Deployment and Provisioning

Deployment and Provisioning Overview

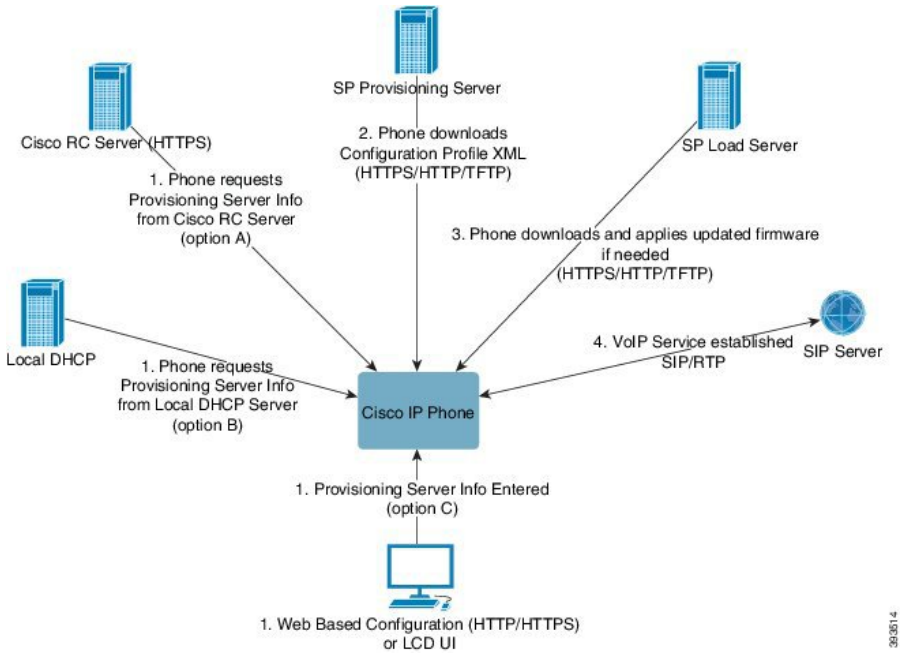
Cisco ATA 191 and 192 Analog Telephone Adapters (ATA) are intended for high-volume deployments by VoIP service providers to residential and small business customers. In business or enterprise environments, these ATAs can serve as terminal nodes. These devices are widely distributed across the Internet, connected through routers and firewalls at the customer premises.

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

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

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

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:

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

In this document, the terms *phone* and *device* mean the ATA.

Deployment

These ATAs provide convenient mechanisms for provisioning, based on two deployment models:

- Bulk distribution—The service provider acquires these ATAs in bulk quantity and either preprovisions them in-house or purchases RC units from Cisco. The devices are then issued to the customers as part of a VoIP service contract.
- Retail distribution—The customer purchases the ATA 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

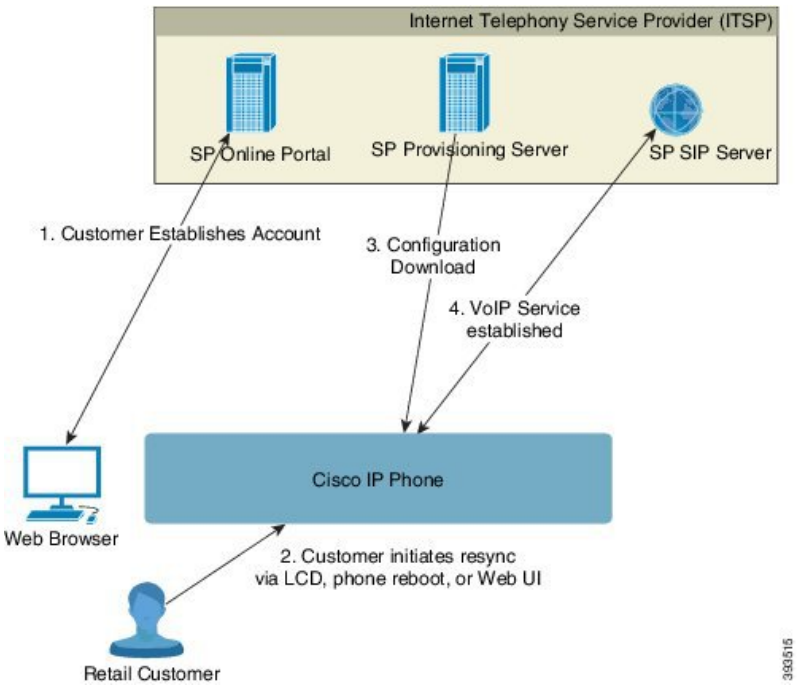
Related Topics

Remote Customization (RC) Distribution

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 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.

