Avaya Terminal Configuration Release 2.0

Administration

555-250-103
Issue 5
January 2004

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

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 is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

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 is not 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 may 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).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer 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
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices operate within the following parameters:

- Maximum power output: -5 dBm to -8 dBm
- Center Wavelength: 1310 nm to 1360 nm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

Federal Communications Commission Statement

Part 15:

Note: 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 instruction manual, may 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.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer’s Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer’s Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier’s Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC’s Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using “Avaya” as manufacturer.

European Union Declarations of Conformity

Avaya Inc. declares that the equipment specified in this document bearing the “CE” (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Table of Contents

Preface

Welcome to Avaya™ Terminal Configuration, an application that runs on Avaya Directory Enabled Management (DEM) and enables users to customize the settings for their telephone from their web browser. This chapter provides an introduction to the structure and assumptions of this guide.

The Purpose of this Guide

This guide describes how to manage and maintain Avaya Terminal Configuration. Before you can perform the procedures in this guide, the DEM software must be installed and configured.

Who Should Use this Guide

This guide is intended for users who are responsible for managing and maintaining Avaya Terminal Configuration. It is assumed that the user is experienced with the following subjects:

- One of the following operating systems
  - Microsoft® Windows® 2000 Server
  - Microsoft Windows 2000 Professional
  - Microsoft Windows XP Professional
- One of the following LDAP services:
  - IBM® Directory Server (IDS) 5.1
  - Microsoft Active Directory™
  - Netscape® Directory Server Version 4.12
  - Novell® NDS® eDirectory™ 8.5
  - Sun™ ONE Directory Server 5.1
- local area networks (LANs)

- voice server administration
- Avaya DEM

Professional services are available through your authorized Avaya dealer to support these requirements.

Organization of this Guide

This guide consists of the following chapters:

- **Preface -** This chapter describes the intended audience for this document and how to get support when managing Avaya Terminal Configuration.
- **Chapter 1: Introduction -** This chapter provides a brief introduction to DEM.
- **Chapter 2: Managing Avaya Terminal Configuration-** This chapter describes how to manage and maintain Avaya Terminal Configuration.

Related Documentation/Training

The following user documentation and training materials are available for installing and administering DEM:

- **Avaya Directory Enabled Management Online Training Course**

  This online training course is available at *http://www.avaya.com/support*.

- **Avaya Directory Enabled Management Installation and Implementation**

  This Portable Document Format (PDF) document is located in the Docs folder of the DEM installation directory. To view this document, you will need Adobe Acrobat® Reader 6.0 or later. You can install Adobe Acrobat Reader 6.0 from the Avaya Integrated Management Release 2.0 CD or download it from the Internet at *http://www.adobe.com/*.

Conventions Used

The following conventions are used in this document:

- Commands and text you should enter appear ***in this style of type***.
- Components of dialog boxes (such as boxes and buttons) and prompts that appear on the screen appear **in this style of type**.
- The terms *option buttons* and *radio buttons* refer to the same object.

Getting Help

For the most up-to-date troubleshooting information, go to *http://www.avaya.com/support*.

If you have questions about or problems with Avaya Terminal Configuration that this guide does not resolve, call Avaya technical support at 1800-242-2121 (USA only) or your local authorized Avaya dealer.

1 Introduction

This chapter describes Avaya Terminal Configuration.

Overview of Avaya Terminal Configuration

Avaya Terminal Configuration is software that runs on Avaya Directory Enabled Management (DEM), enabling users to customize the settings for their telephone from their web browser. Using Avaya Terminal Configuration, users can:

- program feature buttons
- program softkeys
- change the labels displayed for their feature buttons
- set their display name, which is the name the Avaya server displays on the other party's telephone when you make a call
- set the personalized ring pattern
- enable/disable the Audible Message Waiting feature
- set whether they want their telephone to automatically select the last call appearance they used when they lift their handset or activate their speakerphone
- print out the button labels for their telephone

User Requirements

To use Avaya Terminal Configuration, a user must have:

