



Provisioning

- [Provisioning Overview, on page 1](#)
- [Provisioning, on page 2](#)
- [TR69 Provisioning, on page 9](#)
- [Communication Encryption, on page 11](#)
- [Phone Behavior During Times of Network Congestion, on page 11](#)
- [In-House Preprovisioning and Provisioning Servers, on page 11](#)
- [Server Preparation and Software Tools, on page 11](#)
- [In-House Device Preprovisioning, on page 13](#)
- [Provisioning Server Setup, on page 14](#)

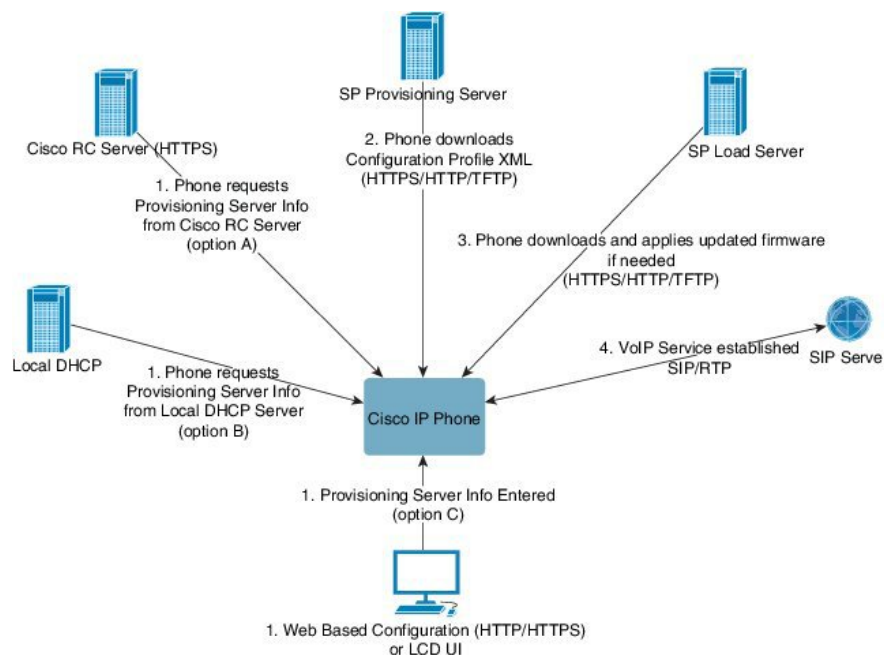
Provisioning Overview

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, DNS SRV, GDS (Activation code onboarding), EDOS device activation.
 - **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.

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 11](#). 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.

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.

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.

Before you begin

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

If you want to set up a proxy server for the onboarding, ensure that the proxy server is configured correctly. See [Set Up a Proxy Server](#).

