.
3. Phone downloads and applies updated firmware if needed via HTTPS, HTTP, or TFTP.
4. VOIP service establishing using specified configuration and firmware.

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

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

TR69 Provisioning

The Cisco IP phone allows the administrator to configure the TR69 parameters using the Web UI. For information related to the parameters, refer to the Administration Guide of the corresponding phone series.

The phones support ACS discovery from DHCP Option 43, 60, and 125.

Option 43: Vendor specific information - for ACS URL

Option 60: Vendor class identifier - The phone identifies itself with "dslforum.org" to ACS

Option 125: Vendor specific information - for gateway association

PRC Methods

RPC Methods Supported

The phones support only a limited set of RPC methods as follows:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: Download RPC method, the file types supported are:
    - Firmware Upgrade Image
    - Vendor Configuration File
    - Custom CA File
- Transfer Complete

Event Types Supported

The phones support event types based on features and methods supported. Only the following event types are supported:

- Bootstrap
- Boot
- value change
- connection request
- Periodic
- Transfer Complete

- M Download
- M Reboot

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect Cisco IP Phone voice and video quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan
- Attacks that occur on your network, such as a Denial of Service attack

Deployment

Cisco IP Phones provide convenient mechanisms for provisioning, based on these deployment models:

- Bulk distribution—The service provider acquires Cisco IP Phones in bulk quantity and either preprovisions them in-house or purchases Remote Customization (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 Cisco IP Phone 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

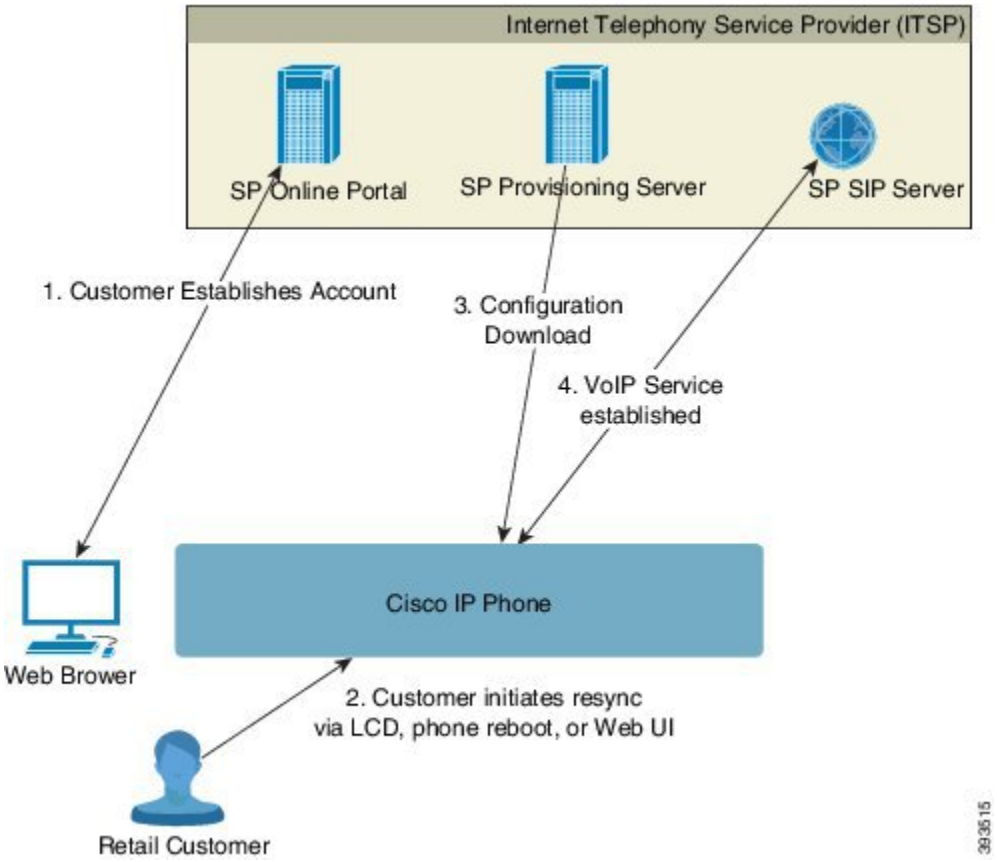
In this model, the service provider issues Cisco IP Phones to its customers as part of a VoIP service contract. The devices are either RC units or preprovisioned in-house.

