Avaya Directory Enabled Management Release 3.0

Installation and Implementation

555-038-101
Issue 9
April 2005

Copyright 2005, Avaya Inc.
All Rights Reserved

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

CE

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 Directory Enabled Management (DEM). This chapter provides an introduction to the structure and assumptions of this guide.

The Purpose of this Guide

This guide describes how to install and configure Avaya Directory Enabled Management (DEM) Release 3.0.

*** Note:** Avaya Directory Enabled Management Release 3.0 must be already installed before performing the procedures in this guide.

Who Should Use this Guide

This guide is intended for technicians who are installing DEM at a customer location. It is assumed that the technician is experienced with the following subjects:

- Microsoft® Windows® Server 2000 and 2003
- One of the following LDAP services:
  - IBM® Directory Server (IDS) 5.1
  - Microsoft Active Directory®
  - Microsoft Active Directory Application Mode (ADAM)
  - Netscape® Directory Server Version 4.12
  - Novell® NDS® eDirectory™ 8.x
  - Sun™ ONE Directory Server 5.1
- local area networks (LANs)

- Avaya voice server installation and implementation
- INTUITY™ AUDIX® system administration

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 installing and/or administering DEM.
- Chapter 1, "Introduction" - This chapter provides a brief introduction to DEM.
- Chapter 2, "Installing Avaya Directory Enabled Management (DEM)" - This chapter describes how to install DEM.
- Chapter 3, "Configuring Avaya Directory Enabled Management (DEM)" - This chapter describes how to configure DEM.
- Chapter 4, "Troubleshooting" - This chapter provides information about possible error conditions and how to respond to them when you install and configure DEM.

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 Administration**

  This Portable Document Format (PDF) document is located in the Docs folder in the Avaya Directory Enabled Management Release 3.0 CD. 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 DEM Release 3.0 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 DEM 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 Directory Enabled Management (DEM) and its components.

Overview of Avaya Directory Enabled Management (DEM)

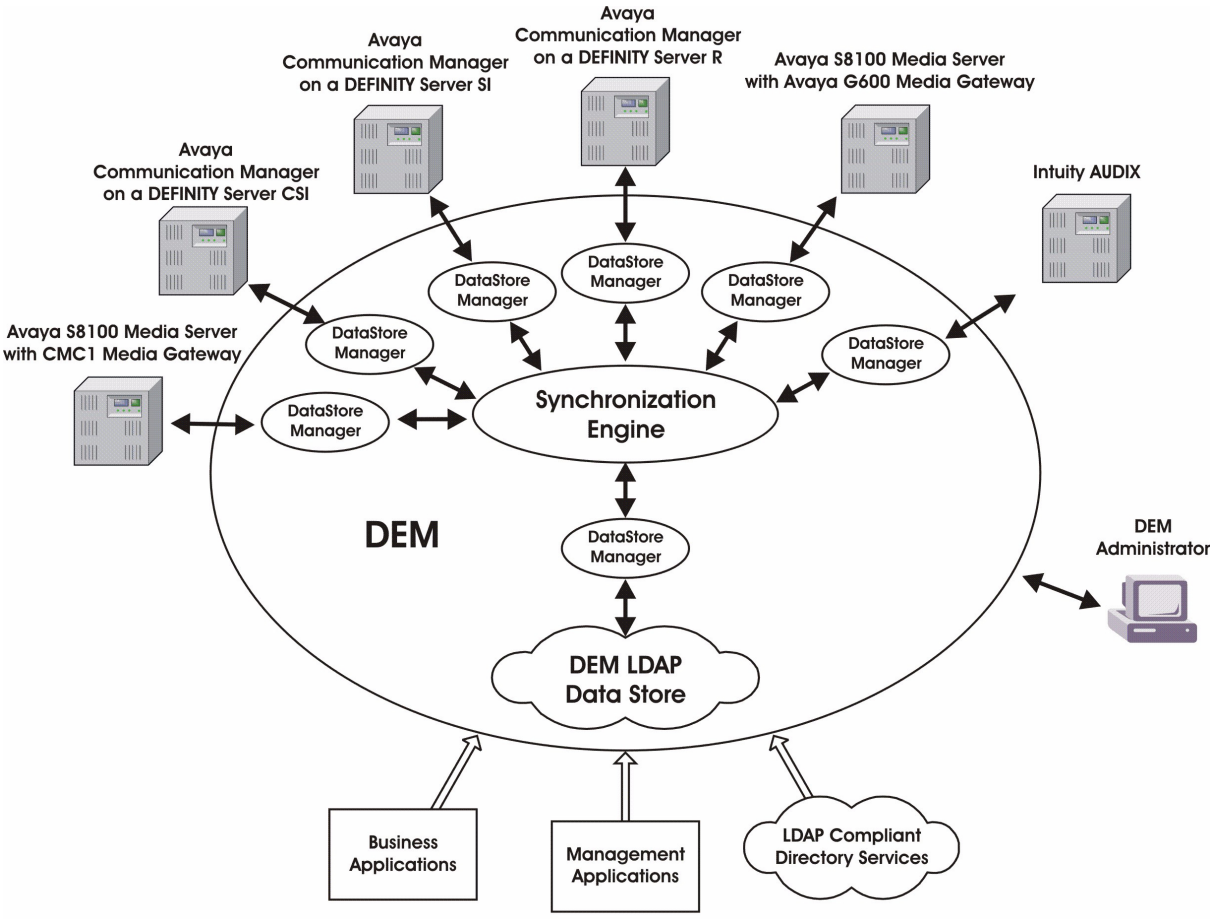
Avaya Directory Enabled Management (DEM) is software that "LDAP-enables" voice server data and Intuity system data, providing real-time, integrated, directory-based read/write access to voice server data, Intuity data, and data derived from enterprise sources (such as corporate databases). DEM interfaces with the voice server (such as Avaya Communication Manager on a DEFINITY® Server SI and Avaya S8100 Media Server with CMC1 Media Gateway), the Intuity system, a company's LDAP server, the DEM Administrator application, and DEM client applications (which are LDAP-based applications that enable users to view and modify the DEM data).

DEM consists of the following components:

- DataStore Managers (DSMs)
- Synchronization Engine
- LDAP Data Store
- DEM Administrator

Figure 1 shows the structure of DEM.

Figure 1. Avaya Directory Enabled Management (DEM)



DataStore Managers

DataStore Managers are software processes that interface with each device type that connects to DEM. A DataStore Manager is the "connector technology" for DEM, enabling different DEM devices (such as voice servers, Intuity systems, and LDAP servers) to communicate with each other. Each DataStore Manager contains low-level mapping information that converts device-specific data types to DEM data types (also known as *DEM virtual objects*). The DEM virtual objects are composed of the "common data representation language" of DEM, enabling all DEM devices to communicate with one another. For example, when a change is made to the voice server data, the DEFINITY DataStore Manager takes the changed data from the voice server, converts it into a DEM schema object (which can be understood by every other DataStore Manager on DEM), and sends this data change (packaged in a *ChangeDescriptor*) to the Synchronization Engine. A ChangeDescriptor is the transport vehicle for a package of data (that is, a data change) through DEM. DEM uses the ChangeDescriptor to keep track of the device supplying the data change and the transaction number.

Each device on DEM must have its own DataStore Manager. For example, the voice server has its own DataStore Manager, and your company's LDAP server has its own DataStore Manager. As the DEM Administrator, it is your responsibility to define, activate, and monitor the DataStore Managers for each DEM device.

Each DataStore Manager monitors its associated device. Every time a data change is made on the device, the DataStore Manager creates a ChangeDescriptor that describes the data change, and then sends the ChangeDescriptor to the Synchronization Engine, which is the hub of DEM. The ChangeDescriptor is propagated to the rest of the system by the Synchronization Engine based on the routing and mapping rules you define for the Synchronization Engine.

Each DataStore Manager receives ChangeDescriptors from the Synchronization Engine for DEM types to which it subscribes.

Synchronization Engine

The Synchronization Engine, the heart of DEM, is a software process that synchronizes changes between native device data (for example, data from a voice server) and data from enterprise directories according to rules that you define.

When a change is made in a device (such as the voice server), the DataStore Manager creates a ChangeDescriptor and sends that ChangeDescriptor to the Synchronization Engine. The Synchronization Engine then applies its rules to the ChangeDescriptor and determines whether that data change affects data used by other devices on DEM. Depending on its rules, the Synchronization Engine routes the ChangeDescriptor to the appropriate DataStore Managers in the system. Those DataStore Managers then convert the virtual object in the ChangeDescriptor to the native data type of the device, and the appropriate data is changed in the device, thereby synchronizing the data across the system.

LDAP Data Store

DEM provides an LDAP server that stores all of the DEM data. However, DEM can be configured to store its data in an existing LDAP directory service on your LAN. As changes are made to data in the DEM devices, the LDAP data store is continuously updated with these changes.

DEM Administrator

DEM Administrator is a software application that enables you to configure, monitor and control DEM. Some of the tasks you can perform via DEM Administrator include:

- synchronize DEM data
- create, manage, and control DataStore Managers
- create, manage, and control Synchronization Engines
- monitor messages generated by DataStore Managers and/or the Synchronization Engine
- manage DEM Administrator users

In Release 1.3, the Goal Oriented State Management (GOSM) feature was added, which enables DEM to automatically return to the last known desired state after a shutdown. GOSM automates system state monitoring and automatic recovery mechanics during normal operation. By default, GOSM is enabled and polls for system status every 5 minutes. You can disable GOSM and change the polling interval. However, it is recommended that you keep GOSM enabled, and that you do not set the polling interval to less than 5 minutes.

To change the GOSM settings:

1. Open the file "gosm.ini." (This file is located in <DEMInstalledDirectory>\bin.)
2. In the [GOSM] section, set **enabled** to **0** or **1**. (**1** is enabled, and **0** is disabled.)
3. Set **interval** to the polling interval you want to use. The default is 5 minutes. You should not set the polling interval to less than 5 minutes.
4. Save your changes, and close the file.

