AVAYA

Avaya Configuration Cradle

Avaya 3600 Series Wireless Telephones Administrator Guide

Notice
All efforts were made to ensure that the information in this book was complete and accurate at the time of printing. However, information is subject to change.

Avaya Web Page
The world wide web home page for Avaya is: http://www.avaya.com

Preventing Toll Fraud
Toll Fraud is the unauthorized use of your telecommunications system by an unauthorized party. For example, a person who is not a corporate employee, agent, subcontractor, or working on your company's behalf. Be aware that there is a risk of toll fraud associated with your system. If toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention
If you s*uspect that you are being victimized* by toll fraud and you need technical assistance or support, call the Technical Service Center's Toll Fraud Intervention Hotline at 1.800.643.2353.

Providing Telecommunications Security
Telecommunications security of voice, data, and/or video communications is the prevention of any type of intrusion to, that is, either unauthorized or malicious access to or use of, your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or a person working on your company's behalf. Whereas, a "malicious party" is Anyone, including someone who may be otherwise authorized, who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there could be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company, including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Your Responsibility for Your Company's Telecommunications Security
The final responsibility for securing both this system and its networked equipment rests with you – an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure your:

- Avaya provided telecommunications systems and their interfaces
- Avaya provided software applications, as well as their underlying hardware/ software platforms and interfaces
- Any other equipment networked to your Avaya products

Federal Communications Commission Statement
Part 15: Class A Statement. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instructions, could cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Industry Canada (IC) Interference Information
This digital apparatus does not exceed the Class A limits for radio noise emissions set out in the radio interference regulations of Industry Canada.

Le Présent Appareil Nomérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A préscrites dans le reglement sur le brouillage radioélectrique édicté par le Industrie Canada.

European Union Declaration of Conformity
The "CE" mark affixed to the equipment means that it conforms to the referenced European Union (EU) Directives listed below:

EMC Directive   89/336/EEC

Low-Voltage Directive   73/23/EEC

For more information on standards compliance, contact your local distributor.

Note concerning shielded cable:

Avaya recommends the use of Sshielded cable is recommended for all external signal connections in order to maintain FCC Part 15 emissions requirements.

Note concerning the Avaya wireless telephones:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

WARNING Changes or modifications to this equipment not approved by Avaya may cause this equipment to not comply with part 15 of the FCC rules and void the user's authority to operate this equipment.

WARNING Avaya products contain no user-serviceable parts inside. Refer servicing to qualified service personnel.

Important Safety Information

Follow these general precautions while installing telephone equipment:

- Never install telephone wiring during a lightning storm.

- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.

- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

- Use caution when installing or modifying telephone lines.

Table of Contents

1. About This Document

This document explains how to set up the Avaya Configuration Cradle, create configuration plans for the Avaya e340/h340/i640 WTs and how to download configuration plans to the handset. It also covers maintaining the software and troubleshooting error messages.

1.1 Questions?

1.2 Icons and conventions

This manual uses the following icons and conventions.

 Caution! Follow these instructions carefully to avoid danger.

 Note these instructions carefully.

NORM This typeface indicates a key, label, or button on the NL Configuration Cradle or WT.

1.3 Notes

- Only use the original OEM plug-in power adapter.

- Do not immerse the Configuration Cradle in water or other liquid. Do not pour liquids into the slots.

- Do not place anything in the Configuration Cradle other than theAvaya 3616, Avaya 3626, or Avaya 3620 WT. You might damage the contacts. Bent contacts can keep the Configuration Cradle from working properly.

- The Configuration Cradle operates in a 50° to 85° F (10° to 30° C) environment. Do not expose it to freezing temperatures or direct sunlight.

 Remove the battery before placing the phone in the configuration cradle.

2. Avaya Configuration Cradle Overview

The Avaya Configuration Cradle is a two-slot cradle designed to automate the process of configuring the 3616, 3620and 3626models of Avaya WT. The front slot of the cradle is for the Avaya 3616/3620 WT; the rear slot is for the Avaya 3626WT. Only one handset may be configured at a time.

The Configuration Cradle is connected to a PC via a serial cable. The Configuration Cradle program runs on the PC and enables the system administrator to establish and store configuration options for System, Group and User levels. The Configuration Cradle program can be downloaded from the following website: http://www.spectralink.com/service/software.php

Configuration plans may be set up in the program and downloaded into a WT or a configured WT may be placed in the cradle and its configuration may be uploaded and edited or saved.

