ERI™

ERI/CICS for z/OS

User’s Manual 3.1

CICS-Lock
CICS-DupS
CICS-View
CICS-SSO

z/OS Version—February 5, 2017

Enterprise Research, Inc. • P.O. Box 9436 • Chapel Hill, North Carolina 27515 • (919) 444-2767
www.erisoft.com

Table of Contents

Preface v

General Information 1

Installation 7

System Administration 25

Preface

ERI/CICS is an integrated set of system enhancements designed for the manager of CICS systems. The CICS management tools in ERI/CICS deliver solutions to the increasing demands for security and productivity in large interactive systems. ERI/CICS includes an ERI/CICS Manager that provides system administration for product-control parameters. The ERI/CICS Manager also simplifies the installation, verification, and support of all of the tools.

Who Is This Book For?

The ERI/CICS User's Manual is designed to be used by CICS system managers. The book provides information about installing, configuring, and using four components in the ERI/CICS product line:

- CICS-Lock, a user-friendly alternative to CICS terminal time-out
- CICS-DupS, a flexible control that prevents the abuse of shared userids and allows swapping between CICS applications from a single terminal session
- CICS-View, a session status monitoring tool that presents summary data about active CICS users and includes powerful Help Desk features
- CICS-SSO, a secure menu facility that delivers single sign-on access to any CICS application on any z/OS image

How This Book Is Organized

This book is organized as follows:

❏ Chapter 1—*General Information*—provides a high-level look at the ERI/CICS tools.

❏ Chapter 2—*Installation*—presents recommendations and requirements for installation, an installation overview, step-by-step installation and activation procedures, and initialization and termination information.

❏ Chapter 3—*System Administration*—explains how to perform system administration for the ERI/CICS Manager and its tools, CICS-Lock, CICS-DupS, and CICS-SSO.

❏ Chapter 4—*Using* ERI/CICS—provides operation information for the CICS-Lock, CICS-DupS, and CICS-View tools.

❏ Chapter 5—*Customizing* ERI/CICS *with User Exits and User Tables*—describes the ERI/CICS user exit points and user table references, and explains how to implement them.

❏ Appendix A—ERI/CICS *Messages*—documents the ERI/CICS messages.

Chapter 1
General Information

This chapter provides a high-level look at the ERI/CICS management and security tools for CICS.

Product Overview

ERI/CICS is an integrated set of system enhancements designed for the CICS system manager.

In addition to the ERI/CICS Manager, ERI/CICS currently supports four tools (Figure 1):

❑ CICS-Lock, a user-friendly alternative to CICS terminal time-out

❑ CICS-DupS, which allows you to control the number of concurrent sessions a user can establish and allows swapping between CICS applications from a single terminal session

❑ CICS-View, a session status monitoring tool that presents summary data about active CICS users and includes powerful Help Desk features

❑ CICS-SSO, a secure menu facility that delivers single sign-on access to any CICS application on any z/OS image.

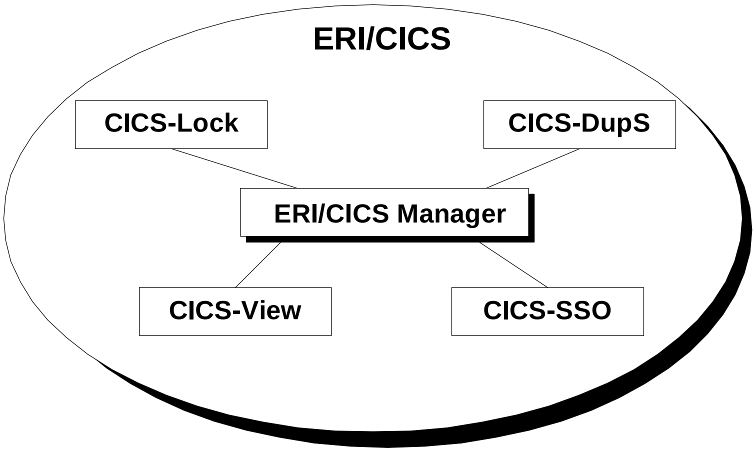


Figure 1   Tools for CICS

CICS-Lock is a user-friendly alternative to CICS terminal time-out. This tool enhances terminal security while providing CICS users with the convenience of extended connect time. CICS-Lock ensures privacy of data even while a CICS session is left unattended.

You can invoke CICS-Lock either by request or automatically after an installation-defined interval expires. CICS-Lock replaces the user's screen with a locked notification message that includes a password validation prompt. After password validation, your CICS session, terminal data, next Tranid, and COMMAREA are restored as if the interrupt did not occur.

The controls and exclusions for CICS-Lock can be updated dynamically by the CICS-Lock Manager. Lock and disconnect intervals can range from 0-999 minutes, where 0 denotes no locking or disconnects. CICS-Lock supports three exit points:

- ❑ The Password Verification Exit (ERIXPWP0), which enables you to write your own routine for verifying user passwords.
- ❑ The Lock Parameter Exit (LCKPRMP0), which enables you to customize lock and disconnect interval processing at the individual user level.
- ❑ The Transaction Time-out Table (LCKTRNTB), which enables you to customize lock and disconnect interval processing by transaction id.

CICS-DupS provides two facilities. The first controls the number of concurrent CICS sessions a single userid is permitted. The limit can range from 0-99, where 0 allows unlimited access. This Session Control facility supports exclusion by CICS userid. More precise control of user access is provided by a multi-session mask feature that can restrict sign-on based on termid or VTAM LU-name. The controls and exclusions for the Session Control facility can be updated dynamically by the CICS-DupS Manager.

The second CICS-DupS facility provides users with concurrent access to two applications from a single terminal session. This "swapping" facility enables users to seamlessly switch between two terminal screens or windows. The CICS-DupS Swap facility increases CICS functionality and user productivity by eliminating the need to attach and sign-on to a second VTAM session when accessing two applications at one time from the same CICS Terminal Owning Region (TOR).

Note: Before implementing the Swap facility of CICS-DupS, refer to *Product Restrictions* on page 7.

CICS-View is an easy-to-use session monitoring tool that presents summary data about active CICS users. Designed for System Administrators and Help Desk staff, CICS-View presents data in user activity tables. Built-in features let you select data using generic searches, cancel user sessions, view user terminal screens, or send non-destructive broadcast messages to one or more users.

CICS-SSO simplifies the transfer of an active CICS session among applications. With CICS-SSO in place, a user logs into any CICS application as he or she would normally. But there's no need to enter subsequent ID/password combinations to CICS applications. Users select applications from a CICS-SSO menu of pre-authorized applications. Applications can be local to the current CICS TOR, or remote in another CICS TOR.

Major Components of ERI/CICS

ERI/CICS includes a set of four system administration managers to simplify the installation, activation, and verification of ERI/CICS.

- ❑ The ERI/CICS Manager supports system administration controls common to all tools (CICS-Lock, CICS-DupS, CICS-View, and CICS-SSO).
- ❑ The CICS-Lock Manager supports system administration controls for CICS-Lock.
- ❑ The CICS-DupS Manager supports system administration controls for CICS-DupS.
- ❑ The CICS-SSO Manager supports system administration controls for CICS-SSO.

The managers are menu driven and support dynamic updates to product-related controls. Access is available to the ERI/CICS Help Facility from any manager panel.

The following major components of ERI/CICS are shared by all tools.

- ❑ **ERI/CICS Subtask and SVC**

  During product initialization, ERI/CICS attaches an z/OS subtask to support communications with the ERI/CICS SVC. The SVC supports ERI/CICS tools by performing authorized external security manager functions.

- ❑ **ERI/CICS Control File**

  ERI/CICS includes a VSAM KSDS file that stores product parameters required during product initialization. These control parameters may be customized by using the ERI/CICS Managers.

- ❑ **ERI/CICS Event Recorder**

  The Event Recorder logs CICS task activity for each CICS user initialized to the product. CICS/z/OS users are initialized to ERI/CICS only after CICS sign-on. Or, initialization occurs with the first terminal task.

  The Event Recorder does not require local customization to sign-on facilities and is completely transparent to the end user. The Event Recorder is event driven and is required to support all ERI/CICS tools.

- ❑ **User Index**

  At the core of ERI/CICS is an index of information about CICS user sessions. The ERI/CICS tool suite is a set of applications that process the user index. The Event Recorder, the data collection component of ERI/CICS, uses standard exit points to record information about user sessions. This information includes signon and signoff events, task initiation and termination, and internal response times. The user index is maintained in memory to optimize access times.

❑ **ERI/CICS Interval Monitor**

The Interval Monitor analyzes data collected by the Event Recorder and performs ERI/CICS storage management. The monitor tracks inactive intervals and performs automatic lock and disconnect processing. This is an interval-driven process that is required to support all ERI/CICS tools.

Following are major components of CICS-Lock.

❑ **CICS-Lock Hot Key and Recognition Character**

CICS-Lock supports an installation-defined function key to invoke terminal Lock processing. This feature provides easy access for user-requested terminal Lock.

If there is contention for a function key, users can assign an optional Recognition Character to use in conjunction with the function key.

Hot key assignment is per CICS Terminal Owning Region (TOR) and can be updated dynamically by the CICS-Lock Manager.

❑ **CICS-Lock Exclusions**

Exclusion from CICS-Lock is supported in several ways; by VTAM LU name, CICS Terminal ID, CICS userid, and CICS Transaction ID. Exclusion entries may contain generic characters and are added or deleted dynamically by the CICS-Lock Manager.

Following are major components of CICS-DupS.

❑ **CICS-DupS Swap Facility Hot Key and Recognition Character**

The CICS-DupS Swap facility supports an installation-defined function key to detect a swap request.

If there is contention for a function key, users can assign an optional Recognition Character to use in conjunction with the function key.

Hot key and Recognition Character assignments are per CICS TOR and can be updated dynamically with the CICS-DupS Manager.

❑ **CICS-DupS Exclusions**

Exclusion from CICS-DupS is supported by userid. Exclusion entries may contain generic characters and are added or deleted dynamically by the CICS-DupS Manager.

Following are major components of CICS-SSO.

❑ **The CICS-SSO Menu Facility**

The CICS-SSO tool includes a customizable application menu facility designed to simplify the transfer of an active CICS sessions among applications. The menu facility supports up to 45 applications per menu with optional sub-menus. Each menu item can be secured using your external security manager.

- **The CICS-SSO Auto-Menu Option**

  This option allows the administrator to prevent end-users from being presented with a blank CICS screen.

- **The CICS-SSO Pass Ticket**

  The Pass ticket option builds a one-time-only encrypted password, which removes the need to prompt an end-user for their real password when passing from one CICS TOR to another.

- **ERI/CICS User Exits and User Tables**

  ERI/CICS contains user exit points and user tables that you can use to customize the product. At the exit points, ERI/CICS issues CICS Link commands to modules that you can replace with your own programs.

  In the current release of ERI/CICS, there are six user exit points:

  - The Password Verification Exit (ERIXPWP0), which enables you to write your own routine for verifying user passwords.
  - The Lock Parameter Exit (LCKPRMP0), which enables you to customize lock and disconnect interval processing at the individual user level.
  - The custom Sign-off Exit (ERICSFPO), which enables you to customize sign off procedures.
  - The custom Sign-on Exit (ERICSNPO), which supports custom sign-on procedures.
  - CICS-SSO Session Pass Exit (ERIPASPO), which enables you to dynamically change CICS-SSO pass parameters or customize access to an application.
  - The CICS-DupS User Temporary Storage (TS) Exit (ERIUTSPO), which enables you to pass a list of application TS queue names to the CICS-DupS Swap facility. The list of queues will be included in the back-up and recovery process.

  At the table reference points, ERI/CICS issues CICS Load commands for modules that you can generate with values unique to your installation. In the current release of ERI/CICS, there are two user tables.

  - The Transaction Time-out Table (LCKTRNTB), which enables you to customize lock and disconnect interval processing by transaction id.
  - The Session Limit Table (ERIDUPTB), which enables you to customize CICS-DupS session limits by userid.

End of Chapter 1

Chapter 2
Installation

This chapter shows you how to install and customize the ERI/CICS Manager and the CICS-Lock, CICS-DupS, CICS-View, and CICS-SSO tools.

Before You Start

The following sections contain important information that you should be aware of before you start the installation process.