In Release 2.0, GOSM was enhanced to provide the capability to re-synchronize a specified set of DEM types in the event of a DataStore Manager recovery operation. If GOSM decides that it needs to restore a DataStore Manager to the running state, GOSM examines that DataStore Manager's operating configuration to determine if an "autosync" section is specified. If an autosync section is specified, the list of types is read from the autosync section. After GOSM successfully reactivates, attaches, and runs the DataStore Manager, GOSM will request the DataStore Manager to re-synchronize those objects in the most optimal way.

You should specify an autosync section for any DataStore Managers that should be re-synchronized automatically by GOSM on a recovery. The autosync section can appear anywhere in the DataStore Manager's configuration data. The following is an example of the format of an autosync section:

```
[autosync]
1=definityStation
2=…
```

New Features in This Release

DEM Release 3.0 has the following new features:

- **Support for Multibyte Characters for certain objects and attributes**

  DEM now handles multibyte characters for certain attributes in Station, Hunt Group, Trunk Group, and VDN Name objects. The multibyte supported fields on the voice system will be stored as HEX characters spanned across five fields (NativeName 1-5). The DEM LDAP driver will combine the HEX characters into one field, convert the HEX into UTF-8 format, and then store the result in deftyVDNNativeName1. When a change is made from LDAP, the reverse will occur: the UTF-8 will be converted into HEX and then written to the voice system. LDAP clients pointing to DEM on port 4000 should store Multibyte character names (for example, Japanese) in the deftyVDNNativeName1 attribute in the UTF-8 format.

- **Administrator ID in the CD**

  DEM now provides via CD a "loginID" object. The value of this loginID object is the logon name of the person who made the change on the voice system. The loginID object uses the following format:
  .loginID=<*Login name from voice system*>.

*** Note:** The loginID object is available only in the CD. It is unavailable in LDAP.

- **Support for Async Calls**

  DEM GWAgent now supports asynchronous LDAP calls.

- **Access to Administration Features**

  DEM now supports the Login Administration feature on the voice system so that DEM clients can add, delete, and modify voice system users. Passwords can be changed, but they cannot be viewed.

- **Announce Recording Event in the CD**

  Whenever an announcement is recorded, it is captured in the CD. The Announce Recording event object uses the following format:
  .anncExtFrom=<*extension recording the announcement*>
  .anncExtSet=<*extension recording to*>
  .anncOp=<*add,delete,modify*>

*** Note:** The Announce Recording event object is available only in the CD. It is unavailable in LDAP. Also, if an announcement is uploaded to the voice system, that announcement will NOT be captured to the CD.

- **DEM Windows LDAP Client Enhancements**

  The following enhancements were added to the DEM Windows LDAP client:

  — More advanced searching capabilities (equals, not equals, contains, is like, and number ranges).

  — Improved interface (buttons and search bar).

- **Support for Authorization Codes**

  DEM now supports Authorization Codes.

- **Support for UDP Tables**

  DEM now supports Uniform Dial Plan (UDP) tables. By default, DEM will synchronize a maximum of 25 UDP tables. You can change this maximum value by performing the following steps:

  a. Log into the DEM Admin.

  b. Click the **Device Configurations** button.

  c. Select the **DataStore Managers for Device Class** option button.

  d. Under Defined Configurations, select **_DefinityR11Root**.

  e. In the Configuration Details list box, search for **[definityUDPTableGroup]**.

  f. In the [definityUDPTableGroup] section, change the **MaxStaticID** value to the maximum number of UDP tables you want to synchronize.

  g. Click the **Save** button.

h. Click the **Done** button.

i. Shut down and restart your voice system DSM.

j. Synchronize **definityUDPTableGroup**.

*** Note:** As of DEM R3.0, DEM Browser and Avaya Terminal Configuration are no longer available.

2 Installing Avaya Directory Enabled Management (DEM)

This chapter describes how to install DEM.

Requirements

DEM requires the hardware and software listed below.

*** Note:** Note that system performance may be adversely affected by lower system speeds and lower memory capacities.

- An IBM-compatible PC with the following hardware:
  - a Pentium® III 500 MHz or higher processor
  - a hard disk with at least 8 GB of space available (13 GB recommended)
  - 128 MB of RAM (256 MB recommended)
  - a network interface card to connect the PC to the company's local area network (LAN)
  - a 56Kbps or higher modem (for required remote support)
  - a CD-ROM drive, a Windows compatible VGA (or better) adapter, and a pointing device
- Microsoft Windows 2000 Server or 2003 Server
- one of the following LDAP services:
  - Netscape Directory Server Version 4.12
  - Novell NDS eDirectory 8.x
  - Microsoft Active Directory
  - Sun ONE Directory Server 5.1
  - IBM Directory Server (IDS) 5.1

- pcANYWHERE® Version 9.0 or later (for required remote support)
- Any of the following Avaya servers connected to the company's LAN:
  - — Avaya Communication Manager on a DEFINITY Server CSI
  - — Avaya Communication Manager on a DEFINITY Server SI
  - — Avaya Communication Manager on a DEFINITY Server R
  - — Avaya S8100 Media Server with CMC1 Media Gateway
  - — Avaya S8100 Media Server with Avaya G600 Media Gateway
  - — Avaya S8300 Media Server with Avaya G700 Media Gateway
  - — Avaya S8500 Media Server
  - — Avaya S8700 Media Server for IP Connect Configurations
  - — Avaya S8700 Media Server for Multi-Connect Configurations

*** Note:** DEM provides Apache Jakarta Tomcat.

DEM supports INTUITY AUDIX messaging Release 5.1 or later systems that are connected to the company's LAN.

For the most up-to-date requirements for DEM, go to *http://www.avaya.com/support*.

Before You Begin

Before installing the DEM software, make sure you have the following information:

- **LDAP information**
  - — LDAP root
  - — LDAP user ID (and its corresponding password) with administrative privileges
  - — LDAP server port (usually 389)
  - — name of the PC hosting the LDAP service

  For Active Directory, keep in mind the following information:

    - Active Directory must be installed. (Use the default settings.)
    - Load the Support Tools found on the Microsoft 2000 Server CD. (The Support Tools will be installed in Start>Programs>2000 Support Tools.)

*** Note:** If you are using Windows 2003, you must run ADSI Edit from a command prompt. Type ***adsiedit.msc*** from a command prompt after installing the support tools from the Windows 2003 install CD.

- ADSI Edit is the application of interest.
- Add a node under the base node by opening ADSI EDIT, right-clicking the root (for example, **DC=Avaya,DC=com)**, going to New-Object, and selecting organization. Type in an object name (for example, ***dem***). This will create the base string where DEM modifies the schema. In this example, **o=dem,dc=Avaya,dc=com**.
- Active Directory requires the user name to be in the following format: cn=adminlogin,cn=users,o=xxx,dc=xxx,dc=xxx

*** Note:** The Administrator must have privileges to **add** and **delete** the schema.

- **Voice server information**

  — an appropriate IP address of the network connection to the SAT server on the voice server

  — IP port number that is associated with the SAT server on that IP address

  If you are using an Avaya S8100 Media Server with CMC1 Media Gateway (formerly called "DEFINITY One") or an Avaya S8100 Media Server with Avaya G600 Media Gateway (formerly called "IP600"), perform the following steps:

  1. Use the IP address of the server processor.
  2. Verify that the port number is 23 for that IP address by entering the telnet command and the IP address from the SAT. For example, if the IP address is 123.45.67.89, you would enter ***telnet 123.45.67.89***. If you receive a login prompt after entering the telnet command and the IP address, the IP address is correct.
     If you do not receive a login prompt after entering the telnet command and the IP address, contact your System Administrator for additional help.

  If you are using an Avaya system with Communication Manager, use the IP address of a C-LAN board where the SAT server access is configured and the IP port that is configured on that board for the SAT server. To determine this information, perform the following steps:

  1. From the SAT, use the command **display ip services** to determine the internal name of the C-LAN board that provides access to the SAT service and the IP port that is associated with it.
  2. Now that you know the internal name of the C-LAN board, use the **display nodes ip** command to identify the IP address of the C-LAN board.

  — login (and its corresponding password) on the voice server that DEM will use. This login must have the following settings:

  - login type set to "Service"
  - service level set to "inads"

  It is recommended that you create this login before the DEM software is installed.

- **Intuity system information**

  — IP address of the Intuity system

  — login (and its corresponding password) on the Intuity system that DEM will use. This login must have administration privileges (for example, craft login).

  It is recommended that you create this login before the DEM software is installed.

- **completed DEM planning form** (See "Planning Form" on page 26.)

Planning Form

Before installing the software, you must know the following information. A blank copy of this form is located at the end of this chapter. You should fill out the planning form before installing the software.

LDAP Information

1. LDAP Root: _____

2. LDAP User ID: _____

3. LDAP User ID password: _____

4. LDAP Server Port (usually 389): _____

5. Name of the PC hosting LDAP: _____

Voice Server Information

1. Type of voice server

   - Avaya Communication Manager on a DEFINITY Server CSI
   - Avaya Communication Manager on a DEFINITY Server SI
   - Avaya Communication Manager on a DEFINITY Server R
   - Avaya S8100 Media Server with CMC1 Media Gateway
   - Avaya S8100 Media Server with Avaya G600 Media Gateway
   - Avaya S8300 Media Server with Avaya G700 Media Gateway
   - Avaya S8500 Media Server
   - Avaya S8700 Media Server for IP Connect Configurations
   - Avaya S8700 Media Server for Multi-Connect Configurations

2. Switch ID of the voice server: _____

3. IP address of the voice server: _____

4. Port for the voice server: _____

5. Voice server login that DEM will use: _____

6. Voice server login password: _____

Intuity Information

1. Messaging server ID of the Intuity system: _____

2. IP address of the Intuity system: _____

3. Intuity login that DEM will use: _____

4. Intuity login password: _____

Install the Software

To install DEM:

1. Insert the Avaya Directory Enabled Management Release 3.0 CD.

   The Welcome dialog box appears.

2. Click the **Next** button.

   The Software License Agreement dialog box appears.