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>
```

Note For the firmware release after the 11.2(3) SR1, the setting of `Firmware Upgrade` is optional.

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

Device Onboards with CDA Retry

To configure a phone for provisioning, a provisioning server information is applied to the phone using either DHCP options, DNS SRV, CDA device activation or Activation code onboarding. From firmware release 12.0(3), to simplify the device onboarding experience and to make it more resilient against failures, retry provisioning with CDA is introduced. During this process, the phone moves to the activation code screen or the phone shows an empty screen. Retry process continues in the backend but the user is not aware of it. This helps you remotely setup the phone if you have missed to add the phone MAC address to CDA service initially and you have added the MAC address later when the phone failed to get any configurations from CDA service first time. In firmware release 12.0(3), with retry mechanism, the phone will try CDA again with exponentially back-off timer. User can also optionally reboot the phone to have it retry CDA after the MAC address has been added on CDA service.

This provisioning occurs during following conditions:

- When the phone is taken out-of-box for the first time and has firmware version 12.0.3 or later pre-installed.
- When the phone undergoes factory reset while running firmware version 12.0.3 or later.

The user can see the following changes in the customization status when CDA retry happens:

- Customization status changed from **GDS-Pending** to **Pending**.
- Customization status changes to **Custom-Pending** to **Pending**.

If remote customization process enters into the final state and the Customization state is set to either **Aborted**, **Acquired**, or **GDS-Acquired**, CDA retry stops.



Note We recommend to keep the `Resync_Error_Retry_Delay` value unchanged during the out-of- box scenario. Also, the value must be always equals to or more than sixty seconds.


Phone Onboarding to Webex Cloud

Phone onboarding provides a simple and secure way to onboard Webex-aware phones to Webex cloud. You can achieve the onboarding process either with activation code onboarding (GDS) or with phone MAC address (EDOS device activation).

For more information on how to generate the activation code, see *Cisco BroadWorks Partner Configuration Guide, Cisco Multi-Platform Phones*.

For more information on Webex-aware phone onboarding, see *Webex for Cisco BroadWorks Solution Guide*.

Enable a Phone to Onboarding to Webex Cloud

After the successful registration of the phone to the Webex cloud, a cloud symbol  appears on the phone screen.

Before you begin

Access the phone administration web page. See [Access the Phone Web Interface](#).

Procedure

Step 1 Select **Voice > Phone**.

Step 2 In the **Webex** section, set the **Onboard Enable** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

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

Default value: Yes

Step 3 Click **Submit All Changes**.

Enable Auto Provisioning with Short Activation Code

Use the steps below to enable auto provisioning with a short activation code.

Before you begin

Ensure that your phones are updated with Firmware Release 11.3(1) or later.

If you want to set up a proxy server for the phone, ensure that the proxy server is configured correctly. See [Set Up a Proxy Server](#).

Review how to set up the CDA server for redirection profile:

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

Procedure


Step 1 Create a redirection profile name that contains a any number of digits between three and 16, inclusive. This becomes the activation code, later. Use one of these formats:

- **nnn**.
- **nnnnnnnnnnnnnnnnnnnn**
- Any number of digits between three and sixteen, inclusive. Example, **123456**

- Step 2** Provide the profile name that you created in step 1 to the Customer Device Activation (CDA) support team at cdap-support@cisco.com.
 - Step 3** Ask the CDA support team to enable your profile for discovery.
 - Step 4** When you get confirmation from the CDA support team, distribute the activation code to the users.
 - Step 5** Instruct users to press pound (#) before entering the digits at the activation screen.
-

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**.
-

DNS SRV for HTTP Provisioning

The DNS SRV for HTTP Provisioning feature enables auto provisioning of your multiplatform phone. Domain Name System Service (DNS SRV) records establish connections between a service and a hostname. When the phone looks for the location of the provisioning service, it first queries on the given DNS SRV domain name, then it queries for SRV records. The phone validates the records to confirm that the server is accessible. Then, it continues to the actual provisioning flow. Service providers can utilize this DNS SRV provisioning flow to provide auto provisioning.

DNS SRV bases the hostname validation on the certificate of the DHCP provided domain name. It is important that all SRV records use a valid certificate containing the DHCP provided domain name.

The DNS SRV query includes the DHCP domain name in its construction as follows:

```
_servicename._<transport>.<domainName>.
```

For example, `_ciscoprov-https._tls.example.com`, instructs the phone to do a lookup for example.com. The phone uses the hostname and port number that's retrieved by the DNS SRV query to build the URL that it uses to download the initial configuration.

DNS SRV is one of many auto provisioning mechanisms that the phone uses. The phone tries the mechanisms in the following order:

1. DHCP
2. DNS SRV
3. EDOS
4. GDS (Activation Code Onboarding), or EDOS Device Activation

The following table describes the SRV record fields.

Table 1: SRV Record Fields

Field	Description	Example
<_servicename.>	The service name begins with an underscore. Server services use symbolic names in SRV records. After the service, a period (.) signifies that the service is established and the next section is beginning.	_ciscoprov-https. Or _ciscoprov-http. DNS SRV doesn't support the TFTP protocol. If you use TFTP, you receive the following error message: Error - TFTP Scheme not supported in SRV lookups.
<_proto.>	The transport protocol begins with an underscore. The period that follows the protocol signals that the protocol section has ended.	_tls. You must use HTTPS with TLS. Or _tcp. You must use HTTP with TCP.
<domainName.>	The service domain name follows the protocol. Hostname validation: All SRV records are validated based on the original DHCP-provided domain name. It is important that all records use a valid certificate containing the original domain name.	example.com
TTL (Time to Live)	Expiration value of the record, in seconds.	86400
Class	Internet-type—Standard BIND notation indicating that it's an SRV record.	IN
<priority.>	Each line contains a priority number. The lower the number, the earlier the phone will attempt the target hostname and port included in this DNS SRV record.	10
<weight.>	If two or more services have the same priority, the weight number determines which line comes first. The lower the number, the earlier the phone will attempt the target hostname and port included in this DNS SRV record.	20
<port.>	optional port number	5060

Field	Description	Example
<target>	The A record of the machine providing the service. A Records are the most basic type of DNS record and are used to point a domain or subdomain to an IP address.	pr1.example.com

Example SRV Configurations

_service._proto.name. TTL class SRV priority weight port target.

_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.

Use DNS SRV for HTTP Provisioning

New phones use DNS SRV as one method of auto provisioning. For existing phones, if your network is set up for provisioning with DNS SRV for HTTP, you can use this feature to resync your phone. Sample configuration file:

```
<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>
```

Before you begin

If you want to set up a proxy server for the HTTP provisioning, ensure that the proxy server is configured correctly. See [Set Up a Proxy Server](#).

Procedure

Perform one of the following actions. Then, [Set the Profile Rule with the SRV Option on the Web Page, on page 8](#) or [Set the Profile Rule with the SRV Option on the Phone, on page 9](#)

- Place the XML configuration file, \$PSN.xml, in the web server root directory.
 - Place the XML configuration file, \$MA.cfg, in the web server root directory/Cisco/.
-

Set the Profile Rule with the SRV Option on the Web Page

You can use the SRV option to download a configuration file to your phone.

Before you begin

[Access the Phone Web Interface](#)


Procedure

- Step 1** Select **Voice > Provisioning**
- Step 2** In the **Profile Rule** field, enter the profile rule with the SRV option. Only HTTP and HTTPS are supported.
Example:
`[--srv] https://example.com/$PSN.xml`
-

Set the Profile Rule with the SRV Option on the Phone

You can use the SRV option on your phone to download a configuration file.

Procedure

- Step 1** Press **Applications** .
- Step 2** Select **Device administration > Profile rule**.
- Step 3** Enter the profile rule with the `[--srv]` parameter. Only HTTP and HTTPS are supported.
Example:
`[--srv] https://example.com/$PSN.xml`
- Step 4** Press **Resync**.
-

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.

TR69 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 audio 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.

In-House Preprovisioning and Provisioning Servers

The service provider preprovisions phones, other than RC units, with a profile. The preprovision profile can comprise a limited set of parameters that resynchronizes the phone. The profile can also comprise a complete set of parameters that the remote server delivers. By default, the phone resynchronizes on power-up and at intervals that are configured in the profile. When the user connects the phone at the customer premises, the device downloads the updated profile and any firmware updates.

This process of preprovisioning, deployment, and remote provisioning can be accomplished in many ways.

Server Preparation and Software Tools

The examples in this chapter require the availability of one or more servers. These servers can be installed and run on a local PC:

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

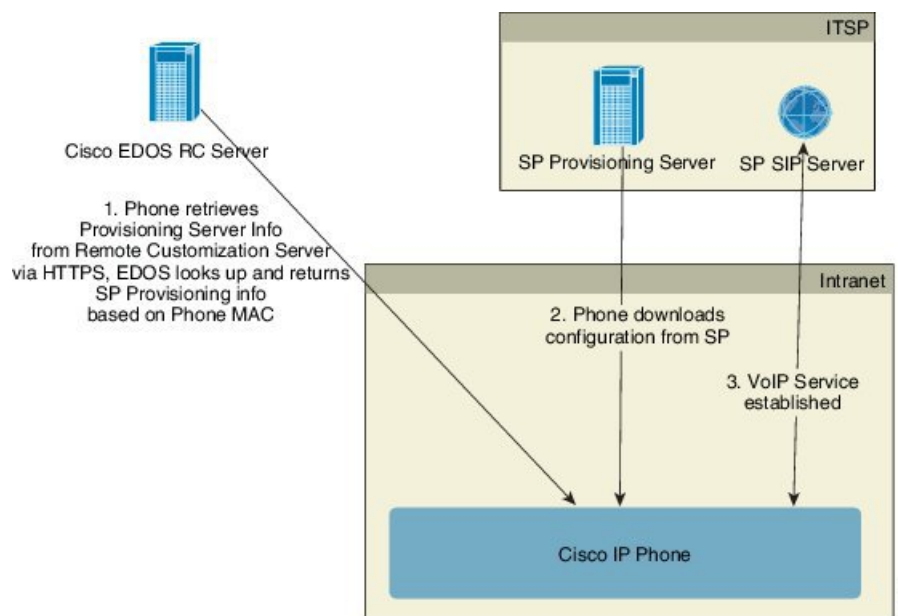
To troubleshoot server configuration, it is helpful to install clients for each type of server on a separate server machine. This practice establishes proper server operation, independent of the interaction with the phones.

We also recommend that you install these software tools:

- To generate configuration profiles, install the open source gzip compression utility.
- For profile encryption and HTTPS operations, install the open source OpenSSL software package.

- To test the dynamic profile generation and one-step remote provisioning using HTTPS, we recommend a scripting language with CGI scripting support. Open source Perl language tools is an example of such a scripting language.
- To verify secure exchanges between provisioning servers and the phones, install an Ethernet packet sniffer (such as the freely downloadable Ethereal/Wireshark). Capture an Ethernet packet trace of the interaction between the phone and the provisioning server. To do so, run the packet sniffer on a PC that is connected to a switch with port mirroring enabled. For HTTPS transactions, you can use the ssldump utility.

Remote Customization (RC) Distribution



All phones contact the Cisco EDOS RC server until they are provisioned initially.

