NEC

GUARDIAN

AN
OPEN APPLICATION INTERFACE
OPERATIONS MANUAL

NEC America, Inc.

NDA-30008
Revision 2.0
June, 1999
Stock # 184292

LIABILITY DISCLAIMER

NEC America reserves the right to change the specifications, functions, or features in this document at any time without notice. NEC America has prepared this document for use by its employees and customers. The information contained herein is the property of NEC America and shall not be reproduced without prior written approval from NEC America.

TABLE OF CONTENTS

Page

Page

Page

This Page Left Blank.

Figure	Title	Page

This Page Left Blank.

LIST OF TABLES

This Page Left Blank.

Chapter 1 General Information

System Overview

Guardian, an Open Application Interface (OAI) application, supports both the telephone user and those who administer the telephone system within an organization or institution. As an OAI application, Guardian is supported by the Applications Manager (APM), particularly in the area of database administration and application configuration.

Guardian is a two-pronged system that provides continuous control of real-time call processing functions as well as a menu-driven terminal interface for system administration. This dual design is illustrated in Figure 1-1 below.

.

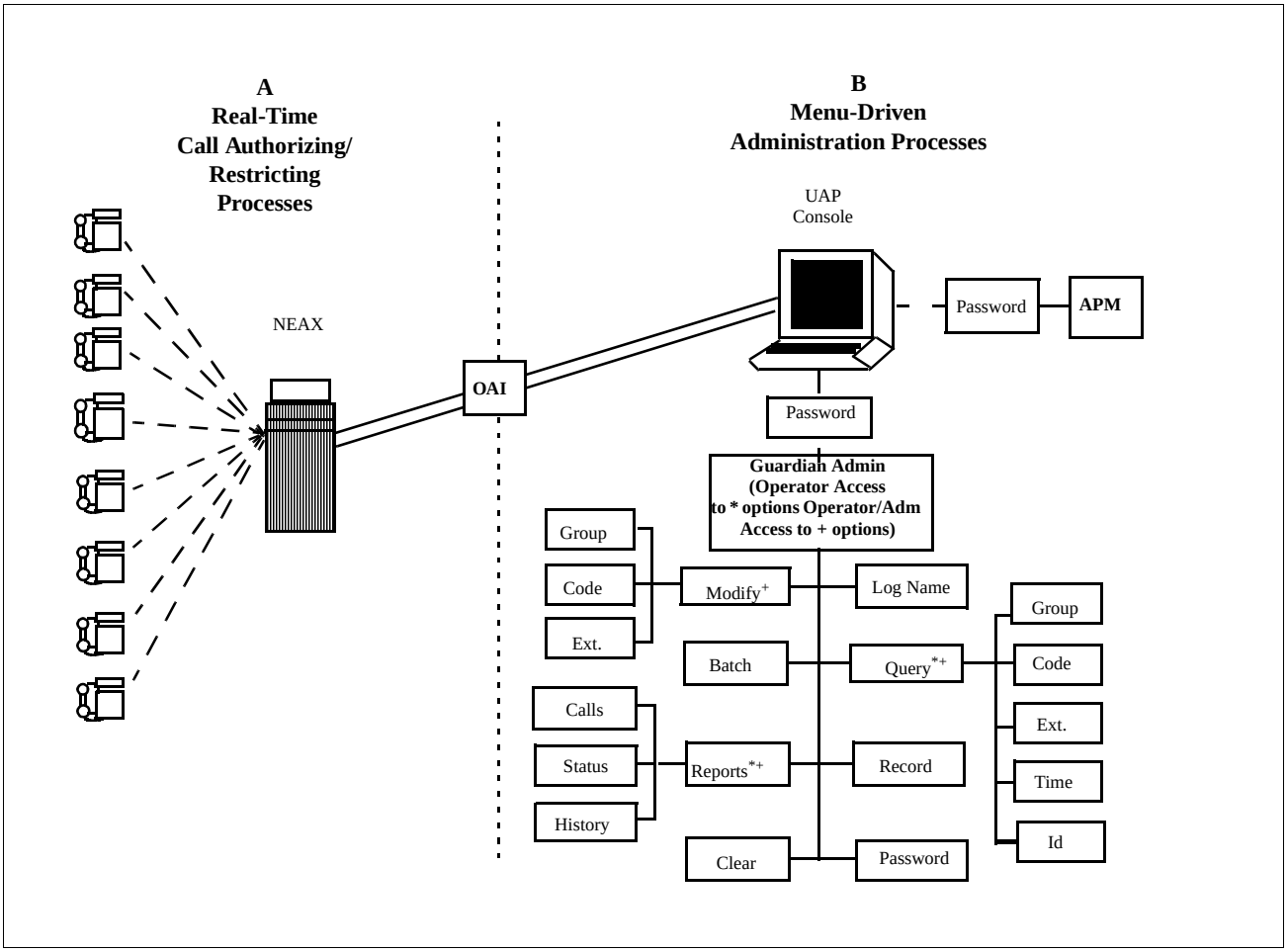


Figure 1-1 Guardian Dual System

The system is designed to support the management of multiple tenants (e.g., a university with four separate campuses or a business housed in several buildings). Each tenant has its own real-time call processing, configuration, and databases, but all tenants are managed by the centralized System Administrator.

System Overview (Continued)

The Guardian system monitors access to telephone extensions in the system, detects invalid attempts to place calls, and restricts service, when necessary. In the Guardian system, each telephone user is assigned an authorization code that corresponds to an individual extension or to a whole group of extensions, as in a college dormitory or a corporate department. Authorization codes, extensions, and groups are administratively assigned defined time periods during which access is prohibited (e.g., weekends or daily after 6:00 p.m.). Any calls attempted during prohibited periods are considered invalid and are not processed. If an extension has an excessive number of invalid calls, Guardian restricts or disables the extension. Calls that are attempted on extensions or with authorization codes that are already disabled are also considered invalid.

Guardian uses one of the following methods to restrict or disable telephone access:

- **System Disable –** Guardian monitors real-time call processing for a frequency of invalid call attempts on any extension that exceeds the designated maximum frequency (e.g., 7 invalid call attempts within a 15-minute period). When an extension exceeds the maximum number of invalid calls, Guardian automatically disables the extension temporarily. Both the maximum frequency and the length of time that the extension is temporarily disabled are configured limits specified by extension group. However, the administrator can override a System Disable at any time.
- **Admin Disable –** Guardian enables the administrator to disable any extension, authorization code, or group of extensions in one of the following ways:
  - **Routinely –** The disablement of any or all extensions, authorization codes, or groups of extensions during specified, regularly occurring time periods, such as weekends or the late night hours
  - **Unconditionally –** The disablement of an extension, authorization code, or group at any time, for as long as desired

Guardian logs information about invalid call attempts and modifications to the status of extensions, authorization codes, and groups. From this log and the databases, Guardian provides a variety of reports in support of system management.

Security

Guardian is a password-protected system. You can enter the system with either an Administrator, an Operator, or the Adm/Operator password. The Administrator password provides unlimited access to all of the Guardian administrative functions that appear on the monitor in menu form. The Operator password enables you to generate reports and to view, but not change, the status of individual extensions, authorization codes, and groups of extensions. The Adm/Operator password provides access to all Operator functions as well as access to the modify menu. The Guardian main menu includes a Maintain Password option through which the Administrator can specify or change the Administrator, Operator or Adm/Operator passwords.

User Procedure

You can use one of the following procedures to place a call from an extension using an authorization code, depending upon the NEAX features that are available and the data assignments that are configured on the NEAX System. During call processing, Guardian verifies the disable status of the code and the extension and either restricts the call or permits it with the routing and service feature privileges assigned to the code.

Procedure No. 1: (Using a Service Access Code)

Step 1: The caller enters the service access code to initiate Guardian.

Step 2: At the tone, the caller enters an authorization code.

Step 3: When the dial tone sounds, the caller enters the destination telephone number.

Step 4: If the authorization code and the extension are valid and enabled, the call is placed, and the caller hears the telephone ringing at the destination. If the authorization code is disabled or unknown to the system, or if the extension is disabled, the call is not be placed, and the caller hears a busy tone.

Procedure No. 2:

Step 1: The caller enters the destination telephone number.

Step 2: If the special dial tone sounds, the call is restricted and requires an authorization code.

Step 3: The caller enters the authorization code.

Step 4: If the authorization code and the extension are valid and enabled, the call is placed, and the caller hears the telephone ringing at the destination. If the authorization code is disabled or unknown to the system, or if the extension is disabled, the call is not be placed, and the caller hears a busy tone.

Database Organization

Guardian requires the five databases described below for each tenant:

- **Group –** Contains definitions for up to 1,000 groups of extensions such as corporate departments or student dormitories. Each group is assigned information that is used to detect and prevent access violation on any of its extensions by group members. If all extensions in the organization are assigned to only one group, that group is assigned the default value of zero in the application configuration during installation. However, if there is more than one group, group 0 is defined in the application configuration, and all other groups are defined in this group database. Groups 1-9 have access to all extensions and authorization codes. Groups 10-1000 have access only to those extensions and authorization codes assigned to them.
- **Extension –** Contains extension numbers that are up to five digits in length with information relating to their verification. Each extension is mutually cross-referenced with its group definition. If an extension used in a call attempt does not appear in this database, the system assumes that it belongs to the default group 0, and the extension is marked as unknown for reporting purposes.
- **Authorization Code –** Contains user-defined authorization codes that are up to ten digits in length with information necessary for their verification. Forced account codes may be substituted for authorization codes. Guardian can work with either forced account or authorization codes but not with both at the same time. Each authorization code is assigned Route Restriction Class (RSC) and Service Feature Class (SFC) values that indicate levels of privileges granted to the code holder.
- **Time Interval –** Contains up to 15 predetermined time intervals used to specify periods during which authorization codes, extensions, and groups can be turned off by the system administrator. These intervals are user-defined and might include weekends, holidays, or evenings.
- **ID** – Contains telephone user identification numbers and the authorization codes that are assigned to them. The ID numbers may consist of seven to ten characters. Guardian initially creates this database from the authorization code database. You can access the database by ID number through the Guardian System Administrator Query Database option and modify it by authorization code through the APM Database Administration option.

These databases are created and maintained through the Database Administration option in the Applications Manager (APM). The Guardian system administrator must have access to the APM at the system administrator security level in order to create the databases. The *Applications Manager Operations Manual* provides step-by-step procedures for creating and changing the database definitions and records. Installation Introduction on page 7 of this manual provides information about the specific fields necessary for each of the databases.

Database Organization (Continued)

Once a database is created or changes are made to it in the APM, it is installed for active use by Guardian. While this installation is taking place, Guardian briefly suspends its real-time control and restriction of PBX call processing. During this period, the PBX reverts to its internal tables that do not reflect the status of extensions, groups, and authorization codes in the databases. The amount of time required to load the database(s) is brief enough that it should not significantly affect the level of control exercised by Guardian.

Menu Organization

The system administrator interacts with Guardian through a series of menu-driven screens. The organization of these screens is illustrated in Figure 1-2. Boldfaced options appear on the Administration Main Menu, the asterisked options (*) appear on the Operator Main Menu and the options indicated by a '+' appear on the Adm/Operator Menu. Chapter 3, "Administration" on page 27 of this manual describes the use of these options and their data entry screens in detail.

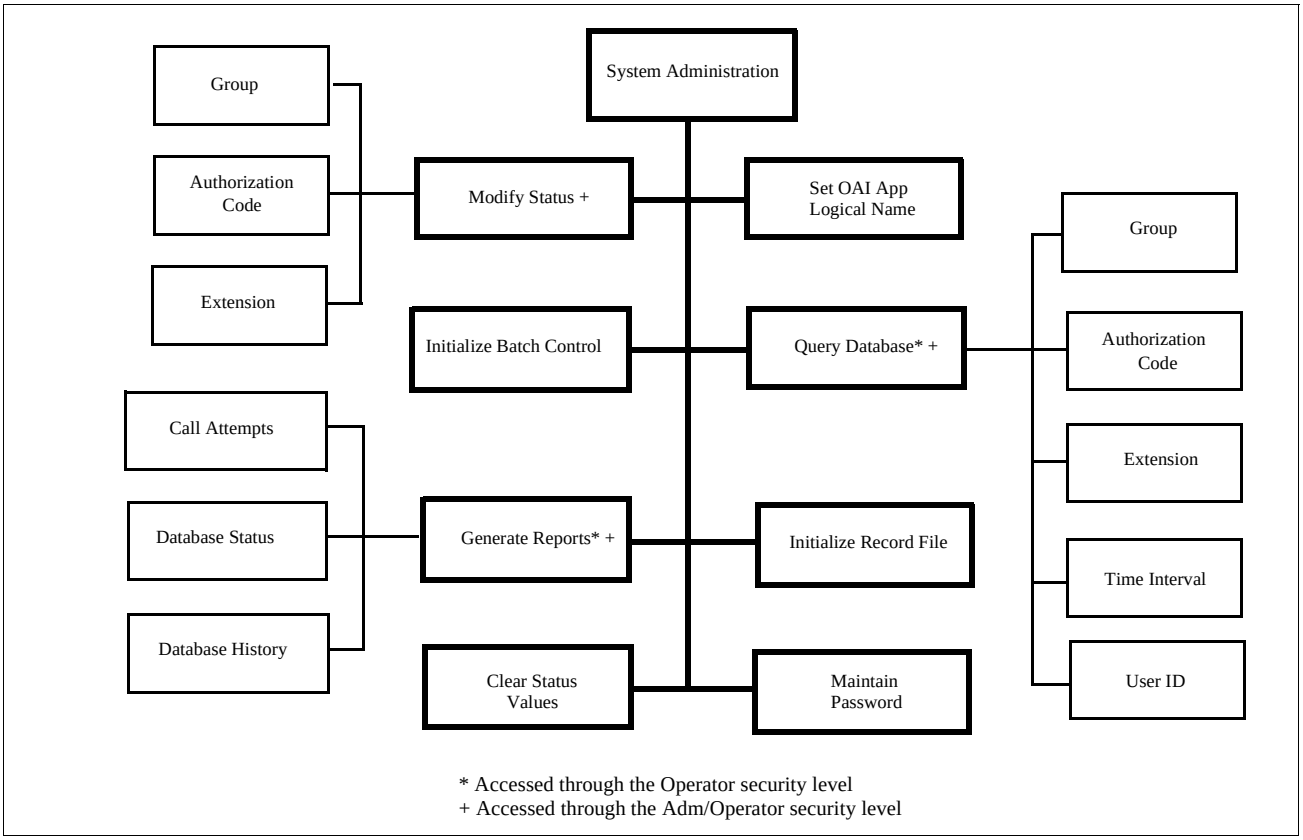


Figure 1-2 Main Menu Organization

This Page Left Blank.

Chapter 2 Installation Introduction

This chapter provides you with specific information and field entries that you need to install and configure Guardian. In addition to this chapter, use the following manuals for installation information:

- *Applications Manager (APM) Installation Manual* – Contains step-by-step instructions for installing the software from the release media.
- *Applications Manager (APM) Operations Manual* **–** Explains how applications like Guardian are configured in the APM environment and how Guardian's databases are created, using the entries and values provided in this chapter.
- NEAX System Manuals - Give very detailed explanations about the assignments that need to be made with the NEAX2400 Maintenance Administration Terminal (MAT) commands, the NEAX2000 Customer Administration Terminal (CAT), or the NEAX2000 Maintenance Operations Console (MOC).

The installation and set up of Guardian involves the following steps. Each of these steps is described in more detail within this chapter:

- **Software Installation** – Load the Guardian software from the release media using the instructions provided in the *APM Installation Manual*. After you install the software, you must assign the Guardian login name, **guardadm** so that users can log in to Guardian from the UNIX prompt. For more information, refer to this section on page 9.
- **Application Configuration** – Guardian is internally supported by the APM and must be configured in the APM environment. This section that begins on page 11 provides the information that must be entered into this APM configuration file. Use the instructions provided in the *APM Operations Manual* for the entries contained in this section.
- **Database Requirements** – Guardian uses five databases which are constructed through the APM Database Administration option. To build the databases, the system creates master definition files and their related master databases. Then, the system creates the application definition files to enable the processing of the master files into application databases. This section defines the information that you must enter to these definition and database files. Use the instructions provided in the *APM Operations Manual* for the entries contained in this section.
- **NEAX Command Assignments** – Before Guardian will function, specific data settings must be assigned at the NEAX2400 Maintenance Administration Terminal (MAT), the NEAX2000 Customer Administration Terminal (CAT), or the NEAX2000 Maintenance Operations Console (MOC). "NEAX Command Assignments" on page 22 specifies the necessary commands and the values at which they are to be set. Use the instructions provided in the appropriate NEAX System Manuals to make the entries contained in this section.
- **Initialization** – Initialize Guardian from the APM Operations Menu using the instructions provided in the *APM Operations Manual*. A password is assigned to the login ID. This section describes the password assignment process.

The installation process, including its presentation in this manual and reference to other manuals, is illustrated below:

GUARDIAN
INSTALLATION REQUIREMENTS

Discussed in section:		Instructions in:
Software Installation	**Software Installation** Software Login ID Protected Databases Update	**APM Installation Manual**
Application Configuration	**Application Configuration** Application Characteristics Primary Parameter Configuration OAI Facilities (Optional) OAI Configuration Parameters (Optional) User-Defined Parameters	**APM Installation Manual**
Database Requirements	**Database Requirements** Master Definition File Master Database File Application Definition File Application Database	**APM Installation Manual**
NEAX Command Assignments	**NEAX2400 MAT Commands**	**NEAX2400 IMS System Manuals**
	NEAX2000 CAT/MOC Commands	**NEAX2000 IVS System Manuals**
Initialization	**Initialization** APM Initialization Password Assignment	**APM Operations Manual**

Software Installation

Use the following steps to complete software installation.

