Deployment and Provisioning

New and Changed Information

New and Changed for Firmware Release 11.2(4)

Revision	New and Changed Sections
Added parameters for Wi-Fi settings	XML Open Format Sample

New and Changed for Firmware Release 11.2(3)SR1

The following sections are new or updated to support the Cisco IP Phone 6800 Series Multiplatform Phones.

Revisions	New and Changed Sections
Added a new topic to introduce Activation Code Onboarding.	Onboard Your Phone with the Activation Code , on page 10

New and Changed for Firmware Release 11.2(3)

The following sections are new or updated to support the Cisco IP Phone 6800 Series Multiplatform Phones.

Revisions	New and Changed Sections
Added a concept topic for Open Profile Encryption.	Open Profile Encryption

Revisions	New and Changed Sections
Added a new topic to introduce RFC 8188-based HTTP content encryption.	RFC 8188-Based HTTP Content Encryption
Updated with details on RFC 8188-based encryption.	Configuration Profile Formats HTTP Provisioning
Updated the introductory details for open profile encryption.	AES-256-CBC Encryption
Updated the description of the **`--key`** option, and added a note about RFC 8188-based encryption.	key Configuration Profile Parameters
Updated the XML open format samples with new parameters and available options	XML Open Format Sample

New and Changed for Firmware Release 11.2(1)

Revisions	New or Changed Sections
Updated the topic with a reference to the comparison of the XML and TR69 parameters	TR69 Provisioning, on page 4
Added a new topic to support the privacy header feature	Set the Phone Privacy Header
Added a new topic to support peer firmware sharing	Peer Firmware Sharing, on page 11
Updated this topic with the encryption methods	Get a Signed Server Certificate
Updated this topic to support the feature of bypass **Set Password** screen	Configuration Access Control, on page 8
Added a new topic to support bypassing the **Set Password** screen	Bypass the Set Password Screen, on page 12

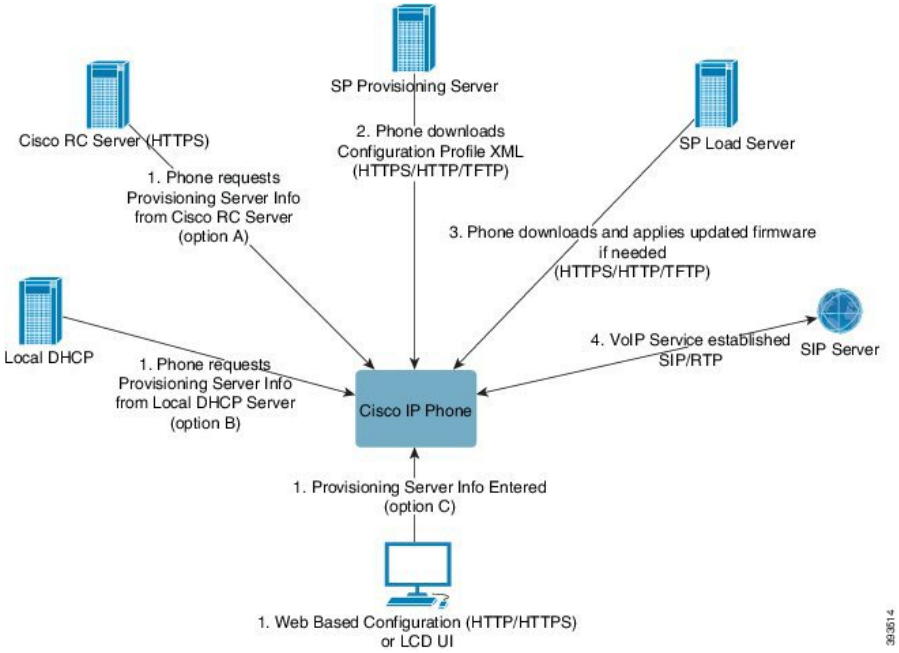
Provisioning Overview

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

Cisco supports the customized, ongoing feature configuration of the phone by using:

- Reliable remote control of the phone.
- Encryption of the communication that controls the phone.
- Streamlined phone 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 the high-volume, VoIP deployments common by service providers. Configuration profiles or updated firmware is transferred to the device using TFTP, HTTP, or HTTPS.



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

1. If the phone is not configured, the provisioning server information is applied to the phone using one of the following options:
    - **A**–Downloaded from the Cisco Enablement Data Orchestration System (EDOS) Remote Customization (RC) server using HTTPS.
    - **B**–Queried from a local DHCP server.
    - **C**–Entered manually using the Cisco phone web-based configuration utility or Phone UI.
2. The phone downloads the provisioning server information and applies the configuration XML using the HTTPS, HTTP, or TFTP protocol.
3. The phone downloads and applies the updated firmware, if needed, using HTTPS, HTTP, or TFTP.
4. The VoIP service is established using the specified configuration and firmware.