In an RC distribution model, a customer purchases a phone that has already been associated with a specific Service Provider in the Cisco EDOS RC Server. The Internet Telephony Service Provider (ITSP) sets up and maintains a provisioning server, and registers their provisioning server information with the Cisco EDOS RC Server.

When the phone is powered on with an internet connection, the customization state for the unprovisioned phone is **Open**. The phone first queries the local DHCP server for provisioning server information and sets the customization state of the phone. If DHCP query is successful, Customization State is set to **Aborted** and RC is not attempted due to DHCP providing the needed provisioning server information.

When a phone connects to a network for the first time or after a factory reset, if there are no DHCP options setup, it contacts a device activation server for zero touch provisioning. New phones will use “activate.cisco.com” instead of “webapps.cisco.com” for provisioning. Phones with firmware release prior to 11.2(1), will continue to use webapps.cisco.com. Cisco recommends that you allow both the domain names through your firewall.

If DHCP server does not provide provisioning server information, the phone queries the Cisco EDOS RC Server and provides its MAC address and model and the Customization State is set to **Pending**. The Cisco EDOS server responds with the associated service provider's provisioning server information including

provisioning server URL and the phone's Customization State is set to **Custom Pending**. The phone then performs a resync URL command to retrieve the Service Provider's configuration and, if successful, the Customization State is set to **Acquired**.

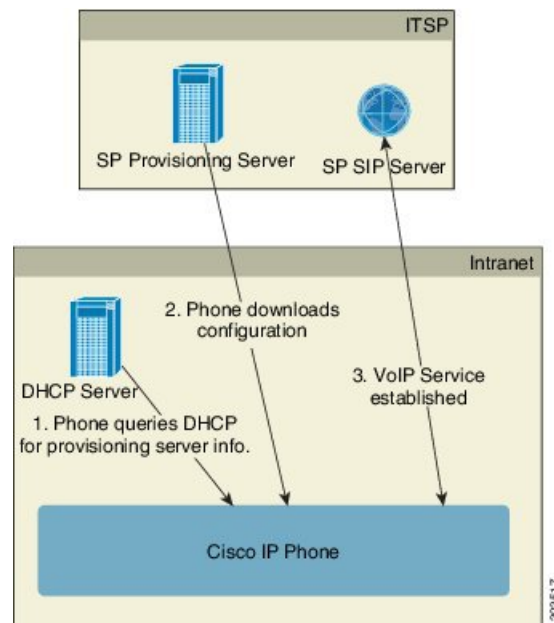
If the DHCP server provisioning fails, the phone queries the Cisco EDOS RC Server and provides its MAC address and model and the Customization State is set to **Pending**. The Cisco EDOS server responds with the associated service provider's provisioning server information including provisioning server URL and the phone's Customization State is set to **Custom Pending**. The phone then performs a resync URL command to retrieve the Service Provider's configuration and, if successful, the Customization State is set to **Acquired**. If queries either for local DHCP server or for EDOS server fails for provisioning, phone retries to onboard over DHCP and EDOS.

If the Cisco EDOS RC Server does not have a service provider associated with the phone, the customization state of the phone is set to **Unavailable**. The phone can be manually configured or an association added for the service provider of the phone to the Cisco EDOS Server.

If a phone is provisioned via either the LCD or Web Configuration Utility, prior to the Customization State becoming **Acquired**, the Customization State is set to **Aborted** and the Cisco EDOS Server will not be queried unless the phone is factory reset.

Once the phone has been provisioned, the Cisco EDOS RC Server is not utilized unless the phone is factory reset.

In-House Device Preprovisioning



With the Cisco factory default configuration, the phone automatically tries to resync to a profile on a TFTP server. A managed DHCP server on a LAN delivers the information about the profile and TFTP server that is configured for preprovisioning to the device. The service provider connects each new phone to the LAN. The phone automatically resyncs to the local TFTP server and initializes its internal state in preparation for deployment. This preprovisioning profile typically includes the URL of a remote provisioning server. The provisioning server keeps the device updated after the device is deployed and connected to the customer network.

The preprovisioned device bar code can be scanned to record its MAC address or serial number before the phone is shipped to the customer. This information can be used to create the profile to which the phone resynchronizes.

