INTERCOMM

EXTENDED SECURITY SYSTEM

ISOGON
CORPORATION
330 Seventh Avenue, New York, New York 10001

LICENSE: INTERCOMM TELEPROCESSING MONITOR

Extended Security System

Publishing History

Publication	Date	Remarks
First Edition	October 1980	Documenting the new feature. This manual corresponds to Intercomm Release 8.0.
Second Edition	November 1980	Revisions and Updates.
Third Edition	May 1981	Revisions and Updates.
SPR 215	May 1982	Release 9.0 Revisions.
Second Printing	April 1984	Incorporating SPR 215
Fourth Edition	February 1987	Release 9.0 updates through SM 1730

PREFACE

Intercomm is a state-of-the-art teleprocessing monitor system executing on the IBM System/370 family of computers and operating under the control of IBM Operating Systems (MFT, MVT, VS1, MVS, XA). Intercomm monitors the transmission of messages to and from terminals, concurrent message processing, centralized access to I/O files, and the routine utility operations of editing input messages and formatting output messages, as required.

This manual documents the installation and use of the Extended Security System (ESS), an Intercomm special feature.

An overview of the ESS security structure is presented in Chapter 1. Formal definitions of the ESS command language are found in Section 2.2 and Appendixes A and B.

This manual is not intended for end users, but for Intercomm systems programmers responsible for installing ESS and establishing and maintaining group manager accounts. Managers of end user groups responsible for establishing and maintaining the security environment within their own groups will also find this manual useful.

This manual is to be used in conjunction with the Operating Reference Manual.

INTERCOMM PUBLICATIONS

GENERAL INFORMATION MANUALS

Concepts and Facilities

Planning Guide

APPLICATION PROGRAMMERS MANUALS

Assembler Language Programmers Guide

COBOL Programmers Guide

PL/1 Programmers Guide

SYSTEM PROGRAMMERS MANUALS

Basic System Macros

BTAM Terminal Support Guide

Installation Guide

Messages and Codes

Operating Reference Manual

System Control Commands

CUSTOMER INFORMATION MANUALS

Customer Education Course Catalog

Technical Information Bulletins

User Contributed Program Descriptions

FEATURE IMPLEMENTATION MANUALS

Autogen Facility

ASMF Users Guide

DBMS Users Guide

Data Entry Installation Guide

Data Entry Terminal Operators Guide

Dynamic Data Queuing Facility

Dynamic File Allocation

Extended Security System

File Recovery Users Guide

Generalized Front End Facility

Message Mapping Utilities

Model System Generator

Multiregion Support Facility

Page Facility

Store/Fetch Facility

SNA Terminal Support Guide

TCAM Support Users Guide

Utilities Users Guide

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 OVERVIEW

Intercomm's Extended Security System (ESS) is designed to provide comprehensive control of access to system and user resources in a multiregion or single region Intercomm system. The security environment is defined dynamically using the ESS command language, thus eliminating the need to maintain security information in static tables and to interrupt service whenever the security environment changes.

ESS was written with four important design criteria in mind:

1. The security environment must be dynamically maintainable and its command language must be usable by non-DP personnel (operator supervisors, department managers, etc.).

2. The security system must be easy to superimpose on an Intercomm under the Multiregion Support Facility (MRS).

3. The security system must be capable of performing extensive security checks.

4. The security system must itself be secure.

ESS permits the Intercomm system manager to define a security tree with three levels of authority--global, group manager, and end user. This is very much in harmony with the philosophy of MRS: define a control region (global) with authority over itself and one or more satellite regions (groups), let maintenance in each satellite region proceed independently of maintenance in other satellite regions (group manager), and let the end users be partitioned into groups and be restricted in their access to regions, files, terminals and on-line programs. More than one account with global authority, and more than one manager of the same group, may be defined.

Each user is identified to ESS as an account with a user ID. System resources are attached to individual accounts. That is, on a user-by-user basis, access to Intercomm regions, subsystems, verbs, files and terminals can be authorized. Terminal security is performed when the user signs on and verb security is performed by the Intercomm Front End (terminal input processing) before any Back End (application program processing) input message queueing. Subsystem and Region security are performed in the Intercomm Back End before a message is passed to an application program for processing.

Accounts can be authorized to use Intercomm system resources only at certain times of the day and accounts can be given expiration dates. In addition, automatic sign-off can be forced if a user leaves a terminal idle for a certain amount of time. An account cannot be signed on at more than one terminal at any point in time and can be forced off via a group manager-level command.

What functions a global or group manager is authorized to perform in ESS is defined by <u>attributes</u> associated with that manager's account. For example, if the account has the attribute ADD, the manager is authorized to issue the ADD command, which adds an account to the security tree. If the account has the attribute NOADD, the ADD command is not authorized. A group manager is assigned a group name attribute by a global manager. System resource access limitations are assigned to the group manager by the global manager. The group manager may then create end user accounts with the same group name and resource lists. Subsequently, the group manager can modify the resources lists assigned to the users within the group, but only a global manager can change assignments for group managers.

The ESS command language is used to dynamically establish and maintain the security environment. Accounts can be added and deleted and their attributes and command authority can be changed on-line during the course of Intercomm execution.

ESS is partially link-pack eligible. By putting ESS in the link pack, the system is protected against tampering. Also, access to data maintained by ESS on external storage is scrambled.

In addition to the security checks mentioned above, ESS provides the following security facilities and features via commands and/or account attributes:

- Password security--a password may be assigned and changed by each account. Such an account will be automatically deactivated after three consecutive invalid sign-on attempts. The password can be made to expire after a given number of sign-ons, thus requiring the user to periodically change the password. On IBM 3270 device types, if a user omits his password from the initial sign-on he will be prompted with a nondisplay field for the password.

- A terminal may be locked to a verb following a successful sign-on.

- Menu processing--a subsystem may be specified to receive a dummy message following sign-on, to cause automatic menu screen generation as a response to sign-on.

- A maximum user count may be specified to control system concurrency.

- A news message may be maintained to be sent to the terminal user following a successful sign-on.

- An account can transmit a message to another active account using the user-id without knowing the terminal used by the other account.

- For CPU-to-CPU, data-collection devices, and printers, an exempt terminal list can be built to designate devices to be ignored by ESS.

- A display function is provided to support the on-line maintenance commands. The scope of display commands allowed is governed by a manager's privilege attributes.

- Two-level file security processing is supported, providing read-only or read-write authority for attached files.

- User-defined security functions--one-to-eight character logical elements may be associated with individual accounts. The SECTEST macro is provided to test authority for these logical functions. This feature can be used to test file/Data Base access not processed via the Intercomm File Handler, or for system files such as Store/Fetch, or the USERSPA area, for example.

In addition to the SECTEST macro for testing for permission to use a logical function, four other programming facilities are provided. One is a SECUSER subroutine that may be called by a user program to request the user-id associated with the current input message (terminal). Another is a user exit named USRSEC00 which, if coded, will be called whenever an ESS log record is created for the audit trail (see Appendix C). The third is another user exit named SECUEXIT which, if coded, will be called when adding or deleting an account, for SIGNON validation, and for SIGNOFF processing. This exit is provided for additional installation-dependent security checking or clean-up processing, as needed. Also, the exit can be used to prevent sign-on, or to cancel/change an invalid user-id when adding an account, or to prevent or validate deleting an account. The fourth is a user exit named USRPRMPT which is called only at system (control region) startup and may be used to suppress automatic generation of the ESS signon request message to some or all non-exempt terminals.

1.1.1 Commands and Attributes

The following is a summary list of ESS commands:

Command	Function
ADD	Add a manager/user account; associate attributes
ATTACH	Attach system resources to an account
DELETE	Delete an account
DETACH	Detach resources from an account
DISPLAY	Display ESS system/account status data
EDITNEWS	Provide system message after sign on
EXCLUDE	Define/add to list of terminals exempt from ESS
FORCE	Force sign off of an active user
INCLUDE	Remove terminal(s) from exempt list
MODIFY	Change account attribute assignments, etc.
SEND	Transmit a message to an active user
SIGNOFF	Terminate an ESS terminal session
SIGNON	Initiate an ESS terminal session

ESS commands and parameters are described in detail in Chapter 2. All ESS commands are a subset of the ESS transaction code (verb) SECU. Authority levels (global, manager, user) for each command are listed in Appendix A. Command/account attribute requirements/options are described in Appendix B.

ESS conveniences such as the Default Attribute List and the Copy List facility, described below, make setting up the security system fast and easy. Most commands and parameter keywords may be abbreviated, using their first three letters.

1.2 EXAMPLE

The following hypothetical example is presented in order to illustrate how ESS is used.

In this example, a portion of the security environment suitable for the structure of the organization is established from scratch. (Other organizations will have different security requirements; the following example should be used only as a learning tool.)

1.2.1 Security Tree

Suppose an organization exists such as the one illustrated in Figure 1. The organization is an Intercomm user with a control region, a test region and two production regions named REGIONA and REGIONB. The structure of the multiregion Intercomm mimics the structure of the organization as illustrated in Figure 2.

