Avaya Directory Enabled Management Release 2.0

Administration

555-038-501
Issue 7
January 2004

Notice

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

Warranty

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

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Standards Compliance

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

Product Safety Standards

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

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

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

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

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

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

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

The LASER devices operate within the following parameters:

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

Luokan 1 Laserlaite

Klass 1 Laser Apparat

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

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

Federal Communications Commission Statement

Part 15:

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

Part 68: Answer-Supervision Signaling

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

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

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

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

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

REN Number

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

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

For G350 and G700 Media Gateways:

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

For all media gateways:

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

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

Means of Connection

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

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

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

For G350 and G700 Media Gateways:

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

For all media gateways:

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

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

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

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

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

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

Canadian Department of Communications (DOC) Interference Information

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

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

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

Declarations of Conformity

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

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

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

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

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

European Union Declarations of Conformity

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), part of Avaya Integrated Management Release 2.0. This chapter provides an introduction to the structure and assumptions of this guide.

The Purpose of this Guide

This guide describes how to manage and maintain Avaya Directory Enabled Management (DEM) using the DEM Administrator application. Before you can perform the procedures in this guide, the DEM software must be installed and configured.

Who Should Use this Guide

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

- Microsoft® Windows® Server 2000
- One of the following LDAP services:
  - IBM® Directory Server (IDS) 5.1
  - Microsoft Active Directory™
  - Netscape® Directory Server Version 4.12
  - Novell® NDS® eDirectory™ 8.x
  - Sun™ ONE Directory Server 5.1
- local area networks (LANs)
- voice server administration
- 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 managing DEM.
- **Chapter 1: Introduction** - This chapter provides a brief introduction to DEM.
- **Chapter 2: Getting Started**- This chapter describes the DEM Administrator window and the responsibilities of the DEM Administrator.
- **Chapter 3: Working with DataStore Managers** - This chapter describes how to create, modify, and control DataStore Managers.
- **Chapter 4: Working with Synchronization Engines** - This chapter describes how to create, modify, and control Synchronization Engines.
- **Chapter 5: Working with Configurations** - This chapter describes how to create and modify DataStore Manager configurations and Synchronization Engine configurations.
- **Chapter 6: Working with DEM Maps**- This chapter describes how to create and modify DEM maps.
- **Chapter 7: Managing GWAgent**- This chapter describes how to set up GWAgent to monitor LDAP data.
- **Chapter 8: Scheduling Administration Events** - This chapter describes how to set the DEM Administrator application to run events automatically at specified times.
- **Chapter 9: Using the Message Log** - This chapter describes how to access the DEM Message Log and manage DEM messages.
- **Chapter 10: Managing DEM Administrator Users**- This chapter describes how to add and modify DEM Administrator login accounts.
- **Chapter 11: Troubleshooting** - This chapter provides information about possible error conditions and how to respond to them when you manage DEM via the DEM Administrator window.
- **Appendix A: Security Keys**- This appendix defines the contents of the DEM security map.

Related Documentation/Training

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

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

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

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

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

Conventions Used

The following conventions are used in this document:

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

Online Help

To access the procedures on how to use the DEM Administrator application, consult the online help. You can access the online help by pressing the F1 key on your keyboard or choosing **Contents** from the **Help** menu.

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)

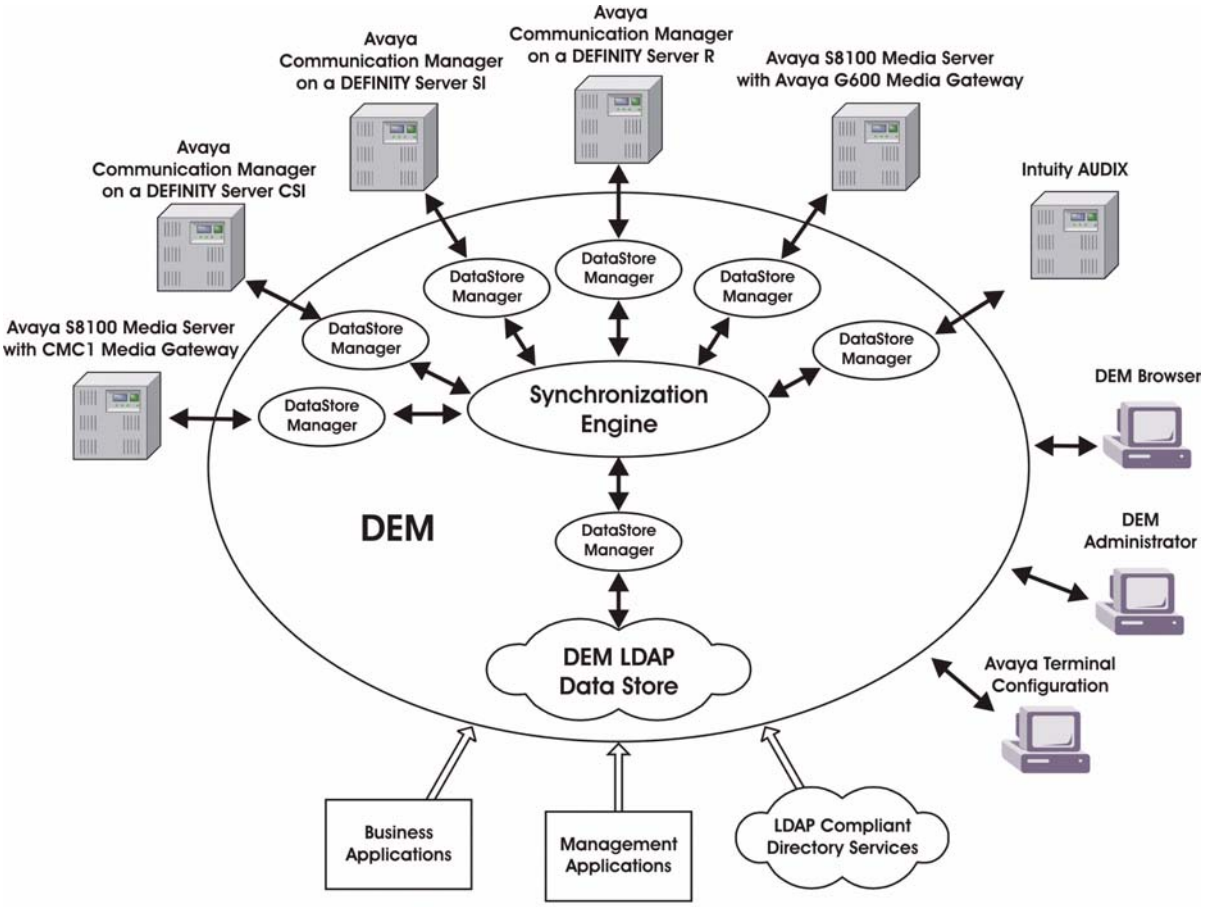
Avaya Directory Enabled Management (DEM) is software that "LDAP-enables" voice server data and Intuity system data, providing real-time, integrated, directory-based read/write access to voice server data, Intuity data, and data derived from enterprise sources (such as corporate databases). DEM interfaces 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
- DEM Browser