Software Requirements

ERI/CICS operates with the following system software:

- ❑ z/OS
- ❑ RACF 1.8 or higher (or SAF compatible security manager)
- ❑ CICS (Version 3, 4 and 5)

CICS must provide the following features and functions:

- ❑ Basic Mapping Support (BMS)
- ❑ Automatic Transaction Initiation (ATI)

MRO Support

ERI/CICS fully supports MRO. Install ERI/CICS only in the Terminal Owning Region (TOR).

Product Restrictions

This release of ERI/CICS contains the following restrictions. Contact ERI if the restrictions are a problem for you.

- ❑ ERI/CICS monitors terminal activity for a maximum of 7,500 active sessions per TOR.
- ❑ CICS-Lock does not schedule lock processing for any conversational tasks.
- ❑ CICS-Lock does not schedule lock processing at devices where BMS paging is active.
- ❑ The Swap facility of CICS-DupS might not support swapping between two screens when the same application is executing. This limitation arises when the application uses the CICS terminal ID to assign

Temporary Storage Queids. The limitation occurs because both screens use the same terminal ID. If you plan to implement the swap facility, please contact ERI for the current information on this restriction.

Security Recommendations

CICS Transaction Definitions

❑ Define all transactions to CICS with external security YES. Transaction LCKU is started by CICS-DupS after detecting that the CICS-DupS Session Limit has been exceeded. In this situation, the user is signed off of CICS. Transaction ERIG preempts your good-morning message transaction to perform single sign-on processing. In this situation, the user is not yet signed on to CICS.

Transaction Security Recommendations

❑ The following transactions reference ERI/CICS programs that enable required user functions. Define them to your external security manager with Universal Access READ.

ERIA
ERIB
ERIG
ERIS
ERIU
ERIX
ERIY
ERIZ
ERI5
EMSA
EMSG
EMSP
LCKA
LCKP
LCKU
LOCK

❑ The following transactions reference the manager programs and should be available only to those who will install and maintain the software. Define them to your external security manager with Universal Access NONE and permit access only as needed.

ERID
ERII
ERIM
ERSM
LCKM

- The following transaction references the CICS-Lock Interval Monitor and is invoked by CICS interval control. Define it to your external security manager with Universal Access NONE. Permit access to the CICS job userid and users who are authorized for transaction ERII.

  LCKS

- The following transactions reference the CICS-View program and should be available only to those who use CICS-View. Several transactions are supplied to provide flexibility in controlling access to CICS-View line commands. Define them to your external security manager with Universal Access NONE and permit access only as needed.

ERBC	Permits access to the CICS-View broadcast facility's command interface.
ERIV	Permits access to all CICS-View line commands.
ERVB	Permits access to the CICS-View broadcast facility.
VIEW	Does not permit access to CICS-View line commands.
VMSG	Permits access to the CICS-View Message command only.
VVUE	Permits access to the CICS-View View command only.

Distribution Library

Your distribution library contains the following products:

❏ ERI/CICS	The operating system interface support manager
❏ CICS-Lock	The user-friendly alternative to CICS terminal time-out
❏ CICS-DupS	The facility to limit concurrent sessions per userid and the facility to swap between applications
❏ CICS-View	The CICS session status monitor.
❏ CICS-SSO	The Single Sign-On option for CICS.

The distribution files are download from the ERI website, please see instructions under the "Suppot" tab.

Table 2-1 Contents of the ERI/CICS download directory

File	DSName	Created By	DSName on Disk	Attributes on Disk[1]	Contents
1	FILE01	IEBCOPY	ERI.INSTLIB		JCL for installation
2	FILE02	IEBCOPY	ERI.COPYLIB	80 x 6160 FB	CICS table macros
3	FILE03	IEBCOPY	ERI.CICS.LOADLIB	SYS1.LINKLIB	ERI/CICS load library (Version 5)
4	FILE04	IEBCOPY	ERI.CICS.LOADLIB.bkup	SYS1.LINKLIB	ERI/CICS load library (Version 3 or 4)
5	FILE05	IEBGENER	ERI.ERIINIT	1000 x 6160 VB	Initialization data for ERICNTL

[1] Adjust attributes to your requirements and standards.

Password Initialization

Access to ERI/CICS is controlled via a calendar-oriented password that is based on your CPU serial number. If you don't know your serial number, you can get it from the ERI/CICS Manager provided with the product. When you first enter the ERI/CICS Manager, the message "ERI1912E Invalid Password" is displayed. Contact your ERI sales representative to obtain the password. During the initial trial period, passwords are issued by your sales representative. After obtaining a license to use ERI/CICS, a password is issued for the duration of the license agreement. Thereafter, only a change in CPU requires a new password.

ERI/CICS Initialization and Termination

The ERI/CICS tools and utilities share product components. These components must be ENABLED during product initialization before any of the tools can be used.

Initialization can be automated or performed manually. A PLTPI program is provided to implement automated initialization. This initialization program uses parameters saved in the ERI/CICS control file to ENABLE ERI/CICS components. We recommend using the PLTPI program for normal operation.

If you do not use the PLTPI program, you can initialize ERI/CICS manually from the ERI/CICS Managers. Alternatively, you can execute transaction ERII to manually invoke the initialization program.

A program to terminate ERI/CICS is provided, and we recommend that you add the termination program to PLTSD. One function of the termination program is to detach the ERI/CICS subtask. If CICS is shutdown without detaching the subtask, a system abend SA03 occurs. Note that PLTSD programs are not executed if an IMMEDIATE shutdown of CICS is requested. In this situation, you should issue the termination transaction, ERID, prior to shutdown.

After executing transaction ERID, ERI/CICS can be re-initialized using transaction ERII or the ERI/CICS managers. When re-initializing, all session data previously recorded by the ERI/CICS components is lost.

Figure 2 shows the relationship of the ERI/CICS components and their dependencies.

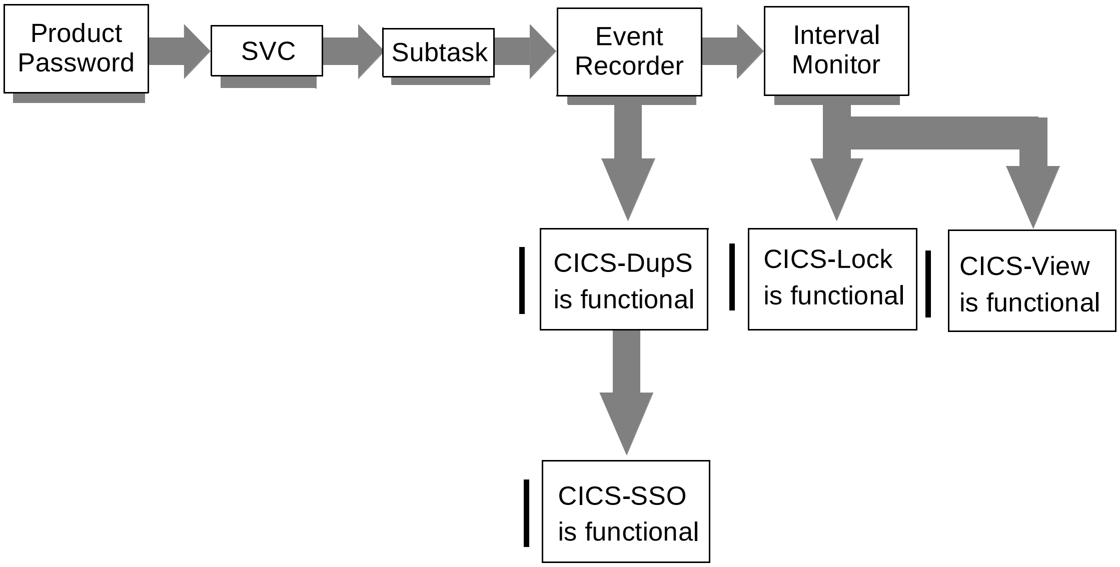


Figure 2 ERI/CICS Components and Their Dependencies

ERI/CICS Start of Day Processing

The ERI/CICS Interval Monitor performs Start of Day Processing the first time that the Interval Monitor is executed after 2400 hours. Message LCK1020I is written to the ERI/CICS log. The message includes the peak active user count and the time that the peak occurred for the previous day. The peak user count is then reset to the current user count.

Default Values

The first time ERI/CICS is initialized, the default values shown below are assigned. Follow the customization steps later in this chapter to tailor ERI/CICS control parameters to meet your installation requirements.

```
ERI/CICS Controls           Status
Subtask                     DISABLED
SVC #                       (Required)
CPU-id                      (Required)
Password                    (Required)
EXTDS Support               ENABLED
Language                    ENGLISH
Event Recorder              DISABLED
Interval Monitor            DISABLED
Monitor Interval            1   min.

CICS-Lock Controls          Status
Lock Hot Key                (Optional)
Hot Key Recognition Char    (Optional)
Lock Interval               015 min.
Disconnect Interval         120 min.
Disconnect Request          LOGOFF

CICS-DupS Controls
Session Limit               0 (Note: 0 indicates unlimited use)
Signon Tranid               CSGM
Session Take-Over           ENABLED
Swap Hot Key                (Optional)
Hot Key Recognition Char    (Optional)
Hot Key Initial Tranid      (Optional)
Termid Mask                 (Optional)
VTAM LU-name Mask           (Optional)

CICS-SSO Controls
CICS-SSO                    DISABLED
Automatic Menu              DISABLED
Hot Key                     (Optional)
Hot Key Recognition Char    (Optional)
PassTicket Generation       NO
```

Here is an overview of the installation and customization steps, with references to the pages where the steps are described in more detail.

❑ **Unload distribution libraries from ERI website)**

Use your standard installation block sizes.

❑ **Update CSD and CICS tables for CICS (Version 3, 4 or 5) (page 15)**

INSTLIB member DEFCSD contains the steps to add ERI / CICS file, transaction, and program definitions to the CSD. COPYLIB members ERIDCT, ERIPLTPI, and ERIPLTSD contain the necessary table entries.

❑ **Update SIT Override Parameters (page 16)**

❑ **Remove Terminal User TIMEOUT Value (page 16)**

❑ **Update CICS JCL (page 16)**

Concatenate your load library to the DFHRPL list.

❑ **Define and initialize ERI/CICS Control File (page 16)**

INSTLIB member DEFCNTL contains the necessary steps.

❑ **Install ERI/CICS SVC (page 16)**

INSTLIB member INSTSVC contains the necessary step.

❑ **Install ERI/CICS node error program (ERIZNEP) (page 17)**

This step is optional and is recommended for customers who plan to implement CICS-SSO passing between multiple CICS address spaces.

❑ **Install ERI/CICS SAF Router Exit (ICHRTX00) (page 17)**

This step is only required if you intend to use ERI pass tickets.

❑ **Install RACF Secured Signon Function (RACF 1.9.2 or higher) (page 17)**

This step is only required if you intend to use RACF pass tickets.

After these installation steps are complete, restart CICS and activate and verify the ERI / CICS components.

❑ **Activate ERI/CICS controls (page 19)**

Review and update the ERI / CICS controls as required by your installation.

❑ **Verify ERI/CICS controls with CICS-View (page 20)**

Perform basic on-line verification test.

❑ **Activate CICS-Lock (page 20)**

Review and update the CICS-Lock Manager controls as required by your installation.

□ **Verify CICS-Lock (page 21)**

Perform basic on-line verification test.

□ **Activate CICS-DupS (page 21)**

Review and update the CICS-DupS controls as required by your installation.

□ **Verify CICS-DupS (page 22)**

Perform basic on-line verification test.

□ **Activate CICS-SSO (page 22)**

Review and update the CICS-SSO controls as required by your installation.

□ **Verify CICS-SSO (page 22)**

Perform basic on-line verification test.

Installing the ERI/CICS Software

Step 1 Upload Distribution Libraries - see ERI website for instructions

The distribution directory contains several libraries:

`INSTLIB`	Sample JCL for installation jobs
`COPYLIB`	CICS table-definition copybooks
`CICS.LOADLIB`	ERI/CICS object modules for CICS
`ERIINIT`	Initialization data for ERICNTL

Step 2 Update CICS Tables for CICS/MVS (Version 2)

Note: Support for CICS Version 2 is dropped. please go to step 3.

Step 3 Update CSD and CICS Tables for CICS (Version 3, 4 or 5)

A job to define the ERI/CICS transactions, programs, and control file is provided in ERI.INSTLIB. Table definition macros are included in ERI.COPYLIB as ERI*xxx*, where *xxx* is a CICS table name. Note to MRO users: these changes are required only in the TOR.