3. Installing the Avaya Configuration Cradle

Set up the Configuration Cradle by first obtaining the appropriate OEM power supply for your country or region. Place the Configuration Cradle on a flat, horizontal surface and plug the power supply into the Configuration Cradle and into an appropriate wall outlet. Plug a straight serial cable into the Configuration Cradle and into an available serial port on the PC.

> The serial cable must be plugged directly into the serial port on the PC. Please do not use port replicators or adaptors, as these do not properly handle the necessary communication requirements between the Configuration Cradle and the PC.

Set up a folder for WT configuration on the PC and download the programming software from http://www.spectralink.com/service/software.php into this folder. Run the PhoneConfig.exe file.

Note that there is no installer or uninstaller since the program does not modify your system or registry. It runs from its current location and stores its settings locally.

Serial port settings are handled automatically by the Configuration Cradle software. If necessary, the COM port the Cradle is using can be set in the **Settings** menu.

4. Planning the Configuration Files

Each configurable option may be categorized as one of three types: System (**Sys**), Group (**Grp**) or User (**Usr**). System level options should be those that are stable across the entire system. DHCP vs. Static IP addressing would be an example of a System option. Options that are designated as Group type should be those that change by category of user. PTT Allow/Disallow and PTT Channel are examples. A unique extension number is assigned to each handset by the system administrator and would be a User type. The remaining User types should be reserved for options that are normally set by the end user. For Standby menu options such as Ring Type and Noise Mode, default values may be entered with the expectation that the user may change them.

4.1 Typical configuration plans

Because the specific options that are available depend on the software version and License Option, the typical plan options for your facility may be different than those listed here.

Typical System file settings:
System file settings typically do not change across an installation. These are typical **Sys** categories:
* License Option
* Network Config
* IP Addressing
* ESSID
* Security
* IP Office Flag

Typical Group file settings:
If certain groups of people require different access to functions, such as PTT, these options would be stored as Group files. Several different Group files can be established and the handsets can be configured by group. Typical **Grp** categories are:
* Push-to-talk options on both Admin and Standby menus

Typical User file settings:
If a setting can be changed by the user in the Standby menu, then it would typically be stored in a User file. These can be the default settings or whatever your system requires. Typical **Usr** categories are:
* Extension
* Static IP address
* Ring Options
* Phone Options

> You may have zones in your facility that require different System settings, such as security or ESSID. These settings can be moved to a Group file or you may set up two System files.

5.   Configuration Cradle Window

When first opened, the **PhoneConfig** program displays the toolbar and a list of
configurable options. All **Editable settings** fields are blank or are set to default values.
Phone settings are unavailable until a handset is read or settings are copied to the
Phone settings fields.

5.1   Initial window
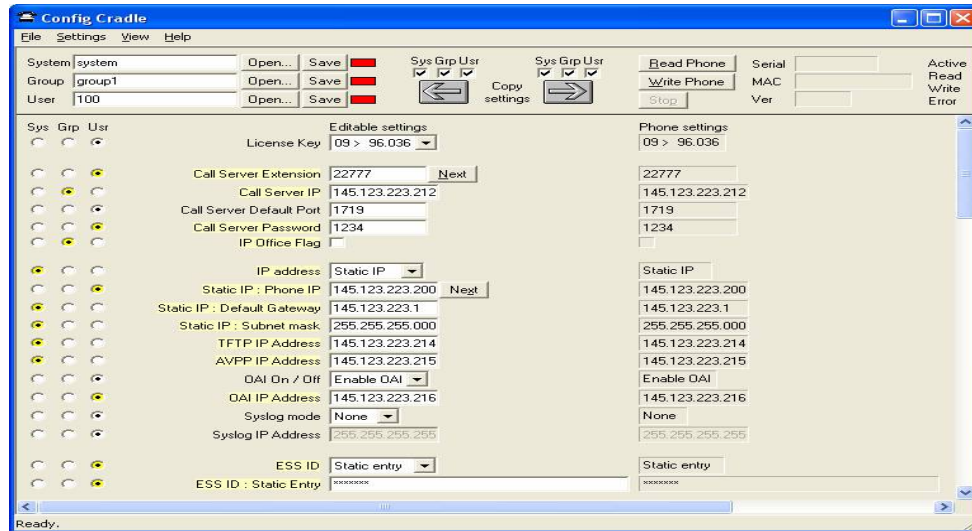
This is the window that appears when the Config Cradle program is first opened.
The default filenames appear and all category buttons on the left default to **Usr**.