Figure 1-1 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 a 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 has been 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=…
```

DEM Browser

DEM Browser is a web-based application that enables users to view and modify data in the DEM LDAP data store. Using the DEM Browser, users can perform the following tasks in the LDAP data store:

- view LDAP objects
- search for LDAP objects
- add LDAP objects
- modify LDAP objects
- delete LDAP objects

Supported DEFINITY Objects

DEM supports the DEFINITY objects listed below. For the most current list, go to *http://www.avaya.com/support*.

Table 1. Supported DEFINITY Objects

DEM Name	Description
definityStation	Stations
definityTrunkgroup	Trunk Groups
definityPersonalcoline	Personal Central Office Line
definityDialplan	Dial Plan
definityCosGroup	Class of Services
definityAttendant	Attendants
definityCovremoteGroup	Coverage Remote Group
definityAbbrdialenh	Abbreviated Dial Enhanced
definityAbbrdial7103a	Abbreviated Dial 7103a
definitySADatamodule	Standalone Data Modules
definityCabinet	Cabinets
definityCircuitpacks	Circuit Packs
definityRoutepat	Route Patterns
definityAnnouncement	Announcements
definityTenant	Tenants
definityIPNetworkRegion	IP Network Region
definityACDAgent	ACD Agent
definityHuntgroup	Hunt Groups
definityCor	Class of Restrictions
definityPickupgrp	Pickup Groups
definityExtpckgrp	Extended Pickup Groups
definityCovansgrp	Coverage Answer Groups
definityCovpath	Coverage Paths
definityCovtod	Coverage for Time of Day
definityPublicUnknownNumbering Group	Public Unknown Numbering Group

Table 1. Supported DEFINITY Objects

DEM Name	Description
definityCamaNumberingGroup	Cama Numbering Group
definityIpNetworkMapGroup	IP Network Map Group
definityVectorCall	Vector Calls
definityVectorDirectoryNumber	Vector Directory Numbers

Supported Intuity Objects

The DEM supports the Intuity objects listed below. For the most current list, go to *http://www.avaya.com/support*.

Table 2. Supported Intuity Objects

DEM Name	Description
intuitySubscriber	Subscribers on the Intuity system

New Features in This Release

DEM has the following new features:

- **Enhanced Goal Oriented State Management (GOSM)**

  In Release 2.0, GOSM has been 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=…

- **Support for Additional DEFINITY Objects and Attributes**

  DEM now supports the following DEFINITY objects:

  — definityVectorCall

  — definityVectorDirectoryNumber

  DEM now supports the following new attributes in the definityACDAgent object:

  — deftyAgentSkillNumber1-60

  — deftyAgentReserveLevel1-60

  — deftyAgentSkillLevel1-60

  — deftyAgentPercentageAlloc1-60

- **Support for Novell NDS eDirectory 8.x**

  DEM now supports Novell NDS eDirectory 8.x.

- **Support for IBM Directory Server (IDS) 5.1**

  DEM now supports IBM Directory Server (IDS) 5.1.

2 Getting Started

This chapter provides the following information:

- how to run the DEM Administrator application
- components of the DEM Administrator window
- the administration tasks you should perform regularly

Starting DEM Administrator

To start DEM Administrator:

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

   The Avaya Directory Enabled Management Administrator Login dialog box appears.

2. In the **Username** box, enter your username.
3. In the **Password** box, enter your password.
4. Click the **OK** button.

The Avaya Directory Enabled Management Administrator window appears.

DEM Administrator Window

The DEM Administrator window consists of the following components:

- **Synchronization Engines** tab
- **DataStore Managers** tab
- **GWAgent** tab
- Toolbar

Synchronization Engines Tab

The **Synchronization Engines** tab enables you to create, modify, delete, and control Synchronization Engines. You can have multiple Synchronization engines defined, but only one Synchronization Engine can be active.

DataStore Managers Tab

The **DataStore Managers** tab enables you to create, modify, delete, and control DataStore Managers. Unlike Synchronization Engines, multiple DataStore Managers can be active at the same time.

GWAgent Tab

The **GWAgent** tab enables you to configure DEM to monitor your company LDAP server.

Toolbar

The DEM Administrator Toolbar contains the following buttons.

Maps Button

The **Maps** button opens the Mapping dialog box, which enables you to create and modify map files that map DEM types to other DEM types.

Device Config Button

The **Device Configurations** button opens the Configuration Editor dialog box. From the Configuration Editor dialog box, you can:

- Add, modify, delete, import, and export Synchronization Engine configurations
- Add, modify, delete, import, and export DataStore Manager configurations

Configurations describe how the DataStore Managers and Synchronization Engines operate at run time.

Logs Button

The **Logs** button opens the Message Log dialog box, which displays messages from DEM that match the criteria you specify. From this dialog box, you can:

- Delete all entries from the log
- Refresh the log
- Specify the criteria of the messages you want displayed in the Message Log dialog box. You can filter the messages according to
  - — device class (that is, messages from DataStore Managers and/or the Synchronization Engine)
  - — message type (for example, transaction and device error)
  - — lowest severity level to display
- Set DEM Administrator to send email to people you specify when messages match the criteria you specify. You can set email to be sent according to
  - — message source (DataStore Managers, and/or the Synchronization Engine)
  - — message type
  - — lowest severity level

Reference Table Button

The **Reference Table** button opens the Map Rule Reference Data dialog box, which enables you to create a table of auxiliary reference data that can be accessed by the maps. For example, you can use this button to map Intuity subscribers to DEFINITY stations.

Scheduler Button

The **Scheduler** button opens the GW Event Scheduling dialog box, which enables you to schedule DEM events (such as synchronizing the data or running a DataStore Manager). You can run the events immediately or set them to be performed at a specific time (and frequency). You can also set the DEM Administrator application to send email to a specific person when an event fails.

User Profiles Button

The **User Profiles** button opens the User Profiles dialog box, which enables you to administer DEM user accounts. From this dialog box, you can:

- add user accounts
- set the privileges of each account
- change the password of each account
- delete a user account

Administrator's Tasks

Once your system has been installed and configured initially, you should perform the following tasks regularly:

- **Access the Message Log and verify that no severe or fatal messages have been received.**

  Refer to Chapter 9 to view the Message Log and to set the DEM Administrator application to send you email automatically if severe or fatal messages occur.

- **Synchronize the data.**

  The frequency of the data synchronization depends on the number of data changes that are made and how often your devices are "down." It is recommended that you perform synchronizations at periodic intervals.

3 Working with DataStore Managers

DataStore Managers are software processes that interface with each device type that connects to DEM. A DataStore Manager enables 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 virtual types, enabling all DEM devices to communicate with one another.

Each device on DEM must have its own DataStore Manager, which monitors that device. DataStore Manager performs the following tasks:

- Receives data change notifications from the device it monitors
- Packages the relevant data into a ChangeDescriptor
- Forwards the change descriptor to the Synchronization Engine for subsequent routing to other interested DataStore Managers
- Receives and processes updates from the Synchronization Engine

As the DEM Administrator, it is your responsibility to define, activate, attach, run, and monitor the DataStore Managers for each DEM device. DataStore Managers will not perform their tasks unless they are running. So, as part of your duties, you must make sure the DataStore Managers are running.

An active DataStore Manager can be in several states. Table 3 shows and describes the possible DataStore Manager states.

Table 3. Description of DataStore Manager States

DataStore Manager State	Action
Offline	DataStore Manager is not running.
Detached	The DataStore Manager is running and is initialized with its configuration data. To place a DataStore Manager in the Detached state, use the **Active** button (if the DataStore Manager is in the Offline state) or the **Detach** button (if the DataStore Manager is in the Running state).
Ready	The DataStore Manager is attached to the Synchronization Engine and its native device. (For example, the DEFINITY DataStore Manager attaches to the voice server.) To place a DataStore Manager in the Ready state, use the **Attach** button.
Running	The DataStore Manager has a two-way communication with both the Synchronization Engine and the DataStore Manager's native device (for example, a voice server). To place a DataStore Manager in the Running state, use the **Run** button. In a typical configuration, all of your DataStore Managers should be in the Running state.
Synching	The DataStore Manager has a two-way communication with both the Synchronization Engine and the DataStore Manager's native device, and the DataStore Manager is synchronizing the DEM objects you requested. When a synchronization is complete, the DataStore Manager automatically changes to the Running state.To place a DataStore Manager in the Synching state, use the **Synchronize** button.

Managing DataStore Managers

This section describe how to

- define DataStore Managers
- modify DataStore Managers
- delete DataStore Managers

Define a DataStore Manager