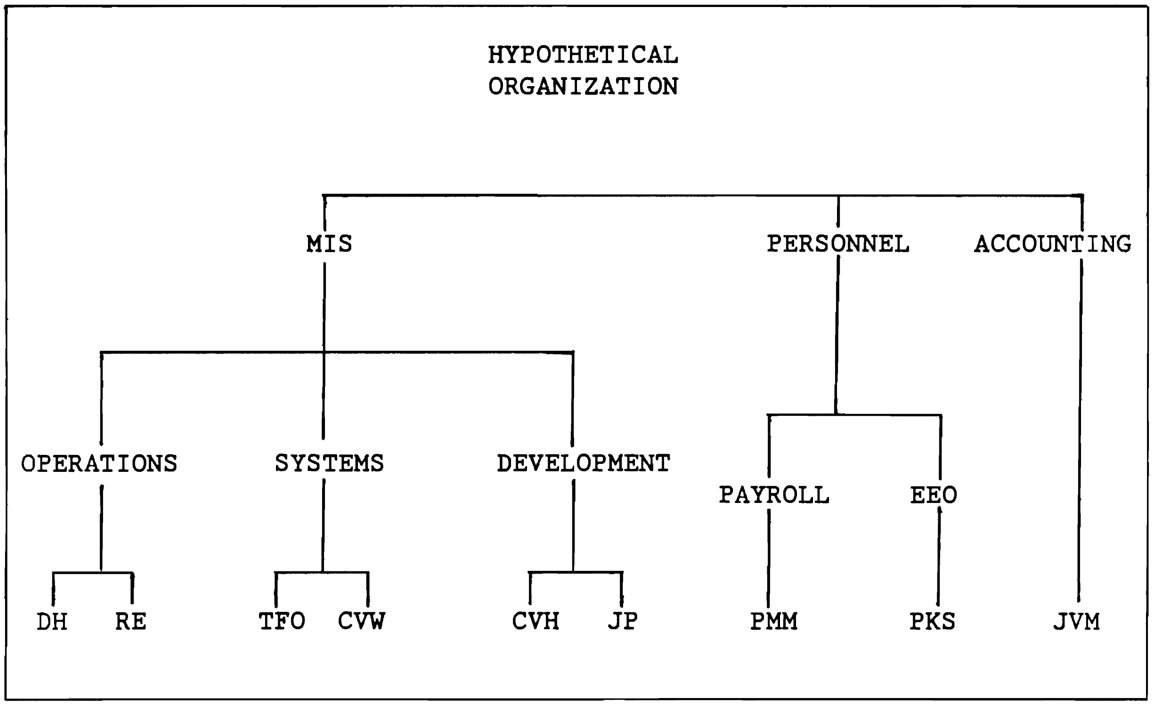


Figure 1. Hypothetical Organization Chart

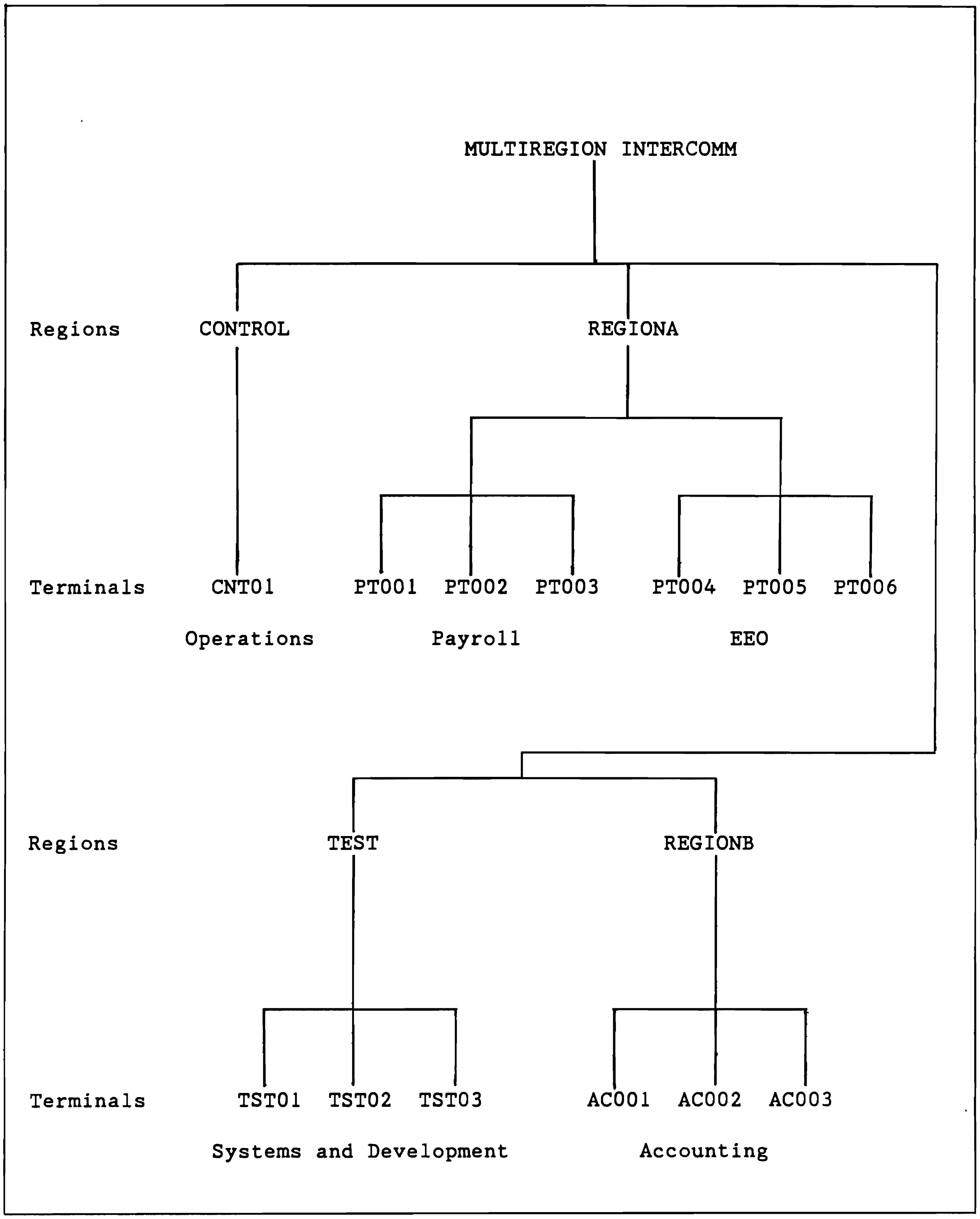


Figure 2. Hypothetical Mulitregion Intercomm

Only the operations staff is authorized to use the control region. Two operators with initials DH and RE make up the operations group.

Two systems programmers, TFO and CVW, make up the systems group and will have global authority, and there are two development end user programmers, CVH and JP. Systems and Development share the TEST region.

The Personnel department has two groups: Payroll, managed by PMM, and the EEO group managed by PKS. Personnel uses REGIONA.

Accounting is managed by JVM and uses REGIONB.

Figure 3 illustrates the security tree that is to be established. As can be seen, the security tree fits the structure of the organization, and of the Multiregion Intercomm installation, very closely.

1.2.2 Establishment of Tree

The following series of ESS command statements illustrate the establishment of the security tree for this hypothetical organization. The ESS verb is SECU and is required for all ESS commands except SIGNON. Command authority levels are described in Appendix A, account attributes are listed in Appendix B. A $ is the system separator (usually a comma) and the @ is the end-of-message character(s).

```
SIGNON$SECURITY@
```

Initially, the only account in existence is SECURITY. SECURITY owns every attribute except INHIBMSG, NOPSWD, and the list-INV attributes. Note that attributes with a sub-value (GROUP, INTVL, etc.) are null by default. While signed on under SECURITY, the Default Attribute List will be modified, the limit of active users will be set and the two accounts in the systems group, TFO and CVW, with GLOBAL authority will be created. No password is required to sign on to SECURITY at this time.

```
SECU$MODIFY$DEFAULTS$INTVL(0030)@
```

A powerful Default Attribute List exists, one that will make it easy to create the systems group accounts. The attribute list of the account SECURITY is the same as the Default Attribute List. The MODIFY$DEFAULTS command is now used to set a system-wide inactive terminal time-out value of 30 minutes via the INTVL attribute (this does not apply to the SECURITY account). After a time-out, the ESS sign-on message/screen is displayed, with a note that the previous session timed out. Default values for EXPDT, PSWDEXP, START, and STOP could also be set at this time.

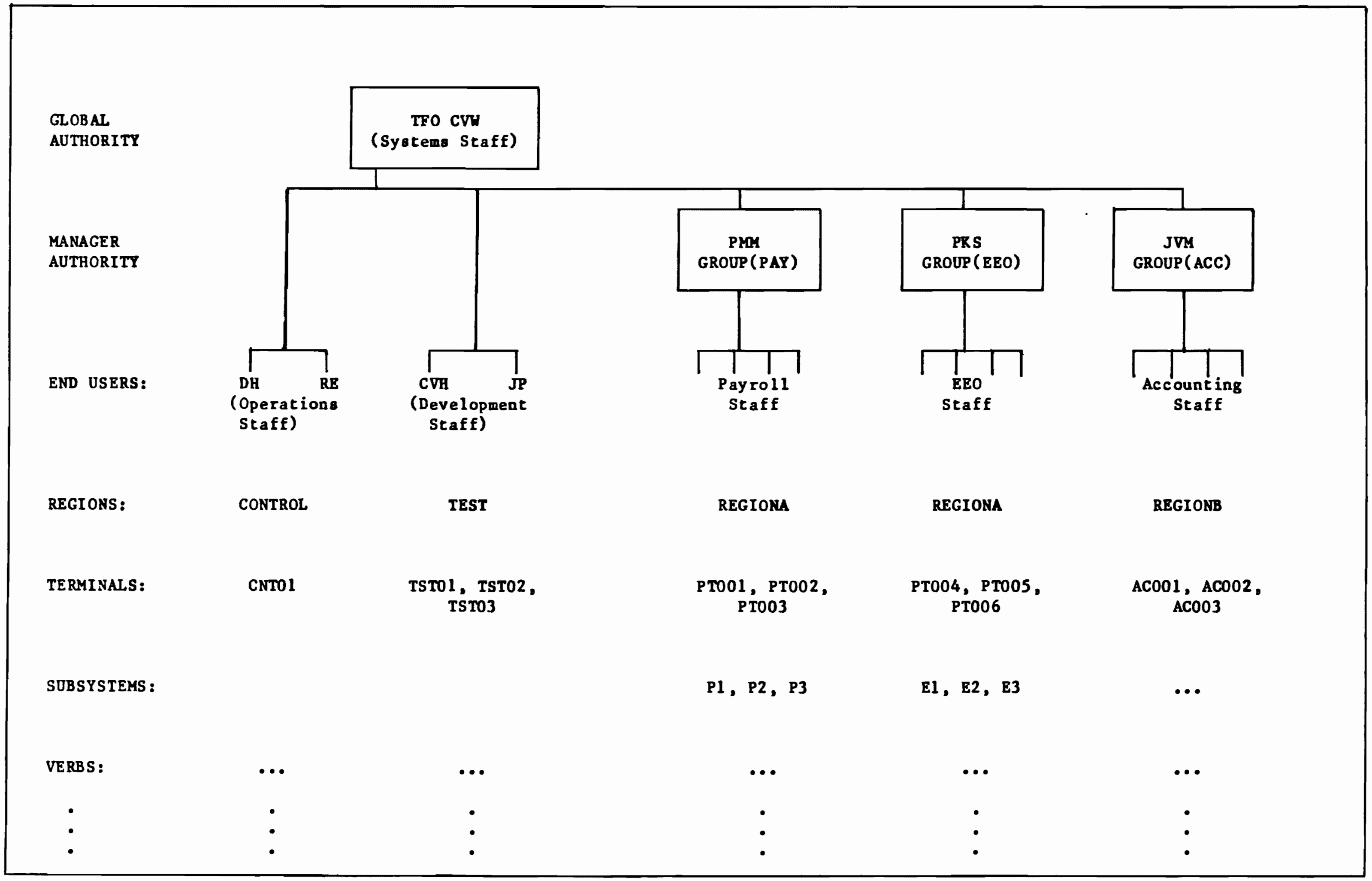


Figure 3. Security Tree

```
SECU$MODIFY$MAXUSERS$100@
```

Set the maximum concurrent users count for the Intercomm system (default is 1). It is known that, for this particular installation, having more than 100 active users affects Data Base access, so MAXUSERS is set to 100.

```
SECU$ADD$TFO@
SECU$ADD$CVW@
```

While still signed on under SECURITY, the two systems group accounts are created. Each will own the attributes currently in the Default Attribute List (which now also includes an INTVL time-out value). Each, therefore, has both global and manager authority. Each account is also required to establish a password when signing on for the first time (see SIGNON and ADD commands).

```
SECU$ATTACH$TFO$REGIONS$TEST@
SECU$ATTACH$TFO$TERMS$TST01$TST02$TST03@
SECU$ATTACH$TFO$SUBSYS....
SECU$ATTACH$TFO$VERBS....
SECU$ATTACH$TFO$FILES....
```

TFO is given the authority to use the proper system resources--regions, terminals, subsystems, verbs and files, if applicable. If a list is not assigned, all resources in that area are available. These lists may subsequently be modified by TFO (or CVW) using the ATTACH and DETACH commands. Note that the SECU verb is security exempt and can therefore be executed in the control region.

```
SECU$MODIFY$DEFAULTS$NOGLOBAL$NOMAXUSERS@
```

The Default Attribute List is made less powerful, but the two previously created accounts retain the GLOBAL attribute, and only they can create other global accounts. At this time, also consider whether the EXEMPT, EDITNEWS, and CONTROL attributes should be removed from the Default Attribute List. Although EXEMPT and EDITNEWS functions require global authority, it may not be desirable for future non-systems global managers to use these functions.

```
SECU$ADD$DH$NOMANAGER@
SECU$ADD$RE$NOMANAGER@
SECU$ATTACH$DH$REGIONS$CONTROL@
SECU$ATTACH$RE$REGIONS$CONTROL@
SECU$ATTACH$DH$TERMS$CNT01@
SECU$ATTACH$RE$TERMS$CNT01@
```

The two operations accounts are created. They will create their own passwords when they sign on. They are prohibited from exercising manager authority via the NO prefix to the MANAGER attribute. They are then confined to the control region and control terminal. Since they have neither global nor manager authority, the only ESS commands they can use are SEND, SIGNON and SIGNOFF. However, they are permitted to use all Intercomm system control commands because there is no attached verb list.

```
SECU$SIGNOFF@
SIGNON$TFO$TFO$WIZARD@
SECU$DELETE$SECURITY@
```

At this point, all the work that needs to be done under account SECURITY is finished. Now, TFO signs off from SECURITY and signs back on under his own account and assigns his password. He then deletes the well-known account SECURITY. The sign-off operation has locked the terminal to the verb SECU, so TFO can sign on without entering the SECU verb.

```
SECU$ATTACH$CVW$REGIONS$&TFO@
SECU$ATTACH$CVW$TERMS$&TFO@
SECU$ATTACH$CVW$SUBSYS$&TFO@
SECU$ATTACH$CVW$FILES$&TFO@
SECU$ATTACH$CVW$VERBS$&TFO@
```