Step 3a Review and run job DEFCSD in your ERI.INSTLIB to update your CSD with group ERICICS.

Step 3b Append group ERICICS to the list specified in the GRPLIST system initialization parameter.

Step 3c Add a DD statement defining ERI.COPYLIB to the assembly SYSLIB in DFHAUPLK or your customized assembly PROC.

Step 3d — Add the following statement to your CICS tables for each of the copybooks:

```
COPY  ERIxxx
```

Step 3e — Assemble the updated tables:

Assemble DCT
Assemble PLTPI (initialization)
Assemble PLTSD (termination)

Note: The PLTSD program terminates the ERI/CICS subtask at CICS shutdown. PLTSD programs are not executed if an IMMEDIATE shutdown of CICS is required. If CICS terminates without executing the program, a system abend SA03 occurs. The ERID transaction is intended for use prior to a CICS shutdown. Once the subtask has been detached, no functions that use it, including password validation, can complete.

Step 4 Update SIT Override Parameters

Automated ERI/CICS operation requires PLTPI and PLTSD entries. We recommend that you specify these table names as override parameters.
CICS-SSO requires the following parameters to pass sessions from one TOR to another: CLSDSTP=NOTIFY and LGNMSG=YES.

Note: For ACF2 users, the ACF2 DEFAULT TERMINAL logonid must match the SIT parameter DFLTUSER.

Step 5 Remove CICS Terminal User TIMEOUT Value.

Since CICS-Lock is a replacement for CICS terminal time-out, we recommend that you remove the TIMEOUT parameter from user definitions. Depending on your CICS release, TIMEOUT is specified in either DFHSNT or the CICS segment of a RACF user profile.

Step 6 Update CICS JCL

Add a DD statement concatenating the ERI/CICS load library to the CICS DFHRPL.

Step 7 Define and Initialize ERI/CICS Control File

Review and run job DEFCNTL in your ERI.INSTLIB to define and initialize the ERI/CICS Control VSAM dataset.

Step 8 Install ERI/CICS SVC

The z/OS system programmer assigns an SVC number and associated LPA library member name for the ERI/CICS SVC. You may continue the installation procedure before this step is complete.

Step 8a — Review and run job INSTSVC in your ERI.INSTLIB to link the ERI/CICS SVC into SYS1.LPALIB as a type 3 or 4 SVC.

Step 8b — Perform an IPL with CLPA to activate the ERI SVC after running INSTSVC.

Step 9 Install ERI/CICS node error program (ERIZNEP)

Note: This step is optional and is recommended for customers who plan to implement CICS-SSO passing between multiple CICS address spaces.

If you have customized your own DFHZNEP, go to Step 9c.

Step 9a Rename DFHZNEP as DFHZNEP$ in your.SDFHLOAD

Step 9b Copy ERIZNEP to your.SDFHLOAD as DFHZNEP.

Step 9c Sample code for modifying your DFHZNEP is included in ERI.COPYLIB as ZNEPESA and ZNEPXA. Review these members for installation instructions.

Step 10 Update SYS1.VTAMLST

Update the CICS VTAM APPL definitions in SYS1.VTAMLST to include PASS in the AUTH parameters. This is required for the ISSUE PASS command CICS-SSO uses to transfer a session from one VTAM to applid to another.

Step 11 Install ERI/CICS SAF Router Exit (ICHRTX00)

Note: This step is only required if you intend to use ERI pass tickets.

Review and run job INSTRTX in your INSTLIB to link the ERI / CICS SAF Router Exit (ICHRTX00) into SYS1.LPALIB. Please confirm with your z/OS System Programmer that you are not currently using exit ICHRTX00.

Note: Contact ERI if you are already using exit ICHRTX00.

Step 12 Installing RACF Secured Signon Function (RACF 1.9.2 or higher)

Note: This step is only required if you intend to use RACF pass tickets.

Step 12a Activate RACF PassTicket classes.

Before you can use the Secured Signon Function of RACF, you must activate the PTKTDATA class. To activate the class and the function, enter:

```
SETROPTS CLASSACT(PTKTDATA)

SETROPTS RACLIST(PTKTDATA)
```

Step 12b

Define Profiles in the PTKTDATA class.

For each VTAM Applid that users are permitted to access with a PassTicket, you must create a profile in the PTKTDATA class. To define the profile use the RDEFINE command:

```
RDEFINE  PTKTDATA profile_name
         SSIGNON(key_description)
         UACC(access_authority)
```

Where

❑ *profile_name* is the CICS VTAM Applid.

❑ *key_description* defines the application key and the key protection method.

❑ *access_authority* is the UACC associated with the resource protected by this profile.

Example

In the following example the VTAM Applid of the CICS region is CICS410P; the Secured Signon application key is masked in the RACF database; the key value is X'C3C9C3E2F4F1F0D7'; universal access is the default, NONE.

```
RDEFINE  PTKDATA CICS410P
         SSIGNON(KEYMASKED(C3C9C3E2F4F1F0D7))
```

Note: Details for defining profiles in class PTKTDATA are provided in the *RACF Security Administrator's Guide*, "Using the Secured Signon Function."

Step 12c

After you define the profiles, you need to refresh the class by entering:

```
SETROPTS RACLIST(PTKTDATA) REFRESH
```

Activating ERI/CICS

Use the following steps to activate ERI/CICS and verify that the major components are functioning. These steps will introduce you to the basic product controls that adapt ERI/CICS to your installation requirements. Detailed information about all product controls is in the next chapter, “System Administration.”

Step 1 Restart CICS with ERI/CICS defined.

Restart CICS with updated JCL, table definitions, and SIT override parameters. During start-up the ERI/CICS PLTPI program writes messages to the system log and to the DCT definition you selected for “ERIL.” The first time you bring up ERI/CICS, expect the following messages:

```
ERI4092E CICS-Lock Initialization error; no valid password found

LCK8020E mm/dd/yy hh:mm:ss CICS-Lock initialization error - No
valid password found
```

Once you have activated the ERI/CICS controls, you get these messages:

```
LCK1012I mm/dd/yy hh:mm:ss ERI/CICS Event Recorder
initialization successful

LCK1013I mm/dd/yy hh:mm:ss ERI/CICS Interval Monitor
initialization successful
```

Step 2 Activate ERI/CICS Controls

Step 2a Access the ERI/CICS Manager.

Step 2b Execute transaction ERIM. Select Tool Managers (option 1) from the System Administration panel. Select ERI/CICS (option 1) from the Tool Managers window.

Step 2c Enter your ERI/CICS product password.

The first time you access the ERI/CICS manager, you must enter your CPU-id and associated password. Your CPU-id is displayed in “Installation Verification” data. ERI provides your product password.

Step 2d Update “Current Status” and “Next Run” controls to support your installation requirements.

- □ Enable the ERI subtask.
- □ Set the ERI SVC number to the value assigned by your z/OS systems programmer.
- □ Disable extended data streaming (EXTDS) support, if desired.
- □ Set the preferred Language: ENG (Alternative English), ENU (English), or DEU (German). Only end-user screens are translated.
- □ Enable the Event Recorder to start user tracking.
- □ Enable the Interval Monitor to activate automated procedures.

- □ Set Monitor Interval. The default value, 1 minute, is appropriate in almost all cases.
- □ Set Temporary Storage to either Main or Aux. This setting determines the location of Temp Storage records that ERI/CICS uses to preserve the user’s environment prior to replacing a screen.

Step 2e Review Installation Verification data for obvious errors.

Step 3 Verify ERI/CICS Controls with CICS-View

Step 3a Execute transaction ERIM. Select CICS-View (option 2) from the System Administration panel.

Step 3b Review the table of user sessions monitored by ERI/CICS.

- □ There is a line of status information for each session ERI/CICS is tracking. Verify that your terminal is in the list, “ERIM” is the Last Tran value for your terminal, and “ACT” (active) is the Term Stat value.
- □ Make a note of the Total Tran value, then press the enter key. Verify that the Total Tran value is incremented by 1, ”ERIV“ is the Last Tran value, and “ACT“ is the Term Stat value.
- □ Review the “User Count,” “Lock Count,” and “Peak User Count” fields at the bottom of the screen for obvious errors.

Step 4 Activate CICS-Lock

Step 4a Access the CICS-Lock Manager.

Step 4b Execute transaction ERIM. Select Tool Managers (option 1) from the System Administration panel. Select CICS-Lock (option 2) from the Tool Managers window.

Step 4c Update “Current Status” and “Next Run” controls to support your installation requirements.

- □ Optionally, assign a Lock Hot Key. If you specify a hot key, a user can initiate lock by pressing that key.
- □ Optionally, assign a hot key Recognition Character. If you specify a recognition character, that character must be in the first position of a screen input field to initiate a lock with the hot key.
- □ Set the Lock Interval to the required value (expressed in minutes). This is the inactivity interval after which CICS-Lock will lock the terminal and prompt the user for their password.
- □ Set the Disconnect Interval to the required value (expressed in minutes). This is the inactivity interval after which CICS-Lock will disconnect the terminal.
- □ Set the Disconnect Request to either LOGoff or SIGnoff. If you specify logoff, ERI/CICS sets the terminal status to RELEASED. If you specify signoff, ERI/CICS initiates the signoff transaction: CESF.

Step 5 Verify CICS-Lock

Step 5a Verify the LOCK transaction.

Exit from the ERI/CICS Managers and execute transaction LOCK. CICS-Lock prompts you for your password. When you enter your password correctly, CICS-Lock restores your screen.

Step 5b Verify the lock hot key function.

If you did not specify a lock hot key, skip this step and continue with Step 5c.

Execute transaction ERIM. If you specified a hot key recognition character, enter that character in the first position of an input field. Press the hot key you selected. CICS-Lock prompts you for your password. When you enter your password correctly, CICS-Lock restores your screen.

Step 5c Verify CICS-Lock user counts.

Return to the CICS-Lock Controls panel and review the “Installation Verification” data at the bottom of the screen. Current User Count is the number of terminals ERI/CICS is tracking, and Current Lock Count is the number of terminals locked by CICS-Lock. These values are updated when you refresh the screen.

Step 6 Activate CICS-DupS

Step 6a Access the CICS-DupS Manager.

Step 6b Execute transaction ERIM. Select Tool Managers (option 1) from the System Administration panel. Select CICS-DupS (option 3) from the Tool Managers window.

Step 6c Update “Current Status” and “Next CICS Run” controls to support your installation requirements.

- ❑ Update Session Limit. This value represents the number of concurrent sessions a user may establish in this CICS TOR.
- ❑ Update Sign-on Tranid. Specify the transaction you want CICS-DupS to start when a user requests Return to Signon after exceeding the Session Limit. CESN is the default.
- ❑ Optionally, disable Session Take-Over. When enabled, Session Takeover provides a means of continuing signon to a new session by canceling the user’s active session.
- ❑ Optionally, assign a Swap Hot Key. Assigning a Swap Hot Key enables the Swap facility, a feature that provides two concurrent logical sessions from one device. Read “Product Restrictions” starting on page 7 before implementing the Swap facility.
- ❑ Optionally, assign a hot key Recognition Character. If you specify a recognition character, that character must be in the first position of a screen input field to invoke the Swap facility.

❑ Optionally, assign a hot key Initial Tranid. This value identifies a transaction that CICS-DupS will start when a user requests swap. If you do not specify a tranid, a default screen that prompts the user for a tranid is presented.

Step 7 Verify CICS-DupS

Step 7a From the CICS-DupS Manager, set the Current Run value for Session Limit to "1." Remember to enter UPDATE on the command line and press Enter.

Step 7b Using the same userid, sign-on at another terminal. CICS-DupS detects that your userid is in use and prompts you for further action. Choose "Return to CICS."

Step 7c Return to your original terminal session. If you implemented the Swap facility, press your swap hot key to open a second screen for that terminal. Swap between screens using the hot key.

Step 8 Activate CICS-SSO

Step 8a Access the CICS-SSO Manager.

Step 8b Execute transaction ERIM. Select Tool Managers (option 1) from the System Administration panel. Select CICS-SSO (option 4) from the Tool Managers window.

Step 8c Update "Current Status" and "Next CICS Run" controls to support your installation requirements.

❑ Enable CICS-SSO to activate CICS-SSO processing.

❑ Enable Automatic Menu. After verifying CICS-SSO processing, return to this panel and disable automatic menu, if desired.