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/ata.cfg
```

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.

Example

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

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 7. 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.

TR-069

The digital subscriber line (DSL) Forum TR-069, CPE WAN Management Protocol (CWMP), is used for communications between a customer premise equipment (CPE) device and an autoconfiguration server (ACS). The TR-069 Agent manages a collection of CPE devices, with the primary capability for auto-configuration and dynamic service provisioning, software image management, status and performance monitoring, and diagnostics.

It supports multiple scenarios, including:

- Device administration—Authenticates administrators, authorizes commands, and provides an audit trail
- Remote Access—Works with VPN and other remote network access devices to enforce access policies
- Network admission control—Communicates with posture and audit servers to enforce admission control policies

The TR-069 Agent CPE devices must be set up and enabled for TR-069. An ACS used to communicate with the CPE must be TR-069 compliant in order to enable the TR-069 Agent.

Provisioning States

The provisioning process involves these provisioning states.

State	Description
MFG-RESET Manufacturing Reset	The device returns to a fully unprovisioned state; all configurable parameters regain their default values. Manufacturing reset can be performed in these ways: • Through the IVR sequence ******73738#1#**. • Press the reset button on the ATA. • Use the web interface to reset the ATA to factory default settings. On phones that do not support IVR, press the reset button or LCD factory reset entry to reset it to the default values. Allowing the end user to perform a manufacturing reset guarantees that the device can always be returned to an accessible state.

State	Description

SP-CUST Service Provider Customization	The Profile_Rule parameter points to a device-specific configuration profile by using a provisioning server that is specific to the service provider. The methods for initiating resynchronization are:
	• Autoconfiguration with a local DHCP server. A TFTP server name or IPv4 address is specified by DHCP. The TFTP server includes the Profile_Rule parameter in the configuration file.
	• Enter a resync URL. The URL starts a web browser and requests a resync to a specific TFTP server by entering the URL syntax: **`http://x.x.x.x/admin/resync?tftp://prvserv/device.cfg`**, where:
	  • **`x.x.x.x`** is the IP address of the IP Telephony device,
	  • **`prvserv`** is the target TFTP server,
	  • **`device.cfg`** is the name of the configuration file on the server.
	• Edit the Profile_Rule parameter by opening the provisioning pane on the web interface and entering the TFTP URL in the Profile_Rule parameter. For example, **`tftp://prserv/spa112.cfg`**.
	• Modify the configuration file Profile_Rule and to contact a specific TFTP server and request a configuration file identified by the MAC-address. For example, this entry contacts a provisioning server, requesting a profile unique to the device with a MAC address identified by the $MA parameter:
	`Profile_Rule tftp.callme.com/profile/$MA/spa112.cfg;`

SEC-PRV-1 Secure Provisioning—Initial Configuration	An initial, device-unique CFG file is targeted to a IP Telephony device by compiling the CFG file with the SPC --target option. This provides an encryption that does not require the exchange of keys.
	The initial, device-unique CFG file reconfigures the device profile to enable stronger encryption by programming a 256-bit encryption key and pointing to a randomly generated TFTP directory. For example, the CFG file might contain:
	`Profile_Rule [--key $A] tftp.callme.com/profile/$B/spa112.cfg;`
	`GPP_A 8e4ca259…; # 256 bit key`
	`GPP_B Gp3sqLn…; # random CFG file path directory`

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

Configuration Access Control

The 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.
- 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.

Additional Information

Related Documentation

Use the following sections to obtain related information.

Cisco ATA 190 Series Documentation

Refer to publications that are specific to your language and call control system. Navigate from the following documentation URL:

https://www.cisco.com/c/en/us/products/unified-communications/ata-190-series-analog-telephone-adapters/index.html

Cisco ATA 190 Series Firmware Support Policy

For information on the support policy for ATAs, see http://www.cisco.com/c/en/us/support/docs/collaboration-endpoints/unified-ip-phone-7900-series/116684-technote-ipphone-00.html.

Phone Behavior During Times of Network Congestion

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.