Perform this procedure to create new DataStore Managers. You must perform this procedure when you add a new device (such as a voice server) to DEM.

When you define a DataStore Manager, you make a new service known to the CORBA orb, which associates the DataStore Manager name to a physical process that runs on the network.

Before you can run an installed DataStore Manager, you must define it.

To define a DataStore Manager:

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

   The **DataStore Managers** tab appears.

2. Click the **Define DSM** button.

   The DSM Definition dialog box appears.

3. In the **DSM Name** box, enter the name of the DataStore Manager.

4. In the **DSM Type** box, enter the type of DataStore Manager you are defining (that is, a DEFINITY DSM, an Intuity DSM, an LDAP server DSM, or an Adapter DSM).

5. From the **Configuration ID** drop-down list box, choose the appropriate configuration for this DataStore Manager.

   The DataStore Manager configuration contains the runtime instructions and configuration settings that the DataStore Manager you are defining will use.

   The configurations can be viewed, modified and imported via the Configuration Editor. See "Managing DataStore Manager Configurations" on page 51 for more information.

6. 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.

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

8. Click the **OK** button.

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

After you install a DataStore Manager, you should activate it. See "Activate a DataStore Manager" on page 32.

Modify a DataStore Manager

You can modify the following attributes of a defined DataStore Manager:

- name
- type (for example, DEFINITY, Intuity, LDAP server, or Adapter)
- DSM configuration this DataStore Manager uses
- comments

You can modify the information for a DataStore Manager that is currently running. However, the information will not be updated until you restart the DataStore Manager.

To modify a DataStore Manager:

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

   The **DataStore Managers** tab appears.

2. Select the DataStore Manager you want to modify.

3. Click the **Modify DSM** button.

   The DSM Definition dialog box appears, displaying the current settings for the selected DataStore Manager.

4. Make your changes.

5. When finished, click the **OK** button.

Delete a DataStore Manager

This procedures enables you to delete a DataStore Manager definition from the DEM Administrator window. However, the DataStore Manager is still installed on the host PC.

To delete a DataStore Manager:

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

   The **DataStore Managers** tab appears.

2. Select the DataStore Manager you want to delete.

3. Click the **Remove DSM** button.

   A warning dialog box appears, prompting you to confirm your action.

4. Click the **Yes** button.

   The DataStore Manager is removed from the DataStore Managers list box.

Controlling DataStore Managers

This section describes how to

- activate a DataStore Manager
- attach/re-attach a DataStore Manager
- synchronize a DataStore Manager
- run a DataStore Manager
- shut down a DataStore Manager
- detach a DataStore Manager
- reinitialize a DataStore Manager
- view the status of the DataStore Managers

Activate a DataStore Manager

You must activate a DataStore Manager before you can attach it and run it. When a DataStore Manager is activated, it is initialized with its configuration data.

To activate a DataStore Manager:

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

   The **DataStore Managers** tab appears.

2. In the DataStore Managers list box, select the DataStore Manager you want to activate.

3. Click the **Activate** button.

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

   Now, you can attach the DataStore Manager.

Attach/Re-attach a DataStore Manager

You can perform this procedure only for DataStore Managers that are currently detached.

Before you can run a DataStore Manager, you must attach it. Attaching the DataStore Manager establishes the connection between the DataStore Manager and the Synchronization Engine. The DataStore submits its "subscription information" to the Synchronization Engine. The subscription information specifies to the Synchronization Engine which DEM object types the DataStore Manager wants to receive notifications about.

To re-attach a DataStore Manager:

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

   The **DataStore Managers** tab appears.

2. In the DataStore Managers list box, select the DataStore Manager you want to re-attach. The status of the selected DataStore Manager is "Detached."

3. Click the **Attach** button.

   The Status column displays "Ready," and a yellow light appears in front of the name of the DataStore Manager.

   Now, you can run this DataStore Manager.

Run a DataStore Manager

When a DataStore Manager is running, it is able to send ChangeDescriptors to the Synchronization and receive ChangeDescriptors from the Synchronization Engine.

To run a DataStore Manager:

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

   The **DataStore Managers** tab appears.

2. In the DataStore Managers list box, select the DataStore Manager you want to run.

3. Click the **Run** button.

   The Status column displays "Running" and a green light appears in front of the name of the DataStore Manager.

Synchronize a DataStore Manager

This procedure enables you to synchronize the data for the selected DataStore Manager. During a synchronization, the selected DataStore Manager publishes a complete image of each object type you specify. The DataStore Manager then sends these objects to the Synchronization Engine, which routes these objects to the appropriate DataStore Managers.

*** Note:** This procedure will cause traffic on your LAN.

The DataStore Manager you want to synchronize must be running.

To synchronize a DataStore Manager:

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

   The **DataStore Managers** tab appears.

2. In the DataStore Managers list box, select the DataStore Manager you want to synchronize.

3. Click the **Synchronize** button.

   The Synchronize Selected DSM dialog box appears. The **Available Types** list box displays the DEM types that the selected DataStore Manager can publish to DEM. (These DEM types are specified in the Publish section of the associated DataStore configuration.)

4. In the **Available Types** list box, select the DEM type you want to synchronize, and click the **Add** button.

   The selected type appears in the **Selected Types** list box.

   If you want to synchronize another type, repeat step 4. If you want to select all of the types displayed in the **Available Types** list box, click the **Add All** button.

5. If you want to optimize, click the **Optimize** check box. Optimization is useful for saving time with a DataStore Manager that has a history log and can determine which objects the system is out of sync with. If the DataStore Manager does not have a history log, it will ignore this request.

6. Click the **Sync!** button.

   The Status column displays “Running” and a green light appears in front of the name of the DataStore Manager.

   To view the status of the synchronization, click the **Refresh** button or click the **Poll Status** check box.

Shut Down a DataStore Manager

This procedure stops the selected DataStore Manager. After the selected DataStore Manager is shut down, the Synchronization Engine stops sending ChangeDescriptors to it.

*** Note:** This procedure terminates the DataStore Manager process.

To shut down a DataStore Manager:

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

   The **DataStore Managers** tab appears.

2. In the DataStore Managers list box, select the DataStore Manager you want to shut down.

3. Click the **Shutdown** button.

   The Status column displays "Offline" and a gray light appears in front of the name of the DataStore Manager.

Detach a DataStore Manager

This procedure breaks the connection between the selected DataStore Manager and the Synchronization Engine. Once this connection is terminated, the Synchronization Engine stops sending ChangeDescriptors to the DataStore Manager.

To detach a DataStore Manager:

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

   The **DataStore Managers** tab appears.

2. In the DataStore Managers list box, select the DataStore Manager you want to detach.

3. Click the **Detach** button.

   The Detach DSM dialog box appears.

4. If you want DEM to queue messages so this DataStore Manager can view the information it missed while it is detached, click the **Queue at Router?** check box.

5. Click the **Detach** button.

   The Status column displays "Detached" and a yellow light appears in front of the name of the DataStore Manager.

Reinitialize a DataStore Manager

Perform this procedure if you made either of the following changes to a running DataStore Manager and you want the changes to take effect:

- changed the configuration ID that the DataStore Manager is using
- modified the contents of the configuration file that the DataStore Manager is using

To reinitialize a DataStore Manager:

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

   The **DataStore Managers** tab appears.

2. In the DataStore Managers list box, select the DataStore Manager you want to reinitialize.

3. Click the **Re-Initialize** button.

View the Status of the DataStore Managers

You can either view the current status of the DataStore Managers or poll the DataStore Managers automatically at a specified time interval.

View the Current Status of DataStore Managers

To view the current status of the DataStore Managers:

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

   The **DataStore Managers** tab appears.

2. Click the **Refresh** button.

   The current status of each DataStore Manager appears.

Poll DataStore Managers at a Specified Interval

In this procedure, the DataStore Managers are polled for status at the time interval you specify. Be aware that this will create additional traffic on your LAN.