- an account on the Avaya voice system (that is, an extension on the Avaya server)
- an account in the Directory server for DEM
- an extension that is administered for one of the supported telephones
- Microsoft® Internet Explorer 5.5 or 6.0
- Sun® Java Runtime Environment (JRE) 1.4.2

Telephones Supported

To use Avaya Terminal Configuration, a user must have one of the following telephones administered for their extension:

- 2420
- 2420 with Expansion Module
- 4606
- 4612
- 4620
- 4620 with Expansion Module
- 4624
- 4630
- 4630 with Expansion Module
- 6408D+
- 6416D+
- 6416D+ with Expansion Module
- 6424D+
- 6424D+ with Expansion Module
- 8410D

Telephone Features Supported

Table 1 shows the features that users can program with Avaya Terminal Configuration.

Table 1. Supported Telephone Features

Abbreviated Dial - Prog (abr-prog)	Call Park (call-park)	Leave Word Calling - Store (lwc-store)
Abbreviated Dial - Special Function (abr-spchar)	Call Timer (call-timer)	Message Retrieval (msg-retr)
Abbreviated Dial - Mark Special Function (abr-spchar~m)	Caller Information (callr-info)	Message Waiting Activation (mwn-act)
Abbreviated Dial - Pause Special Function (abr-spchar~p)	Call Forward Busy/Don't Answer (cfwd-bsyda)	Message Waiting Deactivation (mwn-deact)
Abbreviated Dial - Suppress Special Function (abr-spchar~s)	Conference Display (Conf-dsp)	Next (next)
Abbreviated Dial - Wait Special Function (abr-spchar~w)	Consult (consult)	Normal Mode (normal)
Abbreviated Dial - Indefinite Wait Special Function (abr-spchar~W)	Date and Time (date-time)	Personal CO Line (per-COline)
Abbreviated Dial Number (abrv-dial)	Directory (directory)	Priority Call (priority)
Abbreviated and Delayed Ringing (abrv-ring)	Directed Call Pickup (dir-pkup)	Ringer Cutoff (ringer-off)
Admin (admin)	Drop (Drop)	Send All Calls (send-calls)
ANI Request (ani-requst)	Exclusion (exclusion)	Stored Number Display (stored-num)
Automatic Call Back (auto-cback)	Go To Coverage (goto-cover)	Timer (timer)
Automatic Dialing (autodial)	Headset (headset)	Verify (verify)
Button View (btn-view)	Inspect (inspect)	Whisper Page Activation (whisp-act)
Busy Indication (busy-ind)	Internal Auto Answer (int-aut-an)	Whisper Page Answerback (whisp-anbk)
Call Appearance (call-appr)	Last Number Dialed (last-numb)	Whisper Page Off (whisp-off)
Call Displayed Number (call-disp)	Leave Word Calling - Cancel (lwc-cancel)	Toggle Swap for Conference and Transfer (Togle-swap)
Call Forward (call-fwd)	Leave Word Calling - Lock (lwc-lock)	

As the Avaya Terminal Configuration Administrator, you specify on a system-wide basis which of these features users can program from Avaya Terminal Configuration. For more information, see "Setting the Available Features" on page 17.

2 Managing Avaya Terminal Configuration

This chapter provides the following information:

- how to configure an extension that exists on multiple voice systems
- how to specify which features users can program from Avaya Terminal Configuration
- how to specify whether users can change their display name
- how to disable access to Avaya Terminal Configuration
- how to change the password for an Avaya Terminal Configuration account
- how to reset the password for an Avaya Terminal Configuration account
- how to configure the default font settings for the button labels of all Avaya Terminal Configuration users
- how to set the list of web page links that are displayed in the Links menu of Avaya Terminal Configuration

Configuring Extensions Appearing on Multiple Voice Systems

Using the file “coyote.properties,” you can specify whether all users that have the same extensions on multiple voice systems are permitted to select the voice system they want to access from a drop-down list box in the Avaya Terminal Configuration Login window.