3. Read the software license agreement.

4. To accept the software license agreement, click the **Yes** button.

   The Customer Information dialog box appears.

5. In the **User Name** box, enter your name.

6. In the **Company Name** box, enter the company name.

7. Click the **Next** button.

   If this is a new DEM installation, the Setup Type dialog box appears. Go to Step 8.

   If you have a previous version of DEM installed, you will be prompted to either upgrade or overwrite your current installation of DEM. It is recommended that you **upgrade** your current installation of DEM to preserve your current DEM settings.

   If you want to overwrite your existing DEM installation, click the **Overwrite** option button, and then click the **Next** button. The Setup Type dialog box appears. Go to Step 8.

   If you want to upgrade your existing DEM installation, perform the following steps:

   a. Click the **Upgrade** option button, and then click the **Next** button.

      The Choose Backup Folder Destination dialog box appears. The default folder is **C:\DEM_2.0**.

b. Select the location, and then click the **Next** button.

The Begin Installation dialog box appears, displaying the installation information. If necessary, use the **Back** button to make any changes.

c. Go to Step 37.

8. In the Setup Type dialog box, select the appropriate option button. You can select one of the following installation options:

— **Typical**

This option installs all of the DEM software. *This is the suggested installation option*.

— **Compact**

This option installs the minimum required components of the DEM software.

— **Custom**

This option enables you to specify which components of the DEM software you want to install.

9. Click the **Next** button.

The Choose LDAP Vendor dialog box appears.

10. Select the option button for the type of LDAP server you want to use, and click the **Next** button.

The LDAP Configuration dialog box appears.

11. In the **User** box, enter an LDAP user who has administrative privileges (for example, ***cn=Directory Manager***).

*** Note:** If you are using Active Directory, you must enter the full user name (for example, ***cn=Administrator,cn=users,dc=dem,dc=com***).

If you are using Novell NDS, you must also enter that user's "context" in the **User** box (for example, ***cn=Admin,o=dem***, where ***o=dem*** is the context).

12. In the **Password** box, enter the password for the LDAP user you entered.

13. In the **Confirm Password** box, reenter the password for the LDAP user you entered.

14. Click the **Next** button.

The Configure DEFINITY Servers dialog box appears. This dialog box enables you to specify each voice server that will be connected to DEM.

15. Click the **Add** button.

The DEFINITY Configuration dialog box appears.

16. In the **DSM Name** box, enter the name of the voice server that will interface with DEM.

17. From the **Release Version** box, select the type of voice server.

*** Note:** Select **R11** for Release 11 or later systems.

18. If the voice server is an Avaya S8100 Media Server with CMC1 Media Gateway (formerly called "DEFINITY One") or an Avaya S8100 Media Server with Avaya G600 Media Gateway (formerly called "IP600"), click the **DEFINITY ONE** check box. Otherwise, do not select this check box.

19. In the **Host IP** box, enter the IP address of the voice server.

20. In the **Port** box, enter the port of the voice server.

21. In the **Login** box, enter the voice server login that DEM will use. *This login must be a "service" type login with the service level set to "**inads**."*

22. In the **Password** box, enter the password for the voice server login.

23. In the **Confirm Password** box, reenter the password for the voice server login.

24. Perform one of the following steps:

— If you are using ASG Key, perform the following steps:

1 In the **ASG Key** box, enter the ASG Key password.
2 In the **Confirm ASG Key** box, reenter the ASG Key password.
3 Proceed to Step 25.

— If you are not using ASG Key, go to Step 25.

25. Click the **OK** button.

The Configure DEFINITY Servers dialog box appears, showing the switch ID, host IP, and port you entered for the voice server.

26. Repeat Steps 15 to 25 for each additional voice server that will be connected to DEM.

27. When finished configuring the voice server(s) that will be connected to DEM, click the **Next** button.

The Configure Intuity Servers dialog box appears. This dialog box enables you to specify each Intuity system that will be connected to DEM.

28. Click the **Add** button.

The Intuity Configuration dialog box appears.

29. In the **DSM Name** box, enter the name of the Intuity system that will interface with DEM.

30. In the **Host** box, enter the IP address or machine name of the Intuity system.

31. In the **Login** box, enter the Intuity login that DEM will use. *This login must have administration privileges (for example, craft login*).

32. In the **Password** box, enter the password for the Intuity login.

33. In the **Confirm Password** box, reenter the password for the Intuity login.

34. Click the **OK** button.

The Configure Intuity Servers dialog box appears, showing the system ID and host IP you entered for the Intuity system.

35. Repeat Steps 29 to 34 for each additional Intuity system that will be connected to DEM.

36. When finished configuring the Intuity system(s) that will be connected to DEM, click the **Next** button.

The Begin Installation dialog box appears, displaying the installation information. If necessary, use the **Back** button to make any changes.

37. Click the **Next** button.

The Warning message box appears.

38. Click the **OK** button.

The Python Installation Select Destination Directory dialog box appears. If you are upgrading, you will not see the Python installation.

39. Click the **Next** button.

The Backup Replaced Files dialog box appears.

40. Click the **Next** button.

The Select Components dialog box appears.

41. Click the **Next** button.

The Select Start Menu Group dialog box appears.

42. Click the **Next** button.

The Ready to Install dialog box appears.

43. Click the **Next** button.

Python is installed. After the Python installation is complete, the Installation Completed dialog box appears.

44. Click the **Finish** button.

The Java JRE V1.4.2_06 License Agreement dialog box appears.

45. Read the software license agreement.

46. To accept the software license agreement, click the **I accept the terms in the license agreement** option button, and then click the **Next** button.

The Select Destination Directory dialog box appears.

47. Click the **Next** button.

The Setup Type dialog box appears.

48. Click the **Install** button.

A status box appears showing the status of the installation. When the installation is complete, the InstallShield Wizard Completed dialog box appears.

If Adobe Acrobat Reader 6.0 is not installed, the Adobe Reader 6.0 Setup message box appears. Go to Step 49.

If Adobe Acrobat Reader 6.0 is already installed, the remainder of the DEM files are installed and the associated services are started. When the installation is complete, the InstallShield Wizard Complete dialog box appears. Go to Step 54.

49. At the Adobe Reader 6.0 Setup message box, click the **Next** button.

    The Welcome dialog box appears.

50. Click the **Next** button.

    The Destination Folder dialog box appears.

51. Click the **Next** button.

    The Ready to Install the Program dialog box appears.

52. Click the **Install** button.

    A status box appears showing the status of the installation. When the software is installed, the Setup Wizard Completed dialog box appears.

53. Click the **Finish** button.

    The remainder of the DEM files are installed and the associated services are started. When the installation is complete, the InstallShield Wizard Complete dialog box appears.

54. Select the **Yes, I want to restart my computer now** option button, and then click the **Finish** button.

After you have finished installing Avaya Directory Enabled Management, go to "Configuring Avaya Directory Enabled Management (DEM)" on page 37 to configure DEM initially.

Planning Form

Before installing the software, enter the following information:

LDAP Information

1. LDAP Root: _____

2. LDAP User ID: _____

3. LDAP User ID password: _____

4. LDAP Server Port (usually 389): _____

5. Name of the PC hosting LDAP: _____

Voice Server Information

1. Type of voice server

   - Avaya Communication Manager on a DEFINITY Server CSI
   - Avaya Communication Manager on a DEFINITY Server SI
   - Avaya Communication Manager on a DEFINITY Server R
   - Avaya S8100 Media Server with CMC1 Media Gateway
   - Avaya S8100 Media Server with Avaya G600 Media Gateway
   - Avaya S8300 Media Server with Avaya G700 Media Gateway
   - Avaya S8500 Media Server
   - Avaya S8700 Media Server for IP Connect Configurations
   - Avaya S8700 Media Server for Multi-Connect Configurations

2. Switch ID of the voice server: _____

3. IP address of the voice server: _____

4. Port for the voice server: _____

5. Voice server login that DEM will use: _____

6. Voice server login password: _____

Intuity Information

1. Messaging server ID of the Intuity system: _____

2. IP address of the Intuity system: _____

3. Intuity login that DEM will use: _____

4. Intuity login password: _____

3 Configuring Avaya Directory Enabled Management (DEM)

This chapter describes how to configure DEM. The steps you must perform to configure DEM depend on whether you installed a new DEM system or upgraded from an earlier release of DEM.

Configuring a New DEM

To configure a new DEM installation, you must perform the following procedures:

1. Configure the LDAP schema ("Procedure 1: Configure the LDAP Schema" on page 40). Depending on the type of LDAP you want to use, you must perform one of the following steps:
   - If you want to configure DEM for Active Directory, go to "Configure the LDAP Schema for Active Directory" on page 41. Perform this procedure only if you want to use Active Directory LDAP instead of general LDAP (that is, Netscape or Sun ONE Directory Server 5.1).
   - If you want to use general LDAP (that is, Netscape or Sun ONE Directory Server 5.1, go to "Configure Other LDAP Schema" on page 42).
2. Start the DEM Administrator application, and log in as Administrator ("Procedure 2: Start the DEM Administrator Application" on page 44).
3. Configure GWAgent ("Procedure 3: Configure GWAgent" on page 45).
4. Activate the Synchronization Engine ("Procedure 4: Activate the Synchronization Engine" on page 47).
5. Activate and attach the DEM DataStore Manager ("Procedure 5: Activate and Attach the DEM DataStore Manager" on page 48).

6. Configure additional DEM DataStore Managers ("Procedure 6: Configure Additional DEM DataStore Managers" on page 49).

*** Note:** Perform this procedure only if the customer has requested an additional DEM DataStore Manager.

7. Activate and attach the DEFINITY DataStore Manager ("Procedure 7: Activate and Attach the DEFINITY DataStore Manager" on page 52).

8. Configure additional DEFINITY DataStore Managers ("Procedure 8: Configure Additional DEFINITY DataStore Managers" on page 53).

*** Note:** Perform this procedure only if you did not configure additional voice servers during the software installation, or you want to add additional voice servers after DEM is installed.

9. Activate and attach the Intuity DataStore Manager ("Procedure 9: Activate and Attach the Intuity DataStore Manager" on page 56).