Step 1: Software Installation

To load the Guardian software from the release media, log on to the APM Platform Management Menu, select the Installation of Applications/Packages option, and follow the instructions provided in the *APM Installation Manual*.

Step 2: Login ID

If the Guardian login ID, **guardadm**, already has a password, this software installation is considered an upgrade, and the cursor returns to the APM Platform Management Menu so that you can complete the steps detailed in section Application Configuration on page 11 through section Initialization on page 26.

If the Guardian login ID, **guardadm**, does not already have a password, respond to the following series of prompts that are displayed on the screen:

Prompt: To ensure correct installation, all administrative type files should be closed – – please ensure that all such files are closed at this time.

Response: Make sure that no one is currently performing administrative functions in the UNIX root files. Type **y** to continue the installation.

Prompt: If you know the root password and wish to continue, enter ‘y’; otherwise enter ‘n’ to abort the installation.

Response: To continue, type **y** and press Enter.

To cancel the installation, type **n** and press Enter. The installation is cancelled, and the prompt returns to the APM Platform Management Menu.

Prompt: Please Enter the su/root Password:

Response: Enter the root password and press Enter.

If you enter the wrong root password, an error message displays, and the installation fails. Press Enter to return to the APM Platform Management Menu to start again.

Step 3: Protected Databases Updated

Because a new user (i.e., **guardadm**) has just been installed, you need to execute two commands from the command line under super-user status. The first command (**authck**) updates the protected database files to incorporate user **guardadm**, and the second command (**passwd**) removes any password that user **guardadm** may have inherited during the installation process.

1. From the UNIX login prompt, log on as super user.
2. From the command line, type **/tcb/bin/authck -s** and press Enter.
   The following message appears:
   "The following users have entries in the default user file but not in the protected password database: guardadm
   There are discrepancies between the databases.
   Fix them? (y/n)"
3. Enter **y** and press RETURN.
4. Type **/bin/passwd -d guardadm** at the command line and press Enter.

This completes the necessary updating of the protected databases. See "Application Configuration" on page 11. to configure Guardian in the APM.

Application Configuration

Guardian is configured into the APM system using the **Add** function of the Application Configuration option on the APM System Administration menu.

1. Enter the APM option from the APM Platform Management Menu.
2. Enter the system administrator password at the APM password screen.
3. Enter the Application Configuration option from the System Administration menu.

This section contains the information that you should enter into the configuration file for Guardian. For specific instructions on what these parameters mean and how to make these entries, use the *APM Operations Manual*.

Setting up Multiple Tenants

A tenant is defined as a group of users that may represent a campus, a corporate department, or an entire organization. Using Guardian, you can have one or multiple tenants. For instance, a university may be configured as one tenant, or each of its campuses or academic departments may be configured as a tenant, depending upon the needs of the university. Each tenant is associated with an application name. This name must then be specified before any action can be taken through the Administration menu. Multiple tenants can be handled in either of two ways:

- Each tenant can be configured individually and identified by a unique application name (e.g., Guardian1 or Guardian2). In configuring each tenant, only the application name and the tenant number (through **OAI-Conf** command) must be changed. Once the tenants are configured, the Guardian system administrator can specify a specific tenant's application name so that all actions taken through the menu options affect only the indicated tenant rather than all of the tenants.
- Guardian can be configured once for tenant No. 0, which means all tenants. The single configured application name is then used to gain access to the Administration menus, and all actions taken thereafter through those menu options affect every tenant served by Guardian.

If there is more than one switch in a network, Guardian will work with all the PBX's and maintain its reports and database no differently than a single switch environment.

There should be a separate application configuration in the APM for each Guardian switch. All parameters should be identical except for the destination link, standard out file and Guardian ID (UDP #14).

Note: *The following installation is based upon a single tenant (#0). If you need multiple tenants, complete this configuration for each one.*

Step 1: Application Characteristics

In adding Guardian to the APM Application Configuration file, define it as an OAI application that does not need a CRT or a communication queue, as follows:

Table 2-1 Application Characteristic Entries

Parameter	Entry	Description
OAI Application (Y,N)	Y	Indicates whether or not (Yes or No) this tenant communicates with the NEAX using OAI processes.
CRT Application (Y,N)	N	Indicates whether or not (Yes or No) this tenant requires a terminal screen that is of the same type as the one used by the APM.
Communication Queue (Y,N)	N	Indicates whether or not (Yes or No) this non-OAI application needs an IPC queue to communicate with other process.

Step 2: Primary Configuration Parameters

On the Configuration Entry screen, make the entries shown below to the parameters indicated:

Table 2-2 Primary Configuration Parameter Entries

Parameter	Entry	Description
Application Name	Guardian	The unique logical name of this application.
Executable Filename	/oai/app/guard/grdrt	The path name of the executable file.
Group	(no entry)	(Guardian is not a member of a group of applications.)
Response Mode	I	This is a default value since Guardian does not belong to a group.
Initialization Batch	Y	Guardian is set to initialize automatically when the OAI system is initialized.
Termination Mode	M	Guardian is set to receive a termination message from the APM when it is to terminate, rather than a kill or termination signal.
Standard Output	/oai/log/dbg/grd.dbg	Guardian’s output is sent to this file.
Number of Restarts	5	Guardian may be restarted by the APM up to 5 times that it terminates erroneously.

Step 3: OAI Facilities

According to instructions in the *APM Operations Manual*, designate the following PBX facility for Guardian using the **Facilities** command on the Configuration Entry screen:

Authorization Code Facility (ACF)

Step 4: Secondary OAI Configuration Parameters

Using the **OAI-Conf** command on the Configuration Entry screen, make the entry shown for each of the following parameters required by Guardian. Use the instructions provided for this option in the *APM Operations Manual*:

Table 2-3 Secondary Configuration Parameter Entries

Parameter	Entry	Description
Database Name #1	/oai/app/guard/data/	The path name of the database that contains the back-up files.
Database Name #2	/oai/db/cur/	The path name of the database that contains the current master databases.
Timeout Value #1	30	The number of seconds Guardian waits before trying to reopen a PBX facility that has been closed.
Tenant Number	0	This configuration applies to all tenants. (See “Setting up Multiple Tenants” on page 11..)
Source Link Name	OAI1TCP	The port on the source side of the communication link. Entry should correspond to a Link Name in the APM System Configuration file.
Destination Link Name	PBX1TCP	The port on the destination side of the communication link.
Association Recovery	60	The number of seconds Guardian waits before trying to reestablish an association with the NEAX that has been released.

Step 5: User-Defined Parameters

Make the following additional parameter entries through the **UserDefined** command on the APM Configuration Entry screen.

Table 2-4 User-Defined Parameter Entries

Parameter	Entry	Description
User Defined #1	10	IO Delay Factor – The period of time in which Guardian collects a block of codes before recording them.
User Defined #2	5	IO Block Factor – The number of historical records accumulated and written as a unit to the history file.
User Defined #3	4	Default Disable Time – For Group 0 (default group), the amount of time that any extension in the group is to be system disabled in response to an excessive frequency of invalid call attempts.
User Defined #4	3	Frequency Period – For Group 0, the time interval in minutes in which invalid call attempts are counted to obtain a frequency.
User Defined #5	3	Frequency Count – For Group 0, the number of invalid attempts that are counted before the frequency is considered excessive and the extension is system disabled.
User Defined #6	100	Lifetime Invalid Attempts – For Group 0, the maximum lifetime number of accumulated invalid requests that are allowed before the extension is system disabled.
User Defined #7	/oai/app/guard/grdrc	Record File – The path name of the file in which processing data is recorded for reporting purposes.
User Defined #8	vvvvvvviii	Authcode Mask – A string of characters designating which digits of a dialed authorization code are to be verified, using the following characters: **Note:** *The verifiable digits of the mask must be consecutive.* I or i: Ignore the digit in this position of the code. V or v: Verify the digit in this position of the code.

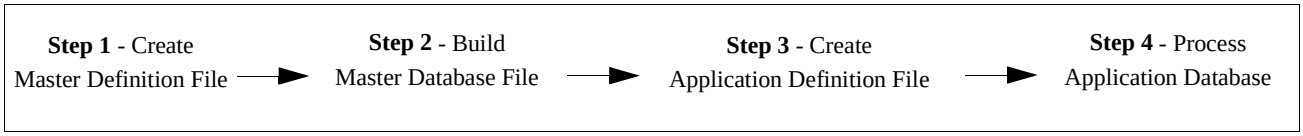
Table 2-4 User-Defined Parameter Entries

Parameter	Entry	Description
User Defined #9	/oai/app/guard/	Base Directory – The path name, where binary files reside.
User Defined #10	/oai/db/cur/grdacf	Authorization Code Database – The path name of the Authorization Code database.
User Defined #11	/oai/db/cur/grdgrpf	Group Database – The path name of the Group database.
User Defined #12	/oai/db/cur/grdextf	Extension Database – The path name of the Extension database.
User Defined #13	/oai/db/cur/grdutf	Time Interval Database – The path name of the Time Interval database.
User Defined #14	1	Integer – Guardian ID (1-10); Unique for each switch in the network.

This completes the configuration of Guardian in the APM. See “Database Requirements” on page 16. to create its databases.

Database Requirements

Each configured Guardian tenant requires five working databases (Group, Authorization Code, Extension, Time Interval, and ID). Each database is created through the Database Administration option on the APM System Administration Menu. Database creation involves the following four-step process for each required database:



1. **Create a Master Definition File**: This step involves creating the master definition file that defines the fields in the master database file. Four master definition files must be created for Guardian the following databases: Group, Authorization Code, Extension, and Time Interval. The Authorization Code master definition file supports both the Authorization Code and the ID databases. When more than one tenant has been configured for Guardian, one master definition file and master database file can support the database required for each tenant. That is, for example, if three tenants have been configured, one Group master definition file and one Group master database file can support three Group databases, one for each tenant.
2. **Build a Master Database File**: This step involves entering tenant-specific data (e.g., extensions, group definitions, authorization codes, student IDs, or time intervals) into the master database fields that were just defined in the four master definition files in Step 1.
3. **Create an Application Definition File**: In this step, a definition file is created for each of the Guardian databases for each tenant. This file defines the formats by which data from the corresponding master file is to be converted to meet the needs of Guardian.
4. **Process the Application Database**: In this step, the Process/Install Application Databases option on the APM Database Administration menu creates the file that will be used by Guardian. When the **Process** command is activated, data is drawn from the master database and converted to the formats specified in the corresponding application definition file. The **Install** command on the Process/Install Application Databases option is activated to enable the Guardian tenant to copy its database into a working file.

Instructions

The information required in all four steps for each Guardian database is provided in table form on the following pages. Using this information with the procedural instructions provided in the *APM Operations Manual*, enter the Database Administration option on the APM System Administration Menu, and build the Guardian databases, one at a time. Any messages displayed during these steps are addressed in the Process and Error Messages chapter of the *APM Operations Manual*.

Note: *Complete Step 4, Process the Application Database, for each database after entering the information on the following pages.*

Group Database Information

The Group database field entries are shown in the table below and defined in "Field Definitions" on page 17. Name the master definition file **grdgrpf_m** and the application definition file **grdgrpf**.

Table 2-5 Group Database Field Entries

Field Description	Master Definition File				Application Definition File	Master Database
	Type	Size	Min. Value	Max. Value	Data Type	Typical Entry
Group ID	N	4	1	1000	Short Integer	2
Interval Index	N	2	0	15	Short Integer	5
Temp Disable Time Max	N	3	0	255	Short Integer	2
Lifetime Invalid Attempts	N	3	0	255	Short Integer	255
Frequency Period	N	2	0	15	Short Integer	10
Frequency Count	N	1	0	7	Short Integer	2

Field Definitions

- **Group ID** – A number that identifies a group, lying within the range from 1 to 1000. This is the key field for database sorting, so entries must be arranged in ascending order.

Note: *Groups 1-9 have access to all authorization codes and extensions; groups 10-1000 have access to only the codes and extensions assigned to them.*

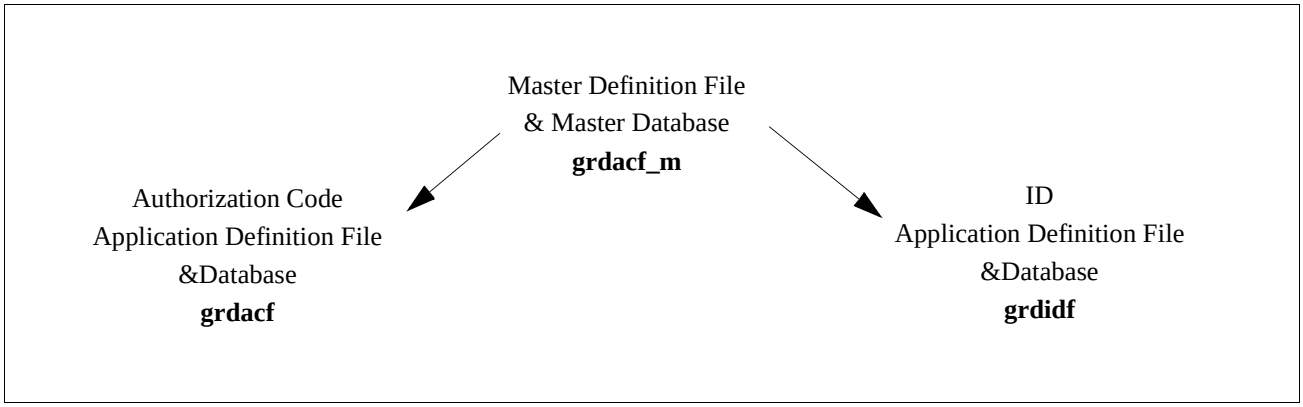
- **Interval Index** – The index to the specific interval of time in the Time Interval Database during which the group extensions are routinely, administratively turned off. The index uses the following values:

  0: Constantly off.
  1-15: Index that corresponds to the desired time interval in the Time Interval Database.

- **Temp Disable Time Max –** Number of 15-minute periods that extensions in the group will be automatically, temporarily turned off by the system in response to an excess frequency of invalid call attempts; maximum 255 periods.
- **Lifetime Invalid Attempts –** The maximum lifetime number of accumulated invalid requests that are allowed before the extensions in the group are turned off by the system; maximum 255 requests.
- **Frequency Period** – The time interval in minutes in which invalid call attempts are counted to obtain a frequency; maximum 15 minutes.
- **Frequency Count** – The number of invalid call attempts that are counted before the frequency is considered excessive, and the extension is turned off by the system; maximum of 7 requests.

Authorization Code and ID Database Information

The Authorization Code master definition file and master database file support both the Authorization Code database and the ID database. Create separate Authorization Code and ID application definition files to process the master database into the two separate databases. Name the master definition file **grdacf_m**, name the Authorization Code application definition file **grdacf**, and name the ID application definition file **grdidf**, as shown below:



The Authorization Code database field entries are shown in the table below and defined in Field Definitions on page 19:

Table 2-6 Authorization Code Database Field Entries

Field Description	Master Definition File				Application Definition File*	Master Database
	Type	Size	Min. Value	Max. Value	Data Type	Typical Entry
Authorization Code*	A	10			ASCII	1246247
Assigned	A	1			ASCII	Y
ID*	A	10			ASCII	585241398
Interval Index	N	2	0	15	Short Integer	5
Extension or Group Flag	A	1			ASCII	G
Extension/Group Value	N	5	0	99999	Long Integer	2
Route Restriction Class	N	2	0†	15†	Short Integer	5
			1‡	8‡		
Service Feature Class	N	2	0†	15†	Short Integer	1
			1‡	8‡		
Reserved	A	2			ASCII	(No Entry)

†Use these values for the NEAX2400.

‡Use these values for the NEAX2000.

*****The fields of the two application definition files (Authorization Code and ID) that are derived from the authorization code master database must be entered in the following sequence:

Order	Authcode Definition File	ID Definition File
#1	Authorization Code	ID
#2	Interval Index	Authorization Code
#3	Extension/Group Value	
#4	Route Restriction Class	
#5	Service Feature Class	
#6	Extension or Group Flag	
#7	Assigned	
#8	Reserved	

Field Definitions

- **Authorization Code** – Key field of the Authorization Code Database consisting of ten digits. Codes must be arranged in ascending order. The authorization code is also the second field in the ID Database.
- **Assigned** – Indicates whether or not (Yes or No) this authorization code has been assigned to a telephone user.
- **ID** – The telephone user identification number assigned to this authorization code.
- **Interval Index** – The index to the specific interval of time in the Time Interval Database during which the authorization code is routinely disabled. The index uses the following values:

  0: Constantly off.
  1-15: Index to an interval in the Time Interval Database.
- **Extension or Group** – The assignment of the authorization code to a single extension or to a group of extensions. Possible field entries are as follows:

  Ext: Extension
  Grp: Group
- **Extension/Group Value** – The actual extension or group to which the authorization code is assigned, corresponding to the Extension or Group assignment:

  If assignment is Ext: An extension number of up to 5 digits in length.
  If assignment is Grp: A group ID ranging from 1 to 1000.
- **Route Restriction Class** – A value from 0 to 15 on the NEAX2400 or a value from 1 to 8 on the NEAX 2000 that represents different combinations of distance and routing privileges available to code holders.
- **Service Feature Class** – A value from 0 to 15 on the NEAX2400 or a value from 1 to 8 on the NEAX 2000 that represents different combinations of PBX call processing features available to code holders.
- **Reserved** – System-reserved space. This field is not modified by the user.