❑ Optionally, assign a Menu Hot Key. If you specify a hot key, a user can display the menu by pressing that key.

❑ Optionally, assign a hot key Recognition Character. If you specify a Recognition Character, that character must be in the first position of a screen input field to invoke the menu with the hot key.

❑ Set PassTicket Generation as required by your installation. PassTickets are used to implicitly authenticate the user when CICS-SSO passes a session from one VTAM Applid to another. Values are ESM, ERI, or NO. Specify "ESM" (External Security Manager) to use RACF PassTickets or "ERI" to use ERI/CICS PassTickets. Specify "No" to require password verification when a session is passed.

Note: Both ESM and ERI PassTickets require additional system components; see "PassTicket Generation" on page 43 for more information.

Step 9 Verify CICS-SSO Menu Processing.

Step 9a Press PF3 to return to the tool managers window; press PF12 to return to the ERI/CICS system administration panel; then press PF3 to end. The automatic menu function of CICS-SSO displays the sample application menu. From the menu, enter “S” beside application CICS-View. CICS-SSO invokes CICS-View, which presents the user session display.

Step 9b Verify the menu hot key function.

If you did not define a CICS-SSO menu hot key, skip this step.

From the main menu, enter “S” beside application ERI / CICS: Tool Managers. The ERI / CICS System Administration screen is presented. If you specified a menu hot key recognition character, place that character in the first byte of an input field. Now press your designated hot key. CICS-SSO returns you to the main menu.

End of Chapter 2

Chapter 3
System Administration

This chapter explains how to perform system administration for the ERI/CICS Manager and its tools, CICS-Lock, CICS-DupS, and CICS-SSO.

System Administration is simplified by the ERI/CICS Managers. This release of ERI/CICS contains four managers: the ERI/CICS Manager, the CICS-Lock Manager, CICS-DupS Manager, and the CICS-SSO Manager. They are menu driven and can be accessed by transaction ERIM. The Managers provide controls required to perform all system administration functions.

For some controls in the Managers, there are two modifiable fields:

❏ "Current Status"

Updates to this field have an immediate impact on the current run of CICS.

❏ "Next CICS Run"

Updates to this field are saved in the ERI/CICS control file and are used during the next run of CICS.

This chapter includes descriptions of each control and any rules that apply. Most controls can be updated dynamically while others require a restart of CICS.

ERI/CICS Manager

The ERI/CICS Manager verifies and updates controls related to the base product such as the product password, SVC number, subtask, EXTDS, Event recorder, Interval Monitor, and language support. In addition, the ERI/CICS Manager confirms CICS and product release, current CPU serial number, product password, and control file allocation.

Product Password

A password is required for access to ERI/CICS. This password is based on your CPU serial number and must be provided before product initialization or customization can continue. Normally, passwords are a concern only when you start a trial, acquire a license, or change to a new CPU. If you license for multiple CPUs, you need a password for each system.

Transaction ERIM provides access to the ERI/CICS System Administration. Menu selections direct you to the ERI/CICS Manager where you can enter or change product passwords. The ERI/CICS Manager panel contains a list of

System Passwords previously saved. The list stores up to 10 combinations of CPU numbers and passwords. The product selects the current password from the list during initialization. System passwords may be saved in advance to create a seamless transition when CPU upgrades are scheduled.

If no valid password is located when you first enter the ERI/CICS Manager Control Panel, an error message is displayed. Similar messages are logged to the System Log and to a CICS transient data set during product initialization.

Installation Verification

An Installation Verification section is presented on the ERI/CICS Manager screen. The information displayed in this section confirms the following:

❑ Current CPU-id

The serial number assigned to this CPU, used by ERI/CICS during password validation.

❑ Current Password

The password selected during product initialization.

❑ CICS Release

CICS release for this region.

❑ MVS Release

MVS release that CICS is executing under.

❑ ERI/CICS Release

ERI/CICS release that is executing.

❑ Control File DD Name

The name of the FCT entry used by ERI/CICS for I/O to the ERI/CICS control file.

❑ Control File DSN

Data Set Name assigned during installation of the ERI/CICS control file.

ERI/CICS Manager Controls

The ERI/CICS Manager has seven controls: Subtask, SVC, EXTDS Support, Language, Event Recorder, Interval Monitor, and Monitor Interval.

Subtask

Purpose: To provide support for ERI/CICS Tools that require access to the ERI/CICS SVC.

Valid Values: ENA (enable) or DIS (disable)

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Note: Once the ERI/CICS subtask is enabled, the “Current Status” field is protected to prevent disabling. Transaction ERID is provided to shut down the subtask and all ERI/CICS tools that require the subtask for execution. You can initialize ERI/CICS again after executing transaction ERID using the ERI/CICS managers.

SVC

Purpose: Indicates the SVC number to be used for the current and next run of CICS.

Valid Values: Type 3 or Type 4 SVC numbers

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Note: During installation of ERI/CICS, the default value assigned to the SVC number is 000. Update the “Current Status” and “Next CICS Run” fields with the SVC number assigned by your MVS System Programmer before enabling the ERI/CICS subtask.

EXTDS (Extended Data Streaming) Support

Purpose: Instructs ERI/CICS to save and then restore EXTDS attributes during CICS-Lock and CICS-View processing.

Valid Values: ENA (enable) DIS (disable)

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

LANGUAGE

Purpose:	Indicates the national language that is displayed on end-user screens. Only those screens and messages displayed by CICS-Lock and CICS-DupS are translated. All other screens, including CICS-View and ERI/CICS Manager screens, are displayed in English.
Valid Values:	ENG (UK English), DEU (German), or ENU (US English)
To Modify:	Enter valid field values. Enter **UPDATE** on the command line.
Action:	The “Current Status” field value is processed immediately. The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Event Recorder

Purpose:	Initializes the Event Recorder and begins the collection of user statistics required by the Interval Monitor.
Valid Values:	ENA (enable) or DIS (disable)
To Modify:	Enter valid field values. Enter **UPDATE** on the command line.
Action:	The “Current Status” field value executes immediately. The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Note: The Event Recorder is event driven and must be ENABLED before the Interval Monitor can be initialized. If the Event Recorder is DISABLED, the Interval Monitor is DISABLED automatically. In addition, the Event Recorder will not initialize unless the ERI/CICS product password has been validated and the ERI/CICS Subtask ENABLED.

Interval Monitor

The Event Recorder must be ENABLED before the Interval Monitor will initialize.

Purpose: Initializes the Interval Monitor and begins analysis of data collected by the Event Recorder.

Valid Values: ENA (enable) or DIS (disable)

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

The effect of disabling this control is to turn off CICS-Lock processing for all users.

Note: The Interval Monitor is an interval driven event. The interval at which the monitor run is set by the Monitor Interval control, which is described later in this section.

Monitor Interval

Purpose: Sets the interval at which the Interval Monitor will execute. The Interval Monitor uses Automatic Transaction Initiation (ATI) for interval processing. ATI must be supported in the CICS region that executes CICS-Lock.

Valid Range: 1 - 9 minutes

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately—the current interval can be dynamically altered.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

CICS-Lock Manager

The CICS-Lock Manager provides on-line system administration for controls unique to the CICS-Lock Tool.

There are two panels associated with the CICS-Lock Manager. The first panel contains primary controls and installation verification data. The second panel supports exclusion entries to CICS-Lock processing.

Installation Verification

An Installation Verification section is presented on page 1 of the CICS-Lock Manager. The “Current User Count” display indicates the current number of users initialized to CICS-Lock for this CICS region. The “Current Lock Count” display indicates the total users currently in a terminal lock condition.

CICS-Lock Manager Controls

The CICS-Lock Manager has five controls: Lock Hot Key, Hot Key Recognition Character, Lock Interval, Disconnect Interval, and Disconnect Request.

To access the CICS-Lock Manager, enter transaction ERIM and select the option for “Tool Managers” and then “CICS-Lock.”

Lock Hot Key

Purpose: Assigns a function key to support user request for terminal lock.

Valid Values: PF1 - PF24, PA1- PA2

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Hot Key Recognition Character

Purpose: Identifies a character used in conjunction with Lock Hot Key to detect a user-requested lock. Locking occurs only if the Recognition Character appears in the first position of an input field when the hot key is pressed.

Valid Values: Any displayable character.

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Note: The combination of Lock hot key and hot key Recognition Character must be unique to CICS-Lock. In other words, the combination must not be the same as a combination used by the CICS-DupS Swap Facility.

Lock Interval

Purpose: Sets the interval that CICS-Lock uses to determine that a CICS terminal session has become unattended. After expiration of this interval, CICS-Lock performs lock processing as described in Chapter 4.

Valid Range: 0 - 999 minutes

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately—the current interval can be dynamically altered.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Note: A value of “000” denotes an unlimited interval. Automatic lock processing will never be scheduled for any user. A value of “999” prevents automatic lock scheduling unless the Lock Parameter Exit is modified. See the chapter *Customizing ERI/CICS with User Exits and User Tables* on page 63 for additional information.

Disconnect Interval

Purpose: Sets the interval that CICS-Lock uses to determine that a CICS terminal session has become unattended. After expiration of this interval, CICS-Lock performs disconnect processing as described in Chapter 4.

Valid Range: 0 - 999 minutes

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately—the current interval can be dynamically altered.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Note: A value of “000” denotes an unlimited interval; disconnect processing will never be scheduled for any user. A value of “999” prevents automatic disconnect scheduling unless the Lock Parameter Exit is modified. See the chapter *Customizing ERI/CICS with User Exits and User Tables* on page 63 for additional information.

Disconnect Request

Purpose: Indicates the type of disconnect processing required when the Disconnect Interval expires.

Valid Range: LOGOFF (Disconnect the device from CICS) or
SIGNOFF (Sign-off the device but leave it attached to CICS)

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field is processed immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

CICS-Lock Exclusions

CICS-Lock supports four types of exclusions from Interval Monitoring; by VTAM LU-name, CICS Terminal ID, CICS userid, and CICS Transaction ID. Exclusion entries may contain generic characters within the exclusion entry name. These characters are represented by an asterisk (*). Any combination of generic and qualifying characters may be used. Exclusion entries can be added or deleted dynamically by the CICS-Lock Manager. All updates to the exclusion list have an immediate impact on the current run of CICS. In addition, exclusion entries are stored in the ERI/CICS control file and reloaded during the next initialization of CICS-Lock.

Exclusion examples:

T Only termid whose length is 1 and contains a “T” in the first position

T*** All termids that begin with “T”

T* Only termids that begin with “T” and are two characters in length where the second character is generic

TT All termids that contain a “T” in the 2nd and 3rd position

Note: When analyzing exclusions by CICS Transaction ID, CICS-Lock evaluates only the next transaction scheduled for the device.

CICS-DupS Manager

The CICS-DupS Manager provides on-line system administration for controls unique to the CICS-DupS Tool.

There is one panel associated with the CICS-DupS Manager. This panel provides system administration for CICS-DupS controls and exclusions.

CICS-DupS Manager Controls

The CICS-DupS Manager has six controls: Session Limit, Sign-on Tranid, Session Take-Over, Swap Hot Key, Hot Key Recognition Character, and Hot Key Initial Tranid.

To access the CICS-DupS Manager, enter transaction ERIM and select the option for “Tool Managers” and then “CICS-DupS.”

Session Limit

Purpose: Sets the CICS session limit per userid for the current and the next run of CICS.

Valid Range: 0 - 99 sessions per userid.

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately—the current interval can be dynamically altered.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Note: A value of “00” indicates unlimited sessions per single userid.

Sign-on Tranid

Purpose: Identifies the transaction CICS-DupS starts, via ATI, when a user requests option 1), “Return to Sign-on,” from the Duplicate Userid panel.

Valid Values: Any sign-on transaction that can be initiated via ATI (the default value is “CSGM”).

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Note: The default value for Sign-on Tranid is CSGM, the CICS Good Morning Message transaction. If you have a locally customized sign-on facility, you may replace the default value. For CICS Version 3, CESN may be used.

Session Take-Over

Purpose: Instructs CICS-DupS to cancel a user’s active session so that the user can establish a new session.

Valid Values: ENA (enable) or DIS (disable)

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Swap Hot Key

Purpose: Assigns a function key to support the Swap Facility.

Valid Values: PF1 - PF24, PA1- PA2

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Hot Key Recognition Character

Purpose: Identifies a character used in conjunction with Swap Hot Key to detect a swap request. Swapping occurs only if the Recognition Character appears in the first position of an input field when the hot key is pressed.