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

A service provider can preprovision Cisco IP Phones 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
- A combination of in-house and remote provisioning

Retail Distribution



The Cisco IP 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 IP Phone 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.

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. The unprovisioned Cisco IP Phone is instructed to resync with a specific provisioning server through a resync URL command. The URL command typically includes an account Customer ID 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 Customer ID number of the new account. The remote provisioning server associates the phone that is performing the resync request with the new account, based on the URL and the

supplied Customer ID. Through this initial resync operation, the phone is configured in a single step. The phone 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. The provisioning server supplies correct configuration parameter values based on the associated service account.

When the device is powered up or a specified time elapses, the Cisco IP Phone resynchronizes and downloads 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.

Related Topics

In-House Device Preprovisioning

Resynchronization Process

The firmware for each Cisco IP Phone includes an administration web server that accepts new configuration parameter values. The Cisco IP Phone may be instructed to resynchronize configuration after reboot, or at scheduled intervals with a specified provisioning server through a resync URL command in the device profile.

By default, the web server is enabled. To disable/enable the Web server, use the resync URL command.

If needed, an immediate resynchronization may be requested via a “resync" action URL. The resync URL command may include an account Customer ID number or alphanumeric code to uniquely associate the device with the user’s account.

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 Customer ID number for the new account is 1234abcd. The remote provisioning server associates the Cisco IP Phone that is performing the resync request with the account, based on the URL and Customer ID.

Through this initial resync operation, the Cisco IP Phone is configured in a single step. The phone 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. The server supplies configuration parameter values based on the associated service account.

Provisioning

A Cisco IP Phone can be configured to resynchronize its internal configuration state to match a remote profile periodically and on power-up. The phone contacts a normal provisioning server (NPS) or an access control server (ACS).

By default, a profile resync is only attempted when the Cisco IP Phone is idle. This practice prevents an upgrade that would trigger a software reboot and interrupt a call. If intermediate upgrades are required to reach a current upgrade state from an older release, the upgrade logic can automate multistage upgrades.

Normal Provisioning Server

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

Although HTTPs is recommnded, 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. For more information about utilizing HTTPS, see Communication Encryption, on page 7. Secure first-time provisioning is provided through a mechanism that uses SSL functionality. An unprovisioned Cisco IP Phone can receive a 256-bit symmetric key encrypted profile that is targeted for that device.

Configuration Access Control

The Cisco IP Phone firmware provides mechanisms for restricting end-user access to some parameters. The firmware provides specific privileges for sign-in 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.
- Disable user access to the administration web server.
- Disable user access for LCD GUI.
- Restrict the Internet domains accessed by the device for resync, upgrades, or SIP registration for Line 1.

Related Topics

Element Tag Properties
Access Control

Communication Encryption

The configuration parameters that are 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 customer activity. 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.

Phone Provisioning Practices

Typically, the Cisco IP Phone is configured for provisioning when it first connects to the network. The phone is also provisioned at the scheduled intervals that are set when the service provider or the VAR preprovisions

(configures) the phone. Service providers can authorize VARs or advanced users to manually provision the phone by using the phone keypad. You can also configure provisioning using the Phone Web UI.

Check the **Status** > **Phone Status** > **Provisioning** from the Phone LCD UI, or Provisioning Status in the **Status** tab of the web-based Configuration Utility.

Related Topics

Manually Provision a Phone from the Keypad, on page 8

Manually Provision a Phone from the Keypad

Procedure

Step 1 Press **Settings**.

Step 2 Select **Device administration** > **Profile Rule**.

Step 3 Enter the profile rule using the following format:

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

For example:

```
tftp://192.168.1.5/CP_x8xx_MPP.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 4 Press **Resync**.

Related Topics

Phone Provisioning Practices, on page 7