10. Configure additional Intuity DataStore Managers ("Procedure 10: Configure Additional Intuity DataStore Managers" on page 57).

*** Note:** Perform this procedure only if you did not configure additional Intuity systems during the software installation, or you want to add additional Intuity systems after DEM is installed.

11. Create a new DEM Administrator login, and delete the default login ("Procedure 11: Create a New DEM Administrator Login" on page 60).

12. Administer DEM ("Procedure 12: Administer DEM" on page 61).

Upgrading from an Earlier Release

If you upgraded from DEM Release 2.0, perform the following procedures:

1. Configure the LDAP schema for your LDAP server ("Procedure 1: Configure the LDAP Schema" on page 40).
2. Start the DEM Administrator application, and log in as Administrator ("Procedure 2: Start the DEM Administrator Application" on page 44).
3. Activate the Synchronization Engine ("Procedure 4: Activate the Synchronization Engine" on page 47).
4. Activate and attach the DEM DataStore Manager ("Procedure 5: Activate and Attach the DEM DataStore Manager" on page 48).
5. Configure additional DEM DataStore Managers ("Procedure 6: Configure Additional DEM DataStore Managers" on page 49).

*** Note:** Perform this procedure only if the customer has requested an additional DEM DataStore Manager.

6. Activate and attach the DEFINITY DataStore Manager ("Procedure 7: Activate and Attach the DEFINITY DataStore Manager" on page 52).
7. Configure additional DEFINITY DataStore Managers ("Procedure 8: Configure Additional DEFINITY DataStore Managers" on page 53).

*** Note:** Perform this procedure only if you want to add additional voice servers.

8. Activate and attach the Intuity DataStore Manager ("Procedure 9: Activate and Attach the Intuity DataStore Manager" on page 56).
9. Configure additional Intuity DataStore Managers ("Procedure 10: Configure Additional Intuity DataStore Managers" on page 57).

*** Note:** Perform this procedure only if you want to add additional Intuity systems.

10. Create a new DEM Administrator login, and delete the default login ("Procedure 11: Create a New DEM Administrator Login" on page 60).

11. Administer DEM ("Procedure 12: Administer DEM" on page 61).

Procedure 1: Configure the LDAP Schema

In this section, you will apply schema updates to the LDAP server so that DEM data will populate the LDAP server.

Depending on the type of LDAP you want to use, perform one of the following steps:

- If you want to configure DEM for Active Directory, go to "Configure the LDAP Schema for Active Directory" on page 41.

*** Note:** Perform this procedure only if you want to use Active Directory LDAP instead of Microsoft Active Directory Application Mode (ADAM), IBM Directory Server 5.1, Netscape Directory Server 4.12, Novell NDS eDirectory 8.x, or Sun ONE Directory Server 5.1 LDAP.

- If you want to use Microsoft Active Directory Application Mode (ADAM), go to "Configure the LDAP Schema for Microsoft Active Directory Application Mode (ADAM)" on page 42.
- If you want to use IBM Directory Server 5.1, Netscape Directory Server 4.12, Novell NDS eDirectory 8.x, or Sun ONE Directory Server 5.1 LDAP, go to "Configure Other LDAP Schema" on page 42.

Configure the LDAP Schema for Active Directory

In this section, you will apply schema updates to the Active Directory LDAP server so that DEM data will populate the Active Directory LDAP server.

*** Note:** If DEM and Active Directory are installed on different servers, you must modify a registry key. Management of the Active Directory Schema is not expected to be a frequently performed task, and care must be exercised when modifying the schema. Windows 2000 has a new administrative group called "Schema Administrators." Management of the schema is restricted to members of the Schema Administrators group. A registry modification to allow write operations is necessary before a Schema Administrator can create and modify classes and attributes using the Active Directory Schema Manager snap-in.

To modify the registry to allow write operations to the schema, create a new REG_DWORD value named "Schema Update Allowed" with a data value of "1" in the following registry key:

HKEY LOCAL MACHINE\System\Current Control Set\Services\NTDS\Parameters

It is unnecessary to reboot the computer. The Active Directory service detects the change automatically. To disable the schema updates on this domain controller, change the data value to "0".

If you are upgrading from a previous DEM release, open the file *ReadMe_3_0.txt*. This file is located in c:\dem\ldap\Active Directory. Refer to the section "Updating Your DEM Schema (Upgrade From Previous Version of DEM)."

If you are configuring a new DEM installation with Active Directory, open the file *ReadMe_3_0.txt*. This file is located in c:\dem\ldap\Active Directory. Refer to the section "Installing Your DEM Schema (New Install of DEM)."

If this is a new installation of DEM or you overwrote the previous installation of DEM, go to "Procedure 3: Configure GWAgent" on page 45. Otherwise, go to "Procedure 2: Start the DEM Administrator Application" on page 44.

Configure the LDAP Schema for Microsoft Active Directory Application Mode (ADAM)

If you are upgrading from a previous version of DEM, open the file *ReadMe_3_0.txt*. This file is located in the folder c:\dem\ldap\ADAM. Refer to the section "Updating Your DEM Schema (Upgrade From Previous Version of DEM)."

If this is a new installation or you are using ADAM with DEM for the first time, open the file *ReadMe_3_0.txt*. This file is located in the folder c:\dem\ldap\ADAM. Refer to the section "Installing Your DEM Schema (New Install of DEM)."

Configure Other LDAP Schema

In this section, you will apply schema updates to the IBM Directory Server 5.1, Netscape Directory Server 4.12, Novell NDS eDirectory 8.x, or Sun ONE Directory Server 5.1 LDAP server so that DEM data will populate the LDAP server.

Update the IBM Directory Server LDAP Schema

To update the IBM Directory Server LDAP schema:

1. From the Start menu, access the Services window.

   The Services window appears.

2. Stop the IBM Directory Server.

3. Copy the schema files "avayaDEMObj.oc" and "avayaDEMAttr.at" from the directory **\DEM\ldap\ids** to the directory **\IBM\LDAP\ETC**.

   The file "avayaDEMAttr.at" contains the DEM attributes for the IBM Directory Server. The file "avayaDEMObj.oc" contains the object classes.

4. Restart the IBM Directory Server in the Services window.

5. If this is a new installation or you overwrote the DEM installation, go to "Procedure 3: Configure GWAgent" on page 45. Otherwise, go to "Procedure 2: Start the DEM Administrator Application" on page 44.

Update the Netscape Directory Server 4.12 LDAP Schema

To update the Netscape Directory Server 4.12 LDAP schema:

*** Note:** If you are using a version of Netscape Directory Server that is later than 4.12, follow the procedure for updating the Sun ONE Directory Server LDAP schema.

1. Copy the schema files "slapd.user_at.conf" and "slapd.user_oc.conf" from the directory **\DEM\ldap\Netscape** to the directory **\Netscape\Server4\slapd-*server name*\config** (where *server name* is the name of the computer hosting LDAP directory).

   The file "slapd.user_at.conf" contains the DEM attributes for Netscape. The file "slapd.user_oc.conf" contains the object classes.

2. From the Start menu, access the Services window.

   The Services window appears.

3. Stop and restart Netscape Directory Server.

4. If this is a new installation or you overwrote the DEM installation, go to "Procedure 3: Configure GWAgent" on page 45. Otherwise, go to "Procedure 2: Start the DEM Administrator Application" on page 44.

Update the Novell NDS eDirectory Server LDAP Schema

To update the Novell NDS eDirectory server LDAP schema, perform one of the following steps:

- If you are upgrading from a previous DEM release, open the file *ReadMe_3_0.txt*. This file is located in c:\dem\ldap\NDS. Refer to the section "Updating Your DEM Schema (Upgrade From Previous Version of DEM)."
- If you are configuring a new DEM installation with Novell NDS eDirectory, open the file *ReadMe_3_0.txt*. This file is located in c:\dem\ldap\NDS. Refer to the section "Installing Your DEM Schema (New Install of DEM)."
- If this is a new installation of DEM or you overwrote the previous installation of DEM, go to "Procedure 3: Configure GWAgent" on page 45. Otherwise, go to "Procedure 2: Start the DEM Administrator Application" on page 44.

Update the Sun ONE Directory Server LDAP Schema

To update the Sun ONE Directory Server LDAP schema:

1. Copy the schema file "98AvayaDEM.ldif" from the directory **\DEM\ldap\SunOne** to the directory **\iPlanet\Servers\slapd-***server name***\config\schema** (where *server name* is the name of the computer hosting LDAP directory).

   The file "98AvayaDEM.ldif" contains the DEM attributes and object classes for Sun ONE Directory Server 5.1.

2. From the Start menu, access the Services window.

   The Services window appears.

3. Stop and restart Sun ONE Directory Server.

4. If this is a new installation or you overwrote the DEM installation, go to "Procedure 3: Configure GWAgent" on page 45. Otherwise, go to "Procedure 2: Start the DEM Administrator Application" on page 44.

Procedure 2: Start the DEM Administrator Application

To start the DEM Administrator application:

1. Log into the network.

2. From the Start menu, select **Programs>Avaya>Directory Enabled Management>DEM Admin**.

   The Avaya Directory Enabled Management Administrator Login dialog box appears.

3. In the **Username** box, enter ***Administrator***.

4. In the **Password** box, enter ***password***.

5. Click the **OK** button.

   The Avaya Directory Enabled Management Administrator window appears. The **Synchronization Engines** tab is displayed.

Go to "Procedure 3: Configure GWAgent" on page 45.

Procedure 3: Configure GWAgent

In this procedure, you will configure GWAgent. GWAgent monitors the LDAP datastore and notifies DEM when changes are made. Perform one of the following procedures:

- Configure and activate the default triggers using the primary LDAP configuration settings (which you configured during installation)
- Configure the GWAgent settings manually.

To configure and activate the default triggers using the primary LDAP configuration settings (which you configured during installation), click the **Set Default** button (recommended).

To configure GWAgent manually:

1. Click the **GWAgent** tab in the Avaya Directory Enabled Management Administrator window.

   The **GWAgent** tab appears.

