

zSecure CICS Toolkit

*User Guide*



**Note**

Before using this information and the product it supports, read the information in [“Notices” on page 115.](#)

**November 2025**

This edition applies to IBM® zSecure CICS® Toolkit 3.2.0 (product number 5655-ABD) , and to all subsequent releases and modifications of this product until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 1988, 2025.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>About this publication.....</b>	<b>vii</b>
IBM zSecure library.....	vii
Related documentation for zSecure (z/OS).....	ix
Accessibility.....	xi
Technical training.....	xi
Support information.....	xi
Statement of Good Security Practices.....	xi
<b>Chapter 1. Introduction.....</b>	<b>1</b>
Application interface.....	1
Command interface.....	1
RRSF concerns.....	2
Dates before and after the year 2000.....	2
<b>Chapter 2. zSecure CICS Toolkit installation.....</b>	<b>3</b>
Installation and post-installation checklist.....	3
Sample JCL.....	4
Create and initialize SMP/E zones.....	5
Allocate TARGET and DLIB data sets.....	6
Update SMP/E DDDEFs.....	6
Receive the product.....	7
APPLY zSecure CICS Toolkit code.....	7
ACCEPT zSecure CICS Toolkit code.....	7
Install the SVC.....	7
Protect the SVC.....	8
Define SCQTLOAD as APF-authorized.....	8
Update the CICS startup JCL.....	8
zSecure CICS Toolkit enablement in PARMLIB.....	9
CQTPCNTL parameter definitions.....	9
Definitions of programs, mapsets, and transactions to CICS.....	9
Update CICS tables.....	10
Define the RACF profiles.....	11
Automatic assignment of UIDs (OMVS AUTOUID).....	17
Automatic creation of home directories (OMVS MKDIR).....	17
zSecure CICS Toolkit restart.....	17
RTST transaction definition.....	18
Manual restart of the zSecure CICS Toolkit subtasks.....	19
Additional considerations.....	19
Globalization.....	19
<b>Chapter 3. Parameters for zSecure CICS Toolkit .....</b>	<b>21</b>
Parameter Descriptions.....	21
CQTPCNTL parameter values verification.....	23
<b>Chapter 4. Application security management.....</b>	<b>25</b>
Operator ID or OPID check.....	25
Application conversion.....	25
Resource profile definitions.....	26
Alternative simple application security interface.....	27
User information retrieval.....	27

Resource access verification.....	28
-----------------------------------	----

**Chapter 5. The zSecure CICS Toolkit command interface..... 29**

Navigating the Main menu.....	29
Adding, altering, or deleting a group (ADDGROUP, ALTGROUP, or DELGROUP command).....	30
Adding a user profile (ADDUSER command).....	31
Changing a profile (ALTUSER command).....	32
Altering the CICS segment for a user (ALTUSER CICS SEGMENT).....	34
Altering the TSO segment for a user (ALTUSER TSO SEGMENT).....	35
Altering the OMVS segment for a user (ALTUSER OMVS SEGMENT).....	37
Altering the WORKATTR segment for a user (ALTUSER WORKATTR SEGMENT).....	39
Connecting a user or group to a group (CONNECT command).....	40
Managing CSDATA fields (CSDATA command).....	41
Deleting a data set (DELETE DATASET command).....	43
Deleting a user profile.....	44
Listing the profile for one or more data sets (LISTDSET command).....	45
LISTDSET Display Example.....	47
Toggling the LISTDSET panel.....	47
Viewing the users authorized, their access authority and access count (LISTDSET USERIDS).....	48
Viewing the program/userid combination (LISTDSET Programs).....	49
Listing the profile for one or more groups (LISTGROUP command).....	49
LISTGROUP Display Example.....	51
Toggling the LISTGROUP panel.....	52
Listing users for a group (LISTGROUP command, USERIDS option).....	52
Deleting user IDs from a LISTGROUP.....	53
Listing the subgroups of a group.....	54
Listing the profiles for a user ID (LISTUSER command).....	55
LISTUSER Display Example.....	58
Toggling the LISTUSER panel.....	59
Listing groups for a user ID (LISTUSER command, GROUPS option).....	59
Listing categories for a user ID (LISTUSER command, Categories option).....	60
Listing the TSO and CICS segments for a user ID (LISTUSER command, Segments option).....	61
Granting or removing access to a resource (PERMIT command).....	62
Maintaining associations (RACLINK command).....	63
Listing and maintaining profiles in a general resource class (RALTER / RDEFINE / RDELETE commands).....	65
Removing user IDs or groups from a group (REMOVE command).....	66
Listing the profiles for a general resource class (RLIST command).....	66
RLIST Display Example.....	68
Listing the members in a profile (RLIST command, MEMBERS option).....	69
Listing user IDs in a profile and the access they have (RLIST command, USERS option).....	70
Listing users/groups in the conditional access list for a profile (RLIST command, CONDACC option).....	70
Managing USRDATA fields (USRDATA command).....	71

**Chapter 6. zSecure CICS Toolkit exit points specifications..... 75**

**Chapter 7. Application programming interface (API)..... 77**

SMF records that zSecure CICS Toolkit created.....	77
Command requests using the COMMAREA.....	78
Change the authorized user.....	79
Perform a search.....	79
Implementing field or record level security.....	79
Access Authority Check function.....	80
Access Authority Check (Extended) function.....	81
Resource Profile List function.....	82
TSQUEUE usage for profiles.....	86