Valid Values: Any displayable character.

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

Hot Key Initial Tranid

Purpose: Identifies the transaction the CICS-DupS Swap Facility starts, via ATI, when a user first requests a swap.

Valid Values: Any transaction that can be initiated via ATI.

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value is processed by the ERI/CICS initialization program during PLTPI for the next CICS run.

CICS-DupS Multi-Session Masks

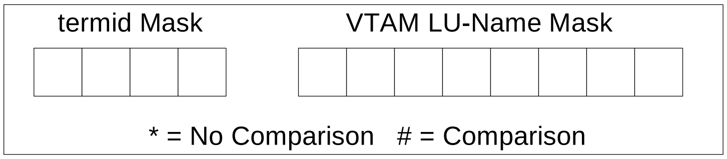
The CICS-DupS Multi-Session Mask feature provides a way of further controlling duplicate userids. You can specify masks that restrict duplicate sign-on according to a user’s termid or VTAM LU-name.

If masks are specified for both termid and VTAM LU-name, the session is permitted if either condition is met. Depending on your naming conventions for CICS VTAM LU-names, it is possible to use the masks to restrict a user’s multiple sessions to a single workstation.

Mask Characters

You build a mask with a combination of the characters “*” and “#”. The “*” character specifies a character position where no comparison occurs. The “#” character specifies a character position that must match to allow a sign-on.

The mask length for termid is four characters. For VTAM LU-name, the mask length is eight characters.



For example, to restrict a user’s multi-sessions to termids where the last three positions are equal, you would set the termid mask to “*###”. In this case, if a user’s first session was assigned a termid of A212 and their next session was assigned a termid of B212, then sign-on would complete successfully. However, if their next session was assigned a termid of C340, the sign-on would fail.

All updates to the masks have an immediate effect on the current run of CICS. In addition, mask entries are stored in the ERI/CICS control file and reloaded during the next initialization of ERI/CICS.

Termid Mask

Purpose: Sets the rules for controlling a user’s ability to sign-on, based on the user’s termid.

Valid Values: Any four-character combination of “*” and “#” characters.

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The field value executes immediately.

VTAM LU-Name Mask

Purpose: Sets the rules for controlling a user’s ability to sign-on, based on the user’s VTAM LU-name.

Valid Values: Any eight-character combination of “*” and “#” characters.

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: The field value executes immediately.

CICS-DupS Exclusions

CICS-DupS supports two types of exclusions: by External Security Manager (ESM) profile access and by CICS userid.

Exclusion by ESM

To implement ESM exclusions, you must have RACF 1.8.1 or higher, or another SAF compatible security manager. To activate this feature, define a resource profile in your ESM, permit READ access to the resource for selected users or groups, and specify the ESM Class Name and ESM Resource Name in the CICS-DupS Manager dialog.

ESM Class Name

Purpose: Identifies the class name used in the ESM profile definition, which is used to control CICS-DupS exclusions.

Valid Values: The ESM class name specified in the profile definition.

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: All updates take effect immediately.

ESM Resource Name

Purpose: Identifies the resource name used in the ESM profile definition, which is used to control CICS-DupS exclusions.

Valid Values: The ESM resource name specified in the resource definition.

To Modify: Enter valid field values.
Enter **UPDATE** on the command line.

Action: All updates take effect immediately.

The following example illustrate how to define a resource and grant access authority. For simplicity, the examples use one of the CICS classes. You can modify the examples to meet your security standards.

```
RDEF TCICSTRN (DUPS) UACC(NONE)

PE DUPS CLASS(TCICSTRN) ID(my group)
```

Based on these examples, you would fill in the ESM Class Name with TCICSTRN and the ESM Resource Name with DUPS.

Exclusion by CICS Userid

CICS-DupS also supports exclusions by CICS userid. Userid exclusion entries may contain generic characters within the exclusion entry name. These characters are represented by an asterisk (*). Any combination of generic and qualifying characters can be used. Entries can be added or deleted dynamically by the CICS-DupS Manager. All updates to the exclusion list have an immediate impact on the current run of CICS. In addition, exclusion entries are stored in the ERI/CICS control file and reloaded during the next initialization of ERI/CICS.

For rules and examples on coding userid exclusion entries, see the exclusion examples in "CICS-Lock Exclusions" on page 35.

CICS-SSO Manager

The CICS-SSO Manager provides on-line system administration for controls unique to the CICS-SSO Tool.

There are two panels associated with the CICS-SSO Manager. The first panel contains primary controls. The second panel supports exclusion entries to automatic menu processing.

The CICS-SSO Manager also provides access to the CICS-SSO Menu Editor.

CICS-SSO Manager Controls

The CICS-SSO Manager has five controls: CICS-SSO Status, Automatic Menu, Menu Hot Key, Hot Key Recognition Character, and PassTicket Generation. To access the CICS-SSO Manager, enter transaction ERIM, select the option for "Tool Managers," and then "CICS-SSO."

CICS-SSO Status

Purpose:	Indicates whether CICS-SSO is active.
Valid Values:	ENA (enable) or DIS (disable).
To Modify:	Enter valid field value. Enter **UPDATE** on the command line.
Action:	The "Current Status" field value executes immediately. The "Next CICS Run" field value takes effect the next time ERI/CICS is initialized.

Automatic Menu

Purpose: Indicates whether the CICS-SSO Automatic Menu feature is active. If Automatic Menu is enabled, the user returns to the CICS-SSO main application menu on exit from an application. If the application erases the screen, CICS-SSO sends the menu immediately; if not, CICS-SSO pops up a prompt to press ENTER, preserving the last message.

Valid Values: ENA (enable) or DIS (disable).

To Modify: Enter valid field value.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value takes effect the next time ERI/CICS is initialized.

Menu Hot Key

Purpose: Assigns a function key to support a user request to return to the CICS-SSO main application menu.

Valid Values: PF1 - PF24, PA1 - PA2.

To Modify: Enter valid field value.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value takes effect the next time ERI/CICS is initialized.

Hot Key Recognition Character

Purpose: Identifies a character used in conjunction with the Menu Hot Key to detect a user request for the main menu. The menu is invoked only if the recognition character appears in the first position of an input field when the hot key is pressed.

Valid Values: Any displayable character.

To Modify: Enter valid field value.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value takes effect the next time ERI/CICS is initialized.

Note: The combination of Menu hot key and hot key recognition character must be unique to CICS-SSO. The combination must not be the same as a combination used by CICS-Lock or the CICS-DupS Swap Facility.

PassTicket Generation

Purpose: Identifies PassTicket generation method. CICS-SSO uses a PassTicket to perform automatic sign-on when a session is passed from one VTAM APPLID to another.
The PassTicket is also used in recovery following an unsuccessful pass. You can override the value specified in the CICS-SSO Manager at the application level using the Menu Editor.

Valid Values: ESM (RACF generated PassTickets), ERI (ERI/CICS generated PassTickets) , NO (No PassTickets; prompt user for password).

To Modify: Enter valid field value.
Enter **UPDATE** on the command line.

Action: The “Current Status” field value executes immediately.

The “Next CICS Run” field value takes effect the next time ERI/CICS is initialized.

CICS-SSO Automatic Menu Exclusions

CICS-SSO supports four types of exclusions from Auto Menu processing: by VTAM LU-name, CICS Terminal-id, CICS userid, and CICS transaction-id. To access the Auto Menu Exclusion panel, press PF8 at the CICS-SSO Controls panel. Updates to the exclusion table take effect immediately. In addition, exclusion entries are stored in the ERI/CICS control file and reloaded the next time ERI/CICS is initialized.

Exclusion entries may contain generic characters within the exclusion entry name. These characters are represented by an asterisk (*). You may use any combination of generic and qualifying characters.

Termid exclusion examples:

TTTT	Termid "TTTT"
T****	All termids that begin with "T"
T*	All termids that begin with "T" and are two characters in length
TT	All termids that contain "TT" in the second and third position

CICS-SSO Menu Editor

The CICS-SSO menu editor is the tool you use to build and manage your menu system. The menu system has two essential components: menus and profiles. *Menus* are for the end user. They present a list of applications the user is authorized to access. Menus can contain up to 45 items, each representing a specific application or sub-menu. *Profiles* are for the CICS-SSO software. They provide the information required to properly invoke and access items selected from the menu.

To access the menu editor, press PF5 at the CICS-SSO Controls panel. The menu editor primary panel contains three input areas: the command line, the title area, and the item area.

Menu Editor Command Line

The menu editor command line supports the following commands:

CAPSON	Turn on uppercase translation for the current session
CAPSOFF	Turn off uppercase translation for the current session
EDIT	Edit the Main Menu Profile
END	Return to the previous menu or screen
HELP	Help screen for menu editor
UPDATE	Make all changes permanent

Menu Title Area

The menu editor title area is the first four lines below the command line. CICS-SSO displays the title you enter here on the menu presented to the end-user. The software centers your text.

Menu Item Area

The menu item area follows the title area. The item area contains the list of profile descriptions available to your users. Menu items are either applications or sub-menus. Items are displayed one, two, or three columns depending on the number of profiles defined for the active menu.

The menu editor supports the following line commands to maintain the item list:

B	Insert blank line
D	Delete profile or blank line
E	Edit menu item profile
H	Display help screen for menu item
I	Insert menu item
S	Select menu item

Line commands are entered in the menu item area. The line commands I and E invoke the profile editor, where menu item profiles are maintained.

Menu Profile Controls

The profile editor is used to maintain the profiles for menu items. These profiles contain the information required to properly invoke and access items selected from the menu. This section documents the profile editor input fields.

Description

Purpose:	Provides a brief description of the menu item. This value appears in the item area of the menu.
Valid Values:	Free-form text, 30 characters available on 1 and 2 column menus, 20 characters on 3 column menu.
Required:	Yes.

Status

Purpose: Indicates whether an item is enabled or disabled. A disabled item cannot be selected from the menu. When an item is enabled, you can update Enabled Help Text. When an item is disabled, you can update disabled Help Text.

Valid Values: ENA (enable) or DIS (disable).

Required: Yes.

VTAM Applid

Purpose: Identifies the applid of the TOR in which the item will be processed.

Valid Values: Any valid CICS VTAM applid or blank. Blank indicates that the item is to be processed in the current TOR.

Required: No.

Profile Type

Purpose: Specifies whether this menu item is an application or a menu.

Valid Values: Application or Menu.

Required: Yes.

ESM Class

Purpose: Identifies the class name used in an ESM profile definition for checking authority to access this menu item.

Valid Values: The class name specified in the ESM profile definition.

Required: No.

ESM Resource

Purpose: Identifies the resource name used in an ESM profile definition for checking authority to access this menu item.

Valid Values: The resource name specified in the ESM profile definition.

Required: No.

Trans Sec

Purpose: Indicates whether transaction security, as specified in the SIT, is used to check authority to access this application.

Valid Values: YES or NO.

Required: Yes, for application profiles; not for menu profiles.

Prog Sec

Purpose: Indicates whether program security, as specified in the SIT, is used to check authority to access this application.

Valid Values: YES or NO.

Required: Yes, for application profiles; not for menu profiles.

PassTicket

Purpose: Identifies PassTicket generation method. CICS-SSO uses a PassTicket to perform automatic sign-on when a session is passed from one VTAM APPLID to another. The PassTicket is also used in recovery following an unsuccessful pass. The value assigned in the profile overrides the global value specified in the CICS-SSO Manager.

Valid Values: ESM (RACF generated PassTickets), ERI (ERI/CICS generated PassTickets) , NO (No PassTickets; prompt user for password).

Required: Yes, for application profiles; not for menu profiles.

Tran/Prog

Purpose: Identifies the transaction or program that CICS-SSO will invoke when this menu item is selected.

Valid Values: Any transaction or program defined to CICS , or one of the following keywords:

NATIVE	Exit to native CICS
LOGOFF	Exit CICS
TSO	Exit CICS and initiate a TSO session

Required: Yes, for application profiles; not for menu profiles.

Transfer Mode

Purpose: Specifies the CICS command that CICS-SSO will use to invoke the application.

Valid Values: One of the following keywords:

LINK	LINK with optional Commarea
LINKI	LINK with input message
XCTL	XCTL with optional Commarea
XCTLI	XCTL with input message
START	START with optional Commarea RETURN
RETURN	IMMEDIATE with optional input message)

Required: Yes, for application profiles; not for menu profiles.