Extension Database Information

The Extension database field entries are shown in the table below and defined in "Field Definitions" on page 20. Name the Extension master definition file **grdextf_m** and the application definition file **grdextf**.

Table 2-7 Extension Database Field Entries

Field Description	Master Definition File				Application Definition File	Master Database
	Type	Size	Min. Value	Max. Value	Data Type	Typical Entry
Extension Number	N	5	0	99999	Long Integer	3601
Group ID	N	4	0	1000	Short Integer	2
Interval Index	N	2	0	15	Short Integer	5

Field Definitions

- **Extension No.** – The extension number of up to 5-digits in length. This is the key field of the database, and entries must be arranged in ascending order.
- **Group ID** – The identification number of the group to which the extension is assigned. This number must lie within the range from 1 to 1000.
- **Interval Index** – The index to the specific interval of time in the Time Interval database during which the extension is routinely, administratively turned off. The index uses the following values:

  0: Constantly off.
  1-15: Index of the Time Interval database corresponding to the desired time interval.

Time Interval Database Information

The Time Interval database field entries are shown in the table below and defined in Field Definitions on page 21. Name the Time Interval master definition file **grdutf_m** and the application definition file **grdutf.**

Table 2-8 Time Interval Database Field Entries

Field Description	Master Definition File				Application Definition File	Master Database
	Type	Size	Min. Value	Max. Value	Data Type	Typical Entry
Interval Index	N	2	0	15	Short Integer	5
Begin Day of Week	N	1	0	6	Short Integer	5
Begin Hour	N	2	0	23	Short Integer	22
Begin Minute	N	2	0	59	Short Integer	0
End Day of Week	N	1	0	6	Short Integer	1
End Hour	N	2	0	23	Short Integer	5

Table 2-8 Time Interval Database Field Entries

End Minute	N	2	0	59	Short Integer	30

Field Definitions

- **Interval Index** – The number by which the following time interval is indexed in the database and referred to by the group, extension, and authorization code databases. This number must lie within the range from 1 to 15.
- **Begin Day of Week** – The day of the week on which the interval begins and the group, authorization code, or extension is administratively turned off. The day of week can be one of the following values:

  0: Sunday
  1: Monday
  2: Tuesday
  3: Wednesday
  4: Thursday
  5: Friday
  6: Saturday

- **Begin Hour** – The hour in which the interval begins and the group, authorization code, or extension is administratively turned off. The begin hour is a value between 0 and 23.
- **Begin Min.** – The minute at which the interval begins and the group, authorization code, or extension is administratively turned off. The begin minute is a value between 0 and 59.
- **End Day of Week** – The day of the week on which the interval ends and the group, authorization code, or extension is turned back on. The day of week can be one of the following values:

  0: Sunday
  1: Monday
  2: Tuesday
  3: Wednesday
  4: Thursday
  5: Friday
  6: Saturday

- **End Hour** – The hour in which the interval ends and the group, authorization code, or extension is turned back on. The hour is a value between 0 and 23.
- **End Minute** – The minute at which the interval ends and the group, authorization code, or extension is turned back on. The minute is a value between 0 and 59.

This completes creation of Guardian's database support. See "NEAX Command Assignments" on page 22. to make the necessary command assignments at the NEAX2400 MAT or NEAX2000 MOC (or CAT).

NEAX Command Assignments

This guide assumes that data settings that affect the operation of all OAI software on a system-wide basis have already been assigned on the NEAX2400 Maintenance Administration Terminal (MAT) commands, the NEAX2000 Customer Administration Terminal (CAT), or the NEAX2000 Maintenance Operations Console (MOC). Such settings include, for instance, system index values and assignment of Interface I/O Port Data in the Interface Processor (IP). For more information about the system data settings and about the Guardian settings discussed in this section, refer to the OAI System Manual and the Command Manual for the specific NEAX system in use:

Guardian is only effective if the Authorization Code or Forced Account Code service feature is engaged, and the station has been assigned to use the feature. The following data assignments set up this configuration on the NEAX MAT.MAT Assignments.

NEAX2400 Commands

AMND: Assignment of Maximum Necessary Digits

This command assigns the maximum number of digits to be read for the authorization code and the destination code.

(a) When this command is used for forced account codes or authorization codes, the tenant number (TN) must be assigned as 0, regardless of what tenant number was configured in the application configuration.

(b) Enter other information as requested by prompts, with the MND assigned to 10 digits.

(c) The number of digits in the authorization code or forced account code must agree with the number of digits specified in the application configuration and in the database creation process.

(d) Use the AATC command to provide the PBX with a backup database of authorization codes, in case the OAI application is not operating.

ARSC Command: Assignment of Route Restriction Class

This command assigns and displays route restriction information for a tenant and route number. This command actually activates the RSC. (Use the ASDT command to associate both the tenant and the service feature class assigned above to a specific station.)

(a) Use the same tenant number that was configured for the application through the APM.

(b) Enter other necessary information as requested by prompts, making sure that anything entered corresponds to the application configuration.

ASDT Command: Assignment of Station Data

Use this command to associate both the tenant and the route restriction class assigned above to a specific station and to specify the telephone class of the station.

(a) Use the same tenant number that was configured for the application through the APM.

(b) Make sure that the station number and route restriction class entered to this command are the same that are entered to the ARSC command (and/or the ASFC command).

ASFC Command: Assignment of Service Feature Class

This command assigns the combinations of PBX call processing features to SFC values from 0 to 15, by tenant. Use of this command activates the specified feature. (Use the ASDT command to associate both the tenant and the service feature class assigned above to a specific station.)

(a) Use the same tenant number that was configured for Guardian through the APM, Tenant #0.

(b) Ensure that the SFI for the desired class(es) is enabled.

(c) Enter other necessary information as requested by prompts, making sure that the service feature class assignment made through this command corresponds to the SFC as it is configured for the application through the APM.

ASPA Command: Assignment of Special Access Code

This command associates the authorization code to the access code. When the access code is dialed, it indicates that an authorization code follows and indicates the number of digits to be read.

(a) Use the same tenant number that was configured for Guardian in its configuration in the APM and enter an access code (ACC) between 1 and 6 digits in length.

(b) Enter the following data as requested by prompts:

SRV (Kind of Service) = SSC (Service Code)

CI (Connection Status Index) = N (Normal Service)

SID (Service Feature Index) = 42 (Authorization Code and Forced Account Code)

NND (Number of Necessary Digits) = Number of digits to be read, including the SID.

ASYD Command: Assignment of System Data

(a) System Data 1:

Index 43, bit 0 -- For remote access to PBX, is authorization code required after ring back tone (RBT)? 0 = Yes, 1 = No.

Index 43, bit 2 -- Will SST be sent after dialing access code? 0 = No, 1 = Yes

(b) System Data 2:

Index 3, bit 5 -- 0 = Authorization Code
1 = Forced Account Code

AATC Command: Assignment of Authorization Code Data

This command should be used to provide the PBX with a backup database of authorization codes, in case the OAI application is not operating.

NEAX2000 Commands

Use the NEAX2000 Customer Administration Terminal (CAT), or the NEAX2000 Maintenance Operations Console (MOC) to enter these commands. (Refer to the *NEAX2000 System Manuals* for more information.)

CM20: (Assignment of Access Code)

Y=Tenant Group: Access Code for ID code class change.

1st data Access Code (1-3 digits)

2nd data Service Type
:086: Authorization code
Use A57 for the first digit of the authorization code
:087: Forced Account code

CM42: (Assignment of Maximum Digits for Authorization Code)

Sets ID code digits.

1st data :11: Authorization code
:12: Forced Account Code
:13: Remote Access to System ID code

2nd data:01–10: Number of digits (The default is 10 digits.)

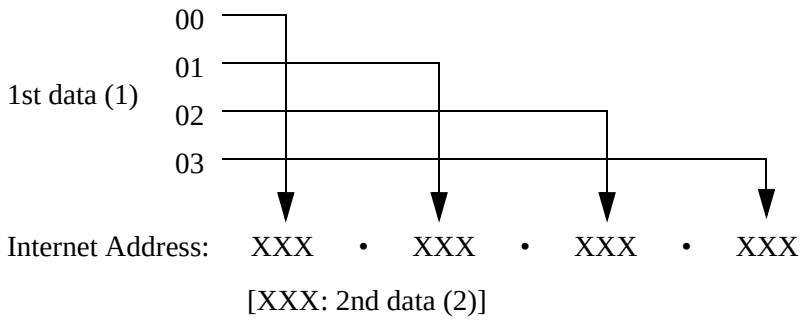
CMD79: (Assignment of Internet Address)

Assigns the Internet Address of TCP/IP-Ethernet.

1st data 00–03: Division No. of Internet Address

2nd data 0–255: Address Data (1–3 digits)

The Internet Address must be assigned to the 1st data 00–03 as follows:



CM08: (Checking ID Codes Using AP01)

Basic Functions

1st data: 217 Check ID code
2nd data::0: Check through MP
:1: Check through AP01 package when using ACF. (Set checking through AP01 package when using ACF.)

CMD53: (Handling of ID Codes When the IP is Down)

Registers ID codes and temporary class data.

1st data: ID code

2nd data :a b b c c d d e e: Temporary class data
:a: 0–2,9: Temporary class type
:b b: 01–08: Temporary connection restriction class
:c c: 01–15: Temporary service restriction class – A
:d d: 01–15: Temporary service restriction class – B
:e e: 01–15: Temporary service restriction class – C
:NONE (Initial value)

Note: *This data uses PBX internal class change data when ACF is in operation and the AP is stopped. The number of digits is set through CMD7B*

CMD7B: (Number of ID Code Digits When IP down)

ACF

1st data: 00: Number of ID code digits when AP stops during ACF operation

2nd data :1–3: Number of ID code digits when AP stops
:0 (Initial Value):No ACF operation

Initialization

Follow steps 1-3 below to complete initialization.

Step 1: Initialization in APM

Enter the APM Operations Menu and initialize Guardian through the Non-CRT Application option, according to instructions provided in the **APM Operations Manual**.

Step 2: Login Password

The first time you initialize Guardian and you enter **guardadm** at the login prompt, you must identify the password that is to be associated with that login ID. To assign a null password, enter the responses indicated for the following prompts:

Prompt: UNIX login prompt

Response: Enter **guardadm** and press Enter.

Prompt: You do not have a password.
1. Select your own password
2. UNIX will select a password for you.

Response: Select option **1** and press Enter.

Prompt: A prompt asks for the new password, and another prompt requests verification of the password.

Response: Press Enter at both prompts. This process assigns a null password.

Step 3: Regular Entry to Guardian

At the UNIX login prompt, enter **guardadm** and press Enter. To exit the password input field, press Enter a second time. The Guardian password entry screen displays.

Chapter 3 Administration

Overview

The Guardian main menu provides tools which you can use to manage and generate reports from the record file, assign or alter passwords, and change or view the status of groups, authorization codes, and extensions.

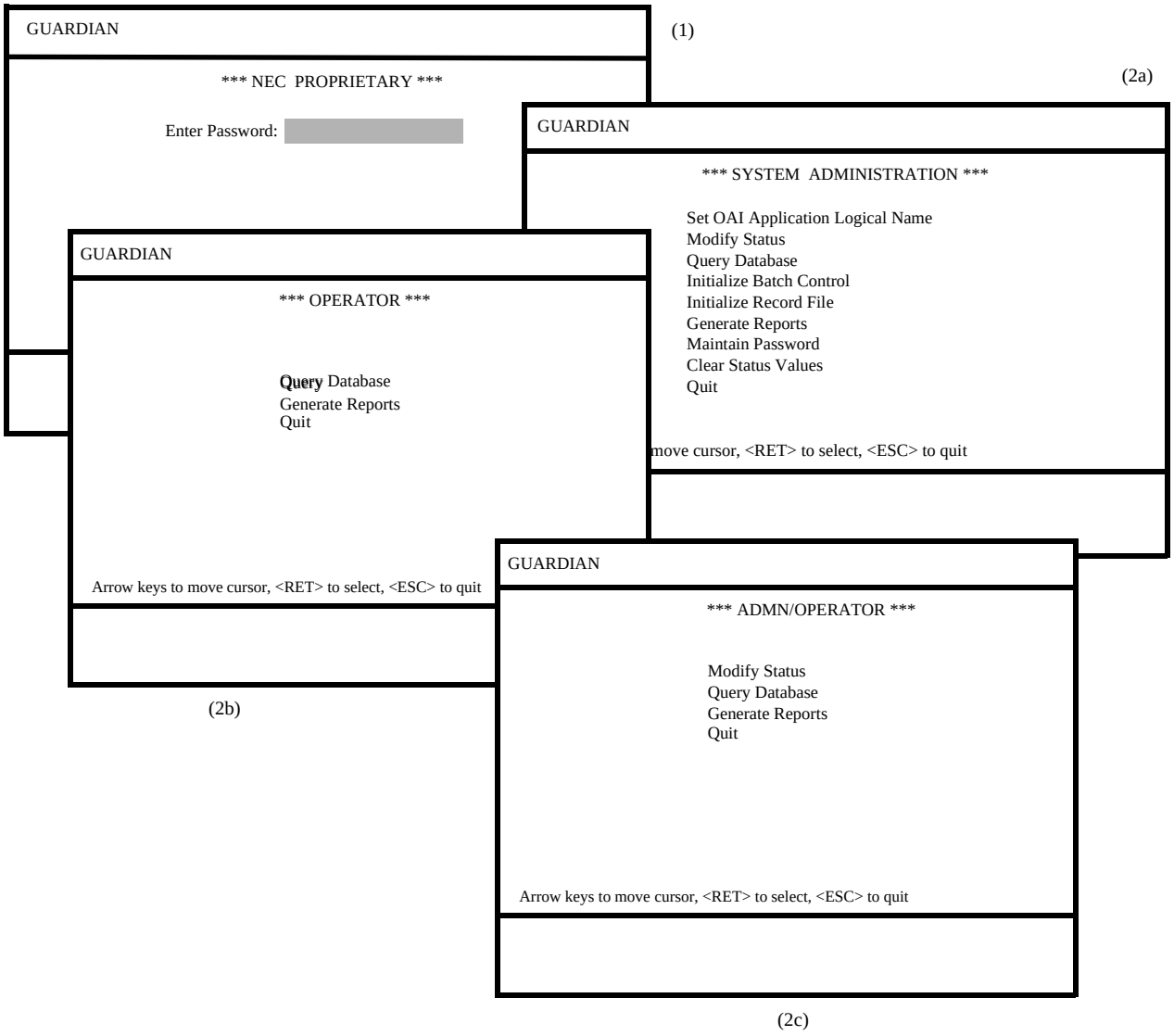


Figure 3-1 Main Menu

Notes

Guardian menus are password protected. You can enter Guardian at one of the following levels by entering the appropriate password:

- Administrator level – Provides access to every menu option. The default password (**guardadm**) can be changed through the Administrator main menu
- Operator level – Allows you to view database information or to generate reports. You must assign this password through the Administrator main menu.
- Admn/Operator level - Provides access to all Operator level menus plus the modify status menu.

All Guardian menu options are described briefly below. Each option is described in more detail in the remaining sections of this chapter:

- **Set OAI Application Name –** Allows you to specify a tenant by logical application name. The work you perform while working at the Administrator level applies only to the specified tenant.
- **Modify Status –** Use this menu option to modify the enable/disable status of a single group, authorization code, or extension. The System Administrator can also use this option to override the System Disable of an extension, if necessary.

  Note: *The ID database can only be modified through the APM Database Administration menu.*

- **Query Database –** Use this menu option to check a working database without making changes to it. This option enables the System Administrator to review the disable status of a group, authorization code, ID, or extension and the parameters by which it is defined in the database.

  Note: *This menu option displays after you enter the Operator password.*

- **Initialize Batch Control –** Initiates the Guardian control of batch modifications to the status of a large number of groups, authorization codes, or extensions. Data entry for this batch control is user-defined and provided.
- **Initialize Record File –** Reinitializes the record file in which data is collected about invalid call attempts and the ongoing status of groups, authorization codes, and extensions.
- **Generate Reports –** Generates various management and control reports about invalid call attempts; the status of groups, authorization codes, and extensions; and the history of processing activities logged in the record file.

  Note: *This menu option displays after you enter the Operator password.*

- **Maintain Password –** Allows you to change the password required for entry into the Guardian main menu. Administrators use this option to assign operator password(s).
- **Clear Status Values –** Removes all modifications to the working status of all groups, extensions, and authorization codes and reinstates the configured status of each.

Notes (Continued)

The System Administrator also requires access to the APM Data Entry menu in order to maintain the Guardian databases.

Note: *Changes to the databases (i.e., adding, deleting, or modifying records) can only be made through the APM. The changes are processed into the Guardian working databases.*

Caution: *If 80% of disk space has been used on the system, the following message appears immediately after you logon: "Disk free space warning." When this message displays, you must free up disk space before performing other activities in the system. You can free up disk space by generating reports and then initializing the record file. If you do not generate the reports before you reinitialize the file, all of the data logged into the record file is lost when it is reinitialized. If you do not free up disk space when you receive this message, you may run out of disk space completely. When no disk space remains in the system, you must initialize the record file without generating the reports. The data logged into the record file is lost.*

Procedure

Action	Result
At the login prompt, enter the Administrator, Operator or Admn/ Operator password and press Enter.	The main menu displays.
Using the arrow keys to position the cursor, select the desired menu option and press Enter.	The desired option displays.
To exit the main menu, select the Quit option and press Enter, or press ESC.	The password screen reappears.