VoIP service providers intend to deploy many phones to residential and small business customers. In business or enterprise environments, phones can serve as terminal nodes. Providers widely distribute these devices across the Internet, which are connected through routers and firewalls at the customer premises.

The 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 phone at the customer premises.

TR69 Provisioning

The Cisco IP Phone helps the administrator to configure the TR69 parameters using the Web UI. For information related to the parameters, including a comparison of the XML and TR69 parameters, see the Administration Guide for the corresponding phone series.

The phones support Auto Configuration Server (ACS) discovery from DHCP Option 43, 60, and 125.

- Option 43–Vendor-specific information for the ACS URL.
- Option 60–Vendor class identifier, for the phone to identify itself with `dslforum.org` to the ACS.
- Option 125–Vendor-specific information for the gateway association.

RPC Methods

RPC Methods Supported

The phones support only a limited set of Remote Procedure Call (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 Certificate Authority (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

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 Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone voice 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 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.

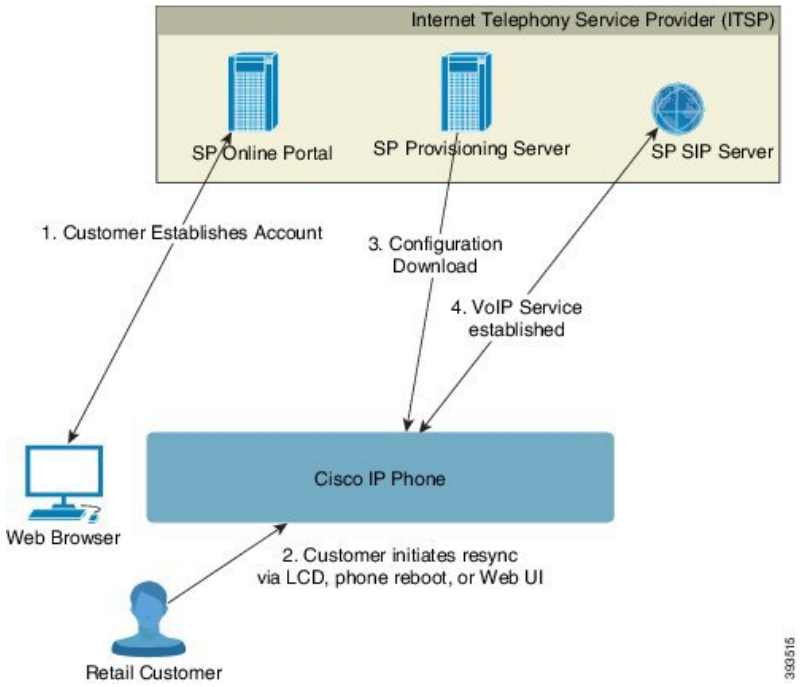
A service provider can preprovision phones with the desired parameters, including the parameters that control resynchronization, through various methods:

- In-house by using DHCP and TFTP
- Remotely by using TFTP, HTTP, or HTTPS
- A combination of in-house and remote provisioning

Retail Distribution

In a retail distribution model, a customer purchases a 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.

Figure 1: Retail Distribution



The 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.

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 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 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 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 phone includes an administration web server that accepts new configuration parameter values. The 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 or 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 phone that is performing the resync request with the account, based on the URL and 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 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 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 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 recommended, 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 5. Secure first-time provisioning is provided through a mechanism that uses SSL functionality. An unprovisioned phone can receive a 256-bit symmetric key encrypted profile that is targeted for that device.

Configuration Access Control

The 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 user interface.
- Bypass the **Set password** screen for the user.
- Restrict the Internet domains accessed by the device for resync, upgrades, or SIP registration for Line 1.

Related Topics

Element Tag Properties
Access Control

Access the Phone Web Page

If your service provider has disabled access to the configuration utility, contact the service provider before proceeding.

Procedure

Step 1 Ensure that the computer can communicate with the phone. No VPN in use.

Step 2 Start a web browser.

Step 3 Enter the IP address of the phone in your web browser address bar.

- User Access: **`http://<ip address>`**
- Admin Access: **`http://<ip address>/admin/advanced`**
- Admin Access: **`http://<ip address>`**, click **Admin Login** and click **advanced**

For example, `http://10.64.84.147/admin`

Step 4 Enter the password when prompted.