To poll the DataStore Managers for status at a specified interval:

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

   The **DataStore Managers** tab appears.

2. In the **seconds** box in the DSM Status area, enter the time interval to update the status. The minimum time interval is 5 seconds.

3. Click the **Poll Status every** check box. The status is updated at the time interval you specified.

When you are finished, click the **Poll Status every** check box (that is, disable it).

4 Working with Synchronization Engines

The Synchronization Engine 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.

The Synchronization Engine performs the following tasks:

- Receives change notifications (ChangeDescriptors) from DataStore Managers
- Determines which DataStore Managers are interested in the ChangeDescriptor
- Translates (maps) the objects in the ChangeDescriptors into objects that the interested DataStore Managers (subscribers) require
- Routes the ChangeDescriptors in the proper sequence

As the DEM Administrator, it is your responsibility to define, activate, and monitor the Synchronization Engine. The DEM will not function properly unless a Synchronization Engine is activated. Only one Synchronization Engine can be active at a time.

Managing Synchronization Engines

This section describes how to

- define a Synchronization Engine
- modify a Synchronization Engine
- delete a Synchronization Engine

Define a Synchronization Engine

To define a Synchronization Engine:

1. Click the **Synchronization Engines** tab.

   The **Synchronization Engines** tab appears.

2. Click the **Define SE** button.

   The SE Definition dialog box appears.

3. In the **SE Name** box, enter the name of the Synchronization Engine.

4. In the **Host PC** box, enter the name of the PC on which the Synchronization Engine is installed.

5. From the **Config. ID** drop-down list box, choose the appropriate Synchronization Engine configuration.

   The Synchronization Engine configuration contains the runtime instructions and configuration settings that the Synchronization Engine you are defining will use.

   The configurations can be viewed, modified, and imported via the Configuration Editor. See Chapter 5 for more information.

6. Click the **OK** button.

   The new Synchronization Engine appears in the Synchronization Engines list box. The Status column displays “Offline.”

Modify a Synchronization Engine

You can modify the following attributes of a defined Synchronization Engine:

- name
- PC on which the Synchronization Engine is installed
- Synchronization Engine configuration this Synchronization Engine uses

To modify a Synchronization Engine:

1. Click the **Synchronization Engines** tab.

   The **Synchronization Engines** tab appears.

2. Select the Synchronization Engine you want to modify.
3. Click the **Modify SE** button.

   The SE Definition dialog box appears, displaying the current settings for the selected Synchronization Engine.

4. Make your changes.
5. When finished, click the **OK** button.

Delete a Synchronization Engine

To delete a Synchronization Engine:

1. Click the **Synchronization Engines** tab.

   The **Synchronization Engines** tab appears.

2. Select the Synchronization Engine you want to delete.
3. Click the **Remove SE** button.

   A warning dialog box appears, prompting you to confirm your action.

4. Click the **Yes** button.

   The Synchronization Engine is removed from the Synchronization Engines list box.

Controlling Synchronization Engines

This section describes how to

- activate a Synchronization Engine
- shut down a Synchronization Engine
- reinitialize a Synchronization Engine

Activate a Synchronization Engine

Only one Synchronization Engine can be active.

To activate a Synchronization Engine:

1. Click the **Synchronization Engines** tab.

   The **Synchronization Engines** tab appears.

2. In the Synchronization Engines list box, select the Synchronization Engine you want to activate.

3. Click the **Activate** button.

   The Status column displays “Active” and a green light appears in front of the name of the Synchronization Engine.

Shut Down a Synchronization Engine

This procedure stops the selected Synchronization Engine. After the selected Synchronization Engine is shut down, it stops sending and receiving ChangeDescriptors.

To shut down a Synchronization Engine:

1. Click the **Synchronization Engines** tab.

   The **Synchronization Engines** tab appears.

2. In the Synchronization Engines list box, select the Synchronization Engine you want to shut down.

3. Click the **Shutdown** button.

   The Status column displays “Offline” and a gray light appears in front of the name of the Synchronization Engine.

Reinitialize a Synchronization Engine

Perform this procedure if you made one of the following changes to an active Synchronization Engine, and you want the changes to take effect:

- changed the configuration ID that the Synchronization Engine is using
- modified the contents of the configuration file that the Synchronization Engine is using

You can only reinitialize a Synchronization Engine that is active.

To reinitialize a Synchronization Engine:

1. Click the **Synchronization Engines** tab.

   The **Synchronization Engines** tab appears.

2. In the Synchronization Engines list box, select the Synchronization Engine you want to reinitialize.

3. Click the **Re-Initialize** button.

5 Working with Configurations

Both DataStore Managers and Synchronization Engines have configuration files, which determine how the associated DataStore Manager or Synchronization Engine operates at run time. This chapter describes how to manage these configurations.

Managing Synchronization Engine Configurations

A Synchronization Engine configuration contains the information that determines how the associated Synchronization Engine operates at run time. When you define a Synchronization Engine, you specify the configuration you want that Synchronization Engine to use.

A Synchronization Engine configuration consists of the following sections:

- **Control Types**

  The Control Types section lists the DEM types for which the Synchronization Engine must find a master. (The master is a DataStore Manager.) If the Synchronization Engine cannot find the corresponding master for the transaction, that transaction fails.

- **Maps**

  The Maps section lists the maps that are currently running. Each line in this section provides the following information for each map:

  — name of the map

  — whether the map is a master or slave

  — from type

  — to type

  — 0 (reserved field)

- **Routerhome**

  The Routerhome section provides the required paths for the Synchronization Engine.

- **Rules for specific objects**

  The Rules section provides the rules that the Synchronization Engine will apply to specific objects when the Synchronization Engine receives or creates these objects.

- **Include**

  The Include section provides the capability to include other files as part of the Synchronization Engine configuration. However, if there are any duplicates in the Include file(s), the information in the Synchronization Engine configuration overrides the same information in the Include file(s). If Include files are used, DEM Administrator merges the Synchronization Engine configuration and the Include file(s) during initialization. If there are any duplicate keys in the Synchronization Engine configuration and the Include file(s), the duplicate information in the Include file(s) is not used. The result of the merge is one configuration set that the Synchronization Engine uses while it is running.

This section describes how to

- create a Synchronization Engine configuration
- modify a Synchronization Engine configuration
- import information into a Synchronization Engine configuration
- export a Synchronization Engine configuration
- delete a Synchronization Engine configuration

Create a Synchronization Engine Configuration

To create a Synchronization Engine configuration:

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

   The Configuration Editor window appears.

2. In the Device Class area, click the **Synchronization Engine** option button.

   The **Defined Configurations** list box displays the defined Synchronization Engine configurations.

3. Click the **Add** button.

   The New Configuration dialog box appears.

4. Enter the name for the new configuration and click the **OK** button.

   The new Synchronization Engine configuration appears in the **Defined Configurations** list box.

5. In the **Defined Configurations** list box, select the new configuration.

   The **Configuration Details** box is empty.

6. Enter the contents of the new configuration in the **Configuration Details** list box. You can type information, import an existing configuration, or paste information from another configuration via Windows Clipboard into the **Configuration Details** list box.

Modify a Synchronization Engine Configuration

To modify a Synchronization Engine configuration:

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

   The Configuration Editor window appears.

2. In the Device Class area, click the **Synchronization Engine** option button.

   The **Defined Configurations** list box displays the defined Synchronization Engine configurations.

3. In the **Defined Configurations** list box, select the Synchronization Engine you want to modify.

   The information for the selected Synchronization Engine configuration appears in the **Configuration Details** box.

4. Make your changes.

   You can type information, import an existing configuration, or paste information from another configuration via Windows Clipboard into the **Configuration Details** list box.

   If you want to find specific information in a configuration, enter the information in which you are interested, and click the **Find** button. The first occurrence that matches the information for which you are searching is highlighted. If you want to find the next occurrence, click the **Find Again** button.