Set OAI Application Logical Name

Guardian can serve multiple tenants (e.g., different departments, different campuses, etc.). Each tenant is identified by a unique logical name that is configured in the APM during installation. When you enter a logical name on this screen, all functions performed are implemented with the tenant associated to that logical name until the logical name is reset.

One tenant could serve more than one switch. Logical names for each switch for that tenant must be entered. Up to ten logical names are permitted.

Use the Set OAI Application Logical Name option on the main menu set or change the name of the tenant. This option can be accessed only under the Administrator password.

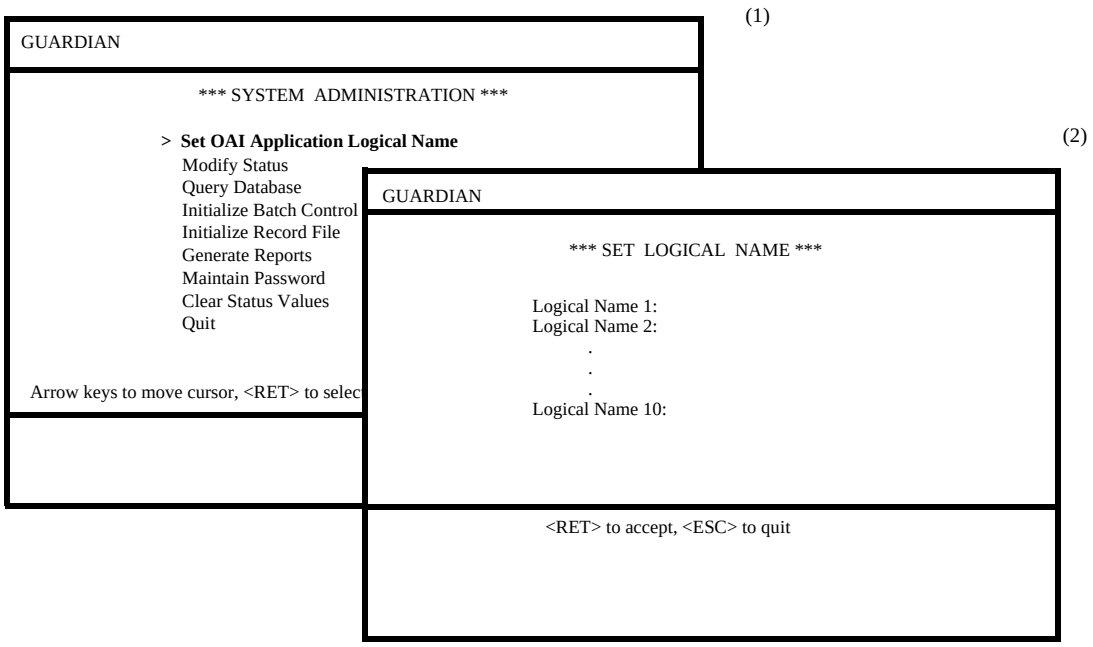


Figure 3-2 Set Logical Name

Notes

The first time entering the System Administration menu, access is denied access to other options until the logical name is entered. Once this application logical name is set, it remains in effect until changed again through this option, and access to other menu options is no longer restricted.

If your system accommodates one tenant, you only need to enter the tenant name once. If your system accommodates more than one tenant, you will need to identify the tenant each time it changes before you use any other menu options. When you enter a new logical name, the system pauses for approximately 3 seconds while Guardian searches for the corresponding tenant.

Procedure

Action	Result
On the main menu, select the **Set OAI Application Logical Name** option and press Enter. (1)	The Logical Name prompt highlights. (2)
Type the Logical Name of the desired tenant from the configuration file and press Enter.	Following a 3-second delay, the message **Set Logical Name Successful** appears. **Note:** *If the name you entered is not in the configuration data or corresponds to a tenant that is not initialized, the error message **Error Setting Logical Name** appears, and the field highlights again for re-entry.*
Press ESC to exit.	Control returns to the main menu.

Modify Status

Overview

The Modify Status option on the main menu allows Administrators to modify the disable status of a single group, authorization code, or extension. This option can only be accessed under the Administrator password.

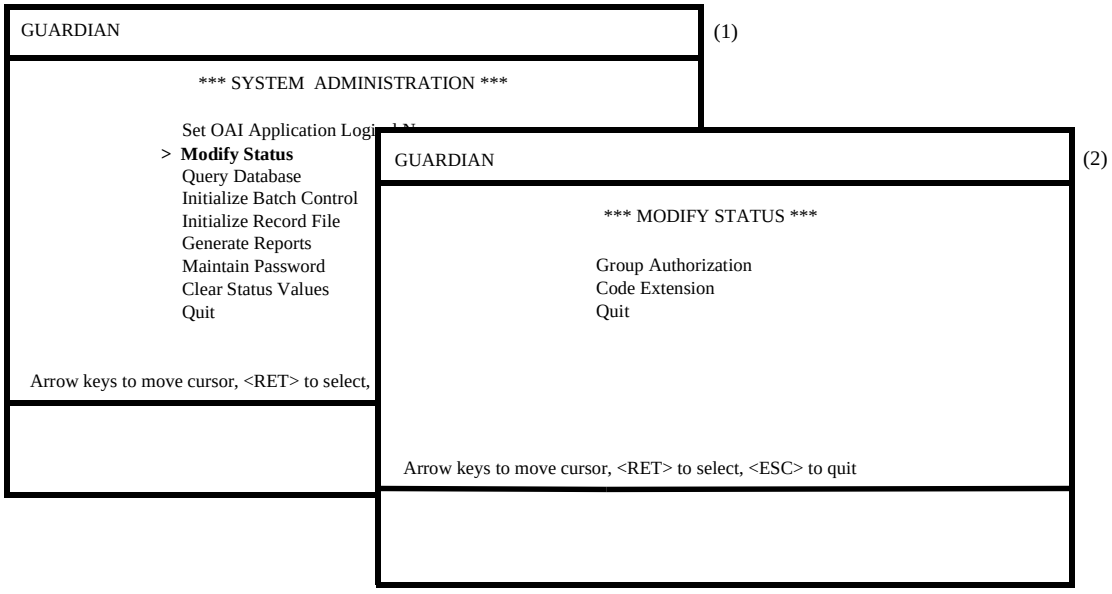


Figure 3-3 Modify Status

Notes

The Modify Status option allows the Administrator to disable a group of extensions, an authorization code, or a single extension in the following ways:

- **Unconditionally –** Disabled constantly and indefinitely, until enabled again by the Administrator.
- **Routinely –** Disabled during the time interval associated with the group, authorization code, or extension in the database, as illustrated in the following example:

  In the Group database, Group 2 is assigned an Interval Index of 5. In the Time Interval database, Interval Index 5 is a period that starts Friday at 10:00 p.m. and ends Monday at 5:30 a.m. When the System Administrator uses the Modify Status option to indicate YES in the *Routinely Disable:* field for Group 2, all of the extensions in this group are turned off during the Friday to Monday time period until either this same field is again changed or the Interval Index is changed.

Notes (Continued)

The System Administrator can also override the System Disable of an extension using this option. When Guardian has temporarily turned off an extension that has been used in an excessive number of invalid call attempts, the administrator can use this option to turn on the extension without altering the System Disable parameters in the Extension database. The next time the number of invalid call attempts on that extension exceeds the tolerated frequency, Guardian disables the extension again.

The ID database can only be modified through the Database Administration option in the APM. The Guardian Modify Status option cannot access the ID database.

There are two kinds of errors that may occur in the Modify Status option:

- **Database Record Not Found**: If the system cannot find the record for the number you enter (group ID, authorization code, or extension number), this error message appears. Press ESC and re-enter the number. If the error message appears again, check the record through the APM master database and use the Process/Install command to reinstate the working database. If the error persists, call the system distributor.
- **Error Processing Modification to Database**: If the record has been retrieved and the status modification has been entered, this message appears. If this occurs, call the system distributor.

Procedure

Action	Result
On the main menu, select the **Modify Status** option and press Enter. (1)	The Modify Status menu displays. (2)
Using the arrow keys to move the cursor, select the desired menu option and press Enter.	A selection screen for the option displays.
To exit the Modify Status menu, select the Quit option and press Enter, or press ESC.	The main menu reappears.

Group

The Group option on the Modify Status menu allows Administrators to alter the disable status of all the extensions in a group simultaneously. When you select the **Group** option, the Modify Group screen displays.

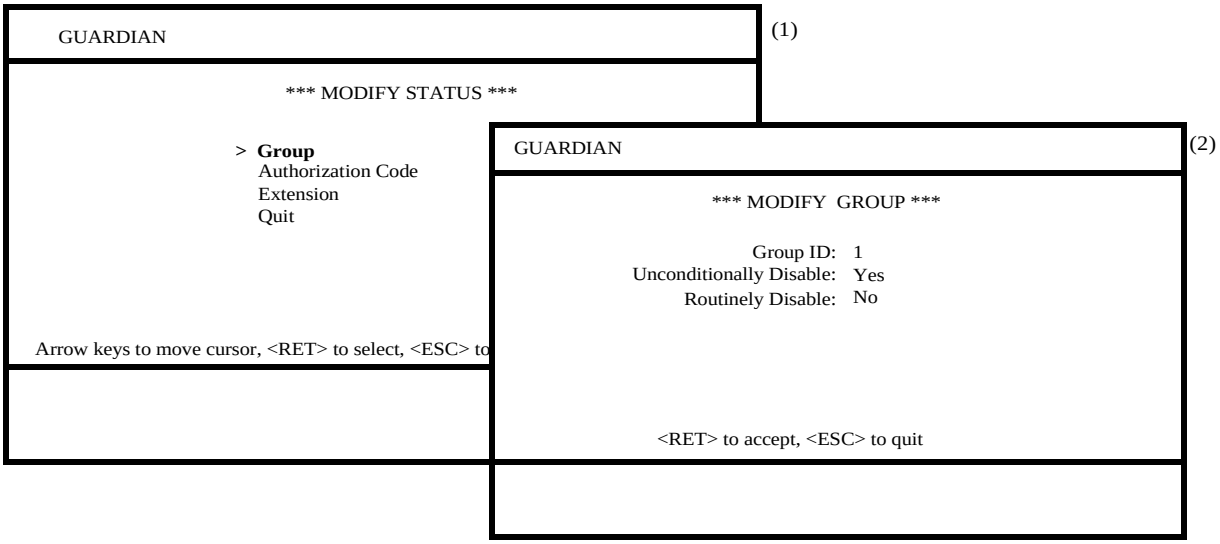


Figure 3-4 Modify Group

Notes

If the group is set to be unconditionally disabled (Yes), all of its extensions are disabled indefinitely as soon as this procedure is completed. If the group is set to be routinely disabled (Yes), all of its extensions are regularly disabled during the time interval that is designated by the Interval Index in the group database record. (You can review the database record using the Query Database option on the System Administration menu or by entering the APM Database Administration option.)

Procedure

Action	Result
On the Modify Status screen, select the **Group** option and press Enter. (1)	The Group Selection screen displays with a prompt for the Group ID.
Type the ID of the group and press Enter. **Note:** *Press ESC to exit the screen and redisplay the Modify Status menu.*	The Modify Group screen displays showing the current status of the group in the second field (Yes or No). (2) **Note:** *If the system does not recognize the Group ID you entered, the message **Error Database Record Not Found** appears. Press ESC and try again, or exit and query the database.*
Enter the desired status to each field (**Yes** or **No**), pressing Enter after each entry.	The message **Modify Group Status Successful** appears. **Note:** *If you enter anything other than Yes or No in the disable fields, the message **Error Processing Status Modification** appears. Either press ESC to return to the Modify Status menu or re-enter the correct status and press Enter.*
Press ESC to exit the screen.	The Group Selection screen reappears for entry of another Group ID.
Press ESC again to exit the Selection screen.	The Modify Status menu reappears.

Authorization Code

Administrators can use the **Authorization Code** option on the Modify Status menu to change the disable status of the designated authorization code. When you select this option, the Modify Authorization Code screen displays.

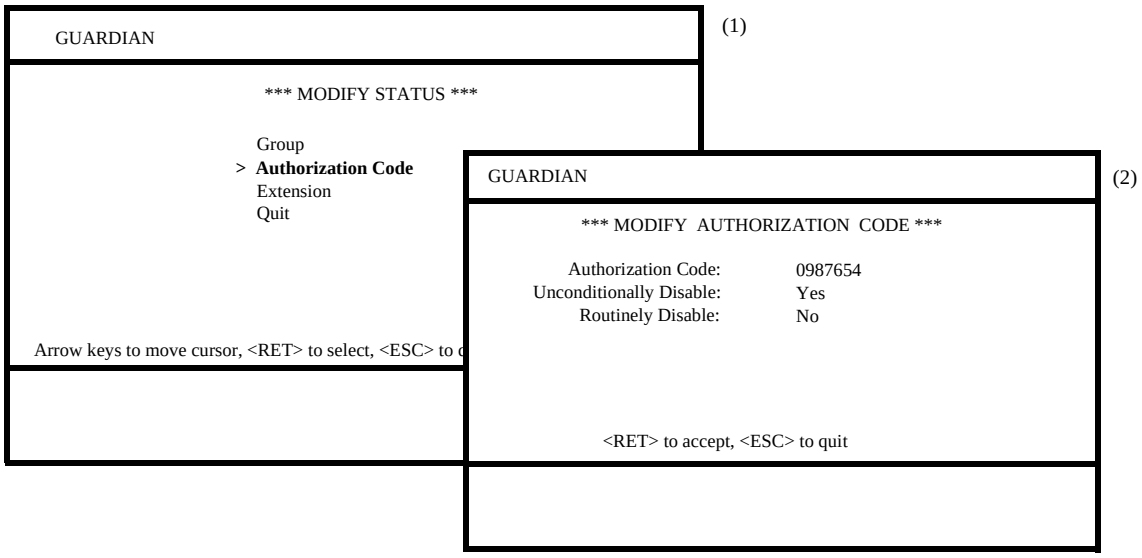


Figure 3-5 Modify Authorization Code

Notes

If the authorization code is set to be unconditionally disabled (Yes), it is disabled indefinitely as soon as this procedure is completed. If the authorization code is set to be routinely disabled (Yes), the authorization code is regularly disabled during the time interval that is designated by the Interval Index in the authorization code database record. (You can review the database record using the Query Database option on the System Administration menu or by entering the APM Database Administration option.)

Procedure

Action	Result
On the Modify Status screen, select the **Authorization Code** option and press Enter. (1)	The Authorization Code Selection screen displays with a prompt for the authorization code.
Enter the authorization code and press Enter. **Note:** *Press ESC to exit the screen and redisplay the Modify Status menu.*	The Modify Authorization Code screen displays showing the current status of the code in the second and third fields (Yes or No). (2) **Note:** *If the system does not recognize the Authorization Code you entered, the message **Error Database Record Not Found** appears. Press ESC and try again or exit and query the database.*
Enter the desired status to each field (**Yes** or **No**), pressing Enter after each entry.	The message **Modify AuthCode Status Successful** appears. **Note:** *If you enter a value other than Yes or No in either of the disable fields, the message **Error Processing Status Modification** appears. Either press ESC to return to the Modify Status menu or re-enter the correct status and press Enter.*
Press ESC to exit the screen.	The Authorization Code Selection screen reappears for entry of another authorization code.
Press ESC again to exit the Selection screen.	The Modify Status menu reappears.

Extension

Administrators can use the Extension option on the Modify Status menu to change the disable status of an extension. When you select this option, the Modify Extension screen displays.

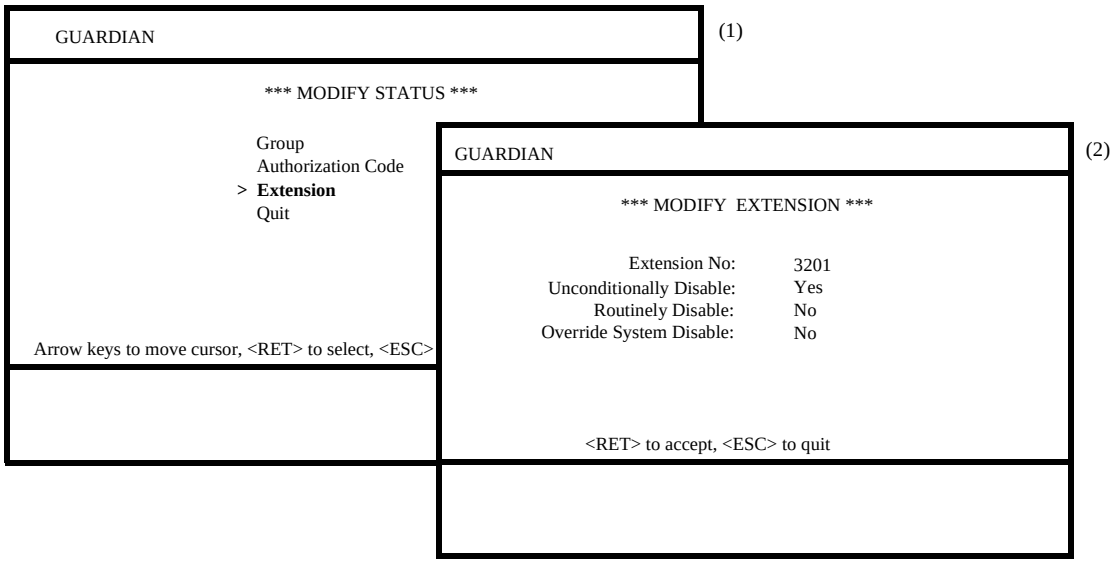


Figure 3-6 Modify Extension

Notes

If the extension is set to be unconditionally disabled (Yes), it is disabled indefinitely as soon as this procedure is completed. If the extension is set to be routinely disabled (Yes), the extension is regularly disabled during the time interval that is designated by the Interval Index in the authorization code database record. (You can review the database record using the Query Database option on the System Administration menu or by entering the APM Database Administration option.)

