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 Cisco IP phones accept configuration profiles in XML format, or in a proprietary binary format generated by the SIP Profile Compiler (SPC) available from Cisco. The Cisco IP phones support 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 Small Business IP Telephony Devices Provisioning Guide*.

This chapter describes:

Additional information is available in:

- *Cisco SPA3xx, SPA50xG, and SPA525G SPC Templates for Configuration Files*, available on the Cisco Support Community at:

  https://supportforums.cisco.com/docs/DOC-10008
- Cisco SPA9000 Administration Guide

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 IP phone continues to process A-records until the first server responds. If no server associated with the A-records responds, the Cisco IP phone logs an error to the syslog server.

Retail Provisioning

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 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 IP phone 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 Cisco IP 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 Cisco IP 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 IP phone supports a more convenient mechanism for in-house preprovisioning. With the factory default configuration, a Cisco IP 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 IP phone 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.

Using HTTPS

The Cisco IP phone provides a reliable and secure provisioning strategy based on HTTPS requests from the Cisco IP 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 Cisco IP phones, you must generate a Certificate Signing Request (CSR) and submit it to Cisco. The Cisco IP phone generates a certificate for installation on the provisioning server that is accepted by Cisco IP phones when they seek to establish an HTTPS connection with the provisioning server.

The Cisco IP phone implements up to 256-bit symmetric encryption, using the American Encryption Standard (AES), in addition to 128-bit RC4. The Cisco IP 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 Cisco IP phone, an attacker might attempt to contact a provisioning server using a standard web browser, or other HTTPS client, to obtain the Cisco IP phone configuration profile from the provisioning server. To prevent this kind of attack, each Cisco IP phone also 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.

Obtaining 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 SPA 9000 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 Provisioning a Phone from the Keypad

Typically Cisco SPA IP phones are 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 Cisco SPA IP phones 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:

Cisco SPA303 and Cisco SPA5XXG

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/spa504.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.

Cisco WIP310

Step 1 Press **Select** to choose Settings and press **Select** again.

Step 2 Navigate to Misc Settings.

Step 3 Navigate to profile rule. Enter the profile rule in the following format:

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

For example, to have the Cisco WIP310 provisioning done by a Cisco SPA9000, enter:

```
192.168.2.64/cfg/generic.xml
```

Step 4 Press the **Resync** softkey.

Cisco SPA525G or Cisco SPA525G2

Step 1 Press the **Setup** button.

Step 2 Navigate to Device Administration and press **Select**.

Step 3 Scroll to Profile Rule and press **Select**.

Step 4 Enter the profile rule by using the following format.

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

For example:

```
tftp://192.168.1.5/spa525.cfg
```

Step 5 Press the **Resync** softkey.

Sample Configuration File

Following is a sample configuration file:

```
Set_Local_Date_(mm/dd) "" ;
Set_Local_Time_(HH/mm) "" ;
Time_Zone "GMT-07:00" ; # options:
GMT-12:00/GMT-11:00/GMT-10:00/GMT-09:00/GMT-08:00/GMT-07:00/GMT-06:00/GMT-05:00/GMT-04:00/
GMT-03:30/GMT-03:00/GMT-02:00/GMT-01:00/GMT/GMT+01:00/GMT+02:00/GMT+03:00/GMT+03:30/GMT+04
:00/GMT+05:00/GMT+05:30/GMT+05:45/GMT+06:00/GMT+06:30/GMT+07:00/GMT+08:00/GMT+09:00/GMT+09
:30/GMT+10:00/GMT+11:00/GMT+12:00/GMT+13:00
FXS_Port_Impedance "600" ; # options:
600/900/600+2.16uF/900+2.16uF/270+750||150nF/220+820||120nF/220+820||115nF/370+620||310nF
FXS_Port_Input_Gain "-3" ;
FXS_Port_Output_Gain "-3" ;
```

```
DTMF_Playback_Level "-16" ;
DTMF_Playback_Length ".1" ;
Detect_ABCD "Yes" ;
Playback_ABCD "Yes" ;
Caller_ID_Method "Bellcore(N.Amer,China)" ; # options:
Bellcore(N.Amer,China)/DTMF(Finland,Sweden)/DTMF(Denmark)/ETSI DTMF/ETSI DTMF With PR/ETSI
DTMF After Ring/ETSI FSK/ETSI FSK With PR(UK)
FXS_Port_Power_Limit "3" ; # options: 1/2/3/4/5/6/7/8
Protect_IVR_FactoryReset “No” ;
```

Updating Profiles and Firmware

Cisco IP phones support secure remote provisioning (configuration) and firmware upgrades. An unprovisioned Cisco IP 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 Small Business IP Telephony Devices 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**.