* **Note:** This procedure only applies to extensions that appear on multiple voice systems.

To configure how Avaya Terminal Configuration handles extensions that appear on multiple voice systems:

1. Open a text editing application (such as WordPad).
2. From the text editing application, open the file “coyote.properties.” This file is located in the Properties folder in the Terminal Configuration folder of the DEM installation directory (for example, Program Files\Avaya\DEM\Terminal Configuration\Properties).

   The file “coyote.properties” appears.
3. Perform one of the following steps:

   — To enable users with the same extension on multiple voice systems to select the voice system they want to access from a drop-down list box in the Avaya Terminal Configuration Login window:

     1 Set **ShowSelector=y**.
     2 Go to Step 4.

   — To prevent users with the same extension on multiple voice systems from selecting the voice system they want to access in the Avaya Terminal Configuration Login window:

     1 Set **ShowSelector=n**.
     2 Go to Step 4.
4. Save your changes and then exit the file.

Setting the Available Features

Using the file "ATCConfig.xml," you specify which features users can program from Avaya Terminal Configuration. Users can access only the features contained in this file.

The file "features.xml" contains the entire list of features Avaya Terminal Configuration supports. This file is provided for reference purposes only.
You must NOT change the information in the file "features.xml."

To specify the features for Avaya Terminal Configuration:

1. Open a text editing application (such as WordPad).
2. From the text editing application, open the file "ATCConfig.xml." This file is located in the Terminal Configuration folder of the DEM installation directory (for example, Program Files\Avaya\DEM\Terminal Configuration).

   The file "ATCConfig.xml" appears.
3. Delete the features you do not want users to access.
4. When you are finished, save your changes and then exit the file.

Enabling the Display Name Feature

Using the file “ATCConfig.xml,” you specify whether users are permitted to change their display name from Avaya Terminal Configuration.

To set whether users can change their display name:

1. Open a text editing application (such as WordPad).
2. From the text editing application, open the file “ATCConfig.xml.” This file is located in the Terminal Configuration folder of the DEM installation directory (for example, Program Files\Avaya\DEM\Terminal Configuration).

   The file “ATCConfig.xml” appears.
3. Perform one of the following steps:
   - To allow users to change their display name, set **change=“y”** in the third line. “y” indicates that the users can change their display name.
   - To prevent users from changing their display name, set **change=“n”** in the third line. “n” indicates that the users cannot change their display name.
4. Save your changes and then exit the file.

Disabling Avaya Terminal Configuration

Using the file “coyote.properties,” you can disable all users from accessing Avaya Terminal Configuration.

To disable/enable access to Avaya Terminal Configuration:

1. Open a text editing application (such as WordPad).
2. From the text editing application, open the file “coyote.properties.” This file is located in the Properties folder in the Terminal Configuration folder of the DEM installation directory (for example, Program Files\Avaya\DEM\Terminal Configuration\Properties).

   The file “coyote.properties” appears.
3. Perform one of the following steps:
   - To enable users to access Avaya Terminal Configuration, set **Disable=n** in the second line. “n” indicates that the users can access Avaya Terminal Configuration.
   - To prevent users from accessing Avaya Terminal Configuration, set **Disable=y** in the second line. “y” indicates that the users cannot access Avaya Terminal Configuration.
4. Save your changes and then exit the file.

Changing User Passwords

Each user must have an ID (which is the user’s 10-digit telephone number on the Avaya voice system) and a password to access Avaya Terminal Configuration. The default password for every Avaya Terminal Configuration account is the user’s extension in reverse. For example, if your telephone number is **74322**, your default password would be **22347**.

The password for each user is stored in the “gwUserSecurityCode” attribute in the Gateway Users object class of DEM. The LDAP user ID and password (encrypted) are stored in LdapUser key and LdapPassword key in the file “coyote.properties.” Users can change their passwords from the Avaya Terminal Configuration Login window. To reset a user’s password to its default (that is, the user’s extension in reverse), see “Resetting User Passwords” on page 20.