2. Click the **Startup** button.

   The GWAgent StartUp Parameters dialog box appears.

3. Click the **Browse** button.

   The Browse for Folder dialog box appears.

4. Select the folder where GWAgent is located. The default location is **c:\DEM\bin**.

5. Click the **OK** button.

   The GWAgent settings are displayed in the GWAgent StartUp Parameters dialog box.

6. Verify that the information displayed in the **Host** box and the **Port** box is correct.

7. Click the **OK** button.

8. Click the **Connect** button.

   The Connect to GWAgent dialog box appears.

9. In the **Server** box, enter the LDAP server.

10. In the **User** box, enter an LDAP user who has administrative privileges.

11. In the **Password** box, enter the password for the LDAP user you entered.

12. Click the **Save these settings as default** check box.

    A check mark appears in the check box.

13. Click the **OK** button.

    You are connected to the DEM Agent.

14. Click the **Populate** button.

    The General Settings dialog box appears.

15. Click the **Add** button.

    The Add New Trigger dialog box appears.

16. Enter ***ou=Gateway Users,o=LDAP root***, where ***LDAP root*** is the root you specified in Step 12 of the software installation.

17. Make sure the **Active** option button is selected. (It is selected by default.)

18. Click the **OK** button.

    Information is displayed.

19. Click the **Add** button.

    The Add New Trigger dialog box appears.

20. Enter ***ou=DEFINITY Servers,o=LDAP root***, where ***LDAP root*** is the root you specified in Step 12 of the software installation.

21. Click the **OK** button.

    Information is displayed.

22. Click the **Add** button.

    The Add New Trigger dialog box appears.

23. Enter ***ou=Messaging Servers,o=LDAP root***, where ***LDAP root*** is the root you specified in Step 12 of the software installation.

24. Click the **OK** button.

    Information is displayed.

25. Select the **Save these settings as default** check box.

    A check mark appears in the check box.

26. Click the **OK** button to close the General Settings dialog box.

27. Click the **Commit** button.

Go to "Procedure 4: Activate the Synchronization Engine" on page 47.

Procedure 4: Activate the Synchronization Engine

In this section, you will activate the default Synchronization Engine "GWSE." During the software installation, GWSE was installed. GWSE has already been defined and registered in the DEM Administrator application.

To activate the Synchronization Engine:

1. Click the **Synchronization Engines** tab (if it is not already selected).

   The Synchronization Engine GWSE appears in the **Synchronization Engines** list box. Its status is **Offline**.

2. Select **GWSE**.

3. Click the **Activate** button.

   A green light appears next to GWSE, and the status changes to **Active**.

Go to "Procedure 5: Activate and Attach the DEM DataStore Manager" on page 48.

Procedure 5: Activate and Attach the DEM DataStore Manager

In this section, you will activate and "attach" the DataStore Manager for the DEM (GWDSM). GWDSM connects DEM to its internal LDAP datastore, which will contain all of the DEM data. (GWDSM was created, defined, and registered during the software installation.)

After GWDSM is "attached," the DEM LDAP datastore will be able to receive data from the DEM via GWDSM. However, before GWDSM can be attached, it must be activated.

To activate and attach the GWDSM:

1. Click the **DataStore Managers** tab.

   The **DataStore Managers** tab appears.

   The GWDSM DataStore Manager appears in the **DataStore Managers** list box. Its status is **Offline**.

2. Select **GWDSM**.

3. Click the **Activate** button.

   A yellow light appears next to the DataStore Manager, and the status changes to **Detached**.

4. Click the **Attach** button.

   The status changes to **Ready**. GWDSM can now pass DEM data from the Synchronization Engine to the LDAP datastore.

If the customer wants additional DEM DataStore Managers, go to "Procedure 6: Configure Additional DEM DataStore Managers" on page 49.

Otherwise, go to "Procedure 7: Activate and Attach the DEFINITY DataStore Manager" on page 52.

Procedure 6: Configure Additional DEM DataStore Managers

*** Note:** Perform this procedure if the customer has requested additional DEM DataStore Managers.

The software installation created, defined, and registered a DataStore Manager for DEM. If you want to attach additional DEM DataStore Managers to DEM, you must create, define, register, activate, and attach a DataStore Manager.

To create, define, register, activate, and attach additional DEM DataStore Managers:

1. Click the **Device Configurations** button on the toolbar.

   The Configuration Editor dialog box appears.

2. In the **Device Class** area, click the **DataStore Manager** option button.

3. Click the **Add** button.

   A dialog box appears, prompting you to enter the name of the configuration file.

4. Enter a name that can be easily associated with the DEM DataStore Manager you are configuring, and click the **OK** button.

   The name you entered for the new configuration file is displayed and selected in the **Defined Configurations** list box.

5. In the **Defined Configurations** list box, select the DEM DataStore Manager that was created during the software installation (_PrimaryLDAP).

   The information for the selected file appears in the **Configuration Details** box.

6. Select all of the information in the **Configuration Details** box, and copy it to the Windows Clipboard.

7. In the **Defined Configurations** list box, select the DEM DataStore Manager configuration you added in Step 4 of this procedure.

   The **Configuration Details** box is empty.

8. Click the mouse inside the **Configuration Details** box, and paste the information from the Windows Clipboard.

9. Make the following changes to the information in this file:

   a. In the **[_connection_]** section, enter the LDAP base (**o=**).

   b. In the **[_connection_]** section, enter the port (**port=**) for the LDAP server you want to use.

   c. In the **[_connection_]** section, enter the IP address (**Server=**) for the LDAP server you want to use.

   d. In the **[_connection_]** section, enter an LDAP user (**cn=**) who has administrative privileges for the LDAP server you want to use.

   e. In the **[_connection_]** section, type ***password=%@LDAP_PW%***.

   f. In the **[_variables_]** section, type ***@LDAP_PW=my_password***, where ***my_password*** is the password for the LDAP server you want to use.

10. Click the **Done** button.

    The changes are saved for the new DataStore Manager configuration.

11. Click the **DataStore Managers** tab.

    The **DataStore Managers** tab appears.

12. Click the **Define DSM** button.

    The DSM Definition dialog box appears.

13. In the **DSM Name** box, enter the name for this DataStore Manager.

14. In the **DSM Type** box, enter ***GWDSM***.

15. From the **Configuration ID** drop-down list box, select the DEM DataStore Manager configuration you created in Step 4 of this procedure.

16. In the **Comment** box, you may enter notes about this DataStore Manager. The information you enter in this box is for your convenience only. DEM does not use this information.

17. Make sure the **Register with IMR** check box is enabled. (It is enabled by default.)

18. Click the **OK** button.

    The new DataStore Manager appears in the DataStore Managers list box. Its status is **Offline**.

    The new DataStore Manager is registered with DEM.

19. On the **DataStore Managers** tab, select the new DEM DataStore Manager you created.

20. Click the **Activate** button.

    A yellow light appears next to the DataStore Manager, and the status changes to **Detached**.

21. Click the **Attach** button.

    The status changes to **Ready**. The DEM DataStore Manager you created can now pass DEM data from the Synchronization Engine to the LDAP server.

Repeat Steps 1 through 21 for each DEM DataStore Manager you want to configure. When finished, go to "Procedure 7: Activate and Attach the DEFINITY DataStore Manager" on page 52.

Procedure 7: Activate and Attach the DEFINITY DataStore Manager

In this section, you will activate and "attach" the DataStore Manager for each voice server. The DEFINITY DataStore Manager connects the voice server to DEM. (The DEFINITY DataStore Manager was created, defined, and registered during the software installation.)

After the DEFINITY DataStore Manager is "attached," the voice server will be able to receive data from DEM via the DEFINITY DataStore Manager. However, before the DEFINITY DataStore Manager can be attached, it must be activated.

To activate and attach the DEFINITY DataStore Manager:

1. On the **DataStore Managers** tab, select the DEFINITY DataStore Manager. The DEFINITY DataStore Manager is named for the voice server that will interface with DEM. (See Step 18 in Chapter 2.)
2. Click the **Activate** button.

   A yellow light appears next to the DataStore Manager, and the status changes to **Detached**.
3. Click the **Attach** button.

   The status changes to **Ready**. The selected DEFINITY DataStore Manager can now pass DEM data from the Synchronization Engine to the voice server.
4. Repeat Steps 1 to 4 for each DEFINITY DataStore Manager (that is, if there is more than one voice server connected to DEM).
5. To pull data in initially from the voice server to which this DSM is pointing, click the **Synchronize** button.
6. After clicking the **Synchronize** button, select the object(s) on the voice server that you want to synchronize with LDAP, and then click **Sync**. For more detailed information on this, see the section "Synchronize a DataStore Manager" in the DEM Administration guide.

If additional voice servers will be connected to DEM and you did not configure these systems during the software installation or you want to add additional voice servers after DEM is installed, go to "Procedure 8: Configure Additional DEFINITY DataStore Managers" on page 53.

Otherwise, perform one of the following steps:

- If you are using an Intuity system, go to "Procedure 9: Activate and Attach the Intuity DataStore Manager" on page 56.
- If you are not using an Intuity system, go to "Procedure 11: Create a New DEM Administrator Login" on page 60.

Procedure 8: Configure Additional DEFINITY DataStore Managers

*** Note:** Perform this procedure if additional voice servers will be connected to DEM and you did not configure these systems during the software installation or you want to add additional voice servers after DEM is installed.

The software installation created, defined, and registered a DataStore Manager for each voice server you specified. If you want to attach additional voice servers to DEM, you must create, define, register, activate, and attach a DataStore Manager for each voice server.

To create, define, register, activate, and attach a DataStore Manager for each additional voice server:

1. Click the **Device Configurations** button on the toolbar.

   The Configuration Editor dialog box appears.

2. In the **Device Class** area, click the **DataStore Manager** option button.

3. Click the **Add** button.

   A dialog box appears, prompting you to enter the name of the configuration file.

4. Enter a name that can be easily associated with the specific voice server you are configuring, and click the **OK** button.