5.2   Configuration Cradle toolbar

The Config Cradle toolbar allows you to name, open, and save configuration files
and download and upload configuration settings to and from the handset in the
Cradle.

The three filename windows allow you to open and save settings by **System**, **Group** or
User type as separate files. The filenames shown above are the default names, but any
filename can be assigned by entering it into the field and clicking the **Save** button. By
default, the files will be saved in a new folder named **ConfigData** under the folder
where the program is stored. The new folder will be created automatically the first
time a file is saved. To open an existing file, click the **Open** button and browse to the
file. Use the **File** menu to customize the file structure, if desired.

The three flags beside the **Save** buttons have four colors to indicate the status of the
file displayed in the window:
- Red: file does not exist. The filename in the window has not been created.
- Yellow: file not loaded. The filename in the window exists in the ConfigData
  folder but has not been loaded into the **Editable settings**.
- Green: unsaved edits. When changes are made in the **Editable settings** field(s) the
  green flag indicates these have not been saved.

- Gray: file up to date. The settings have been saved.

The **Copy settings** arrows and boxes allow you to copy settings to the handset side of the window where they may then be written to the handset in the Cradle. Or the configuration in a handset may be copied to the **Editable settings** area and edited or saved. The **Sys Grp Usr** checkboxes allow you to copy just the settings you require.

When clicked, the **Read Phone** and **Write Phone** buttons initiate the transfer of configuration data from or to the handset in the Cradle. The **Stop** button will halt the transfer.

The **Serial, MAC, and Ver** windows display the serial number, MAC address, and firmware version of the handset in the Cradle. This information is not stored (I'm not sure whether the firmware version is stored in the Config file).

The four labeled flags on the right indicate the status of the configuration transfer:

- **Active**: green when attempting communication with handset in Cradle. Turns yellow if a timeout occurs (may be due to an improperly seated handset). The software will repeatedly re-attempt communication after a timeout so re-seating the handset should correct the problem.
- **Read**: green when information is currently being read from the handset in the Cradle.
- **Write**: yellow when information is currently being written to the handset in the Cradle.
- **Error**: red when an error has occurred. An error message will appear on the status bar at the bottom of the main window.

6. Creating Your Configuration Plan

When first setting up a configuration plan you will enter information into the **Editable settings** fields, indicate which of the three categories each option belongs to, and save as **System**, **Group** or **User** files.

Do not create a plan that saves an option in two different categories. Option categories should be established and should not overlap. Example: PTT settings are typically tagged as **Grp** options and saved in **Group** files.

Once you have established which options will be categorized as System, Group or User, enter the configuration information into the **Editable settings** fields. Start with the System options and enter all system-level field values. Click the **Sys** category button on the left side of the window for each option. Save these settings as a System file by entering the filename in the **System** filename field and clicking **Save**.

Note that when a setting is changed, it is highlighted in yellow until it is saved.

In the same way, create each Group plan by entering the values in the fields designated as Group types. Click the **Grp** category button on the left side of the window for each option. Save each plan under a different name in the **Group** filename field.

Create one basic **User** file for default (or desired) values for each **User** field. Click the **Usr** category button on the left side of the window for each option.

User settings don't necessarily need to be saved for each handset, but they can be saved, if desired. It may be useful, for example, to save a user's ring preferences from a handset being replaced so that the new handset can be configured up the same way. If you determine that each handset configuration should be saved, it is easiest to do this during the configuration process. See *Downloading a configuration plan to a handset* below.