Resetting User Passwords

Avaya Terminal Configuration provides a stand-alone java application that enables you to reset the password of an Avaya Terminal Configuration user. When a password is reset, the password becomes the user's ID (that is, extension) in reverse. For example, if a user's extension is **74322**, that person's password will become **22347** after you reset the password.

The Reset Password application is in a jar resetPwd.jar that is located in the main folder of Avaya Terminal Configuration. Only a signed (trusted) resetPwd.jar will work.

* **Note:** To run the Reset Password application, you must have JDK 1.4 and JRE 1.4.2 installed.

To reset a user's password:

1. In your web browser, enter the URL of the web server (for example, **http://198.152.127.224:8080/TerminalConfig/ResetPassword.html**).

   The Login window appears.

2. Enter the complete Directory server login (for example, **cn=Directory Manager**).
3. Enter the password.
4. Click the **OK** button.

   The Reset Password window appears if the Directory Context is established. Using this window, you can reset the password for five users at a time.

5. Enter the extension and Voice System name for the user whose password you want to reset.
6. Repeat Step 5 for any other users.
7. Click the **Reset** button.

   The password for each user specified is reset. The Status window shows the log of whether the reset password operation for each extension was successful.

8. When you are finished, click the **Exit** button.

Configuring the Default Font Settings

Using the file "coyote.properties," you can configure the following default font settings for the button labels of all Avaya Terminal Configuration users:

- font name
- font size
- vertical alignment (that is, top, bottom, or center)
- horizontal alignment (that is, top, bottom, or center)

To configure the default font settings:

1. Open a text editing application (such as WordPad).
2. From the text editing application, open the file "coyote.properties." This file is located in the Properties folder in the Terminal Configuration folder of the DEM installation directory (for example, Program Files\Avaya\DEM\Terminal Configuration\Properties).

   The file "coyote.properties" appears.
3. In the section "#setting of default font name, size & alignments," perform any of the following steps:
   - — To set the default font name, set **Default.font.name=n**, where "n" is the font name you want to use. For example, if you want to use Arial as the default font, you would set **Default.font.name=Arial**.
   - — To set the default font size, set **Default.font.size=n**, where "n" is the font size you want to use. For example, if you want to use 12 point as the default size, you would set **Default.font.size=12**.
   - — To set the default vertical alignment, set **Default.font.v_align=n**, where "n" is the vertical alignment you want to use. Your choices are CENTER, TOP, and BOTTOM. For example, if you want to use CENTER as the default vertical alignment, you would set **Default.font.v_align=CENTER**.

- — To set the default horizontal alignment, set **Default.font.h_align=n**, where “n” is the horizontal alignment you want to use. Your choices are CENTER, TOP, and BOTTOM. For example, if you want to use CENTER as the default horizontal alignment, you would set **Default.font.h_align=CENTER**.

4. Save your changes and then exit the file.

Setting the Web Page Links

Using the file “coyote.properties,” you can set the list of web page links that are displayed in the Links menu of Avaya Terminal Configuration.

To set the web page links:

1. Open a text editing application (such as WordPad).
2. From the text editing application, open the file “coyote.properties.” This file is located in the Properties folder in the Terminal Configuration folder of the DEM installation directory (for example, Program Files\Avaya\DEM\Terminal Configuration\Properties).

   The file “coyote.properties” appears.
3. In the section “#Corporate Link entries,” type **corporate.link.n=http://x**, where:
   - — “n” is the label you want displayed in the Links menu for the web page link you want to access.
   - — “x” is the web page link that will be accessed.

   For example, if you want to create a web page link to access the Avaya website, you would enter **corporate.link.Avaya=http://www.avaya.com**. In this example, the Links menu would contains an entry “Avaya.” If you selected this entry from the Links menu, a browser window would open, and your browser would access and display the Avaya website.
4. Repeat Step 3 for each web page link you want to add.
5. Save your changes and then exit the file.

Index