   The name you entered for the new configuration file is displayed and selected in the **Defined Configurations** list box.

5. In the **Defined Configurations** list box, select the DEFINITY DataStore Manager that was created during the software installation.

   The information for the selected file appears in the **Configuration Details** box. The DEFINITY DataStore Manager contains the common information that all DEFINITY DataStore Managers share.

6. Select all of the information in the **Configuration Details** box, and copy it to the Windows Clipboard.

7. In the **Defined Configurations** list box, select the DEFINITY DataStore Manager configuration you added in Step 4 of this procedure.

   The **Configuration Details** box is empty.

8. Click the mouse inside the **Configuration Details** box, and paste the information from the Windows Clipboard.

9. Make the following changes to the information in this file:

   a. In the **[_connection_]** section, enter the login (**login=**) for the voice server you want to use.

   b. In the **[_connection_]** section, enter the C-LAN port (**port=**) for the voice server you want to use.

   c. In the **[_connection_]** section, enter the IP address (**Server=**) for the voice server you want to use.

   d. In the **[_connection_]** section, type ***password=%@DEFTY_PW%***.

   e. If you are using ASG Key, type ***yek=%@ASG_KEY%*** at the bottom of the **[_connection_]** section.

   f. In the **[_variables_]** section, enter the switch name (**dsid=**) for the voice server you want to use to identify this voice server in LDAP.

   g. At the bottom of the **[_variables_]** section, type ***@DEFTY_PW=my_password***, where ***my_password*** is the password for the voice server you want to use.

   h. If you are using ASG Key, type ***@ASG_KEY=key_password*** at the bottom of the **[_variables_]** section, where ***key_password*** is the password for the ASG Key.

10. Perform one of the following steps:

   — If you are creating a DataStore Manager for an Avaya S8100 Media Server with CMC1 Media Gateway (formerly called "DEFINITY One"), change each occurrence of **G3** (if present) to ***CONTRY*** in the [_variables_] section.

   — If you are creating a DataStore Manager for a voice server other than an Avaya S8100 Media Server with CMC1 Media Gateway, change each occurrence of **CONTRY** (if present) to ***G3*** in the [_variables_] section.

11. Click the **Save** button.

12. Click the **Done** button.

    The changes are saved for the new DataStore Manager configuration.

13. Click the **DataStore Managers** tab.

    The **DataStore Managers** tab appears.

14. Click the **Define DSM** button.

    The DSM Definition dialog box appears.

15. In the **DSM Name** box, enter the name (that is, switch ID) of the voice server that will use this DataStore Manager.

16. In the **DSM Type** box, enter ***DEFINITY***.

17. From the **Configuration ID** drop-down list box, select the DEFINITY DataStore Manager configuration you created in Step 4 of this procedure.

18. In the **Comment** box, you may enter notes about this DataStore Manager. The information you enter in this box is for your convenience only. DEM does not use this information.

19. Make sure the **Register with IMR** check box is enabled. (It is enabled by default.)

20. Click the **OK** button.

    The new DataStore Manager appears in the **DataStore Managers** list box. Its status is **Offline**.

    The new DataStore Manager is registered with DEM.

21. On the **DataStore Managers** tab, select the new DEFINITY DataStore Manager you created.

22. Click the **Activate** button.

    A yellow light appears next to the DataStore Manager, and the status changes to **Detached**.

23. Click the **Attach** button.

    The status changes to **Ready**. The DEFINITY DataStore Manager you created can now pass DEM data from the Synchronization Engine to the voice server.

Repeat Steps 1 through 23 for each voice server you want to configure.

When finished, perform one of the following steps:

- If you are using an Intuity system, go to "Procedure 9: Activate and Attach the Intuity DataStore Manager" on page 56.
- If you are not using an Intuity system, go to "Procedure 11: Create a New DEM Administrator Login" on page 60.

Procedure 9: Activate and Attach the Intuity DataStore Manager

In this section, you will activate and "attach" the DataStore Manager for each Intuity system. The Intuity DataStore Manager connects the Intuity system to DEM. (The Intuity DataStore Manager was created, defined, and registered during the software installation.)

After the Intuity DataStore Manager is "attached," the Intuity system will be able to receive data from DEM via the Intuity DataStore Manager. However, before the Intuity DataStore Manager can be attached, it must be activated.

To activate and attach the Intuity DataStore Manager:

1. On the **DataStore Managers** tab, select the Intuity DataStore Manager. The Intuity DataStore Manager is named for the Intuity system that will interface with DEM. (See Step 31 in Chapter 2.)
2. Click the **Activate** button.

   A yellow light appears next to the DataStore Manager, and the status changes to **Detached**.
3. Click the **Attach** button.

   The status changes to **Ready**. The selected Intuity DataStore Manager can now pass DEM data from the Synchronization Engine to the Intuity system.
4. Repeat Steps 1 to 3 for each Intuity DataStore Manager (that is, if there is more than one Intuity system connected to DEM).
5. To pull data in initially from the Intuity to which this DSM is pointing, click the **Synchronize** button.

6. After clicking the **Synchronize** button, select the IntuitySubscriber object on the Intuity that you want to synchronize with LDAP, and then click **Sync**. For more detailed information on this, see the section "Synchronize a DataStore Manager" in the DEM Administration guide.

If additional Intuity systems will be connected to DEM and you did not configure these systems during the software installation or you want to add additional Intuity systems after DEM is installed, go to "Procedure 10: Configure Additional Intuity DataStore Managers" on page 57.

Otherwise, go to "Procedure 11: Create a New DEM Administrator Login" on page 60.

Procedure 10: Configure Additional Intuity DataStore Managers

*** Note:** Perform this procedure if additional Intuity systems will be connected to DEM and you did not configure these systems during the software installation or you want to add additional Intuity systems after DEM is installed.

The software installation created, defined, and registered a DataStore Manager for each Intuity system you specified. If you want to attach additional Intuity systems to DEM, you must create, define, register, activate, and attach a DataStore Manager for each Intuity system.

To create, define, register, activate, and attach a DataStore Manager for each additional Intuity system:

1. Click the **Device Configurations** button on the toolbar.

   The Configuration Editor dialog box appears.

2. In the **Device Class** area, click the **DataStore Manager** option button.

3. Click the **Add** button.

   A dialog box appears, prompting you to enter the name of the configuration file.

4. Enter a name that can be easily associated with the specific Intuity system you are configuring, and click the **OK** button.

   The name you entered for the new configuration file is displayed and selected in the **Defined Configurations** list box.

5. In the **Defined Configurations** list box, select the Intuity DataStore Manager that was created during the software installation.

   The information for the selected file appears in the **Configuration Details** box. The Intuity DataStore Manager contains the common information that all Intuity DataStore Managers share.

6. Select all of the information in the **Configuration Details** box, and copy it to the Windows Clipboard.

7. In the **Defined Configurations** list box, select the Intuity DataStore Manager configuration you added in Step 4 of this procedure.

   The **Configuration Details** box is empty.

8. Click the mouse inside the **Configuration Details** box, and paste the information from the Windows Clipboard.

9. Make the following changes to the information in this file:

   a. In the **[_connection_]** section, enter the login (**login=**) for the Intuity system you want to use.

   b. In the **[_connection_]** section, enter the IP address (**Server=**) for the Intuity system you want to use.

   c. In the **[_connection_]** section, type ***password=%@INTUITY_PW%***.

   d. If you are using the IMAPI password, type ***IMAPIpassword=%@IMAPIpassword%*** at the bottom of the **[_connection_]** section.

   e. In the **[_variables_]** section, enter the messaging server name (**dsid=**) for the Intuity system you want to use to identify this Intuity system in LDAP.

   f. At the bottom of the **[_variables_]** section, type ***@INTUITY_PW=my_password***, where ***my_password*** is the password for the Intuity system you want to use.

   g. If you are using the IMAPI password, type ***@IMAPIpassword=my_password*** at the bottom of the **[_variables_]** section, where ***my_password*** is the IMAPI password for the Intuity system.

10. Click the **Save** button.

11. Click the **Done** button.

    The changes are saved for the new DataStore Manager configuration.

12. Click the **DataStore Managers** tab.

    The **DataStore Managers** tab appears.

13. Click the **Define DSM** button.

    The DSM Definition dialog box appears.

14. In the **DSM Name** box, enter the name (that is, messaging server ID) of the Intuity system that will use this DataStore Manager.

15. In the **DSM Type** box, enter ***Intuity***.

16. From the **Configuration ID** drop-down list box, select the Intuity DataStore Manager configuration you created in Step 4 of this procedure.

17. In the **Comment** box, you may enter notes about this DataStore Manager. The information you enter in this box is for your convenience only. DEM does not use this information.

18. Make sure the **Register with IMR** check box is enabled. (It is enabled by default.)

19. Click the **OK** button.

    The new DataStore Manager appears in the **DataStore Managers** list box. Its status is **Offline**.

    The new DataStore Manager is registered with DEM.

20. On the **DataStore Managers** tab, select the new Intuity DataStore Manager you created.

21. Click the **Activate** button.

    A yellow light appears next to the DataStore Manager, and the status changes to **Detached**.

22. Click the **Attach** button.

    The status changes to **Ready**. The Intuity DataStore Manager you created can now pass DEM data from the Synchronization Engine to the Intuity system.

Repeat Steps 1 through 22 for each Intuity system you want to configure.

When finished, go to "Procedure 11: Create a New DEM Administrator Login" on page 60.

Procedure 11: Create a New DEM Administrator Login

In this section, you will create a new DEM Administrator login and delete the default login. This new DEM Administrator login will be used by the DEM Administrator.

To create a new DEM Administrator login and delete the default login:

1. Click the **User Profiles** button on the toolbar.

   The User Profiles dialog box appears.

2. Click the **Add** button.

   The Add User dialog box appears.

3. In the **Username** box, enter the new login.

4. In the **Password** box, enter the password.

5. Click the **Superuser** check box.

   The **Superuser** check box must be enabled.

6. Click the **OK** button.

   The new login appears in the **Users** box.

7. In the **Users** box, select **Administrator**.

   The settings for the selected account appear in the **Security Profile** box.