This example illustrates the use of the Copy List facility associated with the ATTACH (and DETACH) command. TFO gives CVW authority to use the same regions, terminals, subsystems, verbs and files as for his account, as appropriate.

```
SECU$EXCLUDE$tid....
```

At this time the exempt terminal list should also be established (remote CPUs, printers, etc.).

```
SECU$SIGNOFF@
```

TFO can now sign off, having established the account CVW, who will take care of the production groups.

```
SIGNON$CVW$CVW$HOTCHA@
SECU$ADD$CVH$NOMANAGER@
SECU$ADD$JP$NOMANAGER@
SECU$ADD$PMM$GROUP(PAY)@
SECU$ADD$PKS$GROUP(EEO)@
SECU$ADD$JVM$GROUP(ACC)@
```

CVW signs on, defining her own password, and then creates the two development staff user accounts and the manager accounts in the production area. Because of the contents of the Default Attribute List at the time of their creation, the latter accounts will have authority appropriate for managers of end user groups. Also they will have no global authority at all and manager authority in only their own groups. At this time, the appropriate region, verb, terminal, etc., lists must also be established for the five accounts (see Figure 3).

```
SECU$MOD$DEF$NOMANAGER@
```

CVW takes the MANAGER attribute out of the Default Attribute List, leaving the end user accounts to be created with very limited command authority. Also, it may be desirable to remove the PASSWORD or SEND attributes from the system Defaults, to prevent end users from changing their password and/or sending messages to other users. Note the short syntax form that may be used for the command and/or keyword as illustrated for applicable commands in Chapter 2.

```
SECU$SIGNOFF@
```

At this point, CVW is finished with security and the group managers can take over. Note that only TFO or CVW can create additional group managers; a group manager cannot create another manager of the same group because the MANAGER attribute is removed from the Default Attribute List.

```
SIGNON$PMM$PMM$GOTTLIEB@
SECU$ADD$RJE$INHIBMSG$QUETO(hc)$LOCK(verb)...
```

The payroll manager (PMM) can now sign on, establish her password, and start to create accounts within the payroll group. The account RJE will automatically belong to the PAY group because the PAY group manager is creating the account.

```
SECU$ATTACH$RJE$REGIONS$&PMM@
SECU$ATTACH$RJE$VERBS$&PMM@
SECU$ATTACH$RJE$FILES$&PMM@
SECU$ATTACH$RJE$SUBSYS$&PMM@
SECU$ATTACH$RJE$TERMS$&PMM@
```

The payroll manager attaches the group's security resources, as appropriate, to account RJE using the Copy List facility.

Proceeding in the same manner, the rest of the security environment can be established.

Chapter 2

ESS COMMAND LANGUAGE

2.1 OVERVIEW

The ESS command language is used to dynamically establish and maintain the security environment as well as to gain access to the system by initiating a terminal session.

2.1.1 Initiating a Terminal Session

The SIGNON command is used to initiate a terminal session. Users sign on with a user-id or user-id and password, depending on how the account was initially defined. The earliest sign-on time may be controlled by the START attribute.

Upon entering a valid sign-on command, any system news is displayed at the terminal, unless the account does not own the SEENEWS attribute, or owns the INHIBMSG attribute (which overrides SEENEWS, and which prevents both system news and ESS acknowledgement messages from being received).

2.1.2 Terminating a Session

A session can be terminated voluntarily or involuntarily. A user remains signed on until any of the following occurs:

- The SIGNOFF command is issued by the user.
- Some maximum interval between input transactions has elapsed. This interval is set with the INTVL attribute.
- A manager FORCEs the user off the system.
- A new user signs on at the same terminal, which automatically signs off the old user (even if the same user-id is used).

If a transmission I/O error occurs which causes the Intercomm Front End to logically make the terminal unusable by Intercomm, the terminal-down user exit can be used to determine if a signoff of the terminal user should be done. The exits are USRTDWN for BTAM/TCAM devices and HALT for VTAM devices. The exit may call SECUSER to determine if a user is signed-on and, if necessary, internally generate a SECU$SIGNOFF message for the terminal being put down. The down terminal must be placed in MSGHTID in the header of the generated message.

2.1.3 Establishing Accounts

Accounts are established with the ADD command and deleted with the DELETE command. An account is identified by a user-id or a user-id and password. If a password requirement is established, it must be created/entered at sign-on time. An account can be signed on at only one terminal at any one point in time. When an account is added, security attributes can be assigned to it and it will be associated with the manager's group, for example:

```
SECU$ADD$TLC$START(0800)$STOP(1700)$INTVL(0010)@
```

establishes an account with user-id TLC, and START, STOP, and idle time-out attributes specified. Note that the specified attributes override the corresponding values specified in the Default Attribute List (if any).

2.1.4 Specifying Attributes

The Default Attribute List defines system-wide attributes to be automatically associated with an account when the account is created via the ADD command. However, attributes not owned by the issuer of the ADD command will be automatically removed from the new account's attribute list (does not apply to attributes for which a sub-value is specified: INTVL, LOCK, etc.) Conversely, attributes owned by the issuer which are no longer in the Default Attribute List will also be removed from the new accounts attribute list, however, these may be passed on to the new user via an attribute list on the ADD command when the account is created (see restrictions defined in Appendix B). A group managers group name will automatically be assigned end users created by that manager and may only be overriden by an account with global authority.

Attributes which are in both the Default Attribute List, and are owned by the issuer, may be denied an account by prefixing the attribute name with NO; NOINTVL prohibits the Default idle time-out for the specified account, for example (no idle time-out will occur). The attributes assigned a new (ADDed) account are displayed if the account is successfully created and should be verified at that time. Attribute assignments may subsequently be changed via the MODIFY$ACCOUNT command, or displayed via the DISPLAY$ACCOUNT command.

The Default Attribute List may be changed via the MODIFY$DEFAULTS command if the issuer has global authority. The list may be displayed via the DISPLAY$CONTROL command. The following attributes are not in the Default Attribute List when the security system is originally installed: NOPSWD, INHIBMSG, TERM-INV, VERB-INV, REGN-INV, S/S-INV, FUNC-INV. See Appendix B for requirements and restrictions associated with assigning these attributes.

2.1.5 Specifying Processing Restrictions

A number of attributes associated with an account define limitations on its processing and require an associated value to be defined, as follows:

- EXPDT--defines a date on which the account expires.
- INTVL--defines an automatic inactivity sign-off interval.
- LOCK--specifies a verb to which the terminal (user) is locked, following successful sign-on (see Section 2.1.13).
- PSWDEXP--specifies number of uses of a password permitted before a change of password is required (or account deactivated).
- SIGNON--permits the account to sign on.
- START and STOP--specifies the time interval (on a twenty-four hour basis) during which the account may sign on.
- QUETO--specifies the subsystem to be passed a dummy message following sign-on. (See Section 2.1.12.)

All attributes for which a sub-value may be defined (INTVL, LOCK, etc.) initially default to nulls (no restriction) when ESS is installed. System-wide defaults may be set in the Default Attribute List, and will be automatically assigned to each new account as they are created. A group manager's account values for this class of attributes is not passed on to accounts created in his group, nor from a global manager to a group manager/end user. Therefore, if no value is specified in the Default Attribute List, but is desired for an account, it must be individually assigned.

2.1.6 Establishing Passwords

In most installations, greater security is afforded by requiring each individual user to establish a password for his or her own account. A password requirement is automatically defined for an account when the account is created via the ADD command. Then, the user must establish his or her own password when he or she signs on for the first time. The new password may not be the user's account id.

The maximum number of SIGNONs with the same password is controlled by the PSWDEXP attribute. Three consecutive SIGNON tries with an invalid password will deactivate the account (SIGNON attribute removed).

It is strongly recommended that all accounts have a password requirement. A password requirement can be unassigned via the MODIFY$ACCOUNT$user-id$NOPSWD command. If the user forgets or needs to change the password, the account can be reset to the user-id via the MODIFY$PASSWORD$user-id command. Also ensure that the account has the SIGNON attribute. The changed password may not be the user-id. Valid sign-on user-ids are logged (for the audit trail) and can be accessed in user exits. Passwords (valid or invalid) are not passed through user exits.

2.1.7 Giving an Account Authority to Use Resources

Once an account is established, the security resources it is authorized to use can be specified by a global manager using the ATTACH command. For example:

```
SECU$ATTACH$PKS$REGIONS$REGIONA@
```

limits the manager account PKS to REGIONA of a multiregion Intercomm. Note that a subsystem list provides redundent security below the verb list level, but can also be used for messages queued from one subsystem (application program) to another subsystem (does not apply to the Output Utility).

2.1.8 Defining Prohibited Resources

For some accounts, it may be more convenient to define their scope of authority by specifying which resources are prohibited, rather than which are permitted. In these cases, a resource list associated with an account may be inverted by use of the appropriate invert attribute. For example:

```
SECU$ATTACH$JVM$REGIONS$REGIONA@
SECU$MODIFY$ACCOUNT$JVM$REGN-INV@
```

Account JVM is now prohibited from using REGIONA, and permitted to use all other regions. Other resource lists associated with the account, such as those specifying files, subsystems, or verbs, remain in their uninverted form. Thus, for a given account, some resource lists may be inverted and some may be uninverted. A file list may not be inverted.

To change the resource list back into uninverted form, use the negation of the inversion attribute, for example:

```
SECU$MODIFY$ACCOUNT$JVM$NOREGN-INV@
```

Be careful when assigning an -INV attribute, because if no associated list is specified (or later removed), then all resources of the specified type are made unavailable to the account.

2.1.9 Copying Lists

The Copy List facility provides a method of copying (merging) resource lists from one account to another. This is done by specifying the user-id, preceded by an ampersand, as an element of the resource list in the ATTACH or DETACH commands. If the requester has global authority, a list may be copied from any account, however a manager may only copy from a user's or manager's list within the managers own group to an end user in the same group.

2.1.10 News Broadcasts and Messages

There are four classes of ESS messages that may be received at the terminal: the news message; acknowledgement messages; error messages; and switched messages.

A news message can be created or updated with the EDITNEWS command. News is universal to the system. All accounts with the SEENEWS attribute will have this news shown to them after a successful sign-on, unless they own the INHIBMSG attribute.

Acknowledgement messages are sent in response to the successful completion of certain ESS commands (such as SIGNON). These messages are listed in Appendix D.1 (marked with a bullet), or are described under the corresponding command. Ownership of the INHIBMSG attribute prevents the receipt of acknowledgement messages to the SIGNON command and is to be assigned if the QUETO attribute is defined.

SIGNON acknowledgement messages and the news message (if any) are sent together as one message. If any messages were previously queued for the terminal, they will be transmitted before the SIGNON response. At a terminal defined as a CRT, the RLSE command may have to be used to ensure receipt of the SIGNON response.

Error messages are sent in response to the unsuccessful completion of ESS commands. These messages are listed in Appendix D.1, not marked with a bullet. Error messages are not inhibited by the INHIBMSG attribute.

One user can send a message to another active user with the SEND command, if the sender has the SEND attribute.

2.1.11 Displaying Security Information

An account with MANAGER or GLOBAL authority can display security information about the accounts under its jurisdiction, using the DISPLAY command, if the requestor also has the attribute associated with the category of information to be displayed.

2.1.12 Menu Processing

Menu processing logic may be integrated into the security system by specifying a subsystem which is to receive a message following a successful sign-on of an account. This is specified using the QUETO attribute of that account. The subsystem specified receives a message (VMI=X'FF') in the following format:

Bytes	Contents
1-42	Message Header
43-46	Dummy Verb (ONXX)
47	Separator (comma)
48-55	User-id
56	@ (X'26')

Based on user-id, the subsystem can return a menu to the sending terminal. At this time, the user's terminal could be locked by the subsystem to an appropriate verb via an internal LOCK command, if a verb for the LOCK attribute is not defined for the account. If menu processing is defined for an account, the INHIBMSG attribute should also be assigned to the account, otherwise both the SIGNON response and the menu will be queued as separate messages and will cause an out-of-sequence condition.