Import Information into a Synchronization Engine Configuration

Importing information into a Synchronization Engine configuration overwrites the information for the currently selected Synchronization Engine configuration.

To import a Synchronization Engine configuration:

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

   The Configuration Editor window appears.

2. In the Device Class area, click the **Synchronization Engine** option button.

   The **Defined Configurations** list box displays the defined Synchronization Engine configurations.

3. Click the **Add** button.

   The New Configuration dialog box appears.

4. Enter the name for the new configuration, and click the **OK** button.

   The new configuration appears in the **Defined Configurations** list box.

5. In the **Defined Configurations** list box, select the new Synchronization Engine configuration.

6. Click the **Import** button.

   The Open dialog box appears. Configuration files have .ini extensions.

7. Select the file you want to import, and then click the **Open** button.

   The information from the selected file is imported to the configuration. The information appears in the **Configuration Details** list box.

Export a Synchronization Engine Configuration

To export a Synchronization Engine configuration:

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

   The Configuration Editor window appears.

2. In the Device Class area, click the **Synchronization Engine** option button.

   The **Defined Configurations** list box displays the defined Synchronization Engine configurations.

3. In the **Defined Configurations** list box, select the Synchronization Engine you want to export.

4. Click the **Export** button.

   The Save As dialog box appears.

5. Specify the destination location and file name for the information you want to export.

6. Click the **Save** button.

   The information is exported to the destination file.

Delete a Synchronization Engine Configuration

To delete a Synchronization Engine configuration:

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

   The Configuration Editor window appears.

2. In the Device Class area, select the **Synchronization Engine** option button.

3. In the **Defined Configuration** box, select the configuration file you want to delete.

4. Click the **Delete** button.

   The Confirm dialog box appears, prompting you to confirm your action.

5. Click the **Yes** button.

   The selected file is deleted.

Managing DataStore Manager Configurations

A DataStore Manager configuration contains the following information:

- low-level connection information (that is, how the DataStore Manager connects to the device)
- low-level options for converting native device data types to DEM data types

Currently, DEM supports four types of DataStore Managers: DEFINITY DataStore Managers, Intuity DataStore Managers, LDAP server DataStore Managers, and Adapter DataStore Managers. When you define a DataStore Manager using the **DataStore Managers** tab, you specify the configuration you want that DataStore Manager to use.

A DataStore Manager configuration consists of the following sections:

- **Protocol**

  The Protocol section specifies the DLLs (dynamic linked libraries) that the associated DataStore Manager will use.

- **Publish**

  The Publish section specifies what data types the DataStore Manager can publish. ***Never change this information.***

- **Root**

  The Root section contains the following information:

  — DataStore ID, which is the unique name of the DataStore Manager

  — list of the DEM types that are supported by this DataStore Manager

- **Subscription**

  The Subscription section specifies the DEM types (and the associated subscription rules you specify) that this DataStore Manager wants to receive from the Synchronization Engine.

- **Variables**

  The Variables section contains information that was entered when the DataStore Manager was installed.

- **Connection**

  The Connection section contains the logins and passwords the DataStore Manager will use to connect to the device.

- **Include**

  The Include section provides the capability to include other files as part of the DataStore Manager configuration. This section references the DataStore Manager configuration that contains common information for all voice servers. However, if there are any duplicates in the Include file(s), the information in the DataStore Manager configuration overrides the same information in the Include file(s). If Include files are used, DEM Administrator merges the DataStore Manager configuration and the Include file(s) during initialization. If there are any duplicate keys in the DataStore Manager configuration and the Include file(s), the duplicate information in the Include file(s) is not used. The result of the merge is one configuration set that the DataStore Manager uses while it is running.

This section describes how to

- create a DataStore Manager configuration
- modify a DataStore Manager configuration
- import information into a DataStore Manager configuration
- export a DataStore Manager configuration
- delete a DataStore Manager configuration

Create a DataStore Manager Configuration

To create a DataStore Manager configuration:

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. Click the **Add** button.

   The New Configuration dialog box appears.

4. Enter the name for the new configuration, and click the **OK** button.

   The new DataStore Manager configuration appears in the **Defined Configuration** list box.

5. In the **Defined Configurations** list box, select the new configuration.

   The **Configuration Details** box is empty.

6. Enter the contents of the new configuration in the **Configuration Details** list box. You can type information, import an existing configuration, or paste information from another configuration via Windows Clipboard into the **Configuration Details** list box.

Modify a DataStore Manager Configuration

To modify an existing DataStore Manager configuration:

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. In the **Defined Configurations** list box, select the DataStore Manager you want to modify.

   The information for the selected DataStore Manager configuration appears in the **Configuration Details** box.

4. Make your changes.

   You can type information, import an existing configuration, or paste information from another configuration via Windows Clipboard into the **Configuration Details** list box.

   If you want to find specific information in a configuration, enter the information in which you are interested and click the **Find** button. The first occurrence that matches the information for which you are searching is highlighted. If you want to find the next occurrence, click the **Find Again** button.

Import Information into a DataStore Manager Configuration

Importing information into a DataStore Manager configuration overwrites the information for the currently selected DataStore Manager.

To import a DataStore Manager configuration:

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. Click the **Add** button.

   The New Configuration dialog box appears.

4. Enter the name for the new configuration and click the **OK** button.

   The new configuration appears in the **Defined Configurations** list box.

5. In the **Defined Configurations** list box, select the new DataStore Manager configuration.

6. Click the **Import** button.

   The Open dialog box appears. Configuration files have .ini extensions.

7. Select the file you want to import, and then click the **Open** button.

   The information from the selected file is imported to the configuration. The information appears in the **Configuration Details** list box.

Export a DataStore Manager Configuration

To export a DataStore Manager configuration:

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. In the **Defined Configurations** list box, select the DataStore Manager you want to export.

4. Click the **Export** button.

   The Save As dialog box appears.

5. Specify the destination location and file name for the information you want to export. Configuration files have .ini extensions.

6. Click the **Save** button.

   The information is exported to the destination file.

Delete a DataStore Manager Configuration

To delete a DataStore Manager configuration:

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

   The Configuration Editor window appears.

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

3. In the **Defined Configuration** box, select the configuration file you want to delete.

4. Click the **Delete** button.

   The Confirm dialog box appears, prompting you to confirm your action.

5. Click the **Yes** button.

   The selected file is deleted.

6 Working with Maps

This section describes how to:

- Create and modify map files that map DEM types to other DEM types
- Create a table of auxiliary reference data that can be accessed by the maps

By default, DEM 1.3 and later uses Python maps as the type-to-type mapping mechanism. However, DEM still supports the legacy mapping mechanism.

Using Maps

Using the **Maps** button on the toolbar, you can create and modify map files that map DEM types to other DEM types.

CAUTION

The procedures in this section should be performed in conjunction with Avaya Professional Services. Incorrect mapping can cause subtle but serious side effects throughout DEM and its devices.

Create Maps

To create a map:

1. On the toolbar, click the **Maps** button.

   The Mapping dialog box appears.

2. Enter the mapping information in the list box.

3. Click the **Save As** button.

   The Save As dialog box appears.

4. Enter the path and file name for the map. Maps have ".map" extensions.

5. Click the **Save** button.

   The **Map Definition file** box displays the name of the new map file.

6. Click the **OK** button.

Modify Maps

To modify a map:

1. On the toolbar, click the **Maps** button.

   The Mapping dialog box appears.

2. Click the **Open** button.

   The Open dialog box appears.

3. Select the map file you want to open, and click the **Open** button.

   The name of the map file appears in the **Map Definition file** box, and the contents of the selected map appear in the **Map Definition file** list box.

4. Make your changes to the map.

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

Using the Map Rule Reference Data

Using the **Reference Table** button on the toolbar, you can create a table of auxiliary reference data that can be accessed by the maps.

Add Map Rule Reference Data

To add map rule reference data:

1. On the toolbar, click the **Reference Table** button.

   The Map Rule Reference Data dialog box appears.

2. Click the **Add** button.

   The Reference Data Editor dialog box appears.

3. In the **Scope** box, enter the scope.

4. In the **Major** box, enter a unique key to identify a data value.

5. In the **Minor** box, enter a unique key to identify a data value.

6. In the **Value** box, enter a unique key to identify a data value.

7. Click the **OK** button.

   The new record appears in the **Map Rule Reference Data** dialog box.

Modify Map Rule Reference Data

To modify map rule reference data:

1. On the toolbar, click the **Reference Table** button.

   The Map Rule Reference Data dialog box appears.

2. Select the Scope you want to modify.
3. Click the **Modify** button.

   The Reference Data Editor dialog box appears.

4. Make your changes.
5. When finished, click the **OK** button.

Delete Map Rule Reference Data

To delete map rule reference data:

1. On the toolbar, click the **Reference Table** button.

   The Map Rule Reference Data dialog box appears.

2. Select the Scope you want to delete.
3. Click the **Delete** button.

   A Warning dialog box appears.

4. Click the **Yes** button.

   The selected map rule reference data is deleted.

7 Managing GWAgent

GWAgent monitors changes that are made to the LDAP datastore. Using GWAgent, you create triggers that monitor a specific LDAP operation type (such as add, modify, and delete) in a specific sub-tree in the LDAP tree. These triggers are responsible for intercepting data changes in the LDAP datastore and passing that information to GWAgent, which in turn passes the information to DEM.

Viewing Triggers

To view the existing triggers in GWAgent:

1. Click the **GWAgent** tab in the DEM Administrator window.

   The **GWAgent** tab appears.

2. Click the **Connect** button.

   The Connect To GWAgent dialog box appears.

3. In the **Server** box, enter the name of the PC on which DEM is installed.

4. In the **User** box, enter the LDAP user that you entered during the software installation.

5. In the **Password** box, enter the password for the LDAP user.

6. Click the **OK** button.

   You are connected to the Gateway Agent. The existing triggers are displayed.

Adding Triggers

To add triggers in GWAgent:

1. Click the **GWAgent** tab in the DEM Administrator window.

   The **GWAgent** tab appears.

2. Click the **Connect** button.

   The Connect To GWAgent dialog box appears.

3. In the **Server** box, enter the name of the PC on which DEM is installed.

4. In the **User** box, enter the LDAP user that you entered during the software installation.

5. In the **Password** box, enter the password for the LDAP user.

6. Click the **OK** button.

   You are connected to the Gateway Agent.

7. Click the **Populate** button.

   The General Settings dialog box appears.

8. Click the **Add** button.

   The Add New Trigger dialog box appears.

9. Enter the appropriate information.

10. When finished, click the **OK** button.

    Information is displayed.

11. Repeat Steps 8 through 10 if you want to add more triggers.

12. When finished, click the **OK** button to close the General Settings dialog box.

13. Click the **Commit** button.

Deleting Triggers

This procedure deletes all existing triggers from GWAgent.

To delete triggers from GWAgent:

1. Click the **GWAgent** tab in the DEM Administrator window.

   The **GWAgent** tab appears.

2. Click the **Connect** button.

   The Connect To GWAgent dialog box appears.

3. In the **Server** box, enter the name of the PC on which DEM is installed.

4. In the **User** box, enter the LDAP user that you entered during the software installation.

5. In the **Password** box, enter the password for the LDAP user.

6. Click the **OK** button.

   You are connected to the Gateway Agent.

7. Click the **Clear All** button.

   The triggers are removed from the **GWAgent** tab.

8. Click the **Commit** button.

8 Scheduling Administration Events

The Scheduler gives you additional flexibility in managing DEM. The Scheduler enables you to specify a time of day and frequency when you want the DEM Administrator application to perform groups of actions you specify automatically. Using the Scheduler, you can run any actions you want at any time of day you want. For example, synchronizing data among all the active DataStore Managers causes network congestion. You can schedule the synchronization to occur at a time when there is little network traffic (for example, during off hours).

Each event you schedule consists of one or more groups. A group, in turn, consists of one or more items. Each item is an action (for example, synchronize). Two types of groups are supported: synchronous groups and asynchronous groups. In a synchronous group, all of the actions in that group are performed in a linear fashion (that is, action 2 is not started until action 1 is completed, and action 3 is not started until action 2 is completed). In an asynchronous group, all of the actions in that group are performed simultaneously, independently of one another.

When you schedule events, you can specify that the DEM Administrator application send email to people you specify when the events are performed.

Scheduling an Event

To schedule an event:

1. On the toolbar, click the **Scheduler** button.

   The GW Event Scheduling dialog box appears, displaying the scheduled events.

2. Click the **Add Event** button.

   A new event appears at the bottom of the list box.

3. In the **Name** box of the Event Details area, enter the name for the event.

4. In the **Description** box, enter the description of the event.

5. Click the **Set** button to schedule when this event will be performed. (The **Run Now** button runs the event now.)

   The Scheduler dialog box appears.

6. In the Start area, set the date and time you want to perform this event.

7. In the Recurrence Pattern area, select the option button for the frequency that you want the event performed.

   You can run the event once, every n hours, weekly, or every n day(s). If you select the **n Hours** option button or the **n Days** option button, you must specify the number of hours or days at which the event will be performed.

8. When finished setting the time and date, click the **OK** button.

   The **Scheduled** box displays the date and time when the event will be performed.

9. In the **Reports to** box, enter the email address of the person who should be contacted if the event fails.

10. If you want this event disabled, remove the check from the **Enabled** check box. By default, the event is enabled. If the **Enabled** check box is disabled, the event will not be performed. However, the event can still be run manually via the **Run Now** button.

11. Click the **Add Group** button.

    A new group is added under the event. By default, this event is **Synchronous**.

12. If you want to change the setting from **Synchronous** to **Asynchronous** either click the **Asynchronous** check box or right-click the mouse on the new group and select **Toggle Sync**.

13. Click the **Add Item** button.

    The Item Details area becomes enabled.

14. From the **Action** drop-down list box, select the action that this item will perform.

15. From the **Device Class** drop-down list box, select the type of device.

    There are two device classes: DataStore Managers (DSMs) and Synchronization Engines (SEs).

16. In the **Device** box, enter the name of the device.

17. If you are performing a synchronization, you must enter the DEM types that you want to synchronize in the **Arguments** box.

18. Remove the check from the **Critical Action** check box if you do not want this item to be a critical action. By default, this check box is enabled.

    If an item is designated as a critical action and that item fails when the event is performed, the event will stop at that point (that is, the remaining items and groups in this event are aborted).

19. Remove the check from the **Enabled** check box if you want to disable this item. If an item is disabled, that item will not be performed. By default, the item is enabled.

20. Perform one of the following steps:

    — To add more items to this group, repeat Steps 13 through 19.

    — To add more groups to this event, repeat Steps 11 through 19.

Modifying Events

To modify an event:

1. On the toolbar, click the **Scheduler** button.

   The GW Event Scheduling dialog box appears, displaying the scheduled events.

2. Select the event, group, or item you want to modify, and make your changes.

   Use the **Add Group** button to add a new group to the selected event.

   Use the **Add Item** button to add a new item to the selected group.

   Use the **Delete Node** button to delete the selected event, group, or item. When you delete a group or item, the numbers of the other groups or items do not change.

Deleting Events

When you delete an event, all of its groups and items are also deleted.

To delete an event:

1. On the toolbar, click the **Scheduler** button.

   The GW Event Scheduling dialog box appears, displaying the scheduled events.

2. Select the event you want to delete.

3. Click the **Delete Node** button.

   The Confirm Delete dialog box appears.

4. Click the **Yes** button.

   The selected event is deleted.