Return and Reason codes.....	86
Access check and DATA retrieval (RSRD).....	86
Retrieval of USERDATA.....	86
Definitions of USERDATA entries.....	88
Additional considerations.....	88
Use of RACLIST exits.....	89
API specification.....	90
Installation considerations.....	91
ADDGROUP / ALTGROUP / DELGROUP function (add, alter, or delete a group).....	92
ADDUSER function (add user profile).....	93
ALTUSER function (changing a profile).....	94
ALTUSER (CICS SEGMENT) function (alter CICS segment).....	95
ALTUSER (TSO SEGMENT) function (change TSO segment).....	95
ALTUSER (OMVS SEGMENT) function (change OMVS segment).....	96
ALTUSER (WORKATTR SEGMENT) function (change WORKATTR segment).....	97
CONNECT function (connect a user or group to a group).....	97
CSDATA function (list and maintain CSDATA fields).....	98
DELETE DATASET function (delete data set profile).....	100
DELETE USERID function (delete user profile).....	100
LISTDATASET function (list profile for one or more data sets).....	100
LISTGROUP function (list profile for a group).....	102
LISTUSER function (list profile for a user ID).....	103
PASSWORD function (change password).....	105
PERMIT function (grant or remove access).....	106
PERMITX function (grant or remove access - any resource).....	106
RACLINK function (define, list, undefine, or approve user associations).....	107
REMOVE function (remove user IDs or groups from a group).....	108
RALTER/RDEFINE/RDELETE function (list and maintain profiles).....	108
RLIST function (list profiles for general resource class).....	109
USRDATA function (list and maintain users' USRDATA fields).....	111
VERIFY function (verify user ID and password or phrase).....	112
Sample programs.....	113
Simple API interface.....	113
Resource Profile List Interface.....	113
<b>Notices.....</b>	<b>115</b>
Trademarks.....	116
<b>Index.....</b>	<b>119</b>



# About this publication

---

The IBM zSecure CICS Toolkit enhances CICS/RACF® security features by enabling you to issue RACF commands directly from CICS and eliminating the need to use TSO. Application programs can also use IBM zSecure CICS Toolkit for security features instead of relying on internal application security functions. In this manner, all security definitions can be maintained centrally, or distributed among security coordinators.

This publication describes the two components of the IBM zSecure CICS Toolkit: the applications programming interface (API) and the command interface. It explains how to install and use this product.

This publication is intended for the following people:

- Systems support personnel responsible for the installation of IBM zSecure CICS Toolkit.
- CICS Security administrators responsible for implementing the additional RACF command controls provided by IBM zSecure CICS Toolkit.
- Application designers and programmers who are creating CICS applications that must check or manage RACF authorizations or profiles.

Readers must also be familiar with performing security and administration tasks in a CICS environment and with RACF concepts and commands.

For error messages, explanations, and workarounds where applicable, see *IBM zSecure: Messages Guide*.

## IBM zSecure library

---

This topic lists the IBM zSecure user information.

The zSecure library is available at [IBM zSecure documentation \(z/OS®\)](#).

The zSecure products library consists of the following topics:

- *About This Release*  
Provides information about new features and enhancements, incompatibility warnings, and documentation update information for this product version.
- *Documentation*  
Lists and briefly describes the zSecure products library and related documentation.
- *Program Directories*  
Are also provided with the installation media. For the list, see [Program Directories](#).
- *zSecure CARLa-Driven Components Installation and Deployment Guide*  
Provides information about installing and configuring the following zSecure components and IBM Z Security and Compliance Center:
  - IBM zSecure Admin
  - IBM zSecure Audit for RACF, Broadcom-ACF2, and Broadcom-Top Secret
  - IBM zSecure Alert for RACF and Broadcom-ACF2
  - IBM zSecure Adapters for SIEM for RACF, Broadcom-ACF2, and Broadcom-Top Secret
- *zSecure Messages Guide*  
Provides a message reference for all IBM zSecure products and components. This guide describes the message types associated with each product or feature, and lists all IBM zSecure product messages and errors along with their severity levels sorted by message type. This guide also provides an explanation and any additional support information for each message.
- *zSecure Admin and Audit for RACF Getting Started*  
Provides a hands-on guide introducing IBM zSecure Admin and IBM zSecure Audit product features and user instructions for performing standard tasks and procedures. This manual is intended to help new

users develop both a working knowledge of the basic IBM zSecure Admin and Audit for RACF system functionality and the ability to explore the other product features that are available.

- *zSecure Admin and Audit for RACF User Reference Manual*  
Describes the product features for IBM zSecure Admin and IBM zSecure Audit. Includes user instructions to run the admin and audit features from ISPF panels. This manual also provides troubleshooting resources and instructions for installing the zSecure Collect for z/OS component.
- *IBM zSecure Admin and Audit for RACF Line Commands and Primary Commands Summary*  
Lists the line commands and primary (ISPF) commands with very brief explanations.
- *zSecure Audit for ACF2 Getting Started*  
Describes the zSecure Audit for Broadcom-ACF2 product features and provides user instructions for performing standard tasks and procedures such as analyzing Logon IDs, Rules, Global System Options, and running reports. The manual also includes a list of common terms for those not familiar with ACF2 terminology.
- *zSecure Audit for ACF2 User Reference Manual*  
Explains how to use zSecure Audit for Broadcom-ACF2 for mainframe security and monitoring. For new users, the guide provides an overview and conceptual information about using Broadcom-ACF2 and accessing functionality from the ISPF panels. For advanced users, the manual provides detailed reference information, troubleshooting tips, information about using zSecure Collect for z/OS, and details about user interface setup.
- *zSecure Audit for Top Secret User Reference Manual*  
Describes the zSecure Audit for Broadcom-Top Secret product features and provides user instructions for performing standard tasks and procedures.
- *zSecure CARLa Command Language*  
Provides both general and advanced user reference information about the CARLa Auditing and Reporting Language (CARLa). CARLa is a programming language that is used to create security administrative and audit reports with zSecure.  
**Note:** Before September 2023, this content was chapter 1 in the former *zSecure CARLa Command Reference*.
- *zSecure CARLa SELECT/LIST Fields*  
Provides detailed information about the NEWLIST types and fields for selecting data and creating zSecure reports.  
**Note:** Before September 2023, this content was chapter 2 in the former *zSecure CARLa Command Reference*.
- *zSecure Alert User Reference Manual*  
Explains how to configure, use, and troubleshoot IBM zSecure Alert, a real-time monitor for z/OS systems protected with the Security Server (RACF) or Broadcom-ACF2.
- *zSecure Command Verifier User Guide*  
Explains how to install and use IBM zSecure Command Verifier to protect RACF mainframe security by enforcing RACF policies as RACF commands are entered.
- *zSecure CICS Toolkit User Guide*  
Explains how to install and use IBM zSecure CICS Toolkit to provide RACF administration capabilities from the CICS environment.
- *Support for problem solving*  
Solutions to problems can often be found in IBM knowledge bases or a product fix might be available. If you register with IBM Software Support, you can subscribe to IBM's weekly email notification service. IBM Support provides assistance with product defects, answers frequently asked questions, and helps to resolve problems.