Application Data

Purpose: Provides data to be passed to the application as either a Commarea or and Input Message, depending on the transfer mode selected.

Valid Values: Any valid input for the designated application.

Required: No.

Enabled Help Text

Purpose: Specifies help text for this menu item when the profile status is “ENABLE.” This field is accessible only when the profile status is “ENABLE.”

Valid Values: Any free-form text.

Required: No.

Disabled Help Text

Purpose: Specifies help text for this menu item when the profile status is “DISABLE.” This field is accessible only when the profile status is “DISABLE.”

Valid Values: Any free-form text.

Required: No.

End of Chapter 3

Chapter 4
Using ERI/CICS

This chapter provides operational information for the CICS-Lock, CICS-DupS, and CICS-View tools.

Using CICS-Lock

CICS-Lock is a user-friendly alternative to CICS terminal time-out. This tool enhances terminal security while providing CICS users with the convenience of extended connect time. CICS-Lock assures privacy of data even while a CICS session is left unattended.

Users can invoke CICS-Lock either by request or automatically after an installation-defined interval expires. CICS-Lock replaces the user's screen with a locked notification message that includes a password validation prompt. After password validation, the user's CICS session, including terminal data, COMMAREA and next Tranid are restored as if the interrupt did not occur.

CICS-Lock will disconnect terminal sessions automatically after an installation-defined interval expires. All product related and CICS terminal related storage is deleted for that session.

Note: CICS-Lock does not lock or disconnect a terminal session unless the operator is signed on.

Invoking CICS-Lock

There are four ways you can interface with CICS-Lock. Two are user-requested and two are automated and controlled by the product. During installation and customization of ERI / CICS, control values were assigned that impact this user interface. These controls are described below.

Hot Key

The Hot Key interface provides a convenient way to request terminal lock without exiting from an application session. Possible hot key values are PF1 - PF24 and PA1 - PA2. To resolve conflicts with other hot key assignments, a hot key Recognition Character can also be assigned. If a hot key character is assigned, the character must appear in the first byte of an input field.

CICS Tranid

The CICS Tranid assigned during installation can be used to invoke terminal lock from native CICS. The default value is “LOCK.” The CICS Systems Programmer can change that value during installation.

Automatic Locking

CICS-Lock performs automatic locking of unattended terminal sessions after an installation-defined interval expires. The following components of ERI/CICS must be ENABLED before this feature is functional: the Event Recorder, Interval Monitor, and a Lock Interval greater than 00.

The possible value range for Lock Interval is 0 - 999 minutes.

Note: A Lock Interval of 000 indicates no automatic locking.

Automatic CICS Disconnect

CICS-Lock performs automatic CICS session termination of unattended terminal sessions after an installation-defined interval expires. The following components of CICS-Lock must be ENABLED before this feature is functional: the Lock Recorder, Interval Monitor, and a Disconnect Interval greater than 00.

The possible value range for CICS Disconnect is 0 - 999 minutes.

Note: A Disconnect Interval of 000 indicates no automatic session disconnect.

Restoring Your CICS Session

After CICS-Lock acquires a CICS session, password validation must be performed before the session is restored. The pop-up window, which appears after CICS-Lock acquires the session, prompts you for your password. Enter the password in the same form used for CICS sign-on. After the password is validated, the user’s CICS session (including terminal data, COMMAREA, and next Tranid) is restored as if the interrupt did not occur.

Note: The ERI/CICS SVC performs password validation using SAF calls.

Exiting from CICS-Lock

An Exit option is available from the CICS-Lock pop-up window. This option, which is invoked by pressing F3/F15 or entering **EXIT** on the command line, terminates the CICS session.

Note: You cannot return to CICS without completing password validation.

Requesting Help

Help is available from the CICS-Lock pop-up window. To request help, press F1/F13 or enter **HELP** on the command line. Help appears as a roll-down window and provides a short overview of CICS-Lock and a list of the values assigned to the controls described above.

Using CICS-DupS

CICS-DupS provides two facilities: the Session Control facility and the Swap facility. The Session Control facility allows you to control the number of concurrent sessions a user can establish. The Swap facility enables users to seamlessly swap between two applications. Usage information for concurrent session management is provided in the following section. Usage information for the CICS-DupS Swap facility begins on page 55.

Using the Session Control Facility of CICS-DupS

Session Control processing occurs at the completion of CICS sign-on. When a session limit is exceeded, the user is signed off of CICS and the CICS session is acquired by CICS-DupS. There are three options available after session limit detection: return to sign-on, exit CICS, or cancel the active session and return to sign-on. CICS-DupS supports exclusions by CICS userid. Exclusion entries may be generic in form. Like other ERI / CICS product components, all controls are dynamic and can be altered interactively by accessing the CICS-DupS Manager (see the “CICS-DupS Manager” section on page 35).

Invoking the Session Control Facility

The duplicate session limit defined by the system administrator sets a limit on the number of concurrent CICS sessions per userid. CICS-DupS checks the limit when a new user signs on and when the userid associated with a terminal session changes. If the session limit is not exceeded, the user continues uninterrupted. If the session limit is exceeded, CICS-DupS will SIGNOFF the user but not terminate the user’s CICS session. When SIGNOFF is complete, CICS-DupS clears the terminal screen and displays a pop-up window.

Exiting from the Session Control Facility

From the CICS-DupS pop-up window, the user has three options: 1) “Return to sign-on”, 2) “Exit CICS”, or 3) “Cancel active session, return to sign-on.

If option 1) is selected, CICS-DupS starts the transaction defined by the system administrator for “Return to sign-on.” The default value for this transaction is “CSGM,” the CICS Good Morning Message transaction. From this point, the user begins the sign-on process again.

If option 2) is selected, the CICS session is terminated if the terminal definition supports disconnect; if not, the terminal is signed off.

If option 3) is selected, the active session (that raised the duplicate sign-on condition) is cancelled, and CICS-DupS starts the transaction defined for “Return to sign-on.”

Note: Option 3) is presented to the user only if the system administrator enabled the Session Take-Over option (page 21).

Requesting Help

Help for the concurrent session management facility is available from the CICS-DupS pop-up window. To request help, press F1 / F13 or enter **HELP** on the command line. Help appears as a roll-down window and provides a short overview of CICS-DupS and a list of the values assigned to the controls described above.

Using the Swap Facility of CICS-DupS

The CICS-DupS Swap facility enables uses to have concurrent access to two applications from a single terminal session. This facility provides seamless swapping between two terminal screens.

Note: Before implementing the Swap facility of CICS-DupS, refer to *Product Restrictions* on page 7.

When a user initiates the Swap facility, the initial Tranid (identified in the CICS-DupS Manager dialog) is executed. If no initial Tranid was provided, the Swap facility displays a panel informing the user that Swap is initialized and is prompting for a transaction ID.

Once a user initiates swapping, the Swap facility intercepts a CICS signoff and terminates the active window. The user must initiate a second signoff to actually signoff of CICS.

Note: CICS-View reports swap status in the “Term Stat” column of the display. The active (ACT) and in service (INS) indicators are suffixed by “1” or “2” to indicate which swap window is active. No suffix means that swapping is not active at the device.

Invoking the Swap Facility

The CICS-DupS Swap facility is invoked with a hot key and (optionally) a hot key Recognition Character. These values are assigned during the ERI / CICS installation and customization process.

Exiting from the Swap Facility

Once swapping is initiated, the Swap facility intercepts the CICS signoff transaction (CSSF in Version 2 and CESF in Version 3). Entering a signoff transaction terminates the active window and the session resumes. A second signoff transaction signs the user off of CICS.

Using CICS-View

CICS-View is an easy to use session status monitor designed for the CICS System Administrator or Help Desk staff. CICS-View displays data in user activity tables providing a quick way to view CICS user activity. CICS-View also provides built-in functions to support problem resolution.

CICS-View presents a User Table built from data collected by ERI/CICS and maintained in extended memory. The User Table includes data about VTAM sessions that are INSERVICE and ACQUIRED by CICS and have a signed on user. The user is the default userid until the user signs-on with his or her own userid. After a user signs-off, ERI/CICS deletes the data collected for that session.

CICS-View is not a performance monitor—it is a tool to improve your access to real-time information about CICS session activity.

Note: Consoles and printers are excluded from the CICS-View User Table.

Invoking and Exiting from CICS-View

There are two ways to access CICS-View:

- ❑ directly, using transactions ERIV, VIEW, or VMSG from native CICS,
- ❑ through menus, using the ERI/CICS manager.

Transactions ERIV, VIEW, and VMSG invoke the CICS-View application directly from native CICS. Transaction ERIV permits access to line commands; transaction VIEW does not. VMSG permits access to the message line command only. When accessed from transaction ERIV, VIEW, or VMSG, EXIT from CICS-View returns to native CICS.

CICS-View is also available as an option on the ERI/CICS System Administration menu. This method gives you access to line commands and EXIT returns to the ERI/CICS manager.

The User Table Panel

CICS-View presents data in table format. By default, all currently active sessions are displayed. The Search Options Feature, described on page 59, lets you select the terminal sessions included in the table. The User Table is always presented in CICS terminal ID sequence. User Table fields are described in Table 4-1.

Table 4-1 User Table Fields

User Table Field	Description
CICS Term	CICS terminal ID

Table 4-1 User Table Fields (Continued)

User Table Field	Description
Userid	User ID signed on to the CICS terminal session.
VTAM LU-name	VTAM logical unit name for the CICS terminal.
Start Date	Date that the CICS terminal session was signed on and initialized to ERI/CICS.
Start Time	Time when the CICS terminal session was signed on and initialized to ERI/CICS.
Last Time	Completion time of the last completed terminal task or start time of a currently active task.
Last Tran	Transaction ID of the most recent terminal task.
Total Tran	Total number of CICS terminal transactions.
Last Resp	Transaction response time for the last completed terminal task or duration of a currently active task.
Avg Resp	Average transaction response time for CICS terminal transactions. **Note:** CICS-View reports response-time data collected by the CICS-Lock Event Recorder (described in Chapter 1). These response times are included to give you an indication of session status, not for performance measurement.
Term Stat	Terminal Status indicating the state of the terminal session. Possible values are: INS INSERVICE and ACQUIRED by CICS but not currently processing a transaction ACT INSERVICE and ACQUIRED by CICS and has an active transaction LCK INSERVICE and ACQUIRED by CICS and locked by the CICS-Lock tool REL RELEASED from CICS **Note:** CICS-View reports swap status in the “Term Stat” column of the display. The active (ACT) and in service (INS) indicators are suffixed by “1” or “2” to indicate which swap window is active. No suffix means that swapping is not active at the device.

User Table Panel Primary Commands and Function Keys

Primary commands control scrolling through the User Table, access to Search Options and the Help Facility, and navigation through CICS-View. Primary commands are entered on the command line of the User Table panel and most have an equivalent function key. The User Table primary commands and function keys are described in Table 4-2.

Table 4-2 User Table Primary Commands and Function Keys

Command	Function Key	Description
HELp	F1/F13	Request Help Facility for the current panel or window.
FORward	F8/F20	Scroll forward one full page.
BACkward	F7/F19	Scroll backward one full page.
TOP	M F7/F19*	Scroll to the top of the User Table.
BOTtom	M F8/F20*	Scroll to the bottom of the User Table.
SEArch	F5/F17	Invoke the Search Options window from the User Table panel.
MESsage	None	Invoke the “Create / Edit Message” screen.
END	F3/F15	End from the current panel.
EXIt		Exit from CICS-View.

* Enter "M" on the Command line and press the function key.

User Table Line Commands

CICS-View provides several built in functions designed to enhance your ability to perform problem resolution. These functions are implemented as line commands. Below is list of these line commands and a description of their purpose.

C Cancel a user’s CICS session and PURGE any active tasks if data integrity can be maintained.

R Reset terminal session Transaction Count and Average Response Time fields to zeros.

V View the contents of a user's last terminal screen.
Note: To view a terminal screen the session must be INSERVICE, ACQUIRED, and not have an active task.

M Send a non-destructive message to a user’s terminal screen.

Search Options Feature

The Search Options feature of CICS-View provides a way to select sessions for inclusion in the User Table. To invoke the Search Options window from the User Table panel, enter SEARCH on the command line or press F5/F17. From the Search Options window you can enter search criteria, process your search criteria, cancel all Search Options, or invoke the Help Facility.