Parameter	Description
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.
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. If this parameter is provisioned, the Resync Periodic parameter is ignored.
Resync Periodic	Time in seconds between periodic resynchs. 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 From SIP	Controls requests for resync operations by using a SIP NOTIFY event sent from the service provider proxy server to the device. When set to **yes**, the proxy can request a resync by sending a SIP NOTIFY message containing the `Event: resync` header to the device.
Resync After Upgrade Attempt	Resync is triggered on the phone when: • “Resync On Reset" is Yes. • "Resync After Upgrade Attempt" is Yes. • The phone attempts to upgrade firmware (causes the phone to reboot.) If “Resync After Upgrade Attempt" is set to No, resync will not be triggered when upgrade is attempted.
Resync Trigger 1 Resync Trigger 2	A conditional expression (that undergoes macro expansion). If the condition in one of these triggers evaluates to true, a resync operation is initiated as though the periodic resync timer had expired.
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.

Parameter	Description
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.
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 Resync Request Msg	The message sent to the syslog server at the start of a resync attempt. The default value is: `$PN $MAC –Requesting resync $SCHEME://$SERVIP:$PORT$PATH`
Log Resync Success Msg	The syslog message issued upon successful completion of a resync attempt. The default value is: `$PN $MAC –Successful resync $SCHEME://$SERVIP:$PORT$PATH -- $ERR.`
Log Resync Failure Msg	The syslog message that is issued after a failed resync attempt. The default value is: `$PN $MAC - Resyncfailed: $ERR.`
Report Rule	The device provides a mechanism for reporting its current internal configuration to the provisioning server. The URL in this field specifies the destination for a report and can include an encryption key.
HTTP Report Method	The HTTP method used when the server invokes the phone to send a configuration file report using the HTTP protocol. Choose **post** or **put**.
User Configurable Resync	Allows a user resynch the phone from the IP phone screen.

Parameter	Description

Report Rule	The IP phone provides a mechanism for reporting its current internal configuration to the provisioning server. The URL in this field specifies the destination for a report and can include an encryption key.
	Beginning with firmware version 7.5.2b, the IP phone has the capability to do a delta configuration report and a status report. The phone reports the status data if the [--status] keyword is defined.
	Both the status report rule and configuration report rule can be configured in the parameter <Report_Rule>. These two report rules should be separated with a semi-colon.
	If the [--status] keyword or the status report file path is missing, the phone will not report the status data.
	For example, if the following is configured:
	`http://my_http_server/config-525.xml`
	the phone will report the configuration data to *http://my_http_server/config-525.xml*.
	If the following is configured:
	`[--status]http://my_http_server/status-525.xml`
	the phone will report the status data to *http://my_http_server/config-525.xml*.
	If the following is configured:
	`[--delta]http://my_http_server/config-525.xml;`
	`[--status]http://my_http_server/status-525.xml`
	the phone will report the delta configuration data to *http://my_http_server/config-525.xml* and the status data to *http://my_http_server/status-525.xml*.

User Configurable Resync	Allows a user resynch the phone from the IP 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.
Downgrade Rev Limit	Enforces a lower limit on the acceptable firmware version number during an upgrade or downgrade. The device does not complete a firmware upgrade operation unless the firmware version is greater than or equal to this parameter. For example: `7.4.8` The default is (empty).
Upgrade Rule	A firmware upgrade script that defines upgrade conditions and associated firmware URLs. It uses the same syntax as Profile Rule. (See Manually Provisioning a Phone from the Keypad for the Upgrade Rule syntax.) The default is (empty).
Log Upgrade Request Msg	Syslog message issued at the start of a firmware upgrade attempt. The default is `$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH`
Log Upgrade Success Msg	Syslog message issued after a firmware upgrade attempt completes successfully. The default is `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
Log Upgrade Failure Msg	Syslog message issued after a failed firmware upgrade attempt. The default is `$PN $MAC -- Upgrade failed: $ERR.`
License Keys	This field is not used.

Launch a Firmware Update by Using 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 update the phone firmware, enter this command:

http://*phone-ip-address*/**admin/upgrade?***protocol*://*server-name*[:*port*]]/*firmware-path*

- `protocol` defaults to TFTP.
- `server-name` defaults to the host requesting the URL.
- `port` defaults to:
  - 69 for TFTP

  - 80 for HTTP
  - 443 for HTTPS
- firmware-path defaults to /spa.bin (The firmware-pathname typically includes the file name of the binary located in a directory on the TFTP or HTTP server. For example, `http://192.168.2.217/admin/upgrade?tftp://192.168.2.251/spa.bin`) for SPA phones, and `/wip310.img` for the Cisco WIP310.)