## Program Directories

Program directories are provided with the installation media. You can also find the latest versions of the Program Directories at [IBM zSecure documentation](#).

- *IBM zSecure CARLa-Driven Components Program Directory (5655-ABA/ABB/ABC/ABG), GI13-5260*  
This program directory is intended for the systems programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM zSecure CARLa-Driven Components: Admin, Audit, Alert, and the IBM zSecure Adapters for SIEM.
- *IBM zSecure IBM zSecure CICS Toolkit Program Directory (5655-ABD), GI13-5265*  
This program directory is intended for the systems programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM zSecure CICS Toolkit.
- *IBM zSecure Command Verifier Program Directory (5655-ABE), GI13-5267*  
This program directory is intended for the systems programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM zSecure Command Verifier.
- *IBM zSecure Admin RACF-Offline,*  
This program directory is intended for the systems programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of the IBM zSecure Admin RACF-Offline component of IBM zSecure Admin.
- Program Directories for the zSecure Administration, Auditing, and Compliance solutions and IBM Z Security and Compliance Center:
  - *IBM zSecure Administration V3.2.0 Program Directory (5655-ABB), GI13-5276*
  - *IBM zSecure Compliance and Auditing V3.2.0 Program Directory (5655-ABI), GI13-5277*
  - *IBM zSecure Compliance and Administration V3.2.0 Program Directory (5655-ABJ), GI13-5278*
  - *IBM Z Compliance and Auditing V3.2.0 Program Directory (5655-ABK), GI13-5279*
  - *IBM Z Compliance, Auditing and Administration V3.2.0 Program Directory (5655-ABL), GI13-5280*
  - *IBM Z Security and Compliance Center V1.3.0 Program Directory (5655-CC1), GI13-5249*
  - *IBM zSecure Compliance V3.2.0 Program Directory (5655-MCC), GI13-6904*

## Related documentation for zSecure (z/OS)

This section includes titles and links for information related to zSecure products.

See:	For:
<a href="#">IBM zSecure</a>	All IBM zSecure documentation intended for experienced IT professionals who are planning to install, configure, and deploy IBM zSecure. For information about what is specific for a release, system requirements, incompatibilities and so on, select the version of your choice and <i>About This Release</i> ; see "What's new" and "Release notes".
<a href="#">IBM Z® zSecure Compliance</a>	This document is intended for experienced IT professionals who are planning to install, configure, and deploy IBM Z Security and Compliance Center. See also <i>Keeping Up With Security and Compliance on IBM zSystems™</i> (Redbooks®) .
<a href="#">Documentation for z/OS</a>	Information about z/OS. This includes a list of <a href="#">PDF files available for z/OS</a> .
<a href="#">IBM Z Multi-Factor Authentication documentation</a>	Information about IBM Z Multi-Factor Authentication (MFA) documentation.

<b>See:</b>	<b>For:</b>
<a href="#">z/OS Security Server RACF publications</a>	Information about z/OS Security Server Information about z/OS Security Server Resource Access Control Facility (RACF). For information about the RACF commands, and the implications of the various keywords, see the <i>z/OS Security Server RACF Command Language Reference</i> and the <i>z/OS Security Server RACF Security Administrator's Guide</i> . You can find information about the various types of events that are recorded by RACF in the <i>z/OS Security Server RACF Auditor's Guide</i> .
<a href="#">QRadar® DSM Configuration Guide</a>	For more information about QRadar, see the <a href="#">IBM QRadar Security Intelligence Platform</a> documentation.
<a href="#">IBM CICS Transaction Server for z/OS documentation</a>	Information about CICS Transaction Server for z/OS.
<a href="#">IBM MQ</a>	Information about IBM MQ.
<a href="#">IBM Z NetView</a>	Information about IBM Z NetView.

The following list shows some of the most useful z/OS publications for use with zSecure

- *z/OS Communications Server: IP Configuration Guide*
- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Cryptographic Services ICSF Administrator's Guide*
- *z/OS Cryptographic Services ICSF System Programmer's Guide*
- *z/OS Integrated Security Services Enterprise Identity Mapping (EIM) Guide and Reference*
- *z/OS ISPF Dialog Developer's Guide and Reference*
- *z/OS MVS Initialization and Tuning Reference*
- *z/OS MVS Programming Authorized Assembler Services Reference, Vol. 1*
- *z/OS MVS Programming: Assembler Services Reference ABE-HSP*
- *z/OS MVS Programming: Assembler Services Reference IAR-XCT*
- *z/OS MVS Programming: Authorized Assembler Services Guide*
- *z/OS MVS Programming: Authorized Assembler Services Reference ALE-DYN*
- *z/OS MVS Programming: Callable Services for High Level Languages*
- *z/OS MVS Programming: Sysplex Services Guide*
- *z/OS MVS System Codes*
- *z/OS MVS System Commands*
- *z/OS MVS System Management Facilities (SMF)*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Auditor's Guide*
- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF System Programmer's Guide*
- *z/OS Unicode Services User's Guide and Reference*
- *z/OS UNIX System Services Messages and Codes*
- *z/OS UNIX System Services Planning*
- *z/Architecture® Principles of Operation*

## Accessibility

---

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

## Technical training

---

For technical training information, see the IBM Training and Skills website at [IBM Training](#).