The Administrator can override the system disable setting of any extension. If the Administrator needs to turn on an extension after it has been turned off by the system, the Administrator may set the override field to Yes. This override affects only the current system disabling of the extension; it does not protect the extension from being disabled after another episode excessive invalid call attempts. ('No' is the default setting in this field.)

Procedure

Action	Result
On the Modify Status screen, select the **Extension** option and press Enter. (1)	The Extension Selection screen displays with a prompt for the extension.
Enter the extension and press Enter. **Note:** *Press ESC to exit the screen and redisplay the Modify Status menu.*	The Modify Extension screen displays showing the three disable statuses for the indicated extension. (2) **Note:** *If the system does not recognize the Extension you entered, the message **Error Database Record Not Found** appears. Press ESC and try again or exit and query the database.*
Enter the desired status to each field (**Yes** or **No**), pressing Enter after each entry.	The message **Modify Extension Status Successful** appears. **Note:** *If you enter a value other than Yes or No in any of the disable fields, the message **Error Processing Status Modification** appears. Either press ESC to return to the Modify Status menu or re-enter the correct status and press Enter.*
Press ESC to exit the screen.	The Extension Selection screen reappears for entry of another extension.
Press ESC again to exit the Selection screen.	The Modify Status menu reappears.

Query Database

Overview

Use the Query Database option on the main menu to view the records of a working database. You can access this option with either the Administrator or the Operator password. When you select this option, the Query Database Menu displays for one of the three databases.

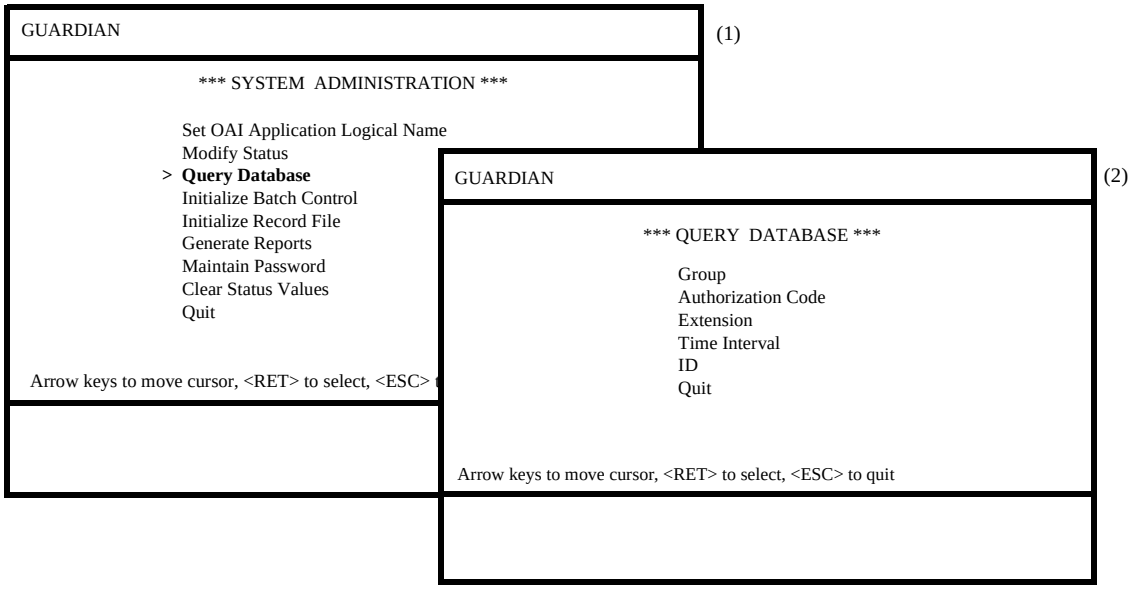


Figure 3-7 Query Database

Notes

Using this option, the System Administrator or Operator can review records in any of the five working databases. These databases include the fields maintained through the APM Database Administration menu and the current disable status of each group, authorization code, or extension. The Query option provides a view-only display of the databases. You cannot make changes through this option.

If the system cannot find the record for the number you entered (group ID, authorization code, or extension number), the error message **Database Record Not Found** appears. Press ESC and re-enter the number. If the message occurs again, check the record through the APM master database and use the Process/Install command to reinstate the working database. If the error persists, call the system distributor.

Procedure

Action	Result
On the main menu, select the **Query Database** option and press Enter. (1)	The Query Database menu displays. (2)
Using the arrow keys to position the cursor, select the desired menu option and press Enter.	The desired option displays.
To exit the Query Database menu, select the Quit option and press Enter, or press ESC.	The main menu reappears.

Group Database

When you select the Group option on the Query Database menu, the Group Database screen displays information in the Group database.

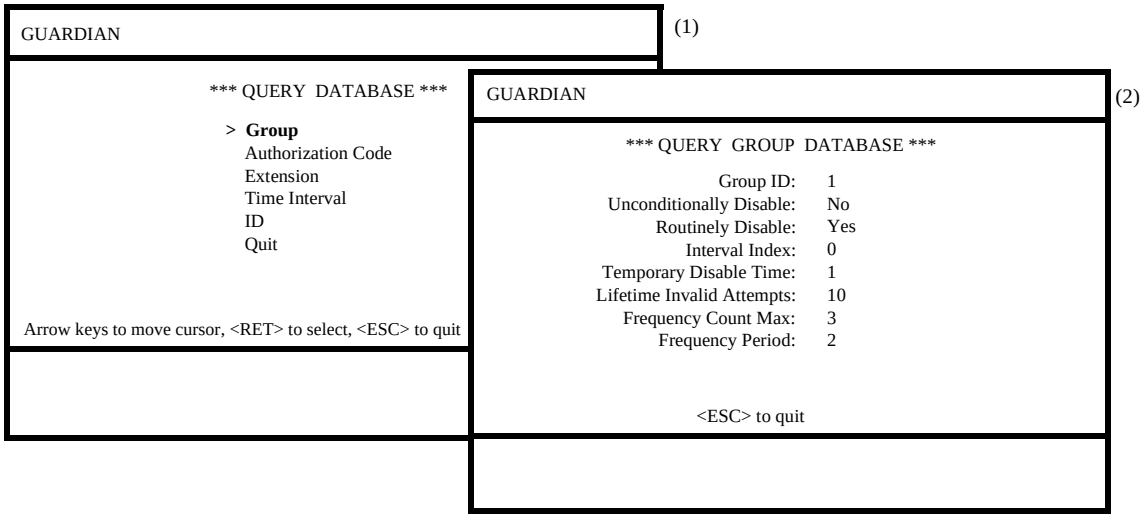


Figure 3-8 Query Group Database

Notes

Fields in the working Group database are defined below. For more information about these fields, refer to Chapter 2, “Installation Introduction” on page 7.

- **Group ID –** The number that identifies a group.
- **Unconditionally Disable –** Indicates whether or not the group is disabled indefinitely by the Administrator.
- **Routinely Disable –** Indicates whether or not the group is scheduled to be routinely disabled during a time interval designated by an Interval Index.
- **Interval Index –** The index to the specific time interval in the Time Interval Database during which all extensions in a group are routinely disabled, if the group is scheduled to be disabled.
- **Temporary Disable Time –** The number of 15-minute intervals that an extension in the group will remain disabled by the system in response to an excessive frequency of invalid call attempts.
- **Lifetime Invalid Attempts –** The maximum lifetime number of accumulated invalid attempts that are allowed before an extension in the group is temporarily system disabled.
- **Frequency Count Max –** The maximum number of invalid call attempts that are counted during the designated period before the frequency is considered excessive and the extension in the group is system disabled.
- **Frequency Period –** The period of time in minutes in which invalid call attempts are counted.

Procedure

Action	Result
On the Query Database menu, select the **Group** option and press Enter. (1)	The Group Database screen displays with the Group ID prompt.
Enter the ID of the group to be reviewed and press Enter.	The remaining fields are completed with data associated with the identified group. (2)
Press ESC to exit the display.	The *Group* field is singled out and highlighted again for entry of another group ID.
To exit the Query Group Database screen, press ESC.	The Query Database menu reappears.

Authorization Code Database

Select the **Authorization Code** option on the Query Database menu to display the Authorization Code Database screen.

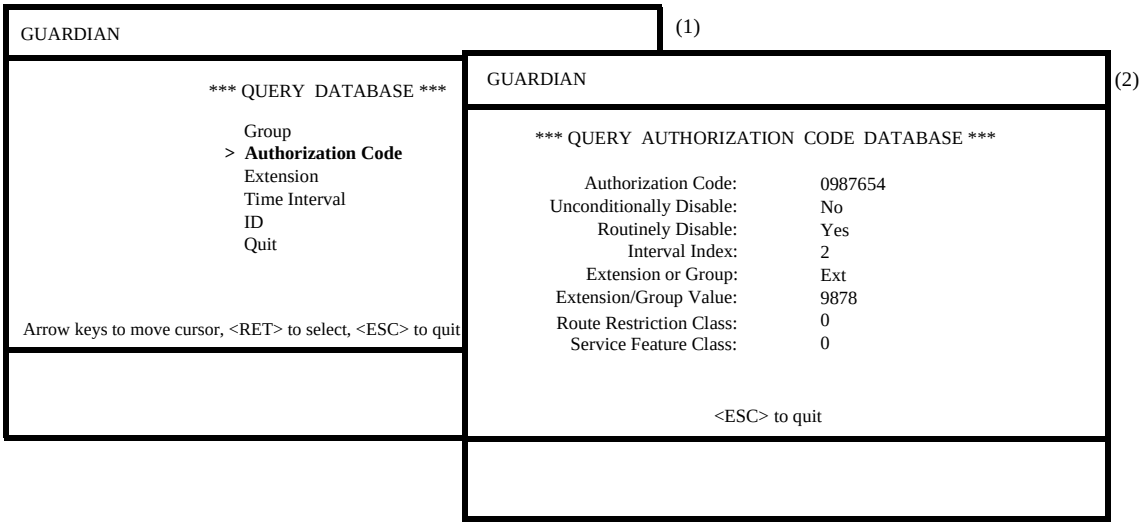


Figure 3-9 Query Authorization Code Database

Notes

Fields in the working Authorization Code database are defined below. For more information about these fields, refer to Chapter 2, “Installation Introduction” on page 7.

- **Authorization Code –** The 10-digit authorization code.
- **Unconditionally Disable –** Indicates whether or not the authorization code is disabled indefinitely by the Administrator.
- **Routinely Disable –** Indicates whether or not the authorization code is scheduled to be routinely disabled during a time interval designated by an Interval Index.
- **Interval Index –** The index to the specific time interval in the Time Interval Database during which the authorization code is routinely disabled, if the authorization code is scheduled to be disabled.
- **Extension or Group –** The assignment of the authorization code, where **Ext** indicates that it is assigned to an extension and **Grp** indicates that it is assigned to a group of extensions.
- **Extension/Group Value –** The actual extension number or group ID to which the authorization code is assigned, depending upon the Extension or Group assignment.
- **Route Restriction Class –** A value from 0 to 15 that represents the combination of distance (e.g., local, national) and routing service (e.g., MCI, Sprint, AT&T) privileges assigned to the authorization code.
- **Service Feature Class –** A value from 0 to 15 that represents the combination of call processing features (e.g., call forwarding, conferencing, call pick-up) that are assigned to the authorization code.

Procedure

Action	Result
On the Query Database menu, select the **Authorization Code** option and press Enter. (1)	The Authorization Code Database screen displays with the authorization code prompt.
Enter the authorization code to be reviewed and press Enter.	The remaining fields are completed with data associated with the selected authorization code. (2)
Press ESC to exit the display.	The *Authorization Code* field is singled out and highlighted again for entry of another authorization code.
To exit the Query Authorization Code Database screen, press ESC.	The Query Database menu reappears.

Extension Database

Select the Extension option on the Query Database menu to display the Extension Database screen. When you enter the desired code, the field values for that extension display.

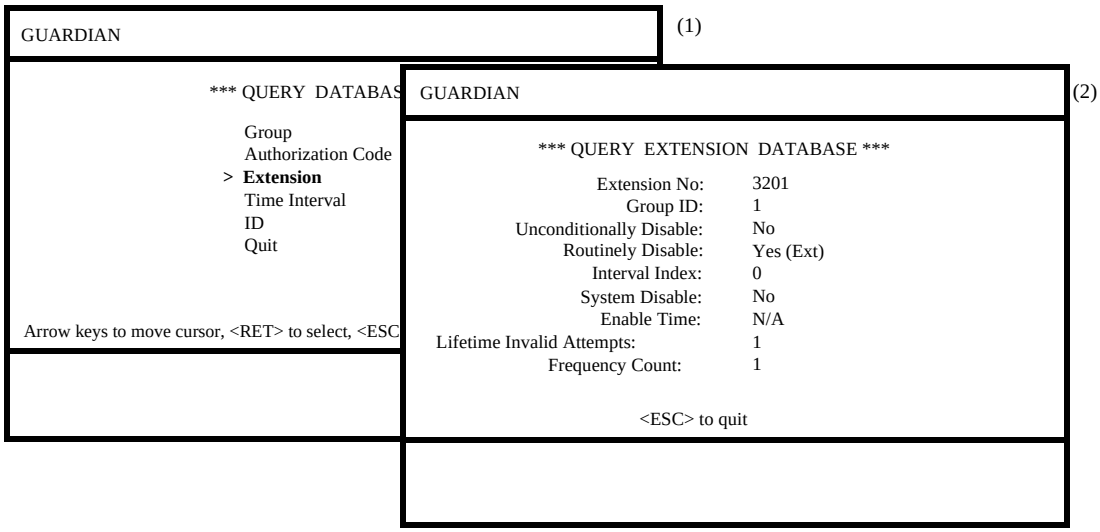


Figure 3-10 Query Extension Database

Notes

Fields in this database are defined below. For more information about these fields, refer to Chapter 2, “Installation Introduction” on page 7.

- **Extension Number –** The actual extension number.
- **Group ID –** The group to which the extension is assigned.
- **Unconditionally Disable –** Indicates whether or not the extension is disabled indefinitely by the Administrator.
- **Routinely Disable –** Indicates whether or not the extension is scheduled to be routinely disabled during a time interval designated by an Interval Index. When the Routinely Disable status of the extension is YES, a notation to the right indicates whether the extension is disabled as part of a group (Grp) or individually as a single extension (Ext). The (Ext) notation also displays if both the extension and its group are disabled.
- **Interval Index –** The index to the specific time interval in the Time Interval Database during which the extension is routinely disabled, if the extension is scheduled to be disabled.
- **System Disable –** The current system status, indicating whether it is disabled (YES) or not (NO). Use the Group Database Query to review system disable limits.

Notes (Continued)

- **Enable Time –** The time at which the extension is to be enabled, if the extension is currently disabled. The amount of time before the extension is enabled depends on the number of 15-minute intervals indicated in the database for the system disable period. If the extension is not system disabled, this field displays a N/A (Not Applicable) notation.
- **Lifetime Invalid Attempts –** The number of invalid attempts currently accumulated against the number allowed during the lifetime of the extension.
- **Frequency Count –** The number of invalid attempts counted during the current time period.

Procedure

Action	Result
On the Query Database menu, select the **Extension Database** option and press Enter. (1)	The Extension Database screen displays with the extension prompt. (2)
Enter the number of the extension to be reviewed and press Enter.	The remaining fields are completed with data associated with the selected extension.
Press ESC to exit the display.	The *Extension* field is singled out and highlighted again for entry of another extension.
To exit the Query Extension Database screen, press ESC.	The Query Database menu reappears.

Time Interval Database

Select the Time Interval Database option on the Query Database menu to display the Time Interval Database screen. When you enter an index number, the field values for that interval display.

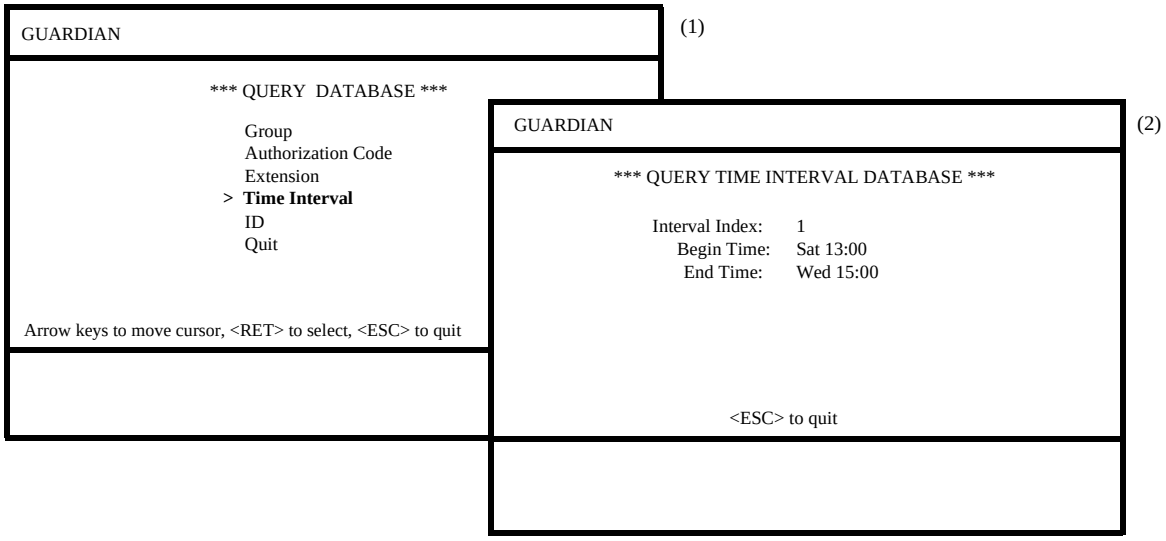


Figure 3-11 Query Time Interval Database

Notes

The time periods specific in this database are those intervals during which extensions, groups of extensions, or authorization codes can be routinely disabled.