2.1.13 Locked Verb Processing

Because all non-exempt terminals are initialized as locked to the SECU verb during ESS startup, ESS provides a LOCK(verb) attribute as an alternative, and thus makes terminal/verb locking an end user-associated, rather than a terminal-associated, function. Thus, a manager or systems account, which does not have the LOCK attribute, does not have to request an UNLK from the terminal before using Intercomm system control commands, for example. Note that the system commands SECU, RLSE, COPY, SPLU, VTST, LOCK and UNLK are by default lock exempt (can be entered at a locked terminal after sign-on, without first unlocking the terminal).

The locked verb must still be in the user's verb list (if defined) to pass ESS security processing. The latter is true for all Intercomm system control commands and user verbs (except SECU). Auto-lock processing will continue to be honored and it can override the LOCK attribute (if defined).

If an end user is not allowed to, or does not know how to, use the UNLK command, that user will always be locked-in to the LOCK attribute defined verb (subsystem), no matter at what terminal he is allowed to SIGNON.

2.2 SYNTAX SUMMARY

All commands must be prefixed by the verb SECU. Since the terminal is locked to the SECU verb at startup, a user may omit that verb from his sign-on command. Subsequent sign-ons may also leave off the verb since sign-off processing relocks the terminal. (Sign-on processing unlocks the terminal unless overridden by the LOCK attribute.) ESS commands are processed by the Edit Utility. The maximum number of elements per input message is 100.

In the following syntax specification, the conventions used are as follows:

$ indicates the system separator character

@ indicates end of transmission sequence

[ ] brackets indicate optional parameters and/or short syntax forms (omitted suffix) of commands and/or keywords within commands

{ } braces indicate alternatives, listed vertically. The default, if any, is underlined.

... ellipses indicate that an element may be repeated.

The commands are alphabetized by the keyword following SECU.

The requirements for issuing each command are given under two headings, "Level of Authority" and "Required Attributes."

If the "Level of Authority" is given as GLOBAL, only accounts with the GLOBAL attribute can issue the command. If the level of authority is given as MANAGER, the MANAGER attribute is required to issue the command affecting accounts in the same group; the GLOBAL attribute is required to issue the command affecting accounts in any group. If the level of authority is given as user, neither the GLOBAL nor the MANAGER attribute is required.

Attributes required to issue the command, in addition to the attribute specifying the appropriate level of authority, are given under "Required Attributes."

The requirements for issuing each command are summarized in Appendix A. The attributes are listed and defined in Appendix B.

ADD

ADD is used to establish an ESS account and associate attributes with the account. The attributes define the account's authority and processing restrictions. By default, a password must be established when the new account signs on, unless the NOPSWD attribute is assigned. Attributes may be changed via the MODIFY command. If successfully added, an account display is returned to the issuer, as described under the DISPLAY command.

Entry Format

```
SECU$ADD$user-id[$attribute[$...$attribute]]@
```

attribute
represents an attribute name (as given in Appendix B) to be associated with, or disassociated from, the account. Only attributes may be specified in the ADD command which are owned by the account issuing the command (see Appendix B). If none are specified, all attributes owned by the issuer, which are also in the Default Attribute List, are associated with the added user (for exceptions-see Sections 2.1.4 and 2.1.5).

user-id
represents a one-to-eight character unique user-id to be associated with the account.

Level of Authority

MANAGER

Required Attributes

ADD

Also, if requestor is a group manager, the manager's group name attribute will be automatically assigned to the added account. However, if the manager has no named group attribute, the account may not be added. When the requestor is a group manager who has resource lists attached to his account, the added user must have resource lists of the same type as the manager (see ATTACH command). The user will not be able to sign on until the appropriate lists are attached to his account by the group manager. If there is no room to add the account, an error message is returned.

ATTACH

ATTACH associates authorized verbs, regions, subsystems, terminals, files or user functions with an account.

Entry Format

```
SECU$ATT[ACH]$user-id${VER[BS   ]}${resource[$...$resource]}@
                      {REG[IONS ]} {&user-id               }
                      {TER[MS   ]}
                      {SUB[SYS  ]}
                      {FIL[ES   ]}
                      {FUN[CTION]}
```

resource
represents a security resource to be attached to the account, of the type specified by the keyword given, as follows:

VERBS--a four-character verb

REGIONS--an eight-character region-ID (low-order blanks, if necessary)

SUBSYS--a two-character set of alphanumeric high/low subsystem codes, or a four-character set of hex high/low subsystem codes. (3-digit numeric codes are not supported). If either subsystem code is nulls (000), the codes must be entered in hex format with 00 representing the null code.

TERMS--a five-character terminal-ID

FILES--an eight-character DD name (low-order blanks, if necessary) followed by a one-character suffix indicating access authorization, as follows:

R--read only

*--read/write

All accounts are automatically allowed to use system files (message queues, Store/Fetch data sets, etc.).

FUNCTION--an eight-character logical user function name (low-order blanks, if necessary) to be tested using the SECTEST macro

resource may be the user-id, preceded by an ampersand, of an account whose resource list (of the type specified by the keyword) is to be copied.

user-id
: represents an account previously defined using an ADD command.

Level of Authority

GLOBAL
MANAGER (copy resource list function only)

Required Attributes

ATTACH

Also, the attribute corresponding to the resource (list) being attached is required. The attribute name is identical to the corresponding resource keyword. For example, the VERBS attribute is required in order to issue an ATTACH$VERBS command.

In addition, the copy list function requires the requestor to have global authority, or if a manager, the copied account (&user-id) must belong to the same group as the manager's account. If the specified account has an existing list, the copied list is merged into it, duplicates are bypassed. Note that a manager cannot attach (add) individual resource items to any account, and can only copy a list to an end user account (not to a manager account, even if in the same group).

If the invert (...-INV) attribute exists in the specified user's account for the list being modified, the newly attached resource(s) is now prohibited.

NOTE: If the user is currently signed on, changes to that user's resource lists will not take effect until the next sign-on. If systemwide security of the resource type is not in effect (see Chapter 3), list validation for a user is not executed even though a list exists for the user account. Adding resources to a manager's account requires GLOBAL authority.

DELETE

DELETE is used to delete an account from the security system. If that account is currently signed on, an error message will be returned. The account can be signed off via the FORCE command. Then retry the DELETE command.

Entry Format

```
SECU$DEL[ETE]$user-id@
```

user-id
represents an account to be deleted from the security system.

Level of Authority

MANAGER

Required Attributes

DELETE

DETACH

DETACH is used to take authorized verbs, regions, subsystems, terminals, files or user functions away from an account.

Entry Format

```
SECU$DET[ACH]$user-id${VER[BS   ]}${resource[$...$resource]}@
                      {REG[IONS ]} {&user-id              }
                      {SUB[SYS  ]}
                      {TER[MS   ]}
                      {FIL[ES   ]}
                      {FUN[CTION]}
```

resource

represents a security resource to be taken away from the account, of the type specified by the keyword given, as follows:

VERBS--a four-character verb

REGIONS--an eight-character region-ID (low-order blanks, if necessary)

SUBSYS--a two-character set of alphanumeric high/low subsystem codes, or a four-character set of hex high/low subsystem codes. (3-digit numeric codes are not supported.) If either subsystem code is nulls (000), the codes must be entered in hex format with 00 representing the null code.

TERMS--a five-character terminal-ID

FILES--an eight-character DD name (low-order blanks, if necessary) followed by a one-character suffix indicating access authorization, as follows:

R--read only

*--read/write

FUNCTION--an eight-character logical user function name (low-order blanks, if necessary) to be tested using the SECTEST macro

resource may be the user-id preceded by an ampersand, of an account whose resource list elements (of the type specified by the keyword) are to be detached from the requested account.

user-id

represents an account previously defined using an ADD command.

Level of Authority

GLOBAL
MANAGER (detach only from end user accounts in the same group)

Required Attributes

DETACH

Also, the attribute corresponding to the type of resource being detached is required. The attribute name is identical to the corresponding resource keyword. For example, the VERBS attribute is required to issue the DETACH$VERBS command.

In addition, the copy list function requires the requestor to have global authority, or if a manager, the copied account (&user-id) must belong to the same group as the manager's account. A copied list detaches only those resources found in the specified account's existing list. Note that a manager can only detach from an end user account (not a manager, even if in the same group).

If the invert (...-INV) attribute exists in the specified user's account for the list being modified, the newly detached resource(s) is now allowed. However, if all resources in the list are detached, and the invert attribute is defined, then none of that resource (except exempt items) is allowed. If no list is required of the type whose attribute is inverted, the invert attribute is ignored.

NOTE: If the user is currently signed on, changes to that user's resource lists will not take effect until the next sign-on. If all resources in an end-user's account are detached by a group manager, the user will not be able to sign on again, unless that manager also no longer has a resource list for the specified resource type or systemwide security of that type has been suppressed (see Chapter 3). To remove a specific list requirement from both the group manager(s) and the end users in the manager's group, a global manager must first detach all resources in the group manager's list of the specified type. Then the Group Manager must sign off and sign on again before detaching the end-user's list. GLOBAL authority is required to detach resources from a manager's account.

DISPLAY

DISPLAY is used to display information about the security system, according to the keyword given, as follows:

ACCOUNT--Account profile, that is, its attributes.

CONTROL--Amount of system space in use by ESS, number of accounts defined, maximum active users allowed, number of free blocks on the Security Data Set, user-ids defined (an asterisk after the id indicates account not allowed SIGNON), Default Attribute List.

EXEMPT--Exempt terminal list

FILES--Attached file list for a specific account

FUNCTION--Attached user function list for a specific account

REGIONS--Attached region list for a specific account

SUBSYS--Attached subsystem list for a specific account

TERMS--Attached terminal list for a specific account

USERS--Signed-on users

VERBS--Attached verb list for a specific account

Entry Format

```
SECU$DIS[PLAY]${CON[TROL  ]         }@
               {EXE[MPT   ]         }
               {USE[RS    ]         }
               {{ACC[OUNT ]}$user-id}
               {{FIL[ES   ]}        }
               {{FUN[CTION]}        }
               {{REG[IONS ]}        }
               {{SUB[SYS  ]}        }
               {{TER[MS   ]}        }
               {{VER[BS   ]}        }
```

user-id
    is the account name for which information is to be displayed.

Level of Authority

MANAGER

Required Attributes

DISPLAY

Also, the attribute corresponding to the type of information being displayed is required. The attribute name is identical to the corresponding keyword. For example, the CONTROL attribute is required to issue the DISPLAY$CONTROL command. In addition, a manager may not display account, or resource list, information for a user-id that does not belong to his group.

An account display is as follows:

```
PROFILE FOR ACCOUNT uuuuuuuu  PASSWORD  { REQUIRED }
                                        { * NONE * }
GROUP gggggggg  LOCK vvvv  QUEUE TO hc  PSWD EXPIRES nnn
EXPIRATION DATE yyddd  START TIME hhmm  STOP TIME hhmm
AUTO SIGN-OFF AFTER hhmm
LAST SIGNON WAS hh:mm:ss:tt  yy:ddd

ATTACHED RESOURCE LISTS ARE:  [NONE]
list-type list-type list-type list-type list-type list-type

ACCOUNT ATTRIBUTES
aaaaaaaa  aaaaaaaa  aaaaaaaa  aaaaaaaa  aaaaaaaa  aaaaaaaa
   .         .         .         .         .        .
   .         .         .         .         .        .
   .         .         .         .         .        .
```

Variable field values are indicated above by lower case letters. Values on lines 2 through 7 will not be displayed if not assigned to the account. Only those attributes assigned the account are listed.

A requested resource list, including the exempt terminal list, is displayed under the title ATTACHED RESOURCE LIST.

A USERS display lists each signed-on terminal and the associated user-id (account name). A terminal where the user is being FORCEd off, or has timed out, is displayed with an asterisk following the user-id. At the end, a count of all signed-on users is displayed.

All displays are prefixed by the heading line:

```
INTERCOMM EXTENDED SECURITY SYSTEM
```

EDITNEWS

EDITNEWS is used to add to or replace the message text sent to authorized accounts after a successful sign-on. Accounts which have the SEENEWS attribute but not the INHIBMSG attribute are sent the message text.

