Avaya™ Terminal Configuration

Release 1.2
Administration

555-250-103
Issue 3
November 2002

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.

Avaya, DEFINITY, MultiVantage, and VisAbility are registered trademarks and trademarks of Avaya Inc.

ALL OTHER TRADEMARKS MENTIONED IN THIS DOCUMENT ARE PROPERTY OF THEIR RESPECTIVE OWNERS.

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 Web site: http://www.avaya.com/support/
If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional 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.

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.410.568.3680
FAX 1.800.457.1764 or 1.410.891.0207
Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management
E-mail: totalware@gwsmail.com

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 NT® Server 4.0 with Service Pack 4 or later
  - Microsoft Windows® Server 2000
- One of the following LDAP services:
  - Novell® NDS® eDirectory™ 8.5
  - Netscape® Directory Server Version 4.12
  - Microsoft Active Directory™
- 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 5.0 or later. You can install Adobe Acrobat Reader 5.0 from the Avaya VisAbility™ Management Suite 1.0 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
- one of the following web browsers:
  - Microsoft® Internet Explorer 5.5
  - Netscape® 6.2

Telephones Supported

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

- 4606
- 4612
- 4624
- 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 7.

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

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 Avaya Terminal Configuration. If you prevent these users from selecting the voice system, you must specify which voice system will be displayed when the users log into Avaya Terminal Configuration.

*** 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 Avaya Terminal Configuration:

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

   — To set which voice system will be displayed when users with the same extension on multiple voice systems log into Avaya Terminal Configuration:

   1 Set **ShowSelector=n**.
   2 Set **SwitchPreference=*system1*,*system2*,*system3*,*system4*** where ***system*** is the name of a voice system. The order in which the voice systems are listed indicates the order in which Avaya Terminal Configuration will search voice systems for the extension entered.

   For example, suppose you are using three voice systems identified as Alps, Rockies, and Urals. When a user logs into Avaya Terminal Configuration, you want Avaya Terminal Configuration to search for that extension on Rockies first. If a match is found, the extension on Rockies is displayed and the process is complete. If no match is found on Rockies, you want Avaya Terminal Configuration to search Alps. If a match is found, the extension on Alps is displayed and the process is complete. If no match is found, you want Avaya Terminal Configuration to search Urals. For this to occur, you would enter **SwitchPreference=Rockies,Alps,Urals**.

   If you set **ShowSelector=n** and do not specify any systems for **SwitchPreference** (that is, you leave **SwitchPreference** blank), users will be given the option to select the voice system they want to access.
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 10.

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 1.3 or later 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.

Index