Allow Web Access to the Cisco IP Phone

To view the phone parameters, enable the configuration profile. To make changes to any of the parameters, you must be able to change the configuration profile. Your system administrator might have disabled the phone option to make the phone web user interface viewable or writable.

For more information, see the *Cisco IP Phone 6800 Series Multiplatform Phones Provisioning Guide*.

Before you begin

Access the phone administration web page. See Access the Phone Web Page, on page 8.

Procedure

Step 1 Click **Voice** > **System**.

Step 2 In the **System Configuration** section, set **Enable Web Server** to **Yes**.

Step 3 To update the configuration profile, click **Submit All Changes** after you modify the fields in the phone web user interface.

The phone reboots and the changes are applied.

Step 4 To clear all changes that you made during the current session (or after you last clicked **Submit All Changes**), click **Undo All Changes**. Values return to their previous settings.

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 10

Onboard Your Phone with the Activation Code

This feature is available in firmware release 11-2-3MSR1, BroadWorks Application Server Release 22.0 (patch AP.as.22.0.1123.ap368163 and its dependencies). However, you can change phones with older firmware to use this feature. You instruct the phone to upgrade to the new firmware and to use the `gds://` profile rule to trigger the activation code screen. A user enters a 16-digit code in the provided field to onboard the phone automatically.

Note The Cisco IP Phone 6861 Multiplatform Phones don't support the onboard activation code.

Before you begin

Ensure that you allow the activation.webex.com service through your firewall to support onboarding via activation code.

Procedure

Step 1 Edit the phone config.xml file in a text or XML editor.

Step 2 Follow the example below in your config.xml file to set the profile rule for Activation Code Onboarding.

```
<?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>
```

Step 3 Save the changes to the config.xml file.

Manually Provision a Phone from the Keypad

Procedure

Step 1 Press **Applications** .

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 9

Peer Firmware Sharing

Peer Firmware Sharing (PFS) is a firmware distribution model which allows a Cisco IP phone to find other phones of the same model or series on the subnet and share updated firmware files when you need to upgrade multiple phones all at the same time. PFS uses Cisco Peer-to-Peer-Distribution Protocol (CPPDP) which is a Cisco proprietary protocol. With CPPDP, all the devices in the subnet form a peer-to-peer hierarchy, and then copy the firmware or the other files from peer devices to the neighboring devices. To optimize firmware upgrades, a root phone downloads the firmware image from the load server and then transfers the firmware to other phones on the subnet using TCP connections.

Peer firmware sharing:

- Limits congestion on TFTP transfers to centralized remove load servers.
- Eliminates the need to manually control firmware upgrades.
- Reduces phone downtime during upgrades when large numbers of phones are reset simultaneously.

Note

- Peer firmware sharing does not function unless multiple phones are set to upgrade at the same time. When a NOTIFY is sent with Event:resync, it initiates a resync on the phone. Example of an xml that can contain the configurations to initiate the upgrade:

  "Event:resync;profile="http://10.77.10.141/profile.xml
- When you set the Peer Firmware Sharing Log server to an IP address and port, the PFS specific logs are sent to that server as UDP messages. This setting must be done on each phone. You can then use the log messages when troubleshooting issues related to PFS.

Peer_Firmware_Sharing_Log_Server specifies UDP Remote syslog server hostname and the port. The port defaults to the default syslog 514.

For example:

```
<Peer_Firmware_Sharing_Log_Server>192.168.5.5</ Peer_Firmware_Sharing_Log_Server>
```

To use this feature, enable PFS on the phones.

Bypass the Set Password Screen

You can bypass the phone **Set password** screen on the first boot or after a factory reset, based on these provisioning actions:

- DHCP configuration
- EDOS configuration
- User password configuration using in the phone XML configuration file.

Table 1: Provisioning Actions that Determine if Set Password Screen Displays

DHCP Configured	EDOS Configured	User Password Configured	Bypass Set Password Screen
Yes	n/a	Yes	Yes
Yes	n/a	No	**No**
No	Yes	Yes	Yes
No	Yes	No	**No**
No	No	n/a	**No**

Procedure

Step 1 Edit the phone `cfg.xml` file in a text or XML editor.

Step 2 Insert the **<User_Password>** tag using one of these options.

- **No password (start and end tag)**–**<User_Password></User_Password>**
- **Password value (4 to 127 characters)**–**<User_Password ua="rw">Abc123</User_Password>**
- **No password (start tag only)**–**<User_Password />**

Step 3 Save the changes to the `cfg.xml` file.

The **Set password** screen doesn't prompt up on the first boot or after a factory reset. If a password is specified, the user is prompted for entering the password when accessing the phone web page or to the phone screen menus.