Upon receiving the phone, the customer connects it to the broadband link. On power-up, the phone contacts the provisioning server through the URL that is configured through preprovisioning. The phone can thus resync and update the profile and firmware, as necessary.

Provisioning Server Setup

This section describes setup requirements for provisioning a phone by using various servers and different scenarios. For the purposes of this document and for testing, provisioning servers are installed and run on a local PC. Also, generally available software tools are useful for provisioning the phones.

TFTP Provisioning

The phones support TFTP for both provisioning resync and firmware upgrade operations. When devices are deployed remotely, HTTPS is recommended, but HTTP and TFTP can also be used. This then requires provisioning file encryption to add security, as it offers greater reliability, given NAT and router protection mechanisms. TFTP is useful for the in-house preprovisioning of a large number of unprovisioned devices.

The phone is able to obtain a TFTP server IP address directly from the DHCP server through DHCP option 66. If a Profile_Rule is configured with the filepath of that TFTP server, the device downloads its profile from the TFTP server. The download occurs when the device is connected to a LAN and powered up.

The Profile_Rule provided with the factory default configuration is *&PN.cfg*, where *&PN* represents the phone model name.

For example, for a CP-7841-3PCC, the filename is CP-7841-3PCC.cfg. For a CP-7832-3PCC, the filename is CP-7832-3PCC.cfg.

For example, for a CP-8841-3PCC, the filename is CP-8841-3PCC.cfg.

For example, for a CP-6841-3PCC, the filename is CP-6841-3PCC.cfg.

For a device with the factory default profile, upon powering up, the device resyncs to this file on the local TFTP server that DHCP option 66 specifies. The filepath is relative to the TFTP server virtual root directory.

Remote Endpoint Control and NAT

The phone is compatible with network address translation (NAT) to access the Internet through a router. For enhanced security, the router might attempt to block unauthorized incoming packets by implementing symmetric NAT, a packet-filtering strategy that severely restricts the packets that are allowed to enter the protected network from the Internet. For this reason, remote provisioning by using TFTP is not recommended.

VoIP can coexist with NAT only when some form of NAT traversal is provided. Configure Simple Traversal of UDP through NAT (STUN). This option requires that the user have:

- A dynamic external (public) IP address from your service
- A computer that is running STUN server software
- An edge device with an asymmetric NAT mechanism

HTTP Provisioning

The phone behaves like a browser that requests web pages from a remote Internet site. This provides a reliable means of reaching the provisioning server, even when a customer router implements symmetric NAT or other protection mechanisms. HTTP and HTTPS work more reliably than TFTP in remote deployments, especially when the deployed units are connected behind residential firewalls or NAT-enabled routers. HTTP and HTTPS are used interchangeably in the following request type descriptions.

Basic HTTP-based provisioning relies on the HTTP GET method to retrieve configuration profiles. Typically, a configuration file is created for each deployed phone, and these files are stored within an HTTP server directory. When the server receives the GET request, it simply returns the file that is specified in the GET request header.

Rather than a static profile, the configuration profile can be generated dynamically by querying a customer database and producing the profile on-the-fly.