Entry Format

```
SECU$EDI[TNEWS][$text[$...$text]]@
```

text

represents a one to sixty-four character string to appear as a single line. Unlimited lines of text may be specified, each delimited by a system separator. The individual lines of text may not contain embedded system separator or New Line characters. Lines longer than 64 characters will be truncated. If text is omitted, the current response message will be scratched. If adding to the current message, the entire message must be reentered.

Level of Authority

GLOBAL

Required Attributes

EDITNEWS

EXCLUDE

EXCLUDE is used to add to the list of terminals which are exempt from ESS.

Entry Format

```
SECU$EXC[LUDE]$terminal-id[$...$terminal-id]@
```

terminal-id
: represents a five-character terminal-ID to be exempted from security control.

Level of Authority

GLOBAL

Required Attributes

EXEMPT

NOTE: If a user is not currently signed on at the terminal being EXCLUDEd, the terminal must also be unlocked (via UNLK command) from the SECU verb. If signed-on, the terminal must be unlocked from SECU (from another terminal) after sign-off.

FORCE

The FORCE command is used to terminate the terminal session of an active user.

Entry Format

```
SECU$FOR[CE]$user-id@
```

user-id
represents the account-ID of the user whose terminal session is to be cancelled.

Level of Authority

MANAGER

Required Attributes

FORCE

For a group manager, only end users in the same group may be forced off.

INCLUDE

INCLUDE is used to remove a terminal from the list of terminals which are exempt from ESS.

Entry Format

```
SECU$INC[LUDE]$terminal-id[$...$terminal-id]@
```

terminal-id
represents a five-character terminal-ID to be removed from the list of terminals exempted from security control.

Level of Authority

GLOBAL

Required Attributes

EXEMPT

MODIFY

The MODIFY command is used to reset an account password requirement, or the maximum active user count, or to change the attribute list associated with an account, or to change the Default Attribute List.

Entry Format

```
SECU$MOD[IFY]${PAS[SWORD]$user-id                         }@
              {MAX[USERS]$count                           }
              {ACC[OUNT ]$user-id$attribute[$...$attribute]}
              {DEF[AULTS]$attribute[$...$attribute]        }
```

attribute
: represents an attribute name (as given in Appendix B) to be associated with the account (or to be a default, as specified). Which attributes may be specified in the MODIFY$ACCOUNT command depends on what attributes are owned by the account issuing the command, as specified in Appendix B.

count
: represents the maximum number of concurrent active users, as a decimal number greater than zero and up to seven digits.

user-id
: represents the user-id of the ACCOUNT whose attributes are to be modified; or, if PASSWORD sub-parameter is entered, resets the account password to force the user to assign a (new) password at the next SIGNON. Note that the NOPSWD 'attribute' may be assigned if password requirement is waived.

Level of Authority

MANAGER for MODIFY$ACCOUNT and MODIFY$PASSWORD

GLOBAL for MODIFY$DEFAULTS and MODIFY$MAXUSERS

Required Attributes

MODIFY for MODIFY$DEFAULTS
MODIFY and MAXUSERS for MODIFY$MAXUSERS
MODIFY and PASSWORD for MODIFY$PASSWORD
MODIFY and ACCOUNT for MODIFY$ACCOUNT

NOTE: a MANAGER must have a GROUP attribute, and only those end user accounts with the same group name attribute may be modified, otherwise the issuer must have the GLOBAL attribute. A manager may not modify an account of another manager in the same group.

For the MODIFY$ACCOUNT command, an account display is returned as described for the DISPLAY command. For MODIFY$DEFAULTS, an account display of the Default Attribute List is returned, however the first line contains CURRENT DEFAULTS instead of an account name and password designation.

NOTE: If the user whose account is being modified is currently signed on, the attribute changes for that account will not take effect until the next sign on. This is also true for changes to the INTVL and STOP times, etc.

SEND

The SEND command is used to transmit a message to an active user.

In contrast to the Intercomm system command SWCH, the sender uses the receiver's user-id, not the terminal-id. The transmitted message will contain the heading:

```
>----INTERCOMM EXTENDED SECURITY SYSTEM----<
MESSAGE FROM uuuuuuuu
```

where uuuuuuuu is the sender's user-id.

Entry Format

```
SECU$SEND$user-id$text@
```

text
represents one to one-hundred-and-twenty-eight characters of text containing no embedded system separator or New Line characters.

user-id
represents the ID of an active (signed-on) account to receive the message.

Level of Authority

User

Required Attributes

SEND

SIGNOFF

The SIGNOFF command is used by the terminal operator to terminate a terminal session.

Entry Format

```
SECU$SIGNOFF@
```

Level of Authority

User

Required Attributes

None

NOTE: SIGNOFF automatically relocks the terminal to the SECU verb.

SIGNON

The SIGNON command is used by a terminal operator to initiate a terminal session.

If the terminal is defined as locked to the SECU verb, the verb may be omitted from the SIGNON command.

Entry Format except when preformatted prompt screen displayed on an IBM 3270 CRT (see below).

```
      [SECU$]SIGNON$user-id[${password                 }]@
                             {user-id$new-password      }
                             {old-password$new-password}
```

old-password$new-password

is used when a password change is desired or required. The old and new passwords may not be the same.

password

represents the one-to-eight character password previously associated with the account.

user-id

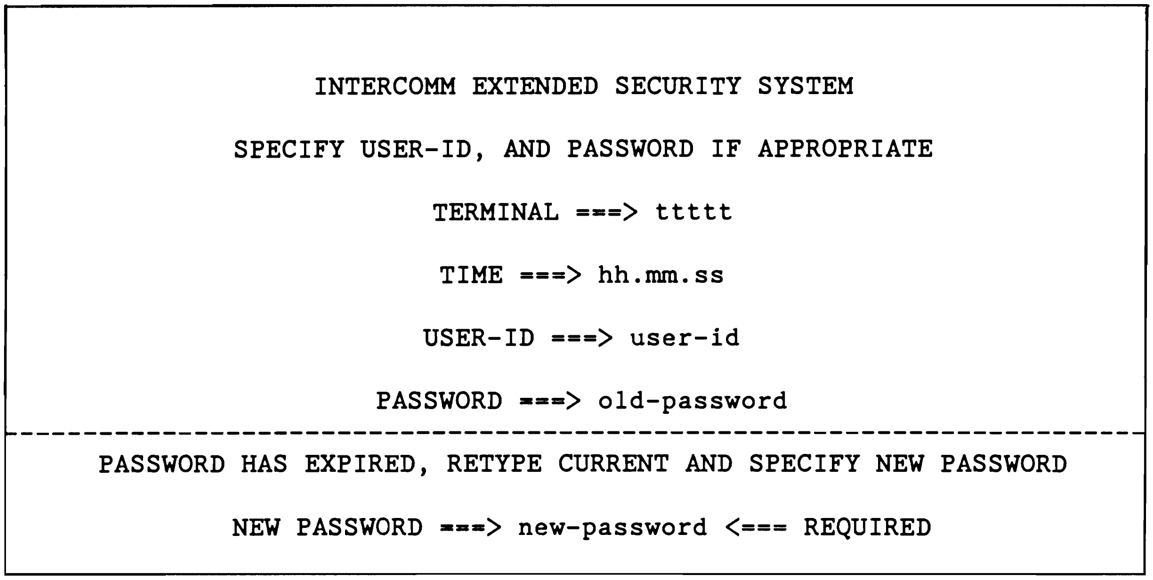
represents the one-to-eight character user-id associated with the account.

user-id$new-password

is used for first SIGNON of a new account, or after the old password has been unassigned.

NOTE: new-password may not be the same as old-password, nor may it be the same as the account's user-id.

Entry Format for IBM 3270 CRT with preformatted display (the SIGNON command is automatic and is omitted):



```
                    INTERCOMM EXTENDED SECURITY SYSTEM

               SPECIFY USER-ID, AND PASSWORD IF APPROPRIATE

                          TERMINAL ===> ttttt

                          TIME ===> hh.mm.ss

                          USER-ID ===> user-id

                       PASSWORD ===> old-password
---------------------------------------------------------------------------
     PASSWORD HAS EXPIRED, RETYPE CURRENT AND SPECIFY NEW PASSWORD

               NEW PASSWORD ===> new-password <=== REQUIRED
```

The area above the line of dashes is the basic display and contains:

ttttt — is the terminal-id of the terminal and is displayed in the format.

hh.mm.ss — is the time when the display was sent to the terminal and is displayed in the format.

user-id — is a blank area where the operator must enter the user-id.

old-password — is a blank non-display area where the account password is to be entered. For the first sign-on of a new account, or after the old password has expired or been unassigned, the account's user-id is to be entered here. If a password is required but omitted, or is entered incorrectly, the prompt screen is returned with <=== REQUIRED after the password entry area. The area below the line of dashes is displayed in addition to the basic screen only when a new or changed password is required.

new-password — is a blank non-display area where the new account password or changed password is to be entered. It may not be the same as the old password, nor the same as the account's user-id.

NOTE: If any ESS or Edit Utility error message is displayed on the screen, erasing the screen via ERASE EOF Key and entering SIGNON (no parameters) will return the prompt display; do not use the CLEAR Key to erase the screen.

Level of Authority

User

Required Attributes

SIGNON

Even though the SECU verb may be omitted from the SIGNON command, once sign-on is successful, the terminal is unlocked from the SECU verb. Therefore, the SECU verb (system command) is required for all other ESS commands. SIGNOFF, whether entered, FORCEd, or due to a timeout, automatically locks the terminal to the SECU verb.

Sucessful signon results in ESS messages (and system news message, if any and allowed) preceded by the heading line:

```
INTERCOMM EXTENDED SECURITY SYSTEM
```

At the end of the ESS (news) messages, the following sign-on logo appears:

```
INTERCOMM SESSION BEGINNING  hh.mm.ss  yy.ddd
TERMINAL(tid)  USER(uuuuuuuu)  GROUP(gggggggg)
 >------------SIGNON COMPLETED------------<
```

If the user is not a member of a group, the GROUP(name) is omitted.

At this time, standard message transmission may proceed. If at a CRT terminal, erase the screen before keying the first message.

If ESS signon response messages are prohibited, a menu display will be transmitted instructing the operator how to proceed.

Chapter 3

INSTALLATION OF ESS

3.1 INTERCOMM MULTIREGION SVC

If not already used for MVS, XA or Multiregion processing, the Intercomm Multiregion SVC must be installed for ESS. Assign a Type 1 SVC number with no locks for the Intercomm Multiregion SVC. Update SETGLOBE global &MRSVC with the appropriate number and reassemble IGCICOM. The load module name should be IGCnnn, where nnn is the SVC number. Then run an IOGEN to pick up the new SVC. Reassemble INTSPA and KEYFLIP. See the Operating Reference Manual.

3.2 SECURITY DATA SET

The Security file is a fixed unblocked BDAM data set with a block size of 256. Read/write password protection is recommended.

3.2.1 Security Data Set Creation

To create the Security Data Set, use the Intercomm SECFILE utility with the following JCL:

```
//SECFILE  EXEC  PGM=SECFILE,PARM=nn
//STEPLIB  (as needed)
//SECURITY  DD  DSN=name,DISP=(NEW,CATLG,DELETE),
//        DCB=DSORG=DA,SPACE=(256,(n[,e]),ROUND),...
```

where nn is a two-digit dataset extent count in the range of 01 to 16, e is the additional blocks to be initialized per extra extent requested via PARM (if more than 01), and n is calculated according to the following formula:

$$n=a\left(\frac{v}{62}+\frac{r}{31}+\frac{t}{50}+\frac{s}{125}+7+\frac{f}{27}+\frac{u}{31}\right)$$

a = expected number of accounts

v = average number of verbs per account

r = average number of regions per account

t = average number of terminals per account

s = average number of subsystems per account

f = average number of file names per account

u = average number of user function names per account

3.2.2 Security Data Set Expansion

If the original Security file runs out of space, an expansion facility within the SECFILE module provides for creating a new larger file, and overlaying it with the existing Security data set. Use the JCL listed above for creating the data set, with SECURITY defining the new expanded version of the file, and with the following DD statement added to define the existing Security data set:

```
//OLDSECUR   DD   DSN=old-name,DISP=OLD
```

3.3 ESS DEFINITION

Define ESS to Intercomm. A BTVERB macro is required in the BTVRBTB Front End Verb Table to define the SECU command, as follows:

```
BTVERB VERB=SECU,SSC=E,CONV=180000
```

Lock exemption and priority queuing for SECU commands are forced by ESS at startup. All nonexempt terminals are locked to SECU at startup. All nonexempt BTERM/LUNIT/LCOMP definitions may omit the LOCK parameter, except dialup and VTAM devices should have LOCK=SECU coded to ensure relocking at reconnect and session initiation time. All nonexempt BTERM/LUNIT/LCOMP definitions must have CONV=YES coded. To implement conversational processing for the BTAM/TCAM Front End, see the BTAM Terminal Support Guide.