Viewing the Last Run Information

You can view the "last run information" for an event or item (if the information is available). If available, the last run information contains the results from the last time the event or item was performed.

To view the last run information:

1. On the toolbar, click the **Scheduler** button.

   The GW Event Scheduling dialog box appears, displaying the scheduled events.

2. Right-click the mouse on the event or item in which you are interested.

3. Select **Show last run info**.

   The Last Run Info dialog box appears, displaying when the event or item was last run and its results (if available).

4. When finished, click the **OK** button.

9 Using the Message Log

Using the **Logs** button on the toolbar, you can access the Message Log dialog box, which displays messages from DEM that match the criteria you specify. From this dialog box, you can:

- Delete all entries from the log
- Refresh the log
- Specify the criteria of the messages you want displayed in the Message Log dialog box. You can filter the messages according to
  - — device class (that is, messages from DataStore Managers and/or the Synchronization Engine)
  - — message type (for example, transaction and device error)
  - — lowest severity level to display
- Set DEM Administrator to send email to people you specify when messages match the criteria you specify. You can set email to be sent according to
  - — message source (DataStore Managers and/or the Synchronization Engine)
  - — message type
  - — lowest severity level

Viewing the Message Log

To view the Message Log, click the **Logs** button on the toolbar. The Message Log dialog box appears.

Filtering Messages in the Message Log

You can set the Message Log to display messages that match any combination of the following criteria:

- type of device (that is, messages from DataStore Managers, Synchronization Engine, or both device types). For example, if you select **DSM**, only messages from DataStore Managers will be displayed.
- type of message (that is, DeviceError messages, Informational messages, TransactionError messages, or all messages). For example, if you select **DeviceError**, only DeviceError messages will be displayed.
- lowest severity of message (that is, Warning, Error, Severe, Fatal, or none). Message severity ranges from None (minimum) to Fatal (maximum). For example, if you select **Severe**, only Severe messages and Fatal messages will be displayed. (In this example, Warning messages and Error messages will not be displayed.) If you select **None**, all messages will be displayed.

To specify the messages displayed in the Message Log:

1. Click the **Logs** button on the toolbar.

   The Message Log dialog box appears.

2. From the **Show Device Classes** drop-down list box in the Filter Settings area, select the type of device message you want to view.

   The messages matching this criterion are displayed.

3. From the **Show Msg Types** drop-down list box, select the type of messages you want to view.

   The messages matching this criterion for the device you specified are displayed.

4. From the **Lowest Severity** drop-down list box, select the lowest severity message you want to view.

   The messages matching the severity level for the message type and device type you specified are displayed.

Configuring the Message Log to Send Email Notifications

You can set DEM to send email when specific types of messages are produced.

*** Note:** For the email feature to work, the TAO_Implementation_Repository and the TAO_Naming_Service must be launched as a service under a user account (that is, not the system account). You can go to Services and perform the following steps:

1. Right-click the service, and select **Properties**.
2. Select the **Log On** tab.
3. Select **This account**, and configure a valid user on the DEM server with an email account.
4. Repeat these steps for both the TAO_Implementation_Repository and the TAO_Naming_Service.

Add an Email Notification

To set the Message Log to send email notifications:

1. Click the **Logs** button on the toolbar.

   The Message Log dialog box appears.

2. Click the **Set Mail Targets** button.

   The Mail Notification Recipients dialog box appears. This dialog box displays the email addresses that are currently assigned to receive notification.

3. Click the **Add** button.

   The Mail Target Settings dialog box appears.

4. In the **Address** box, enter the email address of the person who will receive the email notification. Type the email address after SMTP:.

5. In the **Name** box, enter the name of the person who will receive the email notification.

6. From the **Type** drop-down list box, select the type of message for which you want to send email.

7. From the **Lowest Severity** drop-down list box, select the severity of the message for which you want to send email.

8. From the **Class** drop-down list box, select the device class of the message for which you want to send email.

9. In the **Source ID** box, enter ***All***.

10. Click the **OK** button.

    The new record appears in the Mail Notification Recipients dialog box. When messages are produced that match the criteria you just specified, email will be sent to the person you specified.

11. Repeat Steps 3 through 10 for any other people you want to receive email notification.

12. When finished, click the **OK** button to close the Mail Notification Recipients dialog box.

Modify an Email Notification

To modify an email notification:

1. Click the **Logs** button on the toolbar.

   The Message Log dialog box appears.

2. Click the **Set Mail Targets** button.

   The Mail Notification Recipients dialog box appears. This dialog box displays the email addresses that are currently assigned to receive notification.

3. Select the record you want to modify.

4. Click the **Modify** button.

   The Mail Target Settings dialog box appears.

5. Make your changes.

6. When finished, click the **OK** button.

7. Repeat Steps 3 through 6 for any other records you want to modify.
8. When finished, click the **OK** button to close the Mail Notification Recipients dialog box.

Delete an Email Notification

To delete an email notification:

1. Click the **Logs** button on the toolbar.

   The Message Log dialog box appears.

2. Click the **Set Mail Targets** button.

   The Mail Notification Recipients dialog box appears. This dialog box displays the email addresses that are currently assigned to receive notification.

3. Select the record you want to delete.
4. Click the **Delete** button.

   The Confirm dialog box appears.

5. Click the **Yes** button.

   The record is removed from the Mail Notification Recipients dialog box.

6. Repeat Steps 3 through 5 for any other records you want to delete.
7. When finished, click the **OK** button to close the Mail Notification Recipients dialog box.

Refreshing the Message Log

To refresh the Message Log:

1. Click the **Logs** button on the toolbar.

   The Message Log dialog box appears.

2. Click the **Refresh** button.

Purging the Message Log

This procedure deletes all of the messages from the Message Log.

WARNING

When you purge the Message Log, all of the messages are deleted. You cannot recover messages after they are purged.

To purge messages from the Message Log:

1. Click the **Logs** button on the toolbar.

   The Message Log dialog box appears.

2. Click the **Purge Log** button.

   The Confirm dialog box appears.

3. Click the **Yes** button.

   The records are deleted from the Message Log dialog box.

10 Managing DEM Administrator Users

This chapter describes how to:

- create DEM Administrator accounts
- modify the user privileges of an existing DEM Administrator account
- change the password for a DEM Administrator account
- delete a DEM Administrator account

Creating a DEM Administrator Account

To create a DEM Administrator account:

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 user name.

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

5. Click the **Superuser** check box if you want this user to have superuser privileges.

6. Click the **OK** button.

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

Modifying the Privileges of a DEM Administrator Account

To modify the privileges of a DEM Administrator account:

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

   The User Profiles dialog box appears.

2. In the **Users** box, select the account you want to modify.

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

   — **0** indicates disabled.

   — **1** indicates enabled.

3. Make your changes to the user account.

4. When finished, click the **OK** button.

Changing the Password for a DEM Administrator Account

To change the password for a DEM Administrator account:

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

   The User Profiles dialog box appears.

2. In the **Users** box, select the account whose password you want to modify.

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

3. Click the **Change Pwd** button.

   The Password Maintenance dialog box appears. The **Password** box displays the current password for the selected account.

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

5. Click the **OK** button.

6. When finished, click the **OK** button.

Deleting a DEM Administrator Account

To delete a DEM Administrator account:

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

   The User Profiles dialog box appears.

2. In the **Users** box, select the account you want to delete.

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

3. Click the **Delete** button.

   The Confirm dialog box appears.

4. Click the **Yes** button.

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

11 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:

- Troubleshooting DEM Administrator Startup
- Troubleshooting DEM Administrator Login
- Troubleshooting the Synchronization Engine
- Troubleshooting DataStore Managers
- Troubleshooting GWAgent
- Troubleshooting the Scheduler