Launch a Profile Update by using a Browser Command

Cisco SPA IP phones can synchronize to specific profiles stored on a remote server. The phone resyncs only when it is idle. The update is attempted automatically after the call is complete.

To update the phone profile, enter this command:

`http://`*`phone-ip-addr`*`/admin/resync?`*`protocol`*`://`*`server-name[:port]/profile-pathname`*

- `phone-ip-addr` is the IP address of the phone.
- Parameter following `resync?` defaults to the Profile Rule setting on the web server Provisioning page.
- `protocol` defaults to TFTP.
- `server-name` defaults to the host requesting the URL.
- `port` defaults to:
  - 69 for TFTP
  - 80 for HTTP
  - 443 for HTTPS
- `profile-pathname` defaults to the path for the new synchronization profile (for example, `http://192.168.2.217admin/resync?tftp://192.168.2.251/spaconf.cfg`).

Rebooting a Phone by using a Browser Command

You can remotely reboot a Cisco IP phone by entering a command in a web browser URL field.

To reboot a phone, enter the following command:

`http://`*`phone-ip-address`*`/`**`admin`**`/`**`reboot`**

- `phone-ip-addr` is the IP address of the phone.

Configuring 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 Small Business IP Telephony Devices Provisioning Guide* for more information

The SPA IP phones support a set of pre-loaded 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

General Purpose Parameters

The general purpose parameters GPP_* are used as free string registers when configuring the Cisco IP phones 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**.

Using TR-069

TR-069 (Technical Report 069) provides Service Providers with a common platform to manage all voice devices and other customer-premises equipment (CPE) in large-scale deployments, no matter neither the device type nor the manufacturer.

As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. The protocol allows the automatic configuration of Internet access devices, such as modems, routers, gateways, set-top box, and VoIP-phones. The technical specifications are managed and published by the Broadband Forum.

Cisco IP phones can be managed by using the protocols and standards defined in TR-069. The ACS enables bulk configuration changes and firmware updates for CPEs (IP phones). TR-069 inter operates with any ACS that will inter operate with a MOTIVE client.

To configure the TR-069 client, navigate to **Admin Login > advanced > Voice > TR-069**:

Field	Description
Enable TR-069	From the drop-down menu, select **yes** to enable TR-069. or **no** to disable TR-069.
ACS URL	Enter the URL of the ACS using the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when using SSL or TLS.
ACS Username	Enter the username that authenticates the CPE to the ACS by using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Enter the password grants access to the ACS for this user. This password is used only for HTTP-based authentication of the CPE.
ACS URL In Use	Displays the ACS URL.
Connection Request URL	Displays the ACS making the connection request to the CPE.
Connection Request Username	Enter the username that authenticates the ACS making the connection request to the CPE.
Connection Request Password	Enter the password used to authenticate the ACS making a connection request to the CPE.
Periodic Inform Interval	The duration in seconds of the interval between CPE attempts to connect to the ACS when Periodic Inform Enable is set to **yes**.
Periodic Inform Enable	From the drop-down menu, select **yes** to enable CPE connection requests. Enter **no** to disable connection requests.
TR-069 Traceability	From the drop-down menu, select **yes** to enable TR-069 transaction traceability. Enter **no** to disable traceability.
CWMP V1.2 Support	From the drop-down menu, select **yes** to enable CPE WAN Management Protocol (CWMP) support. Enter **no** to disable CWMP support such that the device does not send any Inform messages to the ACS or accept any connection requests from the ACS.
TR-069 VoiceObject Init	From the drop-down menu, select **yes** to initialize all voice objects to factory default values. Enter **no** to retain the current values.
TR-069 DHCP Option Init	From the drop-down menu, select **yes** to initialize the DHCP settings from the ACS. Enter **no** to leave the settings unchanged.
TR-069 IGD Support	From the drop-down menu, select **yes** to enable TR-069 on the Internet Gateway Device (IGD). Enter **no** to disable traceability. (This is used for debugging purposes.)
TR-069 Fallback Support	From the drop-down menu, select **yes** to enable TR-069 fallback support. Enter **no** to disable fallback support. If the SPA phone first attempt to discover the ACS by using DHCP, it attempts to use DNS to resolve ACS IP address.

Field	Description
TR-069 DHCP Inform Timer	Enter the interval in seconds that the phone should poll the DHCP server.
BACKUP ACS URL	Enter the backup URL of the ACS using the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when using SSL or TLS.
BACKUP ACS User	Enter the backup username that authenticates the CPE to the ACS by using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
BACKUP ACS Password	Enter the backup password grants access to the ACS for the backup user. This password is used only for HTTP-based authentication of the CPE.