A SYCTTBL entry for the dummy subsystem $$$$SECU (provided on SYMREL and MODREL) must be coded, as follows:

```
SYCTTBL SUBC=E,SBSP=$$$$SECU,LANG=RBAL,TCTV=600,OVLY=0,      X
        MNCL=50,NUMCL=100,PRYMSGS=20,RESTART=NO,LOG=NO
```

The combined value coded for PRYMSGS and NUMCL should equal the total number of nonexempt terminals, or a disk queue (for overflow message queuing) must be defined. Sample entries for the BTVERB and SYCTTBL definitions are provided on SYMREL in the members USRBTVRB and USRSCTS, respectively. Neither the SYCTTBL nor the subsystem are used in any satellite regions.

Use the released version of PMIVERBS containing the SECU verb/parameter coding for the Edit Control Table, or add the code from the released version to the installation version and reassemble PMIVERBS (VERBTBL Csect).

Code SECUR=ESS for ICOMLINK to force the following in the Intercomm linkedit:

1. Including RPT00049 with those for other system commands.

2. Including the module INTSEC00 in all region linkedits.

3. Including $$$$SECU as resident in the control region.

4. Removing the include for USRSTART.

If coded, add INCLUDEs for USRSTRT1 and USRSEC00 (all regions), and for USRPRMPT (control region only). Verify that module INTSEC02 resides in STEPLIB or LINKLIST library (control region only). Do not include it in the Intercomm linkedit. If coded, linkedit SECUEXIT (see Chapter 4) with INTSEC02.

For the security file, use the following JCL in the control region only:

```
//SECURITY  DD  DSN=name,DISP=OLD,DCB=(DSORG=DA,OPTCD=R)
```

3.4 LINK PACK AREA PREPARATION

Assemble and link the SVECT macro (Csect SECVECT) into the appropriate system library: for non-MVS systems, use SYS1.LINKLIB; for MVS and XA, use SYS1.LPALIB. Use the following JCL:

```
//     EXEC ASMPCL,Q=REL,NAME=SECVECT,LMOD=SECVECT
//ASM.SYSIN DD   *
         SVECT DSECT=NO[,VERB=NO][,TERM=NO][,SUBSYS=NO]
               [,REGION=NO][,FILE=NO][,USRFUNC=NO]
         END
//LKED.SYSLMOD DD DSN=dsname(SECVECT),DISP=OLD
```

The optional parameters for the SVECT macro may be coded to suppress testing for the corresponding secured resource processing, if such security is not used in the Intercomm system.

Define the appropriate SYS1.PARMLIB entry. For non-MVS systems, use IEAIGGnn; for MVS and XA, use IEAFIXnn (do not link as reentrant). Under XA, NOPROT must be specified on the FIX or MLPA (use IEALPAnn) system parameter and RMODE and AMODE must be 24. After preparing the linkpack, re-IPL the system.

3.5 INITIAL SIGN-ON

It is recommended that a basic Intercomm be brought up temporarily to create the security environment because at Intercomm startup, until the exempt terminal list is established, all defined terminals including write-only devices (printers), remote CPUs, dial-up terminals, etc., will be locked to the SECU verb and will receive a sign-on prompt message, instead of the 'Good Morning...' message which is no longer used. Also, no one can enter messages until his account has been established, except the SECURITY account user.

For the initial sign-on, use the user-id SECURITY, as described in Chapter 1. Then create the security environment using ESS commands. Once the environment is set up, SECURITY may be deleted or assigned a password and modified as necessary.

3.5.1 Limitations on Adding Accounts

During ESS initialization at Intercomm startup, an in-core list of user-ids is built in protected core to facilitate internal access of user account records at SIGNON, etc. This list also contains empty entries available for adding new accounts during that Intercomm execution. The number of empty entries is controlled by the equate labeled DAILYADD in INTSEC02, and is initialized to 20. This value may be changed for the next/first execution under ESS, if desirable, but should be reduced to the minimum necessary once the security environment has been stabilized.

3.6 RESTRICTIONS AND RECOMMENDATIONS

- Be generous with space calculations when creating the Security Data Set.

- Daily (or when changed) backup of the Security Data Set is recommended so that the ESS environment does not have to be recreated in case of head-crash, etc.

- Two on-line Intercomm systems which both must use ESS cannot execute concurrently on the same CPU. If executing on different CPUs, each must use a unique Security Data Set. If a production and test system using ESS must execute on the same CPU, then Multiregion must be installed with a test region, or the test system cannot use ESS.

- ESS requires that all terminals defined in the Front End Network Table (BTAM/TCAM/VTAM) which may input a message, must also be defined with the same terminal-ID in the Back End Station Table. Otherwise, no input from the missing terminal will be processed (even if terminal in exempt list).

- Under VTAM, an operator can request a VTAM session termination by keying the user-id LOGOFF in the ESS signon screen display. The SECUEXIT user exit must be used to issue an internal SPLU command to force session termination when this id is used at sign-on, and then return a code of 4 to the ESS signon processing. An account (with no attributes except SIGNON) must be created on the Security file to allow this psuedo-id to be used. See also the description of SECUEXIT in Chapter 4.

- If a COMTEN Transmission Control Unit (instead of an IBM 37xx) is used with the MAF facility installed, session termination can be requested in the same manner as described above for a VTAM terminal.

- SIGNOFF under TCAM should be followed by an operator-entered LOGOFF command, if other TP monitors (TSO) are accessible from the same terminal. The SECUEXIT user exit can be used to issue an internal TDWN command to logically detach the terminal within Intercomm, if desired.

- SECUEXIT can be used at SIGNON time (called before ESS response messages or menu screen queued) to generate an internal FLSH command. This would flush any residual/switched messages queued for the terminal. Use the ALL subparameter--see System Control Commands.

- For all nonexempt BTAM dial-up (switched line) terminals, the account INTVL (automatic time-out) value should be greater than the elapsed time before automatic disconnect (maximum read time-outs occurred) takes place. Reconnect, with the same or another user-id is allowed after an accidental (user hangs up) or forced (I/O error/time-out) disconnect. However, the SECU verb must precede the SIGNON command since no SIGNOFF has occurred (unless INTVL times out before reconnect or LOCK=SECU is coded on each BTERM).

- For all nonexempt VTAM terminals which are not dedicated to Intercomm, LOCK=SECU must be coded on the LUNIT (or LCOMP) macro to ensure relocking to the SECU verb at each session initiation.

- INTVL time-out calculation under MRS should allow time for the associated satellite region to be restarted (after a system crash) if the user's processing is confined to a satellite region. This would obviate problems with a new SIGNON and associated LOCK or menu screen processing, if any, and also with restarting a conversation. This should be coordinated with restart/recovery provisions for the critical subsystems in that region. Periodically entering RLSE at the teminal will also prevent ESS session time-out.

- The system control commands SECN and SECF may be used in conjunction with ESS to restrict/remove verbs to/from entry only from the control terminal. Note that the closedown commands NRCD and IMCD are always confined to the control terminal. A verb defined via the BTVERB macro as SECURE will always be confined to the control terminal, even if it passes ESS, unless unsecured by the SECF command.

- When defining a MRS Region list to be associated with an account, the control region must always be defined with the identifier CONTROL (low order blanks). Satellite region identifiers must match those specified via the SPALIST macro in each region, and the corresponding RDT used in the control region.

- If an account has an inverted list attribute (REGN-INV, etc.), but no associated list is defined for that account, the comparable security test will always fail (except for exempted subsystems and files), unless that type of security has been suppressed system wide via the SVECT macro.

- All messages queued for subsystems (except the Output Utility, MROTPUT, Closedown and Checkpoint) are checked by ESS for a signed-on user (unless terminal in exempt list), when dequeued for processing. If not signed on, and the terminal is not in the exempt list, the terminal is locked to the SECU verb and the queued message is cancelled. If signed on, but the queued message fails subsystem security (if desired) or region security (if desired), an ESS error message is returned to the terminal and the queued message is cancelled. The cancelled message is logged with a log code of X'FE'.

- If a verb list is defined, all system verbs (RLSE, COPY, etc.) allowed for the user must also be in the list. Only the SECU verb is security exempt. Auto-lock and lock-exempt processing will continue to be honored (BTVERB macro AUTOLOK and LOCKEXE parameters). A 'no verb found' condition returns the standard Intercomm error message. If the found verb does not pass security, an ESS error message is returned and the input message is flushed. The above does not apply to exempt terminals. Fast message switching may continue to be used, however the entered terminal-id must be defined in the Station table.

- File security is performed at SELECT time and applies only to those files processed via the File Handler, and only to those accounts having a file list. If it fails, the return code is C'9'. Security checking for the following system files is exempted: INTERLOG, INTSTORn (Store/Fetch), SYSPRINT, RCT000, VRB000, DES000, SMLOG, STSLOG, STATFILE, CHEKPTFL, THREDLOG, MRS DDQs for disk queueing, files used only for startup and internal system functions, and CONVSFIL.

- If file security is specified for any account, then terminal output message disk queues must all start with the letters INT, PMI, BTAMQ, or VTAMQ to avoid failing file security when a subsystem (MAPEND) calls FESEND directly to queue an output message. File security is bypassed if FESEND is called from the Output Utility. Otherwise, terminal disk queue DD names must be added to all appropriate file lists for those accounts having such a list. Under a Multiregion Intercomm, the above restriction applies only to subsystems/accounts executing in the control region. However, when executing in a satellite region, the disk queue ddname defined for the MROTPUT subsystem must be in all those accounts having a file list, if the name does not start with INT or PMI.

- If file security is specified for any account, and that account accesses any subsystem which queues a message for another subsystem, including the Output Utility and MROTPUT, then the receiving subsystem disk queue ddname must start with the letters INT or PMI. Otherwise, the ddname must be added to the file list for that account.

- For data base access security, the SECTEST macro (for a user function) could be inserted in the Intercomm/DB-access interface program to test the user's authority to access the requested DB function (see Chapter 4). This requires a corresponding function resource list for applicable users.

- All messages entered before ESS initialization completes will be rejected with the 'NO VERB FOUND...' message.

- LOGINPUT cannot be used with ESS in the system (due to sign-on conflicts). Remove INTSEC00 from the linkedit and add the following instructions to LOGINPUT after the label GETRD (to throw away SECU messages):

  ```
          CLC    MSGHRSCH(2),=C'ab'
          BE     READ
  ```

  Substitute the receiving subsystem codes assigned to the SECU verb for the value ab.

3.7 MRS RAP PROCESSING AND ESS

Terminals used by specific user groups should be locked to the region associated with the group via standard BTERM/LUNIT/LCOMP coding. Message queuing is processed according to standard MRS RAP logic. Input messages must pass ESS verb security before being queued. RAP queuing logic does not apply to lock-exempt verbs; they are processed in the control region if they pass ESS security (also applies to SECU). The SECU verb is always allowed by ESS since it is required for SIGNON. If verb security is defined, it is recommended that all users be allowed the RLSE verb (lock-exempt). Global and Group Manager accounts should have access to the control region (defined for region security by the identifier CONTROL), in addition to the group's region (if applicable). Subsystem and region security are processed when the message is dequeued for the subsystem. Therefore, satellite region identifiers defined for ESS region security must compare with the region-ID defined in the SPALIST and RDT. To use region-oriented commands (LOAD, FHST, BEGN/DELY, MNCL, FILE, TALY$BE, etc.), the associated subsystem must be defined for the desired satellite region, the verb/subsystem/region must be allowed the user, and the user must be locked to that region (LOKR, ULKR must also be allowed). Refer also to System Control Commands and Multiregion Support Facility.