6.1   Sample configuration window

Shown below is a typical Static IP configuration using the WEP security method. All PTT settings are saved as a group. The settings in the **Editable settings** field were first uploaded from a configured handset and then copied from **Phone settings**.
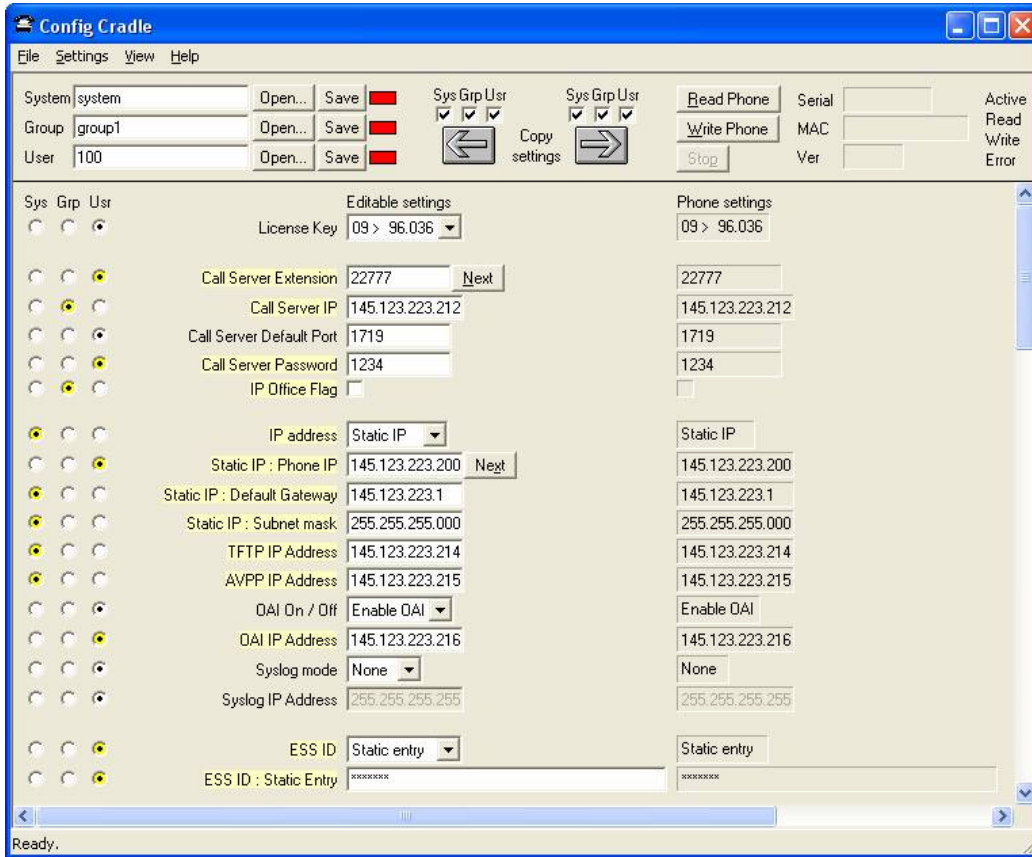
6.2   Configuration planning worksheet

Plan category_____ Filename_____

Sys	Grp	Usr	Label	Editable Setting

7. Downloading and Uploading Configuration Plans

Once your configuration plans are established, the settings are easily downloaded into the handsets.

7.1 Downloading a configuration plan to a handset

1. Place an Avaya WT <u>with the Battery Pack removed</u> into the appropriate slot. Add the pencil by this entry to highlight this.

2. Use the toolbar to open the **System**, **Group** and **User** plans for this handset.

3. Enter information unique to the handset – Extension and IP address (if using static IP). Note that these two fields have a **Next** button that is useful for setting these fields when configuring a quantity of handsets.

4. Copy the settings to the **Phone settings** fields.

5. Click **Write Phone** to begin the download.

6. You may save the settings unique to this handset by ensuring the correct extension number or other filename is entered in the **User** filename field and then clicking **Save**. You may also load files or edit settings for the next handset (steps 2 and 3) during the download.

7. When the **Active** flag turns off, the download has finished and the handset may be removed from the Cradle.

7.2 Uploading a configuration plan from a handset

1. Place an Avaya WT <u>with the Battery Pack removed</u> into the appropriate slot. Add the pencil by this entry to highlight this.

2. Click the **Read Phone** button to begin the upload.

3. When the **Active** flag turns off, the handset's settings will appear in the **Phone settings** fields.

4. You may copy these settings over to the **Editable settings** fields to use them to create configuration plans as described above or to save them by user or extension.

8. Software Maintenance

The Avaya Configuration Cradle uses proprietary software programs written and maintained by SpectraLink Corporation. The software version can be displayed via the **Help** menu.

Download the latest Avaya Configuration Cradle software from: http://www.spectralink.com/service/software.php.

The software is delivered in a zip. Install the update by extracting the zip and overwriting the existing PhoneConfig.exe and other files.

Please follow customary backup procedures to preserve file integrity.