8. Click the **Delete** button.

   The Confirm dialog box appears.

9. Click the **Yes** button.

   The selected account is removed from the **Users** box.

10. Click the **OK** button to close the User Profiles dialog box.

Go to "Procedure 12: Administer DEM" on page 61.

Procedure 12: Administer DEM

After you have completed Procedures 1 through 11, the Synchronization Engine, the DEFINITY DataStore Manager(s) and Intuity DataStore Manager(s) are in the ready state, and the LDAP Data Store is configured. You are ready to start running the Synchronization Engine, the DEFINITY DataStore Manager(s), and Intuity DataStore Manager(s), and to administer DEM. Refer to *Avaya Directory Enabled Management Administration*, which is a PDF that is located in the Docs folder in the DEM installation directory. This document describes how to manage DEM using the DEM Administrator application.

4 Troubleshooting

This chapter provides information that can assist you in solving problems you might encounter when you install and configure DEM initially. This chapter is divided into the following sections:

Refer to the appropriate section to find the information required to solve your particular problem.

Troubleshooting the Installation

This section describes problems you might encounter when trying to install the DEM software.

Problem 1: You receive the message: “Catastrophic Error” or “Error Extracting Support Files”

Perform the following steps:

1. Open Windows Explorer and delete the folder **Program Files\Common Files\InstallShield**.

   If you are unable to delete this folder:

   a. Press CTRL+ALT+DELETE to access Task Manager.

   b. From Task Manager, stop the ikernel process.

   c. Repeat Step 1.

2. Using Windows Explorer, delete the folder **Program Files\InstallShield\Installation Information**.

3. Install the DEM software.

Problem 2: You receive the message: “The InstallShield engine (iKernel.exe) could not be installed.”

Perform the following steps:

1. Press CTRL+ALT+DELETE to access Task Manager.

2. From Task Manager, stop the ikernel process.

Troubleshooting DEM Administrator Startup

This section describes problems you might encounter when trying to start DEM Administrator.

Problem 1: DEM Administrator will not start

If you are unable to log into the DEM Administrator application, and you receive a message such as "Security Mgr Proxy creation failed! Make sure the TAO_Implementation_Repository\n & TAO_Naming_Service services are running. If they are already running, refer to the Troubleshooting section in the DEM Administrator Guide for help," perform the following steps:

1. Open a command prompt window.
2. Type ***cd c:\dem\bin*** and press the ENTER key.
3. Type ***SSDem refresh n*** and press the ENTER key.
4. Log into DEM Administrator.
5. Make sure you can start SE and GWDSM.

Problem 2: DEM Administrator attempts to create the DSN

The system DSN is missing.

Manually install a system DSN named GWADMIN from the ODBC32 icon in the Windows Control Panel. This DSN should point at the mdb file in the \DEM\bin directory.

Problem 3: When you try to start DEM Administrator, the application "hangs"

This problem will occur if you uninstalled DEM and then reinstalled it in a different location.

Perform the following steps:

1. From the Start menu, select **Programs>Command Prompt**.

   The Command Prompt window appears.

2. At the command prompt, type ***kill TAO_GWMGR*** and press the ENTER key.

3. Close the Command Prompt window.

4. From the Start menu, select **Settings>Control Panel**.

   The Control Panel window appears.

5. Double-click on the **ODBC Data Sources** icon.

   The ODBC Data Source Administrator dialog box appears.

6. Click the **System DSN** tab.

   The **System DSN** tab appears.

7. Select **GWADMIN.mdb**, and click the **Configure** button.

   The ODBC Microsoft Access Setup dialog box appears.

8. Click the **Select** button.

   The Select Database dialog box appears.

9. Select **GWADMIN.mdb** in the bin directory where DEM was installed.

10. Click the **OK** button.

11. Click the **OK** button.

12. Click the **OK** button.

Problem 4: The system is unable to reattach to the running DSMs, SE, and DEM Administrator

Manually re-attach (activate) the relevant DSMs and the SE. After reactivating the DSMs and SE, refresh them.

Problem 5: A console alert appears, indicating that the connection to the monitor failed

The monitor process may have stopped, preventing message logging.

Perform the following steps:

1. Open Windows Task Manager and verify that the monitor is running as a process.
2. If it is running as a process, shut it down. If you are unable to shut the monitor process down from the Task Manager, use the "kill" program that is available in the Windows NT Resource Kit.
3. From the Start menu, select **Programs>Command Prompt**.

   The Command Prompt window appears.
4. At the command prompt, type ***tao list MONITOR_POA*** and press the ENTER key.

   This command shows whether the monitor is currently running.
5. If the last line displays "Running at endpoint...," type ***kill MONITOR_POA*** and press the ENTER key.
6. Close the Command Prompt window.
7. Restart DEM Administrator.

Problem 6: You receive a message that the security host is not found

The gwadmin.ini file is not found or the host entry is missing.

Perform the following steps:

1. Open the gwadmin.ini file in \DEM\bin.
2. Verify that the "host" entry in the "Initial" section is set to the host name on which DEM Administrator is running.

Problem 7: DEM Administrator does not respond

Perform the following steps:

1. Open a command prompt window.
2. Type ***cd c:\dem\bin*** and press the ENTER key.
3. Type ***SSDem refresh n*** and press the ENTER key.
4. Log into DEM Administrator.
5. Make sure you can start SE and GWDSM.

Problem 8: You receive a message that DEM Administrator cannot connect to a service

Perform the following steps:

1. Verify the service connection parameters from the Connection menu.
2. Restart DEM Administrator.
3. If DEM Administrator will not start, go to "Problem 1: DEM Administrator will not start" on page 65.

Troubleshooting DEM Administrator Login

This section describes problems you might encounter when trying to log into DEM Administrator.

Problem 1: Login Unsuccessful

When you try to log into DEM Administrator, you receive an error message stating that the login value(s) are incorrect or access is denied.

Make sure you enter the default login and password correctly. The login is case-sensitive. The default login ID is **Administrator**. The default password is **password**.

If you are still unable to log into DEM Administrator, the mdb file may be corrupted or missing. Perform the following steps:

1. Verify that the file GWADMIN.MDB is present. If this file is missing, restore it from a backup.
2. Use ODBC32 manager in Windows Control Panel to repair the GWADMIN.MDB database file.

Problem 2: DEM Administrator window does not appear after you log in

Perform the following steps:

1. Open a command prompt window.
2. Type ***cd c:\dem\bin*** and press the ENTER key.
3. Type ***SSDem refresh n*** and press the ENTER key.
4. Log into DEM Administrator.
5. Make sure you can start SE and GWDSM.

Problem 3: When you log in, you are prompted to enter a new password

Perform the following steps:

1. Verify the service connection parameters from the Connection menu.
2. Restart DEM Administrator.

Troubleshooting the Synchronization Engine

This section describes problems you might encounter with the Synchronization Engine.

Problem 1: Secondary level synchronization errors occur

The configuration data did not contain a "Maps" section.

Examine the Synchronization Engine's active configuration. There should be a section titled "Maps," which lists the maps that are active for the Synchronization Engine. (It can be specified in an "included" configuration.)

Problem 2: Controlled types are not found

The supplied configuration data did not contain a "Controlled Types" section.

Examine the Synchronization Engine's active configuration. There should be a section titled "Controlled Types," which lists the maps that are active for the Synchronization Engine. (It can be specified in an "included" configuration.)

Problem 3: The Lexer.cfg file is not found

The Synchronization Engine will not run without the lexer.cfg file. This file must be in the directory specified by the ROUTERHOME/home section/key pair in the current configuration. (It can be specified in an "included" configuration.)

Troubleshooting DataStore Managers

This section describes problems you might encounter with the DataStore Managers.

Problem 1: A DataStore Manager fails to activate, and the "<DSM Name> failed to launch properly" message appears

If only one particular DSM will not activate, perform the following steps:

1. Click the **Remove DSM** button.
2. Click the **Define DSM** button.
3. For the DSM Name, enter the same name of the DSM you deleted.
4. For the Configuration ID, enter the same ID of the DSM you deleted.
5. Click the **OK** button.
6. Try to activate this DSM. It the DSM does not activate, perform the following steps.

If the DSM does not activate, perform the following steps:

1. Open a command prompt window.
2. Type ***cd c:\dem\bin*** and press the ENTER key.
3. Type ***SSDem refresh n*** and press the ENTER key.
4. Log into DEM Administrator.
5. Make sure you can start SE and GWDSM.

   If these steps do not solve the problem, contact Avaya technical support.

Problem 2: A DataStore Manager fails to activate, and no message appears

Check that the "server" name for the DataStore Manager matches the CORBA registration name for the server. (This should always be the case for DataStore Managers configured during installation.) To check this information:

1. From the Start menu, select **Programs>Command Prompt**.

   The Command Prompt window appears.

2. At the command prompt, type ***c:\dem\bin*** and press the ENTER key.

3. Type ***tao list*** and press the ENTER key.

   A list of CORBA service names should appear.

4. Check that the failing DataStore Manager's "server" name value appears in the list.

5. If the failing DataStore Manager's "server" name value does not appear in the list, delete and redefine that DataStore Manager.

If these steps do not solve the problem, contact Avaya technical support.

Problem 3: A DataStore Manager activates, but it fails to attach or run

Perform the following steps:

1. Make sure the Synchronization Engine is running.

2. Make sure you can ping the IP address of the voice server to which you are trying to connect. If you can ping the IP address of the voice server, make sure you can telnet to the voice server using the IP address and the port (for example, ***telnet 135.9.193.930 9000***, where **9000** is the port).

3. Check the configuration values for the specified DSM. In particular, make sure that the connection parameters are correct. To check the configuration values, perform the following steps:

   a. Click the **Device Configurations** button.

   b. Select the **DataStore Manager for Device Class** option button.

c. Select your DSM in the Defined Configurations list box.

The settings for the selected DSM appear on the right.

d. Make your changes.

e. When finished, click the **Save** button.

f. Shut down and restart your DSM.