To process search criteria, enter PROCESS on the command line or press F5/F17. A User Table is built from data satisfying your criteria. If no selection criteria are entered, all user sessions are displayed. If no sessions are selected by your search criteria, you return to the Search Options window.

Search Options Primary Commands and Function Keys

Primary commands control search criteria processing, access to the Help Facility, and navigation through CICS-View. Primary commands are entered on the Command line of the Search Option window and have an equivalent function key. The Search Option primary commands and function keys are shown in Table 4-3.

Table 4-3 Search Option Primary Commands and Function Keys

Command	Function Key	Description
HELp	F1/F13	Request Help Facility for Search Options.
PROcess	F5/F17	Process search criteria specified in the Search Options window.
CANcel	F12/F24	Cancel the CICS-View pop-up window and return to the User Table panel.

Search Option Parameters

The Search Option parameters let you specify criteria for sessions included in the User Table. The supported parameters are described below.

AND/OR AND: only sessions that meet all search criteria are displayed. OR: all sessions satisfying any search argument are displayed.

Termid Terminal ID may be selected. A generic name may be specified by keying an asterisk (*) in each field position you want to be generic. For example, to select all termids beginning with A, enter "A***" as the termid; to select all termids that end in A, enter "***A".

Userid User ID or generic name may be specified.

LUname VTAM LU name or generic name may be specified.

Tranid Last CICS transaction ID or generic name may be specified.

Note: When using Search Option parameters, the user and lock counts displayed at the bottom of the screen reflect the terminal sessions that are selected.

Message Feature

The Message Feature of CICS-View provides a way to send nondestructive messages to users at active terminals. Messages are queued until the next CICS task at the receiving terminal is complete. Then, the session environment at the receiving terminal is saved and the CICS-View Message panel is displayed. From this panel, you can view queued messages, reply to messages, or resume your CICS session.

Creating, Editing, and Sending a Message

From the Create/Edit Message panel, you can enter message text, send a message, clear the message text, or invoke the Help Facility. You invoke the Create/Edit Message panel by selecting message recipient(s) using the “M” line command on the CICS-View’s User Table and pressing Enter.

After you enter your message into the Create/Edit Message panel, you can send it by entering SENd on the command line or by pressing F5/F17.

If you selected message recipients using the “M” line command, the Message Facility routes the message to the selected users. You can select any users from a CICS-View User Panel page.

The Message Facility saves a message until you clear the message text area or exit CICS-View. Each time you use the “M” line command, the Message Facility presents the Create/Edit window. If you have already entered a message, that message text appears in the message text area. You can send the message as it appears, edit the text before sending it, or clear the message text area and enter a new message.

Create/Edit Message Primary Commands and Function Keys

Primary commands control the creation and editing of messages, access to the Help Facility, and navigation through CICS-View. You can enter primary commands on the Command line of the Create/Edit Message window and have an equivalent function key. Table 4-4 shows the Create/Edit Message commands and function keys.

Table 4-4 Create/Edit Message Commands and Function Keys

Command	Function Key	Description
HELp	F1/F13	Request Help Facility for Create/Edit Message Feature.

Table 4-4 Create/Edit Message Commands and Function Keys

Command	Function Key	Description
SENd	F5/F17	Send the entered message text to all selected users.
CLEar	F6/F18	Clear message text and return to Create/Edit Message panel.
CANcel	F12/F24	Clear message text and return to User Table panel.

Receiving a Message

When someone sends a message to you, the alarm at your terminal beeps twice to alert you of the message. Messages are queued until the next CICS task at your terminal is complete, so you may have multiple messages. The Message Facility saves your CICS session environment and displays the CICS-View Message panel. From this panel, you can view queued messages, reply to messages, or resume your CICS session. If you choose the Reply option, the Message Facility presents the Create/Edit Message panel. Enter your reply in the message text area, and the Message Facility routes it back to the sender.

Message Received Primary Commands and Function Keys

Primary commands control Message Received processing and access to the Help Facility. Primary commands are entered on the Command line of the Message Received panel and have an equivalent function key. Table 4-5 shows the Message Received commands and function keys.

Table 4-5 Received Message Commands and Function Keys

Command	Function Key	Description
HELp	F1/F13	Request Help Facility for Message Received panel.
END	F3/F15	Delete all queued messages and resume CICS session.
REPly	F5/F17	Invoke the Create/Edit Message panel.
FORward	F8/F20	Display the next queued message.

Broadcast Message Feature

The Broadcast Message Feature of CICS-View provides a way to broadcast nondestructive messages to all users, or a filtered subset of users. Message recipients can be filtered using the ERI-View Search Options Feature, or by using a pre-defined list. Messages are queued until the next CICS task at the receiving terminals is complete. Then, the session environment at the receiving terminal is saved and all queued broadcast and non-broadcast messages are displayed. From this panel, you can view queued broadcast and non-broadcast messages, reply to non-broadcast messages, or resume your CICS session.

The Broadcast Message Feature supports two interfaces:

❑ a menu interface via the CICS-View tool
❑ a command interface via tranid “ERBC”

Both interfaces can create, update and send broadcast messages. The menu interface is interactive and designed for the system administrator. The command interface supports access from a CICS command using parameter input.

Creating, Editing and Sending Broadcast Messages

From the Create/Edit Broadcast Message panel you can create and edit messages, update and delete messages from the ERI/CICS control file, send and drop messages, and check the status of a messages. You can save as many messages as you wish in the ERI/CICS control file, but there can be only 16 active or scheduled messages. To invoke the Broadcast Message menu interface, enter MESsage on the CICS-View command line.

Broadcast Message Menu Interface

Primary commands control the creation and editing of messages, access to the Help Facility, and navigation through the Create/Edit Broadcast Message panel. You can enter primary commands on the command line (some commands have an equivalent function key). Table 4-6 shows the Create/Edit Broadcast Message primary commands, any equivalent function key, and a short description of the command.

Table 4-6 Broadcast Message Menu Commands and Function Keys

Command	Function Key	Description
HELp	F1/F13	Request Help Facility
UPDATE	none	Save message to ERI/CICS control file
DELETE	none	Delete message from ERI/CICS control file

Table 4-6 Broadcast Message Menu Commands and Function Keys (Continued)

Command	Function Key	Description
SEND	F5/F17	Save broadcast message to control file and schedule the message
DROP	none	Drop an active or scheduled message
PREv msg	F7/F19	Scroll to previous message
NEXT msg	F8/F20	Scroll to next message
CANcel	F12/F24	Cancel Create/Edit Broadcast Message panel return to CICS-View

Broadcast Message Controls

The Broadcast Message record has 9 controls: Message Id, Message text, Start Date, Start Time, End Date, End Time, Drop on Init, Send at sign-on, and List.

Message Id

Purpose: Unique name identifying the message. The message id is used to save and retrieve the message from the ERI/CICS control file.

Valid Values: Any 8 character name.

To Modify: Enter valid field value. Enter UPDATE or SEND on the command line.

Action: All updates take effect immediately.

Message Text

Purpose: Holds the broadcast message text.

Valid Values: Free formed text, 8 rows by 57 characters.

To Modify: Enter free formed text. Enter UPDATE or SEND on the command line.

Action: All updates take effect immediately.

Start Date

Purpose: The date that the message is scheduled to broadcast.

Valid Values: mm/dd/yyyy

To Modify: Enter valid date. Enter UPDATE or SEND on the command line.

Action: All updates take effect immediately.

Start Time

Purpose: The time that the message is scheduled to broadcast.

Valid Values: hh:mm, military time format. For example: enter 14:30 for 2:30 PM.

To Modify: Enter valid time. Enter UPDATE or SEND on the command line.

Action: All updates take effect immediately.

End Date

Purpose: The date that the message is scheduled to drop.

Valid Values: mm/dd/yyyy

To Modify: Enter valid date. Enter UPDATE or SEND on the command line.

Action: All updates take effect immediately.

End Time

Purpose: The time that the message is scheduled to drop.

Valid Values: hh:mm, military time format. For example: enter 14:30 for 2:30 PM.

To Modify: Enter valid time. Enter UPDATE or SEND on the command line.

Action: All updates take effect immediately.

Drop on Init

Purpose: This control instructs the ERI/CICS initialization program to drop the message the next time ERI/CICS initializes. Note that ERI/CICS must initialize each time CICS is started.

Valid Values: YES (drop messages) or NO (restore message if still active)

To Modify: Enter valid field value. Enter UPDATE or SEND on the command line.

Action: All updates take effect immediately.

List

Purpose: Identifies a pre-defined list of users. The list name points to a table of selected users. The table must be assembled, linked and defined as a CICS program; no CICS translation required. See sample table ERIMSGTB in your.ERI.COPYLIB for coding rules. Additionally, the List name is considered to be a program resource that requires authorization to access. For example, if you create a table of selected users pointed to by a list name, then you must be authorized to access that program before you can update or send the message.

Valid Values: Any 8 character name.

To Modify: Enter valid field value. Enter UPDATE or SEND on the command line.

Action: All updates take effect immediately.

Send at Sign-on

Purpose: This control instructs ERI/CICS to send the message to all users, or selected users, each time they sign-on to CICS.

Valid Values: YES (send at sign-on) or NO (do not send at sign-on)

To Modify: Enter valid field value. Enter UPDATE or SEND on the command line.

Action: All updates take effect immediately.

Status

Purpose: Displays the current status of the message.

Valid Values: INACTIVE (the message is not scheduled or active)
ACTIVE (the message has been broadcast and is active)
SCHEDULED (the message is scheduled for broadcast)
DROPPING (the message is scheduled for drop)

To Modify: Not modifiable.

Action: None.

Message Count

Purpose: Displays the number of active users that are scheduled to read this message. If the Message Status field is INACTIVE, than the message count is 00000.

Valid Values: 00000 - 99999

To Modify: Not modifiable.

Action: None.

Author

Purpose: Identifies the last user to update this message.

Valid Values: Any valid userid.

To Modify: Not modifiable.

Action: None.

The ERI/CICS Interval Monitor and Broadcast Messages

The broadcast process includes two phases. The first phase involves the creating, editing, and sending of the message. This phase only builds the VSAM and CICS Temp Storage records required to support the broadcast process.

Phase two involves the ERI/CICS Interval Monitor. The Interval Monitor is a non-terminal task that performs many functions for all the ERI/CICS tools. One of the many monitor functions is to search for broadcast message queues and analyze message controls, such as start date/time, filters, broadcast requests, and drop requests. When the Interval Monitor detects a broadcast request or drop request, bits are turned on or off in the ERI/CICS User Table for each active user affected by the request. If the request is broadcast, the next time the user completes a CICS task, all scheduled messages for that user are displayed.

Note: The Interval Monitor executes at an interval you specify from the ERI/CICS Controls panel. Using the default value of one minute, it could take up to a minute before a send or drop request is complete.

Broadcast Message Security

CICS-View includes several layers of security. To access the Broadcast Message Menu Interface, the administrator must have access to tranid ERVB. To create and send messages to all users, the administrator must have access to program resource ERIALL. Note that when the LIST control field is blank, the default value is ERIALL; send to all users. When a LIST name is entered, than a security check is performed against the entered list name. The LIST name must be defined as a CICS program. Authorization to this program resource is controlled by your External Security Manager (ESM), such as RACF or ACF2.

Note: If you access the Broadcast Message Menu Interface via the ERI/CICS Manger panels or tranid ERIV, security checking is bypassed.

To access the Broadcast Message Command Interface, the administrator or software product must have access to tranid ERBC.

Broadcast Message Command Interface

The Broadcast Message Command Interface provides access to the Broadcast Facility from a parameter driven CICS transaction, ERBC. Using ERBC, you can generate and broadcast new messages or broadcast previously stored messages. Table 4-7 summarizes the parameters that transaction ERBC supports.

Table 4-7 Broadcast Command (ERBC) Parameter Summary

Parameter	Description	Default
MID=xxxxxxxx	Message identifier	EBCM0nnn
TXT=’msg text’	Text of new message	none
SDT=mm/dd/yyyy	Start date	Current date
STM=hh:mm	Start time	Current time
EDT=mm/dd/yyyy	Expiration date	Current date
ETM=hh:mm	Expiration time	23:59

Table 4-7 Broadcast Command (ERBC) Parameter Summary (Continued)

Parameter	Description	Default
DEL=Y or N	Drop message on ERI/CICS initialization	Y
SSN=Y or N	Send message to eligible users at sign on	Y
USR=uuuuuuuu	Userid filter	none
TRM=tttt	Terminal id filter	none
TRN=xxxx	Transaction id filter	none
LUN=vvvvvvvv	VTAM LU name filter	none
OPR=AND or OR	Filter operator	AND
LST=Program id	Program name that identifies a predefined list of users	none

Detailed information about each parameter is included in the Broadcast Message Menu Interface Section.