Fields in this database are defined below. For more information about these fields, refer to.

- **Interval Index –** The number by which the time interval is indexed in the database and referred to by the group, extension, and authorization code databases.
- **Begin Time** – The day of the week, the hour, and the minute at which the routine disable period begins.
- **End Time** – The day of the week, the hour, and the minute at which the routine disable period ends.

Procedure

Action	Result
On the Query Database menu, select the **Time Interval Database** option and press Enter. (1)	The Time Interval Database screen displays with the Interval Index prompt.
Type the Interval Index to be reviewed and press Enter.	The remaining fields are completed with the beginning and ending times of the selected Interval Index. (2)
Press ESC to exit the display.	The *Interval Index* field is singled out and highlighted again for entry of another extension.
To exit the Query Time Interval Database screen, press ESC.	The Query Database menu reappears.

ID Database

Select the ID option on the Query Database menu and enter a user identification number to display the authorization code associated to that identification number.

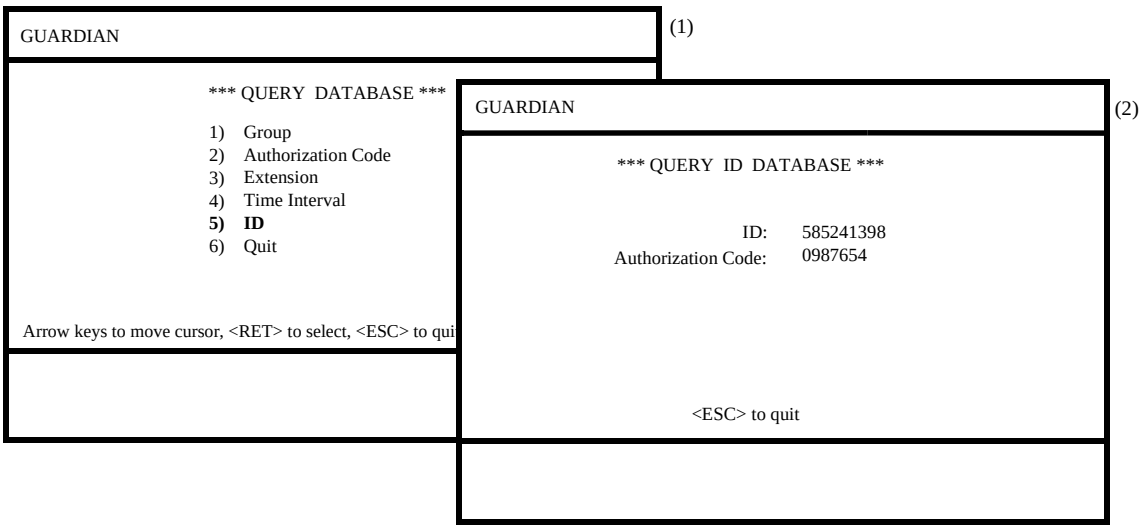


Figure 3-12 Query ID Database

Notes

Fields in the ID database are defined below:

- **ID –** The telephone user identification number consisting of up to 10 characters.
- **Authorization Code** – The authorization code assigned to the telephone user identification number above.

Procedure

Action	Result
On the Query Database menu, select the **ID Database** option and press Enter. (1)	The ID Database screen displays with the ID prompt.
Type the ID to be reviewed and press Enter.	The authorization code assigned to the ID you entered displays. (2)
Press ESC to exit the display.	The *ID* field is singled out and highlighted again for entry of another ID.
To exit the Query ID Database screen, press ESC.	The Query Database menu reappears.

Initialize Batch Control

Use the Initialize Batch Control option on the main menu to activate a batch modification to the disable status of a large number of groups, authorization codes, or extensions. This option provides the internal processing and its control, while the user prepares the actual batch file of changes. You can only access this option with the Administrator password.

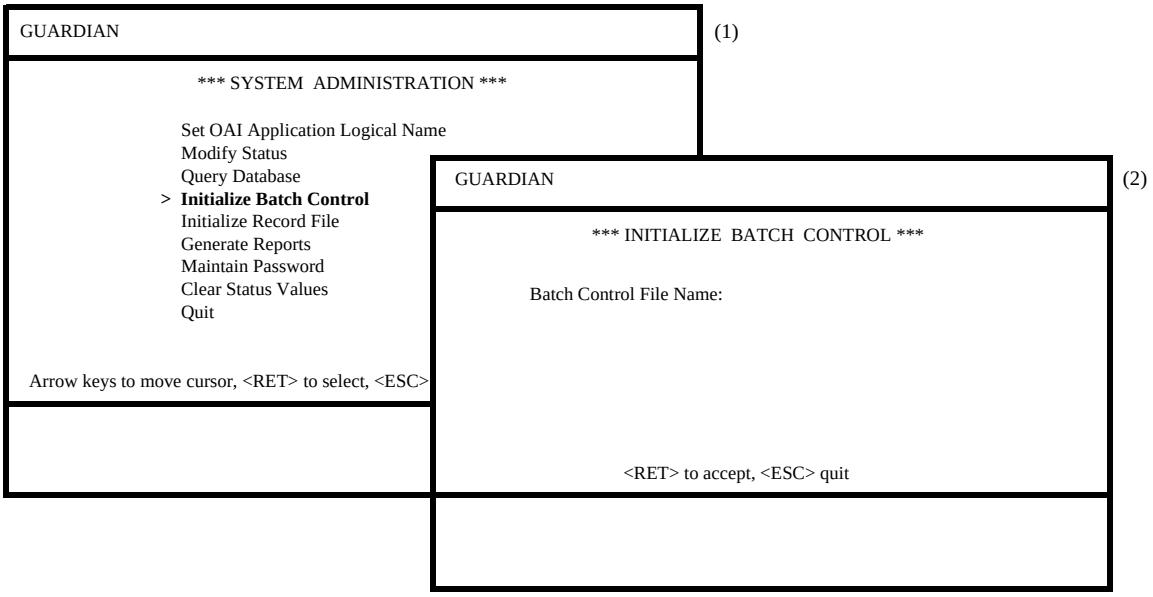


Figure 3-13 Initialize Batch Control

Notes

The following is an example of the Initialize Batch Control function:

If you need to change the disable status of 1000 authorization codes, you can enter the codes into a text file named 'AC_disable'. Select the Initialize Batch Control option, and type **AC_disable** at the prompt, preceded by the full path name. When you press Enter, Guardian reads the file and implements each status change.

Each file record must contain the following three fields prepared in ASCII characters in the format shown below:

Database Record Type | Database Record Key | Admin Disable Flag<NL>

- **Database Record Type –** Specifies which database contains the record to be modified by the batch file record. Valid values are: **G** (Group), **A** (Authorization Code), and **E** (Extension).
- **Database Record Key –** Specifies which record in the database is to be modified and contains the actual Group ID (1-1000), 10-digit Authorization Code, or 5-digit Extension Number.
- **Disabled –** Specifies the change in status to be made to the designated record. Use one of the following values: **YES (**routinely disable), **UC** (unconditionally disable), or **NO** (the group, authorization code, or extension is not to be disabled routinely or unconditionally).

All three fields must contain an entry. Each field must be separated by the ' | ' character, except the last one of the record. You must conclude the record with <NL>, the ASCII New Line character, which is a Hex (0a) or Decimal (10). Batch file records are not valid and will not be processed if any of the three fields does not have an entry or if the record is not concluded by the <NL> character. A few valid entries are provided below.

G | 1 | YES <NL> – Routinely disable Group No. 1 in the Group database.

A | 1234567000 | NO <NL> – Enable Authorization Code 1234567 in the Authorization Code database.

E | 4395 | UC <NL> – Unconditionally disable Extension No. 4395 in the Extension database.

Errors that are encountered during processing of the batch file are logged into a file. The two types of errors that may occur are as follows:

File Not Found – The named batch file could not be found. No processing was performed, but the batch file name was logged.

Bad Batch Control File Record – A record contained an error. This record error was logged in the following format: **Record #10, Item #2**.

After processing is completed, you can use Guardian options for handling the error output, including printing, viewing, and saving errors to disk. When you exit from the screen, the error log file is erased. The only way to reproduce it after leaving the screen is to reprocess the batch file from which it came. Therefore, we recommend that you either print or save the error log file on disk if you need to reference this information later.

Procedure

Action	Result
On the main menu, select the **Initialize Batch Control** option and press Enter. (1)	The batch control file name prompt appears.
Enter the batch control file name and press Enter. **Note:** *Press ESC after a successful batch process to display the file name entry field to process another file.*	If no errors occurred during processing, the message **Batch Modify Successful** appears. If one or more errors occurred during processing, the message **Error in Processing – Select Option For Error Log** appears.
To examine error items, press Enter and use the arrow keys to position the cursor on the desired error output command (**Print File**, **View File**, **Save File**) and press Enter.	**PRINT FILE:** Error items are printed and the output commands redisplay. **VIEW FILE:** Error items are scrolled for display on the screen with **Top of File**, **End of File** and **More** notations indicating placement. The commands serve to move the screen down the page (**DownPage**), up the page (**UpPage**), to the beginning of the file (**Top**), or to the end of the file (**Bottom**). To exit and return to the output commands, select the **Quit** command and press Enter. **SAVE FILE:** A prompt requesting the name of the file in which the error items are to be saved appears with a default file name inserted. Enter the appropriate file name and press Enter. The error items are stored under the indicated file name and the output commands redisplay. To exit the output commands, select the **Quit** command and press Enter.
To exit the Initialize Batch Control option, press ESC.	The main menu reappears.

Initialize Record File

Use the Initialize Record Files option on the System Administration menu to reinitialize the record file. This file contains recorded information used by the system to generate the reports available through the Reports option. This option can only be accessed with the Administrator password.

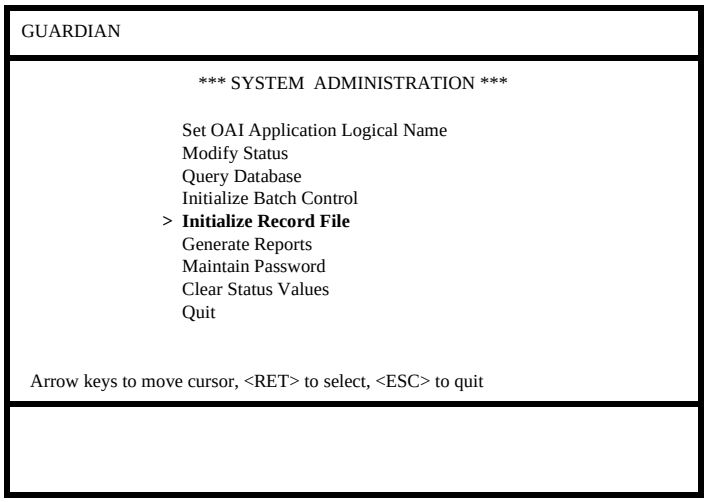


Figure 3-14 Initialize Record File

Notes

When you reinitialize the record file, the system deletes the previous file material and starts a new record of information. Reports generated from the record file reflect the information collected in the file since its most recent reinitialization. For example, if you want reports to reflect details of system processing on a monthly basis, you can reinitialize the record file every month after you generate the reports so that the system can begin collecting data for the next series of monthly reports.

If an error occurs during initialization, retry the process. If the error reoccurs, call the system distributor.

Procedure

Action	Result
On the main menu, select the **Initialize Record File** option and press Enter twice. (1)	Processing is completed, and the message **Initialize Record File Successful** appears.
To exit the Initialize Record File, press ESC.	The cursor returns to the main menu, and the original command line is restored.

Generate Reports

Overview

Use the Reports option on the System Administration menu to generate various management and control reports from the record file and from four of the working databases. The Reports option can be accessed under either the Administrator password or the Operator password. For more information about how to delete information from the record file, refer to "Initialize Record File" on page 54.

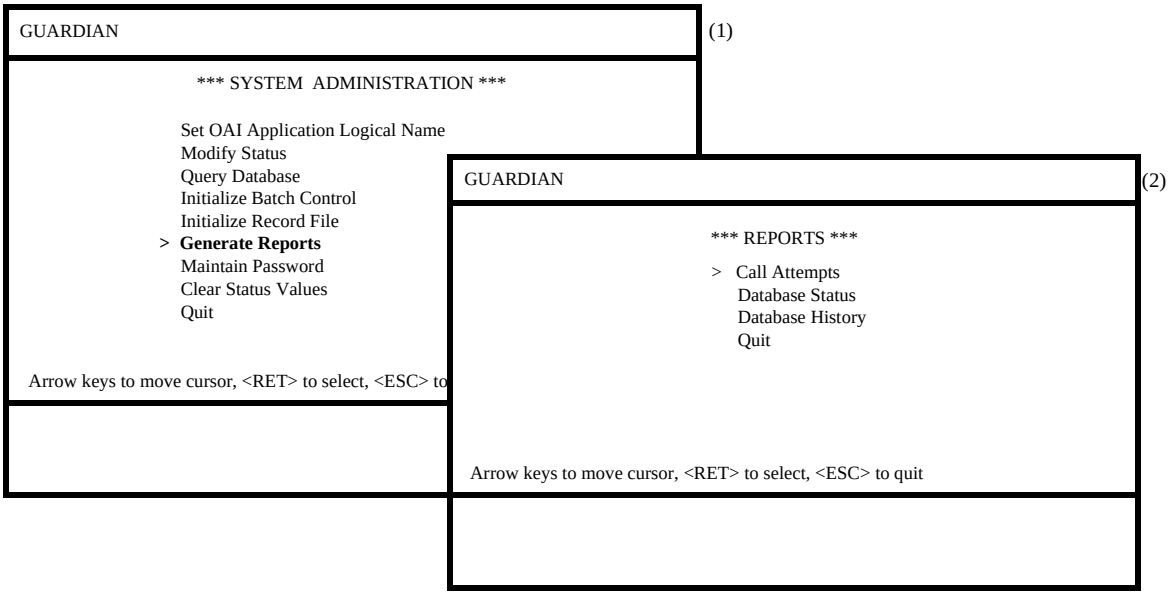


Figure 3-15 Reports Menu

Notes

The system generates reports from data collected in the record file. This file contains information logged since the last time it was initialized. For more information on initializing the record file, refer to "Initialize Record File" on page 54.

- **Call Attempts –** A menu of reports concerning the recorded invalid call attempts that involved unknown or disabled groups, authorization codes, or extensions.
- **Database Status –** A menu of reports reflecting the status of all groups, authorization codes, extensions, and time intervals.
- **Database History –** A menu of reports showing the history of status modifications to groups, authorization codes, or extensions.

When you select the report you want from these options, you can view the information on the screen, print a hard copy, or to save it to a disk.

If the computer has less than 20% of disk space available when you select the Generate Reports option, the following message displays: **Not enough free disk space for reports**. If you disregard this message and the system requires more disk space than is available to process the report, the following message displays: **Report Not Generated**.

Procedure

Action	Result
On the main menu, select the Reports option. (1)	The Reports menu displays. (2)
Use the arrow keys to position the cursor on the type of report desired and press Enter.	The menu of available reports displays.
To exit the Reports menu, select the Quit option and press Enter, or press ESC.	The main menu reappears.

Call Attempts

Use the Call Attempts option on the Reports Menu to generate invalid call attempt reports for calls made from single extensions, within groups, and with authorization codes that are not assigned in the database (unrecognized) or disabled by the administrator or the system.

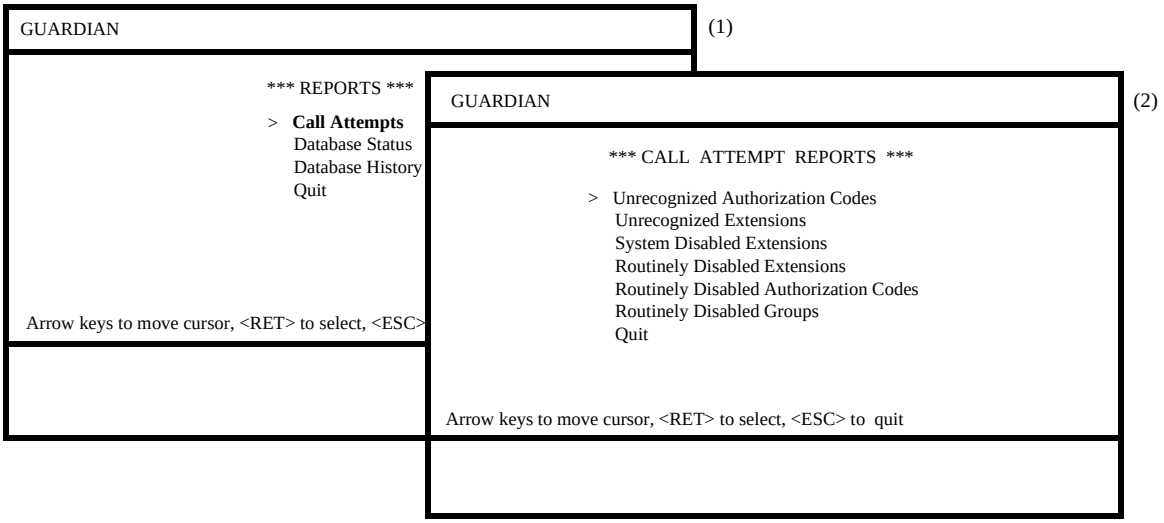


Figure 3-16 Call Attempts Reports

Notes

The following call attempt reports contain date, time, and page number headings.