For a list of formal customer education for IBM zSecure, see the [zSecure Course Offerings](#). This PDF file is part of the [zSecure - Learning](#) information, which also includes CARLa self studies and sample applications.

## Support information

---

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at [www.ibm.com/mysupport](http://www.ibm.com/mysupport).

## Statement of Good Security Practices

---

IT system security involves protecting systems and information through intrusion prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, or misappropriated or can result in misuse of your systems to attack others. Without a comprehensive approach to security, no IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a regulatory compliant, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products, or services to be most effective.

**Important:** IBM does not warrant that any systems, products, or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.



---

# Chapter 1. Introduction

The zSecure CICS Toolkit enhances the CICS and RACF security features that are used by many installations. With zSecure CICS Toolkit, security administrators can run RACF commands directly from CICS, eliminating the need to use TSO. Application programs can use zSecure CICS Toolkit for security features instead of having to rely on internal application security functions. In this manner, you can maintain all security definitions centrally or distribute them among security coordinators.

zSecure CICS Toolkit is divided into two parts: the application programming interface (API) and the command interface.

---

## Application interface

CICS systems and application programmers can use the zSecure CICS Toolkit API to check resource access, and issue RACF commands from a CICS application program.

The zSecure CICS Toolkit application programming interface (API) provides unique functions:

- Quickly check access to a list of resources.
- Obtain an overview of all the resources that a user has access to.
- List and manage user, group, and resource profiles in the RACF database.

These allow RACF administration functions by an installation-written application program. zSecure CICS Toolkit supports MRO environments and is easily installed, used, and maintained.

---

## Command interface

Central and local RACF administrators can use the command interface to run many RACF commands directly from CICS instead of TSO. The command interface provides greater distribution of certain capabilities and responsibilities to CICS users. It eliminates the need to use the TSO application and reduces CPU overhead.

**Note:** zSecure CICS Toolkit uses a unique concept for granting the user authority to run commands. For example, a user can be allowed to reset the password or resume a user without being able to perform other tasks that are normally available through the RACF GROUPSPECIAL authority. Using the zSecure CICS Toolkit functions, the user does not require the GROUPSPECIAL attribute and does not need to be connected to the group of the user that is being reset.

Using this methodology, the responsibility of simple user and resource administration can be decentralized to any other area with access to a CICS terminal. This enables central security personnel to perform other tasks and assist decentral administrators.

RACF protects both the transaction that is used to start the zSecure CICS Toolkit command interface and the Toolkit commands themselves. Even if there is no security on the zSecure CICS Toolkit transaction, the user must be *permitted* to the commands to run them. A user must also be *permitted* to have access to the target profile (for example the user ID for a password reset). The only exception is a user with the SPECIAL attribute or a user with access to the TOOLKIT.SPEC resource. For information about this resource, see [Chapter 2, “zSecure CICS Toolkit installation,” on page 3](#).

There are advantages to using the command interface for searches:

- You can use more extensive search masks to retrieve information about profiles.
- You have greater flexibility in the criteria that are used.

All changes to RACF profiles produce SMF records similar to those created by the TSO RACF commands.

## RRSF concerns

---

There is a significant difference between the zSecure CICS Toolkit actions and the TSO RACF commands.

All additions, updates, and deletions of RACF profiles that zSecure CICS Toolkit makes are done using either the RACROUTE or ICHEINTY interface. In the remainder of this manual, the function is called by the equivalent RACF command processor name. For example, when the manual talks about the API interface that connects a user to a group, it is called the CONNECT command. The actual processing is **not** the CONNECT command. Instead, it is a set of direct RACF database updates that has the same result as the RACF CONNECT command. Therefore, the updates are considered application updates. The difference between the TSO RACF command and the zSecure CICS Toolkit action is only apparent if you need propagation of updates through the RACF remote sharing facility (RRSF).

If you want to propagate the changes made by zSecure CICS Toolkit through RRSF, activate propagation of **application updates** through the operator RACF SET AUTOAPPL command either from the console, or through PARMLIB. You probably have already set the equivalent SET AUTODIRECT option to propagate RACF commands. For the automatic propagation of application updates, you must also define appropriate profiles in the RRSFDATA resource class. The profiles must allow propagation of the RACF updates that are made by the CICS region. The ID that needs access to the RRSFDATA profiles is the CICS region ID, and **not** the signed on user ID. For more information about the definition of appropriate RRSFDATA profiles, see the "Automatic Direction" section in "The RACF remote sharing facility (RRSF)" chapter in the *RACF Security Administrator's Guide*.

## Dates before and after the year 2000

---

When a date is specified for the REVOKEDATE and RESUMEDATE parameters, zSecure CICS Toolkit interprets the dates the same way as the corresponding RACF commands do.

The date format is *YYDDD*, where *YY* is the year and *DDD* is the day number.

- If the specification for *YY* is 71 or greater, the date is treated as being in the 20th century; for example, 1971.
- If the specification for *YY* is 70 or less, the date is treated as being in the 21st century; for example, 2070.

These rules also provide compatibility with previous releases.

## Chapter 2. zSecure CICS Toolkit installation

Systems support personnel can use the information in this chapter to install zSecure CICS Toolkit. Depending on your order, either z/OSMF or SMP/E is used for the installation process.

Before you begin the installation, see the *Program Directory: IBM zSecure CICS Toolkit* for information about the prerequisites. If you have ordered the product as CBPDO, see [“Installation and post-installation checklist” on page 3](#) for pointers to instructions for installation and post-installation tasks. If you have ordered the product as ServerPac, the install process requires installation and deployment of the portable software instance through z/OSMF. In that case, the SMP/E steps in the checklist have already been done.