Required ERBC Parameters

When using ERBC, you must specify MID=, TXT=, or both. If MID= is specified without TXT=, it refers to a previously stored message. If TXT= is specified without MID=, a message id is generated to store the new message. If both MID= and TXT= are specified, the new message is stored with the provided message id.

Note: Generated message ids have the form EBCM0xxx, where xxx is a value from 001 to 200. The administrator is responsible for deleting generated message ids that are no longer needed.

The first character following TXT= is treated as a delimiter. All data between that character and the next occurrence of that character are treated as message text. Be sure to choose a character that does not occur in your message.

If you specify MID= without TXT=, the message id you provide must identify a message that has already been saved. If you specify both MSG= and TXT=, the message id you provide must not identify a message that has already been saved.

Examples:

```
ERBC TXT=’This is a test’

ERBC MID=TEST0001,TXT=’This is message TEST0001’

ERBC MID=TEST0002 TXT=/It’s time to read your messages/
```

Optional ERBC Parameters

There are additional, optional, parameters that you can use to control when your message will be broadcast, when it expires, and who receives it.

Examples:

```
ERBC TXT='This message will first be sent on 1 January, 1997, at 10:00 AM, and
will not be sent after 1 February, 1997 at 10:00PM',SDT=01/01/1997,STM=10:00,E
DT=02/01/1997,ETM=22:00"
```

```
ERBC TXT=/This message is for all users at terminals that have a 'T' in the first
character of the CICS terminal id/TRM=T***
```

User Count Information

The CICS-View screen includes three user counts recorded by ERI/CICS. They are:

User Count	The number of currently active sessions.

Lock Count	The number of active sessions that are currently locked by CICS-Lock.

Peak Count	The peak number of active users recorded by ERI/CICS and the time that the peak occurred. ERI/CICS writes this value to the ERI/CICS log during ERI/CICS Start of Day processing or product shutdown. The value is reset at ERI/CICS initialization and ERI/CICS Start of Day processing.

Requesting Help

Help is available from both the User Table panel and Search Options window. To request help, press F1/F13 or enter HELP on the command line. Help appears as a pop-up window and provides context sensitive information including an overview, available commands, and supported options.

End of Chapter 4

Chapter 5
Customizing ERI/CICS with User Exits and User Tables

ERI/CICS contains user exit points that you can use to customize the product. At these exit points, ERI/CICS issues CICS Link commands to several modules. You can replace these modules with your own programs. Your exit programs must be CICS command level and must be AMODE 31. ERI provides skeleton exit programs in the COPYLIB product distribution file.

There are six user exit points in the current release of ERI/CICS:

- ❑ The Password Verification Exit (ERIXPWP0), which enables you to write your own routine for verifying user passwords.
- ❑ The Lock Parameter Exit (LCKPRMP0), which enables you to customize lock and disconnect interval processing at the individual user level.
- ❑ The custom Sign-off Exit (ERICSFPO), which enables you to customize sign-off procedures.
- ❑ The custom Sign-on Exit (ERICSNPO), which supports custom sign-on procedures.
- ❑ CICS-SSO Session Pass Exit (ERIPASPO), which enables you to dynamically change CICS-SSO pass parameters or customize access to an application.
- ❑ The CICS-DupS User Temporary Storage (TS) Exit (ERIUTSPO), which enables you to pass a list of application TS queue names to the CICS-DupS Swap facility.The list of queues will be included in the back-up and recovery process.

At the table reference points, ERI/CICS issues CICS Load commands for modules that you can generate with values unique to your installation. In the current release of ERI/CICS, there are two user tables:

- ❑ The Transaction Time-out Table (LCKTRNTB), which enables you to customize lock and disconnect interval processing by transaction id.
- ❑ The Session Limit Table (ERIDUPTB), which enables you to customize CICS-DupS session limits by userid.

Password Verification Exit (ERIXPWP0)

The password verification exit (ERIXPWP0), allows you to use your own routine for verifying user passwords. It is provided for customers who have their own security system or security software not supported by ERI/CICS. Two versions of a skeleton exit program are distributed in COPYLIB:

ERIXPWP, an assembler source module; and ERIXPNPC, a COBOL source module.

ERIXPWP0 is invoked with a CICS LINK command from program LCKTMOP0 and receives control with the 20-byte COMMAREA shown below.

Byte	Description
1-8	Userid from CICS INQUIRE TERMINAL
9-16	Password entered by user
17-20	Return code

If you modify or replace this module, your program must update the return code before executing a CICS RETURN command. If your program sets the return code to a value other than zero, CICS-Lock sends a message to the user and writes a record to the log. The user is permitted a maximum of three password attempts. After three failures, the device is disconnected.

Your exit program load module name must be ERIXPWP0. The distributed PPT and RDO definitions for this program specify assembler. If your program is coded in another language you must update the definition.

Lock Parameter Exit (LCKPRMP0)

The Lock parameter exit (LCKPRMP0), enables you to set lock intervals and disconnect intervals for individual users as they are initialized to ERI/CICS. It is provided primarily for customers who maintain user profiles containing this information in an external source.

Global values for lock and disconnect intervals are specified in the Lock Manager dialog. These global values apply by default to all users in a CICS Terminal Owning Region or standalone region. LCKPRMP0 is invoked when a user is initialized to ERI/CICS and may be replaced with a program that sets values to override the installation defaults.

LCKPRMP0 is invoked with a CICS LINK command and receives control with the 12-byte COMMAREA shown below.

Byte	Description
1-8	Userid from CICS INQUIRE TERMINAL
9-10	Lock interval applied for this user
11-12	Disconnect interval applied for this user
13-16	Termid

Lock and disconnect intervals are expressed in minutes. The following values have special meaning.

Value	Meaning
-1	Use CICS-Lock default interval
0	Bypass processing for this interval type. In lock interval, never lock this user In disconnect interval, never disconnect this user
1-1440	Interval in minutes

If an invalid value is specified, the default is used.

Table 5-1 shows how the global values specified in the Lock manager dialogue and the individual user values set in LCKPRMP0 interact. A value of 0 for either MGRVAL or PRMVAL results in no locking.

Table 5-1 Interaction of Global and Individual User Values

Lock Manager Value (MGRVAL)	LCKPRMP0 Exit Value (PRMVAL)	➩	Value Used at Execution Time
0	Any	➩	0 (Never Lock)
Any	0	➩	0 (Never Lock)
999	-1	➩	0 (Never Lock)
1 - 998	-1	➩	MGRVAL
1 - 999	1 - 1440	➩	PRMVAL

Your exit program load module name must be LCKPRMP0. The distributed PPT and RDO definitions for this program specify assembler. If your program is coded in another language you must update the definition.

Session Pass Exit (ERIPASP0)

The session pass exit (ERIPASP0), allows the administrator to customize access to applications defined to CICS-SSO. This exit provides for another level of security for the application, and allows an administrator to dynamically change CICS-SSO profile parameters. Two versions of a skeleton exit program are distributed in ERI.COPYLIB. ERIPASPA is an Assembler source module; ERIPASPC is a Cobol source module.

ERIPASP0 is invoked with a CICS LINK command at two points:

PREPASS This exit point is right before the CICS session is to be passed to another CICS region if the application resides in another APPLID, or before the application is invoked if it resides in the same CICS region.

POSTPASS This exit point occurs right after the CICS session has been passed to another CICS region.

The ERIPASX0 program is called with the following COMMAREA.

Byte	Description
1 - 8	Exit Point PREPASS/POSTPASS
9 - 16	User ID from CICS INQ TERM
17 - 24	VTAM APPLID of Application
25 - 32	Application Tranid or Program name
33 - 38	Transfer Mode Link/XCTL/ Start...
39 - 116	Application Data
117 - 120	Return Code

Gaining control at these two entry points gives the administrator the ability to effect how the application will be invoked and to further control access to the application. The sample exit explains the action taken when you set the return code to a value other than zero and also the effect it has on the users SIGN-ON status.

Your exit program load module name must be ERIPASP0. The distributed PPT and RDO definitions for this program specify assembler. If your program is coded in another language you must update the definition.

Transaction Time-Out Table (LCKTRNTB)

The ERI/CICS transaction time-out table (LCKTRNTB) enables you to set lock intervals and disconnect intervals, based on transaction ids. To implement these intervals, you must create a transaction table module. This section, along with the sample program LCKTRNTB, provide guidelines for creating a module.

ERI/CICS queries your transaction time-out table by issuing a CICS LOAD command for program LCKTRNTB. If LCKTRNTB is found, the table entries are used by the lock and disconnect expiry analysis code.

The values you specify in the transaction table are applied only when automatic locking occurs. The table is not used when user-initiated locks (from the LOCK transaction or Hot Key) are processed. Also note that any exclusions you specify in the Lock Manager dialog override transaction table entries.

Transaction table entries are shown below.

Byte	Description
1-4	Transaction id
5-6	Lock interval applied for this transaction
7-8	Disconnect interval applied for this transaction

Lock and disconnect intervals are expressed in minutes. The following values have special meaning.

Value	Meaning
-1	Use the interval associated with the user
0	Bypass processing for this interval type. In lock interval, never lock this transaction In disconnect interval, never disconnect this transaction
1-1440	Interval in minutes

If you specify an invalid interval, ERI/CICS ignores the value and performs lock and disconnect processing as though the table had no entry for the target transaction id.

Here is a sample entry for the transaction TEST with a lock interval of 10 minutes and a disconnect interval of 1 hour.

```
DC    CL4’TEST’,H’10’,H’60’
```

Table 5-1 shows how the values specified in the transaction table interact with the global values from the Lock Manager dialog and the individual user values set in the Lock parameter exit, LCKPRMP0.

Table 5-2 Interaction of Global, Individual User, and Transaction Interval Values

Lock Manager Value (MGRVAL)	**Lock Param Exit (PRMVAL)**	**Trans Table (TRNVAL)**	⇨	**Value Used at Execution Time**
0	Any	Any	⇨	0
Any	0	Any	⇨	0
Any	Any	0	⇨	0
999	-1	-1	⇨	0
999	-1	1 - 1440	⇨	TRNVAL
1 - 998	-1	-1	⇨	MGRVAL
1 - 998	-1	1 - 1440	⇨	TRNVAL
1 - 999	1 - 1440	-1	⇨	PRMVAL
1 - 999	1 - 1440	1 - 1440	⇨	TRNVAL

Here are some requirements for coding and implementing a transaction time-out module.

❑ The name of your transaction table must be LCKTRNTB.

❑ LCKTRNTB must be an assembler program.

❑ LCKTRNTB must not contain any code except the table entries as described in this section and illustrated in the sample program.

❑ You must define program LCKTRNTB to CICS in your CSD or PPT. We suggest that you define the program as resident.

Session Limit Table (ERIDUPTB)

The ERI/CICS session limit table (ERIDUPTB) enables you to set session limits based on userids. To implement these limits, you must create a session limit table module. This section, along with the sample program ERIDUPTB, provide guidelines for creating a module.

ERI/CICS queries your session limit table by using a CICS LOAD command for program ERIDUPTB. If ERIDUPTB is found, the table entries are used by the CICS-DupS session limit analysis code. Note that any exclusions you specify in the CICS-DupS Manager dialog override session limit table entries.

The session limit table entries are shown below.

Byte	Description
1-8	Userid from CICS INQUIRE TERMINAL
9-10	Session limit applied for this user

If you specify an invalid session limit, ERI/CICS ignores the value and performs session limit processing as though the table had no entry for the target userid.

Here is a sample entry for the userid ERIUSR1 with a session limit of 4.

```
      DC    CL8’ERISUER1’,CL2’04’
```

Here are some requirements for coding and implementing a session limit module.

- The name of your session limit table must be ERIDUPTB.
- ERIDUPTB must be an assembly language program.
- ERIDUPTB must not contain any code except the table entries as described in this section and illustrated in the sample program.
- You must define program ERIDUPTD to CICS in your CSD or PPT. We suggest that you define the program as resident.

End of Chapter 5

Appendix A
ERI/CICS Messages

Please see separate document on the ERI Website.

- - - Message Guide - - -

Index