- **Unrecognized Authorization Codes –** A list of authorization codes that are not assigned in the database but that have been used in call attempts, including the time at which the calls were attempted. (Sorted chronologically by extension).
- **Unrecognized Extensions –** A list of extensions that are not assigned in the database but that have been used in call attempts, including the time at which the calls were attempted. (Sorted chronologically by extension).
- **System Disabled Extensions –** A list of extensions on which calls have been attempted and that are currently disabled by the system, including the time at which the calls were attempted and the time at which the extension is to be enabled. (Sorted chronologically by extension).
- **Routinely Disabled Extensions –** A list of all extensions on which calls have been attempted during the time interval that the extensions are scheduled to be disabled, including the times at which the calls were attempted. (Sorted chronologically by extension).

Notes (Continued)

- **Routinely Disabled Authorization Codes –** A list of all authorization codes with which calls have been attempted during the time interval that the codes are scheduled to be disabled, including the times at which the calls were attempted. (Sorted chronologically by extension).
- **Routinely Disabled Groups –** A list of groups in which extensions have been used in call attempts during the time intervals that the groups are scheduled to be disabled, including the times at which the calls were attempted. (Sorted chronologically by extension).

When you select this option and the report you want, the following sequence of messages displays while the system prepares the report: **Sorting...**, **Processing...**, and **Done**.

Procedure

Action	Result
On the Reports menu, select the **Call Attempts** option and press Enter. (1)	The Call Attempt Reports screen displays. (2)
Use the arrow keys to position the cursor on the desired report and press Enter.	A new command line appears containing output commands (Print File, View File, Save File).
Use the arrow keys to position the cursor on the desired output command and press Enter.	**PRINT FILE:** The report prints and the output commands reappears. **VIEW FILE:** Report items are scrolled for display on the screen with **Top of File**, **End of File** and **More** notations indicating placement. The commands serve to move the screen down the page (**DownPage**), up the page (**UpPage**), to the beginning of the file (**Top**), or to the end of the file (**Bottom**). To exit and return to the output commands, select the **Quit** command and press Enter. The output commands redisplay. **SAVE FILE:** A prompt for the name of the file in which the report is to be saved appears with a default file name inserted. Enter the appropriate file name and press Enter. The system stores the report under the indicated file name, and the output commands redisplay. To exit the output commands, select the **Quit** command and press Enter.
To exit the Call Attempts option, press ESC.	The Reports menu reappears.

Database Status

Use the Database Status option on the Reports menu to generate reports concerning the current status of all groups, authorization codes, and extensions in the system.

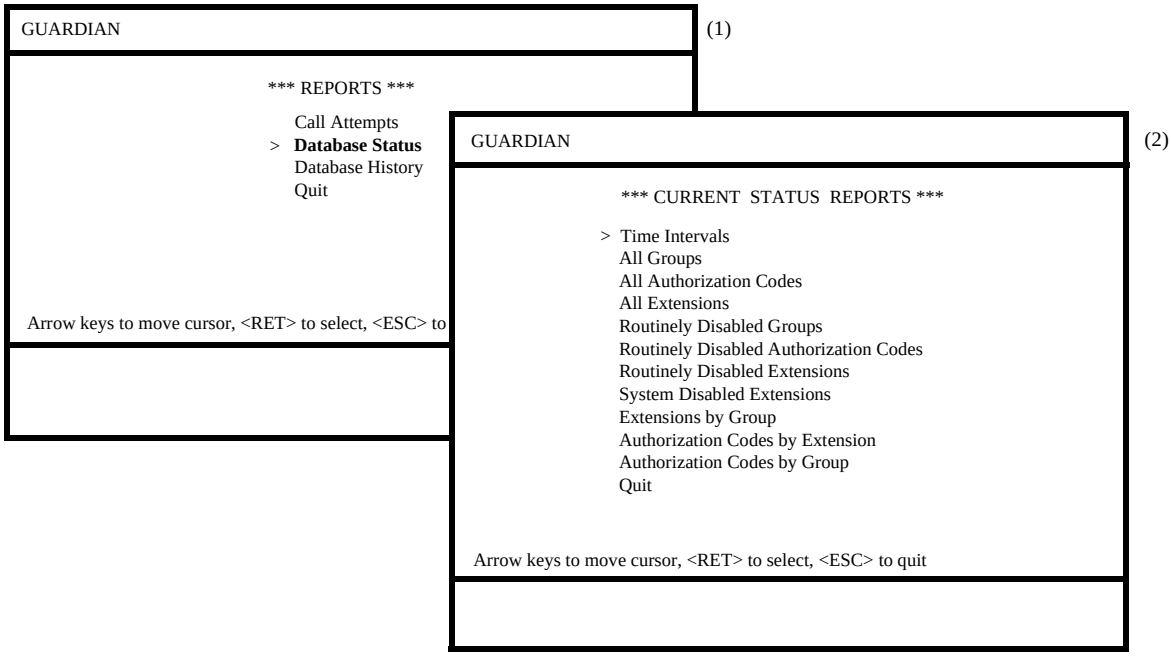


Figure 3-17 Current Database Status Reports

Notes

The status reports listed below are available through this option. The reports notated with (Range Available) can be prepared for a designated portion of the database as well as for the whole file. When any one of these reports is selected, a Report Range screen displays where you can enter the first and last items of the range to be included in a report.

- **Time Intervals –** A list of the beginning and ending times for each interval associated with an Interval Index.
- **Groups (Range Available) –** A printout of the Group database.
- **Authorization Codes (Range Available) –** A printout of the Authorization Code database.
- **Extensions (Range Available) –** A printout of the Extension database.
- **Routinely Disabled Groups –** A list of all groups that are scheduled to be routinely disabled, including the time interval of the disablement.
- **Routinely Disabled Authorization Codes –** A list of all authorization codes that are scheduled to be routinely disabled, including the time interval of the disablement.
- **Routinely Disabled Extensions –** A list of all extensions that are scheduled to be routinely disabled, including the time interval of the disablement.
- **System Disabled Extensions –** A list of all extensions that are currently disabled by the system in response to an excessive frequency of invalid call attempts, including the anticipated enable time.
- **Extensions by Group (Range Available) –** A list of all groups and the extensions that are assigned to each.
- **Authorization Codes by Extension (Range Available) –** A list of authorization codes that are assigned to single extensions.
- **Authorization Codes by Group (Range Available) –** A list of the authorization codes that are assigned to groups.

Procedure

Action	Result
On the Reports menu, select the **Database Status** option and press Enter. (1)	The Current State Reports screen displays. (2)
Use the arrow keys to position the cursor on the desired report and press Enter.	**Range Available Reports**: The Report Range screen displays. Enter the code, extension, or group with which the report should begin and the code, extension, or group with which the report should end and press Enter. **All Reports**: A new command line containing output commands **(Print File**, **View File**, **Save File**) appears.
Use the arrow keys to position the cursor on the desired output command and press Enter. **Note:** *The message, **Processing.**, indicates that the report is being prepared, and **Done** indicates that it is ready.*	**PRINT FILE:** The report prints and the output commands reappears. **VIEW FILE:** Report items are scrolled for display on the screen with **Top of File**, **End of File** and **More** notations indicating placement. The commands serve to move the screen down the page (**DownPage**), up the page (**UpPage**), to the beginning of the file (**Top**), or to the end of the file (**Bottom**). To exit and return to the output commands, select the **Quit** command and press Enter. The output commands are redisplayed. **SAVE FILE:** A prompt for the name of the file in which the report is to be saved appears with a default file name inserted. Enter the appropriate file name and press Enter. The system stores the report under the indicated file name, and the output commands redisplay.
To exit the output commands, select the **Quit** command and press Enter.	The Current State Reports menu displays.
To exit the Current State Reports menu, press ESC.	The Reports menu reappears.

Database History

Use the Database History option on the Reports menu to generate reports concerning the history of routine disable activity of groups, authorization codes, and extensions, including system disabling of extensions in response to excessive invalid call attempts.

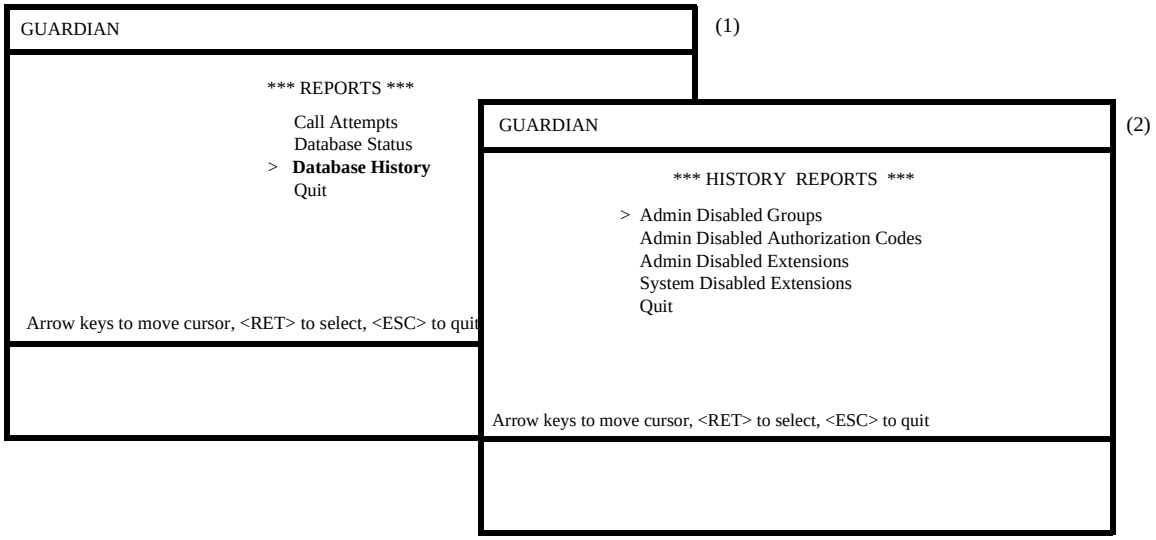


Figure 3-18 Database History Reports

Notes

The history reports provide information that has been recorded since the last time the record file was initialized. The fields contained in the history reports are listed below. For more information on initializing the record file, refer to "Initialize Record File" on page 54.

- **Admin Disabled Groups –** A list of all groups that have been unconditionally or routinely disabled during the reporting period. (Sorted chronologically by group).
- **Admin Disabled Authorization Codes –** A list of all authorization codes that have been unconditionally or routinely disabled during the reporting period. (Sorted chronologically by group).
- **Admin Disabled Extensions –** A report of all extensions that have been unconditionally or routinely disabled during the reporting period. (Sorted chronologically by group).
- **System Disabled Extensions –** A report of all extensions that have been disabled by the system during the reporting period because of an excessive frequency of invalid call attempts.

Procedure

Action	Result
On the Reports menu, select the **Database History** option and press Enter. (1)	The History Reports screen displays. (2)
Use the arrow keys to position the cursor on the desired report and press Enter.	A new command line containing output commands (**Print File**, **View File**, **Save File**) appears.
Use the arrow keys to position the cursor on the desired output command and press Enter. **Note:** *The message, **Processing..**, indicates that the report is being prepared, and **Done** indicates that it is ready.*	**PRINT FILE:** The report prints and the output commands are redisplayed. **VIEW FILE:** Report items are scrolled for display on the screen with **Top of File**, **End of File** and **More** notations indicating placement. The commands serve to move the screen down the page (**DownPage**), up the page (**UpPage**), to the beginning of the file (**Top**), or to the end of the file (**Bottom**). To exit and return to the output commands, select the **Quit** command and press Enter. The output commands are redisplayed. **SAVE FILE:** A prompt for the name of the file in which the report is to be saved appears with a default file name inserted. Enter the appropriate file name and press Enter. The system stores the report under the indicated file name, and the output commands redisplay. To exit the output commands, select the **Quit** command and press Enter.
To exit the Database History option, press ESC.	The Reports menu reappears.

Maintain Password

System Administrators can use the Maintain Password option on the main menu to change an access level password for the Guardian System Administration menu. This option can only be accessed with the Administrator password.

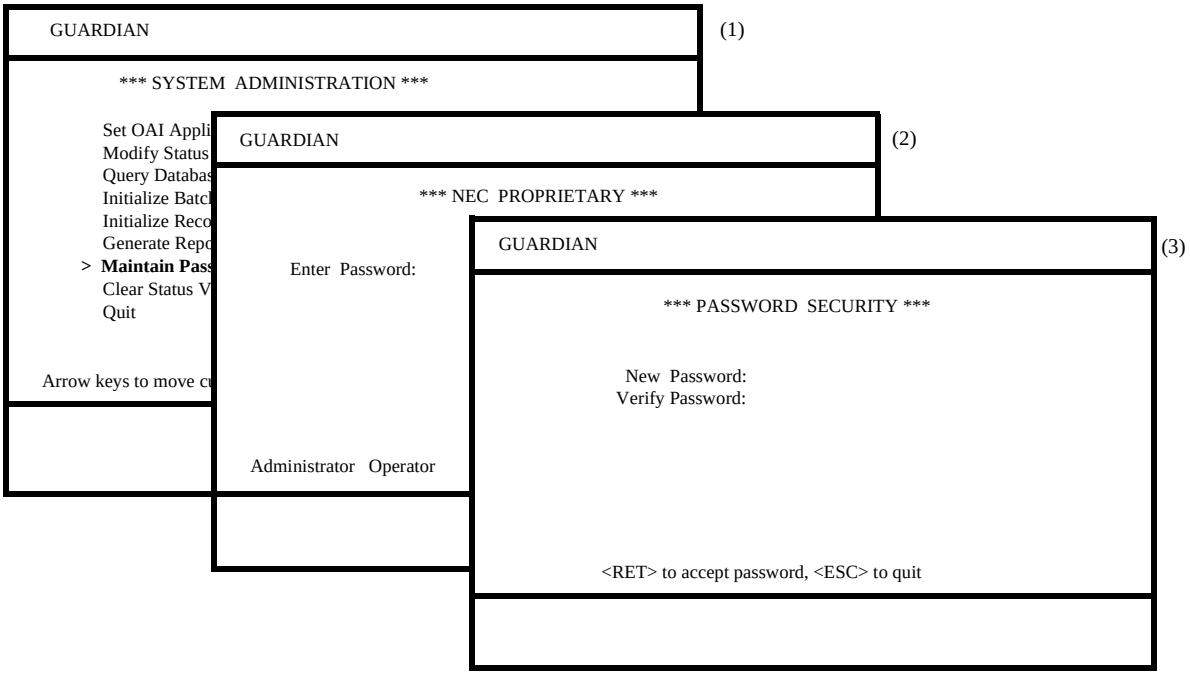


Figure 3-19 Password Security

Notes

Only the System Administrator is authorized to alter the security passwords. The Administrator password must be entered before any other password may be changed. If you enter a password that is not in the file, the **Invalid password** message displays. If you enter a password that already exists in the password file, the system displays a message indicating that the password already exists. Any new password you enter into the system becomes effective immediately.

Procedure

Action	Result
Select the **Maintain Password** option on the main menu (1) to display the Guardian Password Entry screen. (2) Enter the correct Guardian administrator password.	If the password you enter is valid, a new command line displays two security levels (Administrator/Operator). (3)
Select the level of password that you want to change (**Administrator**, **Operator, or Admn/Operator**) and press Enter.	The cursor is positioned on the *New Password* field for data entry.
Enter the new password.	The cursor is immediately positioned on the *Verify Password* field for data entry.
Re-enter the new password in the *Verify Password* field.	If the two entered passwords match, the message **Modify password successful** appears. Press Enter to display the main menu. If the two entered passwords do not match, the message **Passwords do not match, try again** appears, and the cursor is again positioned on the *New Password* field.
To exit the Password Security screen, select the **Quit** command and press Enter.	The main menu displays.

Clear Status Values

Use the Clear Status Values option on the main menu to clear all status modifications and to re-initialize the group, authorization code, and extension databases. You can only access this option with the Administrator password.