### Installation and post-installation checklist

Systems support personnel responsible for installing zSecure CICS Toolkit can use the following checklist to perform installation and post-installation tasks.

If you are installing from ServerPac, all the target data sets are created as part of the z/OSMF deployment. You can continue with the post-installation steps, starting at Step 5 in the table. If you are installing from CBPDO, all steps in the table are required.

Step	Description	Instructions	Job name	Status
1	Load sample installation JCL.	<a href="#">“Sample JCL” on page 4</a>		
2a	Create and initialize SMP/E zones.	<a href="#">“Create and initialize SMP/E zones” on page 5</a>	CQTJSMPx (SCQTINST)	
2b	Allocate TARGET and DLIB data sets.	<a href="#">“Allocate TARGET and DLIB data sets” on page 6</a>	CQTJALL (SCQTINST)	
3	Update SMP/E DDEFs.	<a href="#">“Update SMP/E DDEFs” on page 6</a>	CQTJDDD (SCQTINST)	
4a	RECEIVE zSecure CICS Toolkit.	<a href="#">“Receive the product” on page 7</a>	CQTJREC (SCQTINST)	
4b	APPLY zSecure CICS Toolkit.	<a href="#">“APPLY zSecure CICS Toolkit code” on page 7</a>	CQTJAPP (SCQTINST)	
4c	ACCEPT zSecure CICS Toolkit.	<a href="#">“ACCEPT zSecure CICS Toolkit code” on page 7</a>	CQTJACC (SCQTINST)	
5	Install the SVC.	<a href="#">“Install the SVC” on page 7</a>		
6	Protect the SVC.	<a href="#">“Protect the SVC” on page 8</a>	CQTJRDEF (SCQTSAMP)	
7	Define data sets as APF-authorized.	<a href="#">“Define SCQTLOAD as APF-authorized” on page 8</a>		
8	Update the CICS startup JCL.	<a href="#">“Update the CICS startup JCL” on page 8</a>		
9	Check product enablement through <b>IFAPRDxx</b> in PARMLIB.	<a href="#">“zSecure CICS Toolkit enablement in PARMLIB” on page 9</a>		

Table 1. Installation checklist (continued)

Step	Description	Instructions	Job name	Status
10	Update the <b>CQTPCNTL</b> parameters.	<a href="#">“CQTPCNTL parameter definitions” on page 9</a>	CQTJCNTL (SCQTINST)	
11	Define programs, mapsets, and transactions to CICS.	<a href="#">“Definitions of programs, mapsets, and transactions to CICS” on page 9</a>	CQTJRDO (SCQTSAMP)	
12	Update the CICS tables.	<a href="#">“Update CICS tables” on page 10</a>	CQTJPLT CQTJSRT (SCQTSAMP)	
13	Define RACF profiles to control access to zSecure CICS Toolkit functions.	<a href="#">“Define the RACF profiles” on page 11</a>	CQTJRDEF (SCQTSAMP)	
14	Grant additional authorizations to the CICS Started Task to setup OMVS UID and HOME directory for user IDs.	<a href="#">“Automatic assignment of UIDs (OMVS AUTOUID)” on page 17</a> and <a href="#">“Automatic creation of home directories (OMVS MKDIR)” on page 17</a>		
15	Restart zSecure CICS Toolkit.	<a href="#">“zSecure CICS Toolkit restart” on page 17</a>		

## Sample JCL

Systems support personnel responsible for installing zSecure CICS Toolkit can access the installation jobs from the SCQTINST and SCQTSAMP data sets or copy the jobs from the installation files.

The example jobs that can be used during installation are located in the SCQTINST and SCQTSAMP data sets that are part of the installed product. The SCQTINST data set contains examples for the SMP/E steps, and the SCQTSAMP data set contains examples for the post-install steps. To access the SMP/E examples, you can copy the data set from the installation files. For the CBPDO install, use the JCL in the figure below to create a copy of the SCQTINST library from the downloaded network files. You can use the TRANSFERONLY keyword on the RECEIVE command to stop SMP/E processing after the download of the package into the *ntsd*ir.

If you install from ServerPac, SMP/E processing has already been done, and there is no need to create a copy of the SCQTINST data set. After the z/OSMF deployment, you can continue with the post-install actions, starting at Step 5.

To copy the jobs from the downloaded network files, submit the following job. Add a job card and change the indicated parameters to values that meet your site requirements before you submit.

```

//STEP1 EXEC PGM=GIMUNZIP,REGION=M,PARM='HASH=NO'
//SYSUT3 DD UNIT=SYSALLDA,SPACE=(CYL,(1,1))
//SYSUT4 DD UNIT=SYSALLDA,SPACE=(CYL,(15,5))
//SMPJHOME DD PATH='/usr/lpp/java/J8.0/' <====NOTE 1
//SMPCPATH DD PATH='/usr/lpp/smp/classes/' <====NOTE 1
//SMPOUT DD SYSOUT=
//SYSPRINT DD SYSOUT=
//SMPDIR DD PATHDISP=KEEP,
// PATH='/ntsdire/orderid/SMPRELF/' <====NOTE 2
//SYSIN DD
<GIMUNZIP>
<ARCHDEF
name="CBCACHE.IBM.HCQT320.F2.pax.Z"
volume="volser" <====NOTE 3
newname="your-prefix.CQTINST"> <====NOTE 4
</ARCHDEF>
</GIMUNZIP>
//

```

Update the indicated lines using the following notes.

**Note:**

1. Change these directories to your installation's java and SMP classes directories.
2. Change *ntsdire* to the directory that holds your Shopz order.
3. Change *volser* to a volume name where you want the output data set to reside.
4. Change *your-prefix* to the high-level qualifier(s) for the output data set.

## Create and initialize SMP/E zones

Before starting the SMP/E installation, systems support personnel responsible for installing zSecure CICS Toolkit must decide on the SMP/E zones to use.