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

Troubleshooting DEM Administrator Startup

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

Problem 1: DEM Administrator will not start

This problem will occur if one of the following conditions exists:

- The Naming Service and the Implementation Repository NT services have not started.
- The mdb file that is used for validating database access is not in the correct location, or it is locked by a previous instance of the TAO_GWMGR process.

Perform the following steps:

1. Make sure the Naming Service and the Implementation Repository NT services have started by examining the Control Panel/Services applet. From Task Manager, verify that the Naming_Service and ImplRepo_Service executables are running.
2. Make sure the mdb file is in the \DEM\bin directory.
3. If the GWAdmin client will not start properly (that is, "loops" on Login dialog box or exits after the login information is entered), use Task Manager to determine whether the TAO_GWMGR process is running. If the TAO_GWMGR process is running, shut it down from the command line (for example, c:\DEM\bin\kill <process ID seen in Task Manager>). After the process is shut down, restart it from the command line by entering the following command and pressing the ENTER key:

   c:\DEM\bin\tao_imr ImplRepoService=iioploc://hostname:ImplRepoService activate GWMGR

   where ***hostname*** is the machine name of the PC running DEM.

   After entering this information, try to start DEM Administrator.

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: After the system reboots, the gwcfg window appears and “hangs”

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

Perform the following steps:

1. Close the gwcfg window.
2. From the Start menu, select **Programs>Command Prompt**.

   The Command Prompt window appears.
3. From the \\DEM\bin folder, type ***kill TAO_GWMGR*** and press the ENTER key.
4. Close the Command Prompt window.
5. From the Start menu, select **Settings>Control Panel**.

   The Control Panel window appears.
6. Double-click on the **ODBC Data Sources** icon.

   The ODBC Data Source Administrator dialog box appears.
7. Click the **System DSN** tab.

   The **System DSN** tab appears.
8. Select **GWADMIN.mdb**, and click the **Configure** button.

   The ODBC Microsoft Access Setup dialog box appears.
9. Click the **Select** button.

   The Select Database dialog box appears.
10. Select **GWADMIN.mdb** in the bin directory where DEM was installed.
11. Click the **OK** button.

12. Click the **OK** button.

13. Click the **OK** button.

If the gwcfg window appears again, contact Avaya technical support.

Problem 4: 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 5: 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 6: 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_imr list MONITOR_POA*** and press the ENTER key.

   This commands lists the CORBA servers that are currently running.
5. If the monitor is listed, type ***kill MONITOR_POA*** and press the ENTER key.
6. Close the Command Prompt window.
7. Restart DEM Administrator.

Problem 7: 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 8: DEM Administrator does not respond

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, type ***tao_imr list TAO_GWMGR*** from the command line, and press the ENTER key.

   This command lists the services that are running.
4. If GWMgr appears in the service list, type ***kill TAO_GWMGR*** at the command line and press the ENTER key.

Problem 9: 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 82.

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

You enter your login and password and click the **Login** button in the Avaya Directory Enabled Management Administrator Login dialog box, but the Avaya Directory Enabled Management Administrator window does not appear. No error messages appear.

Perform the following steps:

1. Using the Services applet in Windows Control Panel, confirm that the TAO Implementation Repository and TAO Naming Service have started.
2. Perform one of the following steps:
   - If the services have started, use Task Manager to check whether the TAO_GWMgr CORBA service has started.
   - If the services have not started, verify that the services exist and start them.
   - If errors are displayed, contact Avaya technical support.

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

Perform the following steps:

1. In the **DataStore Managers** tab, verify that the host is correct for the DataStore Manager.
2. Perform one of the following steps:
   - If the host is incorrect, perform the following steps:
     1. Delete the DataStore Manager.
     2. Define a new DataStore Manager with the correct host.
     3. Activate the new DataStore Manager.
   - If the host is correct, try to activate the DataStore Manager.

     If the DataStore Manager does not activate, perform the following steps:
     1. From the Start menu, select **Programs>Command Prompt**.
        The Command Prompt window appears.
     2. At the command prompt, type
        TAO_IMR ImplRepoService=iioploc://hostname:10014/ImplRepoService activate GWMRG
        where ***hostname*** is the machine name of the PC running DEM.
     3. Press the ENTER key.
     4. Close the Command Prompt window.
     5. Activate the DataStore Manager.

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 ***TAO_IMR ImplRepoService=iioploc://hostname:10014/implRepoService list***

   where ***hostname*** is the machine name of the PC running DEM.

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

2. Make sure that the "host" value for the DSM specifies the correct machine-name.

3. Check the configuration values for the specified DSM. In particular, make sure that the connection parameters are correct.

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

This section describes problems you might encounter with GWAgent.

Problem 1: You cannot start GW Agent

The registry settings for GW Agent are incorrect.

Use the registry editor to examine and correct the GW Agent entries. Make sure the path to the ltap.config file is correct.

Problem 2: You cannot connect to LDAP

The entries in the ltap.config file are incorrect.

Open the ltap.configure file and verify that the entries for the host and port of the true LDAP server are correct.

Problem 3: The triggers are unavailable and/or unpopulated

This problem can be caused by the following conditions:

- The trigger database is empty.
- The path to the trigger database does not exist.

Recreate the triggers.

Problem 4: All of the triggers fail

The triggers are incorrect and must be repopulated.

Recreate the triggers.

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.

A Security Keys

This appendix defines the contents of the security map.

Table 4. Security Map Keys

Key	Definitions
CFG.DEF.ADD	Configuration Editor Add button
CFG.DEF.DEL	Configuration Editor Delete button
CFG.DETAILS.SAVE	Configuration Editor Save button
CFG.EXPORT	Configuration Editor Export button
CFG.IMPORT	Configuration Editor Import button
CFG.OK	Configuration Editor OK button
CFG.SEC.ADD	Configuration Editor Add Key button
CFG.SEC.DEL	Configuration Editor Delete Key button
CFG.SEC.MOD	Configuration Editor Modify Key button
DSM.DEF.DEFINE	DataStore Managers tab, Define DSM button
DSM.DEF.MODIFY	DataStore Managers tab, Modify DSM button
DSM.DEF.REMOVE	DataStore Managers tab, Remove DSM button
DSM.LIFE.ACTIVATE	DataStore Managers tab, Activate button
DSM.LIFE.ATTACH	DataStore Managers tab, (Re)Attach button
DSM.LIFE.DETACH	DataStore Managers tab, Detach button
DSM.LIFE.REINIT	DataStore Managers tab, Re-Initialize button
DSM.LIFE.RUN	DataStore Managers tab, Run button

1 of 3

Table 4. Security Map Keys

Key	Definitions
DSM.LIFE.SHUTDOWN	DataStore Managers tab, Shutdown button
DSM.LIFE.SYNC	DataStore Managers tab, Synchronize button
LOGS.MAILTARGETS.ADD	Logs/Mail Notification Recipients dialog box, Add button
LOGS.MAILTARGETS.DELETE	Logs/Mail Notification Recipients dialog box, Delete button
LOGS.MAILTARGETS.MODIFY	Logs/Mail Notification Recipients dialog box, Modify button
LOGS.SETMAILTARGETS	Logs dialog box, Set Mail Targets button
LOGS.PURGE	Logs dialog box, Purge Log button
MAPS.MAPPING.OPEN	Mapping dialog box, Open button
MAPS.MAPPING.SAVE	Mapping dialog box, Save button
MAPS.MAPPING.SAVEAS	Mapping dialog box, Save As button
REF.TOP	Map Rule Reference dialog box, Top level access (overrides the other keys)
REF.ADD	Map Rule Reference dialog box, Add button
REF.DEL	Map Rule Reference dialog box, Delete button
REF.LIST	Map Rule Reference dialog box, List viewability
REF.MOD	Map Rule Reference dialog box, Modify button
SCHED.TOP	Scheduler dialog box, Top level access (overrides other keys)
SCHED.EVENT.ADD	Scheduler dialog box, Add Event button
SCHED.GONOW	Scheduler dialog box, Run Now button
SCHED.GROUP.ADD	Scheduler dialog box, Add Group button

2 of 3

Table 4. Security Map Keys

Key	Definitions
SCHED.ITEM.ADD	Scheduler dialog box, Add Item button
SCHED.NODE.DELETE	Scheduler dialog box, Delete Node button
SCHED.SAVE	Scheduler dialog box, Save button
SCHED.SET	Scheduler dialog box, Set button
SCHED.TREE	Scheduler dialog box, Tree viewability
SE.DEF.DEFINE	Synchronization Engines tab, Define button
SE.DEF.MODIFY	Synchronization Engines tab, Modify button
SE.DEF.REMOVE	Synchronization Engines tab, Remove button
SE.LIFE.ACTIVATE	Synchronization Engines tab, Activate button
SE.LIFE.REINIT	Synchronization Engines tab, Re-Initialize button
SE.LIFE.SHUTDOWN	Synchronization Engines tab, Shutdown button
SEC.TOP	Security dialog box, Top level access (overrides other keys)
SEC.ADDUSER	Security dialog box, Add button
SEC.CHGPWD	Security dialog box, Change Pwd button
SEC.DELUSER	Security dialog box, Delete button
SEC.PROFILE	Security dialog box, Profile window visibility
SEC.ULIST	Security dialog box, Users list visibility

3 of 3

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 DEFINITY Network 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