Warning: users allowed to use LOKR/ULKR must be sure to reinitialize the terminal's standard region association before signing off. Verb security should be defined for System Control Commands that are not associated with a subsystem (STAT, TPUP/TDWN, SPLU, VTST, etc). Region security is not applicable to these commands, because they are always processed in the control region.

3.8 RESTART PROCESSING AND ESS

Message restart processing to requeue messages in progress is performed before ESS startup processing. All requeued input messages are assumed to have successfully passed verb/terminal security processing during the last Intercomm execution. Requeued output messages (log code F2) are not processed by ESS. Messages requeued for a satellite region by the control region are security checked in the satellite region when dequeued for subsystem processing. Since satellite region processing is quiesced (if requested, otherwise closed down, or abends, as appropriate) until control region restart, security in the satellite regions is not affected by control region restart, as long as the existing users sign on again as soon as the ESS sign-on prompt message is received. When the entire system crashes, always restart the control region first, so that the current users can sign on again. Critical subsystems for which messages must be restarted, should be executed only in a satellite region, thus allowing users to remain signed on in the control region.

Currently, the subsystem controller (SYCT400) bypasses subsystem/region security for restarted messages (queued for the subsystem with log code R or P); therefore, the user issuing the original input message does not have to be signed on. However, the subsystem will not be able to access nonsystem files processed by the Intercomm File Handler (select request rejected by file security). User function security will also fail. To force failure at the subsystem/region security level for restarted messages, delete the statements at sequence numbers 00527000 through 00530000 from SYCT400.

Chapter 4

USER-CODED INTERFACES

4.1 SECUEXIT USER EXIT

A user exit may be coded, which receives control whenever the ADD, SIGNON, SIGNOFF, or DELETE command is issued. The user exit may indicate via return code in Register 15 whether processing is to continue. This exit may process only in the control region.

The CSECT name of this user exit must be SECUEXIT, which must be linkedited with INTSEC02 on STEPLIB, JOBLIB, or LINKLIST. This user exit may not exit to the Dispatcher, and must return control to ESS. All system addresses must be picked up from the SPA. Use GETSPA macro to acquire the SPA address.

At the time this user exit receives control, the exit owns an exclusive security lock. Thus, processing through the user exit is single-threaded. The lock is not in effect if a signoff is being processed.

This user exit must be written in Assembler Language. Great care should be exercised in designing and implementing the user exit, since a program check causes Intercomm to hang, and requires cancelling and restarting the Intercomm job.

At entry, the registers are initialized as follows:

R13 - Address of caller's save area
R14 - Return address to ESS
R15 - SECUEXIT address
R0 - Reason Code, as follows:

Reason Code	Purpose
0	Validate sign-on attempt: if the user-id is LOGOFF and is rejected by the user exit, the exit routine must cause a response message to be returned to the entering terminal (use MSGHTID in passed message header - see below)
4	Notify of sign-off: exit is called at the beginning of signoff processing, therefore the exit may perform internal cleanup routines (cancel a conversation in progress if the terminal is locked to a verb, for example)
8	Validate add new user-id (account name)
12	Validate deleting an old account

R1 - Standard parameter list in the following format:

Word	Contents--Address of:
1	8-character active user-id that issued command
2	Input message header
3	8-character new user-id if Reason Code is 8 or old user-id to be deleted if Reason Code is 12.

The user exit must use one of the following return codes (in register 15).

Return Code	Description
0	Processing may continue
4	Abort (Sign-on, DELETE or ADD only). Applicable ESS error message sent to terminal.

In the case of ADD processing, the exit may provide a different new user-id in the area addressed by the third parameter and pass a return code of 0 to force Security to utilize the altered user-id. The alteration is displayed, at the terminal issuing the ADD command, when processing is completed.

4.2 USRSEC00 USER EXIT

This user exit is called whenever an ESS log record (see Appendix C) is created. It may be used for user-oriented statistics gathering or signoff cleanup processing, for example.

The CSECT name of this user exit must be USRSEC00, which must be resident in the control region and, optionally, in all region linkedits. This user exit may not exit to the Dispatcher and must return control to ESS.

At the time this user exit receives control, the exit may or may not own an exclusive security lock; therefore single-threaded processing is not guaranteed. Nevertheless, care must be exercised in implementing this user exit, since a program check could cause Intercomm to hang.

At entry, the registers are initialized as follows:

R13 - address of the caller's save area
R14 - return address to ESS
R15 - USRSEC00 address

R1- address of a one-word parameter list containing the address of the ESS log record.

No return code processing is performed.

4.3 SECUSER SUBROUTINE

SECUSER is a thread-reentrant subroutine (entry in INTSEC00) that returns the active user-id in a provided area. The following are examples of how it is called:

Assembler Language:

```
             CALL  SECUSER,(USERNAME),MF=(E,list)
             .
             .
             .
 USERNAME    DS    CL8
```

COBOL:

```
             nn    USER-ID  PIC X(8)
                        .
                        .
                        .
               CALL  'COBREENT' USING SECUSER, USER-ID.
```

For reentrant subsystems, USERNAME/USER-ID must be defined in Dynamic Working Storage. If the associated user-id is not found, or no longer signed on, the provided area will contain blanks.

For reentrant COBOL and PL1 subsystems, the SECUSER subroutine must be added to the list in REENTSBS via the following statement:

```
SUBMODS  NAME=SECUSER
```

Also define the SECUSER index number in the copy member ICOMSBS or PENTRY, as appropriate. PL1-Optimizer subsystems can call the subroutine directly if SECUSER is added to PLIENTRY.

4.4 SECTEST MACRO

The SECTEST macro is used to test the authority of the current user to use a logical user function. The code generated is always link-pack eligible.

The form of the SECTEST macro is as follows:

```
[symbol]    SECTEST   FUNCTION,function-id
```

where function-id is an Rx or (R)-type address, or the label, of the eight-character user function name to be tested.

SECTEST provides a return code in register 15 as follows:

Return code	Description
0	Authorized
4	Not authorized, or user no longer signed on

User error notification must be handled by the program using the SECTEST macro. No system messages are created.

4.5 USRPRMPT USER EXIT

This user exit allows the user to suppress the generation of some, or all, sign-on prompt messages at ESS startup. This may be necessary when interfacing to a remote CPU or other hardware that emulates a 3270 CRT, but where the terminals specified to Intercomm may not be in host CPU communication mode at Intercomm startup. This precludes a terminal down condition when Intercomm is not able to transmit the sign-on prompt message. At first transmission from the terminal, Intercomm will respond with the prompt screen (if not an exempt terminal) as transaction requests are not honored until the user successfully signs on. This exit is not necessary for VTAM devices because the prompt message remains queued until the terminal logs on to Intercomm.

Standard register conventions are used. At entry, register 1 points to the five-character terminal-id for which the exit may request transmission of the prompt message via a zero return code in register 15, or suppress the prompt message via a non-zero value returned in register 15. The exit must save and restore the callers registers (except 15) and may not give up control. The exit should examine a local table of terminal-ids for which prompt messages should be suppressed. This suppression is only in effect at startup. Use the sign-off exit to subsequently suppress prompt messages (via internal flush command).

Appendix A

COMMANDS

The following list gives the ESS commands, the level of authority required to issue them, and the other attributes required to issue them. If the level of authority is given as GLOBAL, only accounts with the GLOBAL attribute can issue the command. If the level of authority is given as MANAGER, the MANAGER attribute is required, and to issue a command affecting an account, the MANAGER and account must have the same group name attribute. The GLOBAL attribute is required to issue the command affecting accounts in any group. If the level of authority is given as user, neither the GLOBAL nor the MANAGER attribute is required; the account need only have the attribute listed under "Other Attributes."

Command[$keyword]	Requirements	
	Level of Authority	Other Attributes
ADD	MANAGER	ADD
ATTACH	MANAGER	ATTACH and appropriate resource attribute
DELETE	MANAGER	DELETE
DETACH	MANAGER	DETACH
DISPLAY	MANAGER	DISPLAY
EDITNEWS	GLOBAL	EDITNEWS
EXCLUDE	GLOBAL	EXEMPT
FORCE	MANAGER	FORCE
INCLUDE	GLOBAL	EXEMPT
MODIFY$ACCOUNT	MANAGER	MODIFY and ACCOUNT
MODIFY$DEFAULTS	GLOBAL	MODIFY
MODIFY$MAXUSERS	GLOBAL	MODIFY and MAXUSERS

Command[$keyword]	Requirements	
	Level of Authority	Other Attributes
MODIFY$PASSWORD	MANAGER	MODIFY and PASSWORD
SEND	User	SEND
SIGNOFF	User	None
SIGNON	User	SIGNON

Appendix B

ATTRIBUTES

The following security attribute names are to be used to authorize or invoke the corresponding functions. To disallow the corresponding attribute, specify the attribute name preceded by NO (as, for example, NOACCOUNT) not including the variable argument, if any (as, for example, NOSTOP).

The column headed PREREQ indicates what attribute an account must have to add or modify the attribute indicated on another account. For example, for account X to modify account Y's EXEMPT attribute, account X must have the GLOBAL attribute. An asterisk indicates that the account must have the attribute itself. For example, for account X to give account Y the authority to attach facilities (via the ATTACH command), account X must itself have the ATTACH attribute. Most commands also require a MANAGER or GLOBAL authority level as described in Appendix A.

ATTRIBUTE	FUNCTION	PREREQ
ACCOUNT	Allows account commands: DISPLAY$ACCOUNT, MODIFY$ACCOUNT.	*
ADD	Allows ADD command.	*
ATTACH	Allows ATTACH command.	*
CONTROL	Allows DISPLAY$CONTROL command.	*
DELETE	Allows DELETE command.	*
DETACH	Allows DETACH command.	*
DISPLAY	Allows DISPLAY command.	*
EDITNEWS	Allows EDITNEWS command.	*
EXEMPT	Allows INCLUDE, EXCLUDE and DISPLAY$EXEMPT commands.	GLOBAL
EXPDT(yyddd)	Specifies Julian account expiration date.	MANAGER
FILES	Allows file name list functions for ATTACH, DETACH, and DISPLAY commands.	*

ATTRIBUTE	FUNCTION	PREREQ
FORCE	Allows FORCE command.	*
FUNC-INV	Inverts user function list. User functions attached to the account are prohibited. If no list is attached, all user functions are thus prohibited.	GLOBAL
FUNCTION	Allows user-function list functions.	*
GLOBAL	Allows group boundary crossings and certain system attribute assignments.	*
GROUP (groupname)	Specifies eight character group association name (low-order blank padding if necessary).	GLOBAL
INHIBMSG	Inhibits all ESS messages at sign-on, except error messages.	ACCOUNT
INTVL(hhmm)	Specifies sign-off interval due to terminal inactivity. If not specified, no time-out will be set (default is zero). Code in same format as START (see below) attribute.	MANAGER
LOCK(verb)	Specifies verb that terminal will be locked to following sign-on (user account requires SIGNON).	none
MANAGER	Allows functions within group boundaries.	GLOBAL
MAXUSERS	Allows MODIFY$MAXUSERS command.	*
MODIFY	Allows MODIFY command.	*
NOPSWD	Eliminates password requirement at sign-on.	PASSWORD
PASSWORD	Allows password change and MODIFY$PASSWORD.	*
PSWDEXP(nnn)	Specifies maximum number of sign-ons before the account is deactivated, unless the attribute PASSWORD is assigned to the account to allow a password change.	MANAGER
QUETO(hhcc)	Specifies the high/low subsystem codes in hexadecimal (00-FF) to receive message from sign-on; for menu processing.	none

ATTRIBUTE	FUNCTION	PREREQ
REGIONS	Allows Multiregion region list functions.	*
REGN-INV	Inverts Multiregion region list. Regions attached to the account are prohibited. If no list is attached, all regions are thus prohibited (if executing under MRS).	GLOBAL
SEENEWS	Allows account to receive ESS news message.	*
SEND	Allows inter-user messages (SEND command).	*
SIGNON	Allows account sign-on.	*
START(hhmm)	Specifies earliest session sign-on time in hours and minutes: 24 hour clock - an hours range from 00 (midnight) to 23 (11 pm), therefore a STOP time of 6:30 pm, for example must be specified as 1830 (12 plus 6 = 18).	MANAGER
STOP(hhmm)	Specifies latest valid session sign-on time, in same format as START.	MANAGER
SUBSYS	Allows subsystem list functions.	*
S/S-INV	Inverts subsystem list. Subsystems attached to the account are prohibited. If no list is attached, all secured subsystem accesses are thus prohibited.	GLOBAL
TERM-INV	Inverts terminal list. Terminals attached to the account are prohibited. If no list is attached, only exempt terminals may be used.	GLOBAL
TERMS	Allows terminal list functions.	*
USERS	Allows USERS subcommand of DISPLAY.	*
VERB-INV	Inverts verb list. Verbs attached to the account are prohibited. If no list is attached, all verbs but SECU are thus prohibited.	GLOBAL
VERBS	Allows verb list functions.	*

Appendix C

AUDIT TRAIL

An audit trail of the security environment is maintained on the Intercomm system log. Log entries are created using log code X'C9', and are fifty-nine bytes long, consisting of the Intercomm message header (forty-two bytes), the user ID (eight bytes), an eight byte data field, and a one-byte type code. All data fields are left-justified, low order binary zeros or blanks, as appropriate. If no data, the field contains binary zeros.