You can choose one of the following options:

- Install zSecure CICS Toolkit in new (dedicated) zones in a new CSI.  
This option is the only one for which sample jobs are provided.
- Install zSecure CICS Toolkit in new (dedicated) zones in an existing CSI.
- Install zSecure CICS Toolkit in existing zones in an existing CSI.

The sample jobs that are provided do not accommodate all possible combinations of CSIs and zones. The only option for which sample jobs are provided is the first option. The jobs can be used to set up a dedicated GLOBAL and PRODUCT CSI with dedicated TARGET and DLIB zones. For more information, see [“Performing pre-installation steps” on page 6](#).

The example jobs are provided in SCQTINST. Adapt the JCL and submit the jobs to complete the creation and initialization of the SMP/E environment. The jobs all use lowercase strings for the values that must be adapted to fit your installation standards. The following values are used.

### **Your-Global**

The data set prefix that you want to use for the GLOBAL SMP/E data sets. This prefix is used for the name of the GLOBAL CSI and for the SMP/E data sets shared between all SMP/E zones.

### **Your-Product**

The data set prefix that you want to use for the zSecure CICS Toolkit data sets. This data set prefix is also the prefix for the SMP/E data sets specific to zSecure CICS Toolkit.

### **sysallda**

The unit name that is used for all data set allocations.

### **volser**

The name of the DASD volume in your system where you want to create the zSecure CICS Toolkit data sets.

**Note:** In an SMS environment, the ACS routines might assign another volume than the one specified from the *volser*.

**Note:** The value for *Your-Global* cannot be the same as that for *Your-Product*. If you want to use similar prefixes, add an extra qualifier for the GLOBAL zone. For example, you might use the following two values:

- SMPE.TOOLKIT.GLOBAL as the value for *Your-Global*
- SMPE.TOOLKIT as the value for *Your-Product*

Use the following table to record the values for the installation variables suitable for your environment.

<i>Table 2. Pre-installation steps to define SMP/E zones</i>	
<b>Variable</b>	<b>Your Value</b>
<i>Your-Global</i>	
<i>Your-Product</i>	
<i>sysallda</i>	
<i>volser</i>	

## Performing pre-installation steps

Before beginning the installation, systems support personnel responsible for installing zSecure CICS Toolkit must define the required SMP/E zones.

### Procedure

1. Create a global CSI:

The sample job for creation of a new GLOBAL CSI is provided in member CQTJSMXA. This job also defines a GLOBAL zone in this new CSI.

- ▶ Adapt and submit job CQTJSMXA.

2. Create a product CSI:

The sample job for creation of a new product CSI is provided in member CQTJSMXB. This job also defines a TARGET and DLIB zone in this new CSI.

- ▶ Adapt and submit job CQTJSMXB.

3. Define an options entry for zSecure CICS Toolkit:

The sample job for defining an options entry specific for zSecure CICS Toolkit is provided in member CQTJSMXC. It specifies the utilities and the data set prefix to be used during the remaining SMP/E installation steps.

- ▶ Adapt and submit job CQTJSMXC.

## Allocate TARGET and DLIB data sets

Systems support personnel responsible for installing zSecure CICS Toolkit must allocate the TARGET and DLIB data sets.

zSecure CICS Toolkit adds six target data sets and six distribution data sets to your SMP/E environment. Example JOB CQTJALL contains the necessary JCL to allocate the required TARGET and DLIB data sets.

- ▶ Submit CQTJALL

## Update SMP/E DDDEFS

Systems support personnel responsible for installing zSecure CICS Toolkit perform this step to define to SMP/E the data sets that you allocated in the previous step. If you choose to include appropriate DD-statements in all of your SMP/E jobs, you can omit this step. If you want to use the suggested setup through dynamic allocation, this step is required. The example job CQTJDDD contains the JCL needed for this step.

The installation process also uses SMP/E CALLLIBS processing. This function is used to resolve external references during installation. When zSecure CICS Toolkit is installed, ensure that DDDEFs exist for the CSSLIB library.

**Note:** The DDDEFs are used only to resolve the link edit for zSecure CICS Toolkit with CALLLIBS. These data sets are not updated during the installation of zSecure CICS Toolkit. The provided sample job includes the required DDDEF.

- ▶ Submit job CQTJDDD.

## Receive the product

To RECEIVE the downloaded product, use the FROMNTS keyword to point to the directory that contains the SMP/E Modification Control Statements.

If you are installing from CBPDO, the SMPMCS file in the *ntsdir* directory contains the SMP/E Modification Control Statements that are needed for correct installation of zSecure CICS Toolkit.

- ▶ Submit job CQTJREC.

## APPLY zSecure CICS Toolkit code

Systems support personnel responsible for installing zSecure CICS Toolkit must add the code, examples, and documentation to the system.

The SMP/E statement that is needed is

```
APPLY GROUPEXTEND SELECT(HCQT320)
```

Because of the use of a SELECT for the product FMID, SMP/E does not require the use of the FUNCTIONS keyword. An example job is included in member CQTJAPP. Before you run this job, specify the data set name of your GLOBAL CSI.

- ▶ Submit the job CQTJAPP.

## ACCEPT zSecure CICS Toolkit code

If systems support personnel responsible for the installation of zSecure CICS Toolkit are satisfied with its implementation, they can ACCEPT the product. After you ACCEPT, the product is a part of your system.

zSecure CICS Toolkit does not normally cause any further systems programming work. An example ACCEPT job is provided in CQTJACC.

- ▶ Submit job CQTJACC.

## Install the SVC

Systems support personnel must install a type 3 SVC to be used for zSecure CICS Toolkit.