When the phone requests a resynch, it can use the HTTP POST method to request the resynch configuration data. The device can be configured to convey certain status and identification information to the server within the body of the HTTP POST request. The server uses this information to generate a desired response configuration profile, or to store the status information for later analysis and tracking.

As part of both GET and POST requests, the phone automatically includes basic identifying information in the User-Agent field of the request header. This information conveys the manufacturer, product name, current firmware version, and product serial number of the device.

The following example is the User-Agent request field from a CP-8841-3PCC:

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

The following example is the User-Agent request field from a CP-6841-3PCC:

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

User Agent is configurable, and the phone uses this the value if it has not be configured (still at default).

When the phone is configured to resynch to a configuration profile by using HTTP, it is recommended that HTTPS be used or the profile be encrypted to protect confidential information. Encrypted profiles that the phone downloads by using HTTP avoid the danger of exposing confidential information that is contained in the configuration profile. This resynch mode produces a lower computational load on the provisioning server when compared to using HTTPS.

The phone can decrypt profiles encrypted with one of these encryption methods:

- AES-256-CBC encryption
- RFC-8188 based encryption with AES-128-GCM ciphering



Note The phones support HTTP Version 1.0, HTTP Version 1.1, and Chunk Encoding when HTTP Version 1.1 is the negotiated transport protocol.

HTTP Status Code Handling on Resync and Upgrade

The phone supports HTTP response for remote provisioning (Resync). Current phone behavior is categorized in three ways:

- A—Success, where the “Resync Periodic” and “Resync Random Delay” values determine subsequent requests.
- B—Failure when File Not Found or corrupt profile. The “Resync Error Retry Delay” value determines subsequent requests.
- C—Other failure when a bad URL or IP address causes a connection error. The “Resync Error Retry Delay” value determines subsequent requests.

Table 2: Phone Behavior for HTTP Responses

HTTP Status Code	Description	Phone Behavior
301 Moved Permanently	This and future requests should be directed to a new location.	Retry request immediately with new location.
302 Found	Known as Temporarily Moved.	Retry request immediately with new location.
3xx	Other 3xx responses not processed.	C
400 Bad Request	The request cannot be fulfilled due to bad syntax.	C
401 Unauthorized	Basic or digest access authentication challenge.	Immediately retry request with authentication credentials. Maximum 2 retries. Upon failure, the phone behavior is C.
403 Forbidden	Server refuses to respond.	C
404 Not Found	Requested resource not found. Subsequent requests by client are permissible.	B
407 Proxy Authentication Required	Basic or digest access authentication challenge.	Immediately retry request with authentication credentials. Maximum two retries. Upon failure, the phone behavior is C.
4xx	Other client error status codes are not processed.	C
500 Internal Server Error	Generic error message.	Phone behavior is C.
501 Not Implemented	The server does not recognize the request method, or it lacks the ability to fulfill the request.	Phone behavior is C.

HTTP Status Code	Description	Phone Behavior
502 Bad Gateway	The server is acting as a gateway or proxy and receives an invalid response from the upstream server.	Phone behavior is C.
503 Service Unavailable	The server is currently unavailable (overloaded or down for maintenance). This is a temporary state.	Phone behavior is C.
504 Gateway Timeout	The server behaves as a gateway or proxy and does not receive timely response from the upstream server.	C
5xx	Other server error	C