The type code is a one-byte hex code which determines the contents of the eight-byte data field in the log record, as follows:

Type	Meaning	Data
00	Successful SIGNON.	Terminal-ID
01	Successful SIGNOFF, or FORCEd off (see 0B).	Terminal-ID
02	Sign-on attempt at unauthorized terminal (terminal-id in MSGHTID).	---
03	Sign-on attempt failed due to invalid password.	---
04	Unauthorized security command issued or keyword used, or account not in manager's group. Unathorized password change attempt.	Command Keyword ---
05	Sign-on attempt after expiration date.	Expiration Date
06	Sign-on attempt before start time.	---
07	Sign-on attempt after stop time.	---
08	Sign-on attempted for inactive account.	---
09	Account deactivated due to 3 consecutive invalid passwords.	---

Type	Meaning	Data
0A	User session timeout; due to terminal inactivity or stop time exceeded.	Terminal-id
0B	FORCE command issued to cancel user session (usually followed by an 01 record).	Forced User-id
0C	Message failed subsystem security check.	Subsystem-ID
0D	Message failed region security check.	Region-ID
0E	Subsystem SELECT request failed file security check.	DD-name
0F	SECTEST returned non-zero code on user's logical function test.	Function-ID
10	Message failed verb security check.	Verb
11	SIGNOFF forced by new SIGNON at the same terminal.	Terminal-id

Appendix D

ERROR MESSAGES

ESS issues three classes of messages and codes. ESS routinely sends diagnostic and informative messages to terminal users as they issue various ESS commands as described below. More serious messages, listed in Messages and Codes, are sent to the control terminal operator. These messages indicate serious system problems, for example I/O errors on the security data set or a serious attempt to breach security. In the event of a serious problem, ESS abends the Intercomm region or regions (abends are listed in Messages and Codes).

All diagnostic and informative messages to the terminal user are preceded by the ESS heading line:

>----INTERCOMM EXTENDED SECURITY SYSTEM----<

For the IBM 3270 CRT prompt display screen, see the SIGNON command. The following message descriptions appear in alphabetical order.

Messages which are purely informative and do not indicate an error condition are indicated in this listing by a bullet. The bullet is not actually part of the message.

ACCOUNT DEACTIVATED, 3 PASSWORD FAILURES

Command: SIGNON

Cause: Three attempts to sign on with user-id and password have failed because of an incorrect password.

● ACCOUNT HAS BEEN DELETED

Command: DELETE

ACCOUNT DATE HAS EXPIRED

Command: SIGNON

Cause: An account's expiration date has been passed.

Action: Manager must MODIFY the EXPDT attribute of the issuing account.

ACCOUNT NOT AVAILABLE FOR SIGNON

Command: SIGNON

Cause: Account has been marked inactive due to 3 password failures, and/or has no SIGNON attribute.

Action: Manager must verify cause, and then if desired, account SIGNON attribute must be activated, or account can be deleted from the Security Data Set.

ACCOUNT SIGNED ON, DELETE REJECTED

Command: DELETE

Cause: An account cannot be deleted while signed on.

Action: Manager must FORCE account off, then retry command. Or wait and try DELETE later.

● ENTER ESS SIGNON

Command: SIGNOFF or SIGNON entered at a non-IBM 3270 terminal, or Intercomm started.

Cause: If SIGNOFF - processed successfully, whether or not user already signed off. If SIGNON - user-id missing.

Action: If SIGNOFF or startup - none or enter SIGNON command. If SIGNON - reenter command with correct user-id (and password, if required).

Note: For 3270 CRTs - see SIGNON command description.

ERROR - ICP INTEGRITY FAILURE

Command: SIGNOFF or SIGNON

Cause: Can occur when an active account times out, is forced off, or a second user enters SIGNON command at an active terminal (forcing first user off), or current user enters SIGNOFF command. SIGNOFF processing found that the terminal entry for this terminal is missing from the active (signed-on) terminal list in protected core due to simultaneous occurrance of 2 or more of the above, or due to a core clobber. Does not occur when user has signed off successfully.

Action: Ignore message if SIGNOFF entered, or reenter SECU$SIGNON.... command (terminal may not be locked to SECU). Because SIGNOFF is incomplete, a subsequent SIGNON may not be successful, or a premature time-out may occur. If problem continually reoccurs, close down Intercomm with a dump and submit an MSR. Include Intercomm log and console log for time period of command failures.

● FORCE HAS BEEN SCHEDULED

Command: FORCE

INVALID CHARACTERS IN NUMERIC FIELD

Command: ADD or MODIFY

Cause: A numerical quantity has been incorrectly specified in the INTVL, PSWDEXP, EXPDT, START or STOP attributes.

Action: Reissue correct command.

● LIST ELEMENT(S) ADDED

Command: EXCLUDE

● LIST ELEMENT(S) DELETED

Command: INCLUDE

MAXIMUM USERS SIGNED ON, TRY LATER

Command: SIGNON

Cause: The number of accounts permitted to be signed on at one time has been reached.

Action: Manager must try later, or MODIFY the count of MAXUSERS. At an IBM 3270 CRT, erasing the screen and entering SIGNON will restore the prompt display screen.

● MAXIMUM USERS UPDATED

Command: MODIFY$MAXUSERS

MESSAGE REJECTED, CANCEL PENDING

Command: All

Cause: At another terminal, a manager has issued the FORCE command, thus terminating the receiver's terminal session.

● MESSAGE TRANSMITTED

Command: SEND

● NEWS DATA HAS BEEN REPLACED

Command: EDITNEWS

PASSWORD IS EXPIRED, ENTER OLDPSWD,NEWPSWD

Command: SIGNON entered at a non-IBM 3270 CRT

Cause: The password has been used as many times as permitted or an initial password must be defined for a new/modified account.

Action: Reenter SIGNON with old-password$new-password to change the account password or with user-id$new-password to assign on initial password. The new password may not be the same as the old password, nor may it be the account's user-id (See SIGNON command). Or manager must MODIFY the account PSWDEXP attribute.

PASSWORD NOT VALID FOR USER-ID

Command: SIGNON entered at a non-IBM 3270 CRT.

Cause: Probable user syntax error, or password omitted and required.

Action: Reenter command with user-id and correctly spelled password.

● PASSWORD WILL BE REQUIRED FOR SIGNON - INITIAL PASSWORD IS USERID

Command: MODIFY$PASSWORD

PREVIOUS SESSION HAS BEEN TIMED OUT

See: USER SESSION HAS BEEN TIMED OUT

Note: Message appears only at the bottom of a 3270 sign-on screen.

REQUESTED ACCOUNT DOES NOT EXIST

Command: All (except SIGNON/OFF)

Cause: The account (user-id) does not exist on the Security Data Set.

Action: ADD the account to the Security Data Set and reissue the command or, if user-id was misspelled, reissue command using correct user-id.

REQUESTED ACCOUNT IS NOT SIGNED ON

Command: FORCE

Cause: The account (user-id) is not signed on.

Action: If user-id was misspelled, reissue corrected FORCE command.

REQUESTED FUNCTION IS NOT AUTHORIZED

Command: All

Cause: Issuing account did not own the appropriate attributes or did not own either the GLOBAL or the appropriate MANAGER attribute, or ADD or DELETE of an account was rejected by the user exit, or ADD was not possible because there is no room left in the in-core user list. In the latter case, the new account cannot be added until the next execution of Intercomm (see Section 3.5).

SECURITY FILE OUT OF SPACE

Command: ADD

Cause: The Security Data Set is full.

Action: Verify whether any existing accounts have expired and can be deleted. If not, recalculate Security Data Set space requirements and create an expanded Security Data Set according to instructions in Section 3.2. Close down Intercomm and restart with the new data set.

SIGNON TIME FOR ACCOUNT HAS PASSED

Command: SIGNON

Cause: Sign-on attempted after time of day specified in the account's STOP attribute.

Action: Account cannot proceed without having its STOP attribute changed via the MODIFY command.

SIGNON TIME FOR ACCOUNT NOT REACHED

Command: SIGNON

Cause: Sign-on attempted before time of day specified in the account's START attribute.

Action: Account cannot proceed without having its START attribute changed via the MODIFY command.

● SPECIFIED RESOURCE(S) HAVE BEEN ATTACHED

Command: ATTACH

• SPECIFIED RESOURCE(S) HAVE BEEN DETACHED

Command: DETACH

SYNTAX ERROR, REQUEST REJECTED

Command: All

Cause: Syntax error.

Action: Reissue command using the correct syntax.

TERMINAL NOT AUTHORIZED FOR USER-ID

Command: SIGNON

Cause: The account is not authorized to use the terminal.

Action: Move to an authorized terminal or ATTACH the terminal-id to the account's terminal list.

TRANSACTION 'vvvv' IS NOT AUTHORIZED FOR USER (uuuuuuuu)

Command: (Not a response to a command)

Where: vvvv is the verb associated with the input message, uuuuuuuu is the id of the user signed on at the terminal.

Cause: Entered verb, or verb to which terminal is locked, is not authorized for the specified user. Input message cancelled.

Action: Contact manager for authority to use the verb, or check proper verb used. Check user is signed on under correct id.

USER-ID IS CURRENTLY ACTIVE

Command: SIGNON

Cause: A second user attempted to sign on with a user-id already in use at another terminal.

Action: Wait for the first user to sign off, or sign on under another account. At an IBM 3270 CRT, erasing the screen and entering SIGNON will cause the prompt display screen to be restored.

USER-ID IS NOT AUTHORIZED

Command: SIGNON

Cause: The account (user-id) does not exist on the Security Data Set or was rejected for SIGNON by the user exit, or a required resource list is missing from the user's account.

Action: If user-id is misspelled, reissue the corrected SIGNON command. Otherwise, contact manager regarding invalid user-id (account name).

USER SESSION HAS BEEN TIMED OUT

Command: (Not a response to a command.)

Cause: The terminal has been inactive for the length of time specified in the INTVL attribute, and has been automatically signed off.

Action: Terminal user must sign on again in order to proceed.

---

xxxxxxxx yyyyyyyy NOT AUTHORIZED FOR USER (uuuuuuuu)

Where: xxxxxxxx is SUBSYSTEM or REGION-ID
yyyyyyyy is the associated subsystem code: hex/EBCDIC or region-id (CONTROL if control region).

Cause: A message queued for a subsystem did not pass ESS subsystem/region security tests.

Action: A manager can allow user to use the requested facility or should report the security infraction.

WARNING ACCOUNT ACTIVE - CHANGES EFFECTIVE AS OF NEXT SIGNON

Command: ATTACH, DETACH, MODIFY$ACCOUNT

WARNING REQUIRED LIST DETACHED - USER CANNOT SIGN ON

Command: DETACH

Action: A manager of the group to which the user belongs must attach a new list (of the resource type being detached) before the user can successfully sign on.

INDEX