### Procedure

1. Include the SCQTLPA data set in your LPALSTxx member in PARMLIB. You can also copy SCQTSVC00 from the supplied SCQTLPA to an existing LPALIST data set, for example, SYS1.LPALIB.
2. Determine the SVC number to be used for the zSecure CICS Toolkit SVC. In this example, use 222.
3. Perform the following steps:
  - a) Update the IEASVCxx member in PARMLIB with an entry to define the zSecure CICS Toolkit SVC. An example is `SVCPARM 222, REPLACE, TYPE(3), APF(NO), EPNAME(CQTSVC00)`
  - b) Perform an IPL to install the SVC into the system.

You can also use the SETPROG operator command to dynamically install the SVC. An example is

```
SETPROG LPA,ADD,MODNAME=CQTSVC00,DSNAME=TOOLKIT.SCQTLPA,SVCNUMDEC=222
```

If you install the SVC through SETPROG, the definition is not retained across an IPL.

4. Add the DFHSRT entry with the following format:

```
DFHSRT TYPE=SYSTEM, ABCODE=FXX, ROUTINE=DFHSRTRR
```

where *XX* is the hexadecimal number of the SVC.

For example, if the number assigned to the SVC is 222, the entry is FDE.

For more information about updating the DFHSRT table, see [“Update CICS tables” on page 10](#).

- Update the LPALST $xx$  and IEASVC $xx$  members and IPL your system.

## Protect the SVC

To prevent unauthorized use of the zSecure CICS Toolkit SVC, a RACHECK is issued from the SVC to ensure that the caller is authorized.

### About this task

Before CICS can use zSecure CICS Toolkit, it must be granted access through RACF.

### Procedure

1. Define the SVC to RACF with the **RDEFINE** command. You must use resource class FACILITY.

```
RDEFINE FACILITY TOOLKIT.SVC UACC(NONE)
```

2. Grant access to each CICS region that runs the toolkit code.

Use the following command:

```
PERMIT TOOLKIT.SVC CLASS(FACILITY) ID(userid) ACCESS(READ)
```

where *userid* is the ID of the CICS region.

A sample of the preceding RACF definitions is included in member CQJRDEF in SCQTSAMP.

## Define SCQTLLOAD as APF-authorized

The zSecure CICS Toolkit subtask programs perform the retrieval and updates to the profiles in the RACF database. Use of these RACF functions requires APF authorization.

The data set containing these subtask programs is SCQTLLOAD. This data set must be APF-authorized. To define SCQTLLOAD as APF-authorized, you must update the IEAAPF $xx$  or PROG $xx$  member in PARMLIB with the name of the SCQTLLOAD data set.

- Update PROG $xx$  and activate by operator command SET PROG= $xx$ .

## Update the CICS startup JCL

Several changes must be made to the CICS startup JCL.

### Procedure

1. Add the SCQTRPL data set that contains the zSecure CICS Toolkit programs and maps to the DFHRPL concatenation.

For example:

```
//DFHRPL DD DISP=SHR,DSN=APPL1.LOADLIB  
//      DD DISP=SHR,DSN=APPL2.LOADLIB  
//      DD DISP=SHR,DSN=APPL3.LOADLIB  
//      DD DISP=SHR,DSN=APPL4.LOADLIB  
//      DD DISP=SHR,DSN=CICS.TOOLKIT.SCQTRPL
```

2. The SCQTLLOAD data set contains the zSecure CICS Toolkit programs that are used as MVS subtasks. Add this data set to the CICS STEPLIB.
3. If you decide to add a zSecure CICS Toolkit loadlib to the STEPLIB concatenation, rather than copying the modules to an existing loadlib, you must also make that loadlib APF-authorized because *all* loadlibs in the CICS STEPLIB must be APF-authorized.

To define the zSecure CICS Toolkit loadlib as APF-authorized, you must update the IEAAPFxx or PROGxx member in SYS1.PARMLIB with the name of the zSecure CICS Toolkit loadlib.

An example of updating the JCL STEPLIB parameter:

```
//STEPLIB DD DISP=SHR,DSN=LOADLIB1
//          DD DISP=SHR,DSN=LOADLIB2
//          DD DISP=SHR,DSN=CICS.TOOLKIT.SCQTLLOAD
```

## zSecure CICS Toolkit enablement in PARMLIB

At startup of the zSecure CICS Toolkit tasks, zSecure CICS Toolkit verifies whether the product is enabled or disabled by IFAPRDxx in PARMLIB.

If the product is enabled or not defined in IFAPRDxx, initialization of zSecure CICS Toolkit continues normally.

If the product is disabled, a message (CQT907) is issued, and zSecure CICS Toolkit initialization is terminated. Disabling the product does not affect the remainder of CICS initialization.

To explicitly enable zSecure CICS Toolkit, include an entry such as the following one in an active IFAPRDxx member.

```
PRODUCT OWNER('IBM CORP')
        NAME('zSecure Toolkit')
        ID(5655-ABD)
        VERSION(*) RELEASE(*) MOD(*)
        STATE(ENABLED)
```

If you want to disable zSecure CICS Toolkit, create an entry like this one, and replace the parameter STATE(ENABLED) by the parameter STATE(DISABLED).

- ▶ Update IFAPRDxx and activate by operator command SET PROD=xx.

## CQTPCNTL parameter definitions

CQTPCNTL defines certain parameters that zSecure CICS Toolkit uses.

These parameters include the SVC number and the RACF resource class that is used. See [Chapter 3, “Parameters for zSecure CICS Toolkit,”](#) on page 21 for CQTPCNTL parameter definitions and information about customizing CQTPCNTL.

- ▶ Adapt CQTPCNTL and Submit CQTJCNTL.

After the definitions are made, transaction RTCK can be run to check the parameters in CQTPCNTL.

## Definitions of programs, mapsets, and transactions to CICS

You must define the programs, mapsets, and transactions that zSecure CICS Toolkit uses. The preferred method for these definitions is through CICS Resource Definition Online (RDO).