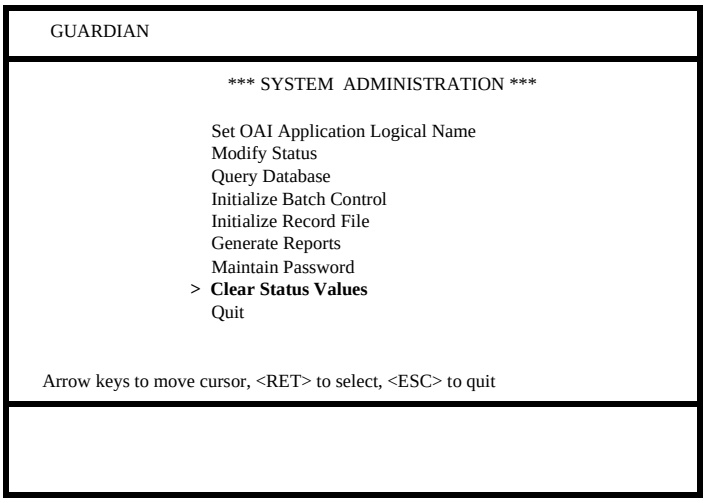


Figure 3-20 Clear Status Values

Notes

When you initialize the databases, they are installed to Guardian from the Applications Manager, where they were originally created. The Guardian Administrator can make changes as necessary (add, modify, and delete records) to the databases, but any changes made through Guardian do not change the database versions in the Applications Manager. When you use the Clear Status Values option, the Applications Manager's versions of the databases group, authorization code, and extension databases are re-installed in Guardian, overriding those previously in use and changed by Guardian. In effect, this reinstallation erases all modifications made to the disable status of all groups, authorization codes, and extensions, since those changes are made by the System Administrator directly to the Guardian databases, not via the Application Manager.

Procedure

Action	Result
Select the **Clear Status Values** option on the main menu (1) and press Enter twice.	When processing is complete the message **Init System Data Successful** appears.
Press ESC.	The cursor returns to the main menu.

Appendix A Report Formats

Introduction

The following report formats illustrate the content and arrangement of the various reports available to the System Administrator. These formats reflect the reports as they appear in hard copy form. When they appear on-screen, the display includes **Top of File**, **More**, and **End of File** notations and a command line that can be used to move to the next page (**DownPage**), to the preceding page (**UpPage**), to the top of the file (**Top**), and to the end of the file (**Bottom**).

A Disable Time Interval field appears in many of the reports and includes the times at which the group, authorization code, or extension is routinely turned off (Begin) and turned back on (End). The time interval appears in Day Hour:Minute format. The times at which the invalid call attempts are placed appear in a Month/Day/Year Hour:Minute format.

The Call Attempt Reports and the Database History Reports contain information that has been collected in the Record File since its last initialization. For instance, the following samples assume that the Record File was last initialized on November 1, 1990.

Call Attempt Reports

The Call Attempt Reports present lists of call attempts that are considered invalid. A call attempt may be invalid because it is attempted during the time that the designated group, authorization code, or extension is routinely disabled, because it involves a group, authorization code, or extension that the system does not recognize among its databases, or because it is made on an extension that has been disabled by the system in response to an excessive frequency of invalid call attempts. The first listed invalid call attempt for each group, authorization code, or extension is the first one to occur after the group, code, or extension has been routinely or unconditionally disabled by the administrator or disabled by the system in response to excessive invalid call attempts.

1. **Unrecognized Authorization Codes** – A list of call attempts made with authorization codes that are not assigned in the database or are not recognized by Guardian. (Sorted by extension in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

Call Attempt Report
(Unrecognized Authorization Codes)

Auth Code	Time Call Placed		Ext	Group ID
2187500	11/06/90	6:28	1294	2
3897612	11/04/90	10:37	2345	1
5987364	11/04/90	14:10	2345	1
8288348	11/11/90	5:47	2345	2
8352678	11/10/90	17:52	3201	3
8782719	11/15/90	7:23	3201	1
9876543	11/12/90	8:02	9878	1

Number of Records: 7

2. **Unrecognized Extension Numbers –** A list of calls that have been attempted from extensions that are not assigned in the database or are not recognized. The authorization code shown for each extension and used in the call attempt is included in the authorization code database and enabled by the administrator. (Sorted by extension in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

Call Attempt Report
(Unrecognized Extensions)

Ext	Time Call Placed		Auth Code
2301	11/15/90	14:13	1859427
3979	11/06/90	22:31	2192738
4331	11/10/90	8:02	3492780
5230	11/07/90	12:41	2429379
5575	11/11/90	17:52	9874732

Number of Records: 5

3. **System Disabled Extensions –** A list of calls that have been attempted from extensions during times that those extensions were disabled by the system since the Record File was last initialized. (Sorted by extension in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

Call Attempt Report
(System Disabled Extensions)

Ext	System Enable Time		Group ID	Auth Code	Time Call Placed	
1294	11/06/90	6:15	2	2187500	11/06/90	5:38
2345	11/04/90	13:45	1	3897612	11/04/90	1:11
2345	11/04/90	13:45	1	5987364	11/04/90	3:36
2345	11/11/90	13:45	1	8288348	11/04/90	5:47
3201	11/10/90	19:30	1	8352678	11/10/90	16:52
3201	11/15/90	7:30	1	8782719	11/15/90	6:02

Number of Records: 6

4. **Routinely Disabled Extensions –** A list of call attempts that were made using authorization codes that were routinely disabled at the time. (Sorted by authorization code in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

Call Attempt Report
(Routinely Disabled Extensions)

Ext	Routine Disable Time Interval Begin		End		Time Call Placed		Auth Code	Group ID
1294	Mon	5:1	Fri	24:0	11/09/90	22:03	2187500	3
2345	Wed	12:0	Thu	8:0	11/07/90	20:47	3897612	1
2345	Wed	12:0	Thu	8:0	11/08/90	7:24	3897612	1
2345	Constant		---		11/08/90	7:21	5987364	1
3201	Constant		---		11/10/90	10:12	5987364	1
3201	Sun	1:1	Sun	24:0	11/11/90	16:31	1827548	2
9878	Wed	12:0	Thu	8:0	11/08/90	7:59	9876543	1

Number of Records: 7

5. **Routinely Disabled Authorization Codes –** A list of call attempts that were made using authorization codes that were routinely disabled at the time. (Sorted by authorization code in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

Call Attempt Report

(Routinely Disabled Authorization Codes)

Auth	Routine Disable Time Interval				Time		
Code	Begin		End		Call Placed		Ext
2187500	Sat	1:1	Mon	5:1	11/03/90	5:16	1294
2396857	Sat	1:1	Mon	5:1	11/10/90	10:18	1295
2396857	Sat	1:1	Mon	5:1	11/11/90	21:11	1295
2429879	Constant		---		11/11/90	8:24	5692
3492780	Sun	1:1	Sun	24:0	11/11/90	20:06	4178
6659636	Mon	5:1	Fri	24:0	11/05/90	12:25	3412
9874732	Wed	12:0	Thu	8:0	11/07/90	7:42	9878

Number of Records: 7

6. **Routinely Disabled Groups –** A list of call attempts that have been made within the regular time intervals during which group extensions are routinely disabled. (Sorted by group in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

Call Attempt Report
(Routinely Disabled Groups)

Group ID	Time Interval Begin		End		Time Call Placed		Auth Code	Ext
0	Sat	1:1	Mon	5:1	11/03/90	5:16	2396857	1295
0	Sat	1:1	Mon	5:1	11/10/90	10:18	2187500	1294
0	Sat	1:1	Mon	5:1	11/11/90	21:11	2396857	1295
1	Wed	12:0	Thu	8:0	11/07/90	7:42	9874732	2847
2	Sun	1:1	Sun	24:0	11/11/90	20:06	3492780	4178
3	Mon	5:1	Fri	24:0	11/05/90	12:25	6659636	3412
3	Mon	5:1	Fri	24:0	11/12/90	12:13	6659636	3412
4	Constant		——		11/11/90	8:24	2429379	5692

Number of Records: 8

Current State Reports

1. **Time Interval Database –** A list of indexes showing the beginning and ending times for each interval during which groups, authorization codes, and extensions can be routinely disabled. (Sorted by index in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

Current State Report
(Time Intervals)

Interval Index	Routine Disable Time Interval Begin		End	
0	Constant		—	
1	Sat	1:00	Mon	5:00
2	Wed	12:00	Thu	8:00
3	Sun	1:00	Sun	24:00
10	Mon	5:00	Fri	24:00

Number of Records: 5

1. **Group –** A complete print-out of the Group database, sorted in ascending order.

Note: *A group can be both unconditionally and routinely disabled at the same time.*

Date: 11/15/90 **Pg1**

Tenant: 1

Current State Report
(Groups)

Group ID	Admin Disable Status	Routine Disable Time Interval Begin	Routine Disable Time Interval End	Temp Disable Period	Frequency Cnt	Frequency Time	Lifetime Count
0	NO	– – – –	– — – –	60 min	3	1	10
1	YES	Wed 12:00	Thu 8:00	60 min	2	3	10
2	NO	– – – –	– – – –	30 min	2	2	100
3	UNCDTL	– – – –	– – – –	45 min	3	3	150
4	UNCDTL	– – – –	– – – –	60 min	5	7	100
5	YES	Sat 1:00	Mon 5:00	30 min	3	5	75
6	NO	– – – –	– – – –	60 min	5	3	50

Number of Records: 7

2. **Authorization Codes –** A complete print-out of the Authorization Code database, sorted in ascending order.

Note: *An authorization code can be both unconditionally and routinely disabled at the same time.*

Date: 11/15/90 **Pg1**

Tenant: 1

Current State Report
(Authorization Codes)

Auth Code	Admin Disable Status	Routine Disable Time Interval Begin	End	Ext/Group Flag	Value	RSC	SFC
2187500	NO	– – – –	– – – –	Ext	11111	2	1
2396857	UNCDTL	– – – –	– – – –	Grp	0	10	11
2429379	YES	Mon 5:00	Fri 24:00	Grp	3	5	4
3492780	UNCDTL	– – – –	– – – –	Ext	3201	1	1
6659636	YES	Mon 5:00	Fri 24:00	Grp	3	2	1
6874392	NO	– – – –	– – – –	Grp	3	10	11
8759210	YES	Sat 1:00	Mon 5:00	Grp	0	2	1
9874732	UNCDTL	– – – –	– – – –	Ext	2345	5	4

Number of Records: 8

3. **Extensions –** A complete print-out of the Extension database sorted in ascending order.

Note: *An extension can be both unconditionally and routinely disabled at the same time.*

Date: 11/15/90 **Pg1**

Tenant: 1

Current State Report
(Extensions)

	Disable	Time Interval		Group			
Ext	Status	Begin	End	ID	Disabled	Enable Time	
789	YES	Sat 1:00	Mon 5:00	0	NO		
1289	YES	Sat 1:00	Mon 5:00	0	NO		
2345	UNCDTL	– – – –	– – – –	1	NO		
3201	NO	– – – –	– – – –	1	YES	11/15/90	16:45
4556	UNCDTL	– – – –	– – – –	1	NO		
5436	YES	Sun 1:00	Sun 24:00	2	NO		
8976	YES	Sun 1:00	Sun 24:00	2	YES	11/15/90	22:30
9878	NO	– – – –	– – – –	1	NO		

Number of Records: 8

4. **Routinely Disabled Groups –** A list of all groups that are currently scheduled to be routinely disabled during the specified time interval (Day Hour:Minute). (Sorted by group in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

Current State Report
(Routinely Disabled Groups)

Group ID	Routine Disable Time Interval Begin		End	
0	Sat	1:00	Mon	5:00
3	Mon	5:00	Fri	24:00
4	Constant		—	
6	Sat	1:00	Mon	5:00

Number of Records: 4

5. **Routinely Disabled Authorization Codes –** A list of all authorization codes that are currently scheduled to be routinely disabled during a specified time interval (Day Hour:Minute). (Sorted by authorization code in ascending order.)

Note: *Includes only authorization codes that are routinely disabled individually. For those that are disabled by their group, refer to the Routinely Disabled Group report*

.

Date: 11/15/90 **Pg1**

Tenant: 1

Current State Report
(Routinely Disabled Authorized Codes)

Auth Code	Routine Disable Time Interval Begin		End	
2429379	Mon	5:00	Fri	24:00
6659636	Mon	5:00	Fri	24:00
8759210	Sat	1:00	Mon	5:00
9874732	Sat	1:00	Mon	5:00

Number of Records: 4

6. **Routinely Disabled Extensions –** A list of all extensions that are currently scheduled to be routinely disabled during a specified time interval (Day Hour:Minute). (Sorted by extension in ascending order.)

Note: *Includes only extensions that are routinely disabled individually; for those that are disabled by their group, refer to the Routinely Disabled Group report.*

Date: 11/15/90 **Pg1**
Tenant: 1

Current State Report
(Routinely Disabled Extensions)

Ext	Routine Disable Time Interval Begin		End	
789	Sat	1:00	Mon	5:00
1289	Sat	1:00	Mon	5:00
5436	Sun	1:00	Sun	24:00
8976	Sun	1:00	Sun	24:00
10230	Sat	1:00	Mon	5:00

Number of Records: 5

7. **System Disabled Extensions –** A list of all extensions that are currently disabled by the system in response to an excessive frequency of invalid call attempts, including the time at which they will be enabled again (Month/Day/Year Hour:Minute). (Sorted by extension in ascending order.)

Date: 11/15/90 **Pg1**
Tenant: 1

Current State Report
(System Disabled Extensions)

Ext	System Enable Time		Group ID
3201	11/15/90	16:45	1
8976	11/15/90	22:30	2
10230	11/15/90	14:15	0

Number of Records: 3

8. **Extensions by Group –** A report of all extensions that are assigned to groups. (Sorted by group in ascending order.)

Date: 11/15/90 **Pg1**
Tenant: 1

Current State Report
(Extensions by Group)

ID	Ext
1	789
	1289
	10230
2	2345
46	3201
	4556

Number of Records: 6

9. **Authorization Codes by Extension –** A report of all authorization codes that are assigned to extensions. (Sorted by extension in ascending order.)

Date: 11/15/90 **Pg1**
Tenant: 1

Current State Report
(Authorization Codes by Extension)

Ext	Auth Code
1295	2396857
2345	2134475
2847	9874732
3201	3492780
3412	6659636
4556	1294372
5692	8321983

Number of Records: 7

10. **Authorization Codes by Group –** A report of all authorization codes that are assigned to each group. (Sorted by group in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

Current State Report
(Authorization Codes by Group)

Group ID	Auth Code
1	5483928
	6721936
	9174732
	9473268
2	9956121
	1298432
46	2429379

Number of Records: 7

History Reports

1. **Admin Disabled Groups –** A list of groups whose status has been changed since the last Record File initialization, with all the extensions in each group to be disabled during the indicated time interval. (Sorted by group in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

History Report
(Admin Disabled Groups)

Group ID	Routine Disable Time Interval Begin		End		Date Group Status Modified		Modified Status	
0	Sat	1:00	Mon	5:00	11/02/90	14:22	UNCDTL	
0	Sat	1:00	Mon	5:00	11/12/90	16:14	UNCDTL	
1	Wed	12:00	Thu	8:00	11/12/90	15:32	YES	
2	Sun	1:00	Sun	24:00	11/09/90	9:57	YES	
3	Mon	5:00	Fri	24:00	11/12/90	15:46	NO	
4	Constant		—		11/07/90	10:34	YES	

Number of Records: 6

1. **Admin Disabled Authorization Codes –** A list of authorization codes whose status has been changed since the last Record File initialization, causing the authorization codes to be disabled during the indicated time intervals. (Sorted by authorization code in ascending order.)

Date: 11/15/90 **Pg1**
Tenant: 1

History Report
(Admin Disabled Authorization Codes)

Auth Code	Routine Disable Time Interval Begin		End		Date Authcode Status Modified		Modified Status
1298432	Wed	12:0	Thu	8:00	11/5/90	8:52	UNCDTL
2429379	Wed	12:00	Thu	8:00	11/12/90	9:32	YES
5483928	Sat	1:00	Mon	5:00	11/1/90	11:12	NO
6721936	Sat	1:00	Mon	5:00	11/15/90	10:11	UNCDTL
9174732	Mon	5:00	Fri	24:00	11/1/90	11:34	NO
9473268	Sun	1:00	Sun	24:00	11/15/90	10:19	NO
9956121	Wed	12:00	Thu	8:00	11/13/90	15:47	YES

Number of Records: 7

2. **Admin Disabled Extensions –** A list of extensions whose status has been changed since the last Record File initialization, with all extensions on the list being disabled during the indicated time interval. (Sorted by extension in ascending order.)

Date: 11/15/90 **Pg1**
Tenant: 1

History Report
(Admin Disabled Extensions)

	Routine Disable Time Interval				Date Extension Status Modified		Modified
Ext	Begin		End				Status
1289	Sat	1:00	Mon	5:00	11/01/90	9:16	UNCDTL
2345	Wed	12:00	Thu	8:00	11/12/90	8:34	YES
2503	Mon	5:00	Fri	24:00	11/01/90	9:34	YES
4556	Wed	12:00	Thu	8:00	11/09/90	15:23	NO
9878	Wed	12:00	Thu	8:00	11/08/90	9:36	UNCDTL
10230	Sat	1:00	Mon	5:00	11/05/90	12:59	UNCDTL

Number of Records: 6

3. **System Disabled Extensions –** A list of the extensions that have been disabled by the system since the last Record File initialization, including the time that each extension was turned back on. If the Administrator overrode the system disable, the time at which the Administrator enabled the extension is listed. (Sorted by extension in ascending order.)

Date: 11/15/90 **Pg1**

Tenant: 1

History Report
(System Disabled Extensions)

Ext	Time Ext Disabled		System Enable Time		Group ID
1230	11/7/90	10:32	11/8/90	8:15	2
2345	11/2/90	1:02	11/2/90	16:45	1
2345	11/14/90	12:24	11/15/90	9:30	1
3864	11/6/90	11:49	11/7/90	9:30	2
4556	11/11/90	5:03	11/12/90	8:45	46
9878	11/7/90	9:11	11/8/90	12:30	1

Number of Records: 6

This Page Left Blank.