4. For DEFINITY DataStore Managers, check that the configuration contains the following lines:

```
[_includes_]
Include0=_DefinityRoot
```

5. For the PrimaryLDAP DataStore Manager, check that the configuration contains the following lines:

```
[_includes_]
Include0=_GWDSM
```

6. For the Intuity DataStore Managers, check that the configuration contains the following lines:

```
[_includes_]
Include0=_IntuityRoot
```

If these steps do not solve the problem, contact Avaya technical support.

Problem 4: The Protocol Adapter module failed to load

When this message appears, the DataStore Manager is unusable. The following conditions can cause this error:

- The DataStore Manager configuration specified an incorrect driver file in the Protocol section.
- The DataStore Manager configuration is missing a driver key in the Protocol section.
- The driver file specified in the DataStore Manager configuration is correct, but that file is missing.

Perform the following steps:

1. Verify that the configuration specified is the correct configuration for this DataStore Manager.
2. Verify that the name of the Protocol Adapter is correct.
3. Verify that the driver key is specified in the [_Protocol_] section of the DataStore Manager. (It can be specified in the an “included” configuration.)
4. Verify that the specified driver is a dynamic link library (DLL) file and is located in \DEM\bin.

Troubleshooting GWAgent

Perform the steps in this procedure if:

- you are using an LDAP client pointing to DEM's port 4000, and DEM's GWAgent is not responding to your client's LDAP calls
- you cannot even connect to DEM on port 4000 (GWAgent).

Perform the following steps:

1. Verify that the LDAP login parameters are correct. See Step 8 in "Changing LDAP Settings for DEM" on page 79 to view the LDAP settings.
2. Verify that you set default triggers. (See the GWAgent tab in DEM Administrator.)
3. Verify whether you are changing objects (such as users or inetorgpersons) outside of the default triggers that are set. If you are changing objects outside of the default triggers, you must set custom triggers on the GWAgent tab. Perform the following steps:
   a. Click the **Connect** button on the GWAgent tab. If you are not connect already to GWAgent Admin port 4001, DEM will display that information on the bottom of this tab.
   b. Click **Populate**.
   c. Click the **Add** button.
   d. Enter the full DN of the LDAP node for which you want DEM to monitor changes.
   e. Click the **OK** button.
   f. Click the **Commit** button.
4. If you are still encountering difficulties, perform the following steps to start GWAgent:
   a. From the Services window, stop the **Gateway LDAP Agent** service.
   b. Right-click the **Start** button on the Windows task bar, and select **Open All Users**.

c. Navigate to Programs\Avaya\Directory Enabled Management.

d. Right-click **Start GWAgent**, select **Properties**, and copy the "Target" string.

e. Open a command prompt window.

f. Type ***cd <install directory>\dem\bin*** and press the ENTER key.

g. Copy the Target string to the command line, and press the ENTER key.

You should see "Waiting for client connections" on the last line. If not, an error message should be displayed, indicating the cause of the problem.

Troubleshooting the Scheduler

This section describes problems you might encounter when scheduling tasks with DEM Administrator.

Problem 1: Scheduled events will not run

The mdb file is corrupted or missing.

Perform the following steps:

1. Verify that the file GWADMIN.MDB is present. If this file is missing, restore it from a backup.
2. Use ODBC32 manager in Windows Control Panel to repair the GWADMIN.MDB database file.

Troubleshooting Transactions Using DEM Logs

If you make a change from LDAP or the voice system and your change does not work, perform the following steps:

1. Verify that your voice system DSM and GWDSM are in the running state.
2. If you are making a change from LDAP port 4000, verify that GWAgent is running. See "Troubleshooting GWAgent" on page 76.
3. If you are making a change from LDAP port 4000, verify that the voice system accepted your change.

   Full logs of all transactions are located in the directory <install directory>:\dem. There is a log for each DSM and the Synchronization Engine (GWSE). A change from LDAP port 4000 takes the following path:

   GWDSM.log>GWSE.log>YourVoiceSystemDSM.log

   A change from the voice system takes the following path:

   YourVoiceSystemDSM.log>GWSE.log>GWDSM.log

   Immediately after making a change to LDAP or a voice system, open each log to see where the problem occurs. The latest transaction appears at the bottom of each log.

Changing LDAP Settings for DEM

If you discover that your LDAP login parameters are incorrect after you install DEM, you must change these login parameters in the following locations:

- PrimaryLDAP configuration
- GWAgent settings

Perform the following steps:

1. Log into DEM Administrator.
2. Click the **Device Configurations** button.
3. Select the **Datastore Managers for Device Class** option button.
4. Under Defined Configurations, select **PrimaryLDAP**.
5. In the Configurations Details box, change all required login parameters. To change the password, select the **@LDAP_PW=<encrypted value>** in the "secured elements" list box, which is located below the Configurations Details list box, and click **Modify Key**.
6. Click the **Save** button, and then click the **Done** button.
7. Shut down and then restart your GWDSM DSM.
8. Click on the GWAgent tab in DEM Administrator.
9. Click the **Startup** button.
10. Click the **Browse** button and navigate to the directory <install directory>\dem\bin.
11. Click the **OK** button.
12. Modify the LDAP settings.
13. Click the **OK** button.
14. Click **Set Default** to reset triggers. This will automatically restart the Gateway LDAP Agent service as well.

Problems Modifying an Object via LDAP Port 4000 with Active Directory and ADAM

*** Note:** This section applies to Active Directory and ADAM users only.

Be aware that you may need to specify the "modtype=strict" parameter for the GWDSM. The problem may be that during a Modify operation from an LDAP client pointing to DEM's LDAP port 4000, Active Directory and ADAM *do NOT require* the object class to be sent as one of the attributes. During an Add operation, Active Directory and ADAM *require* the object class to be sent as one of the attributes. This is the only case with Active Directory and ADAM. The GWDSM.log file would contain an error message such as:

-E:08/23/04-10:23:12 LDAP modify failed:_ModifyObject: 19|DSM|GWDSM|TID:868

Therefore, on a Modify operation you must configure DEM to use the "modtype=strict" configuration so that the objectclass is not sent from DEM GWDSM as one of the attributes.

Perform the following steps:

1. On the toolbar, click the **Device Configurations** button.

   The Configuration Editor window appears.

2. In the Device Class area, click the **DataStore Manager** option button.

   The Defined Configurations list box displays the defined DataStore Manager configurations.

3. Select **PrimaryLDAP**.

4. Add the following key under the [_Root_] section: **modtype=strict**.

5. Click the **Save** button.

6. Click the **Done** button.

7. Shut down and restart the GWDSM DSM.

Glossary and Abbreviations

C

CD ROM
Compact-disk read-only memory, An optical computer disk widely used for distributing and installing software and electronic documentation.

client
An application that runs on one processor while drawing on data or other resources that are on a server located elsewhere. A DEM client is a workstation capable of modifying DEM data.

configuration file
A file that describes how a DataStore Manager (DSM) or Synchronization Engine (SE) operates at run time.

D

DataStore Manager (DSM)
A software process that interfaces with a device type (such as a DEFINITY system, an Intuity system, a PC running Avaya Site Administration, or an LDAP server) that connects to the DEM. DataStore Managers enable different DEM devices to communicate with each other.

Directory Enabled Management (DEM)
A software application that "LDAP-enables" DEFINITY system data and Intuity system data, providing real-time integrated directory-based read/write access to DEFINITY data, Intuity data, and data derived from enterprise sources (such as corporate directories).

distributed application
A computer application that runs on one or more clients and uses shared resources, such as databases. These resources reside on a common server. Distributed design lets multiple users run programs using common, centrally maintained files.

domain
An addressable location on a network, such as a group of computers, single computer, or subdirectory. See Domain Name Server (DNS).

Domain Name Server (DNS)
An Internet computer that maintains a database of domain names.

DNS
See Domain Name Server (DNS).

DSM
See DataStore Manager (DSM).

E

Ethernet
A local area network (LAN) that works over short distances on twisted-pairs or coaxial cables at speeds up to 10 mbps or 100 mbps.

H

host
A server.

host name
The name of the PC on which the DEM software is installed.

I

IP (Internet Protocol) address
A 32-bit number that uniquely identifies endpoints on the Internet, commonly specified in the form $n_1.n_2.n_3.n_4$ where each n_n is a decimal number between **0** and **255**. Part of the IP address represents the address of a local network's gateway to the Internet and part represents the host-machine address within that local network. The available bits are apportioned to the network address or local address using a system of classes. The Class A addresses used by the largest organizations on the Internet reserve the first 8 bits for the network portion of the address and remaining 24 for the host machine. Class B addresses, the most common class, assign 16 bits to the network and 16 to the host machine. The Class C addresses used by small networks reserve the first 24 bits for the network and the remaining 8 bits for the host.

L

LAN
See local area network (LAN).

LDAP
See lightweight directory access protocol.

Lightweight Directory Access Protocol (LDAP)
An open Internet standard used to manage DEM data.

local area network (LAN)
A short-range data communication network linking computers and peripherals, such as printers. Ethernet and Token-Ring are common LAN architectures.

N

Network Interface Card (NIC)
A circuit board that can be fitted to a personal computer (PC) to allow the PC to communicate with other machines on a network.

NIC
See Network Interface Card (NIC).

P

PBX
Private Branch Exchange: a customer-owned telephone switch that connects a company's internal telephone network with the local telephone service provider's central office. The DEFINITY system is a PBX.

S

SE
See Synchronization Engine (SE).

server
Any system that maintains and administers files that are used by independent client applications.

Synchronization Engine (SE)
A software process that synchronizes changes between native device data (for example, data from a voice server) and data from enterprise directories based on the routing and mapping rules you define.

T

TCP/IP
Transmission Control Protocol/Internet Protocol: a standard that lets different computer hardware and different operating systems (such as PCs, Apple computers, UNIX workstations, and mainframes) communicate with each other over a network. TCP/IP is the most complete, most widely accepted network protocol currently available.

W

WAN
See wide area network.

wide area network
A data network that connects local area networks (LANs) using common-carrier telephone lines, bridges, and routers.

Index