An example job to make these definitions is provided in member CQTJRDO in SCQTSAMP. You must define the following mapsets:

```
CQTBST0 CQTBCH0 CQTB000 CQTB100 CQTB200 CQTB300
CQTB400 CQTB500 CQTB550 CQTB560 CQTB580 CQTB590
CQTB600 CQTB700 CQTB800 CQTB860 CQTB900 CQTBAA0
CQTB000 CQTB000 CQTB000 CQTB000 CQTB000 CQTB000
```

You must define the following programs:

```

CQTPAPI0  CQTPAPPL  CQTPSNP0  CQTPATCH  CQTPCHEK  CQTPDTCH
CQTPLT00  CQTPSTRT  CQTP0000  CQTP0010  CQTP0020  CQTP0030
CQTP0031  CQTP0040  CQTP0041  CQTP0042  CQTP0043  CQTP0044
CQTP0050  CQTP0055  CQTP0056  CQTP0058  CQTP0059  CQTP0060
CQTP0070  CQTP0080  CQTP0081  CQTP0082  CQTP0083  CQTP0084
CQTP0086  CQTP0090  CQTP0091  CQTP0100  CQTP0110  CQTP0111
CQTP0112  CQTP0113  CQTP0114  CQTP0120  CQTP0130  CQTP0131
CQTP0132  CQTP0133  CQTP0134  CQTP0135  CQTP0136  CQTP0140
CQTP0160  CQTP0161

```

In addition to the regular executable programs, some modules contain data that is used by all zSecure CICS Toolkit programs. This data must be permanently available to all zSecure CICS Toolkit programs. You can make the data permanently available by defining these programs as *resident*. The following programs must be defined as resident programs:

```
CQTPAPRM  CQTPMSGE  CQTPCNTL
```

All the zSecure CICS Toolkit programs (both the regular programs and the resident programs) must be defined with EXECKEY(CICS).

In the precursor product Consul zToolkit, the programs that are part of the Application Programming Interface (API) used different names. If you have existing applications that use those names, you must also define three other programs. These programs are alias names of the new modules:

```
CRTKAPI  CRTKSNP  CRTKAPPL
```

To use the functions of zSecure CICS Toolkit interactive command interface, you must also define the online transactions. If you use only the functions from the API interface, definition of these transactions is not required. The following transaction must be defined for the following programs:

```

RTCK  --> PROG(CQTPCHEK)
RTST  --> PROG(CQTPSTRT)
RTMM  --> PROG(CQTP0000)

```

► Update and submit CQ TJRDO.

If you want these definitions to be active at startup, you must also include the *group* TOOLKIT in a *list* that is used to activate CICS resources.

## Update CICS tables

Follow the following steps to update CICS tables to suppress abends if the CICS Toolkit SVC is not installed, and to automatically start and stop the CICS Toolkit functions.

To avoid a CICS abend if the CICS Toolkit SVC is not available, you must add an entry to the CICS System Recovery Table (SRT).

- Add the following entry to your DFHSRT source:

```
DFHSRT TYPE=SYSTEM, ABCODE=Fxx, RECOVER=YES
```

For the exact definition of the parameter ABCODE=Fxx, see [“Install the SVC” on page 7](#). An example is provided in SCQTSAMP member CQTSRTT1.

- The SRT must be translated with the CICS table update procedure that is in use at your installation. Typically, the procedure is called DFHAUPLE, and it is in a data set named similarly to CICSTS61.XDFHINST. An example is provided in SCQTSAMP member CQ TJSRT.

► Adapt and submit CQ TJSRT.

It is possible to automatically start and stop the CICS Toolkit sub-tasks on CICS start and stop. If you do not want to automatically start and stop the sub-tasks, you can also use the RTST transaction as described in [“RTST transaction definition” on page 18](#). Automatic processing is activated through entries to the CICS Program List tables (PLT).

The PLT programs must be found during CICS startup. That means that the CQTPLT00 program must already be defined to CICS. The RDO example defines the resources, but does not automatically activate the definition. You must either include the TOOLKIT group in a list or ensure in some other way that the resource definition is active during CICS startup.

- Add the following entry to your PLTPI:

```
DFHPLT TYPE=ENTRY, PROGRAM=CQTPLT00
```

This entry must be placed after the DFHDELIM entry. An example is provided in member CQTPLTT1.

- Add the following entry to your PLTSD:

```
DFHPLT TYPE=ENTRY, PROGRAM=CQTPDTC
```

An example is provided in member CQTPLTT2.

- If you are installing into a CICS TS 5.4 or earlier release, you must translate the DFHPLT tables as described previously for DFHSRT. An example is provided in SCQTSAMP member CQTJPLT.
  - ▶ Adapt and submit CQTJPLT.
  - ▶ Verify and adapt the PLTPI and PLTSD specification in CICS SYSIN.
- If you are installing into a CICS TS 5.5 or later release, you must add the DFHPLT tables to the data set that is allocated to the DFHTABLE DD-statement.
  - ▶ Verify and adapt the PLTPI and PLTSD specification in CICS SYSIN.

## Define the RACF profiles

Follow these steps to use the zSecure CICS Toolkit RACF command interface to define RACF profiles.

### Overview

In this procedure, the following steps are required:

1. Define the zSecure CICS Toolkit commands to RACF.
2. Give the users access to the commands that they are allowed to use (ADDUSER, ALTUSER, DELUSER, and so on).
3. Define the subsequent levels of authority within those commands that the user can access. For example, after you give a user access to the ALTUSER command, you must specify which users they can alter.

Details of the steps are provided in the following sections.

### Procedure

1. Define the zSecure CICS Toolkit commands to RACF.

Table 3 on page 11 contains a list of the zSecure CICS Toolkit commands and the first and subsequent levels of authority that is required for each:

COMMAND	LEVEL	SUBSEQUENT LEVELS
ADDGROUP	TOOLKIT.ADGR	ADGR.grpname
ADDUSER	TOOLKIT.ADUS	ADUS.dfltgrp
ALTGROUP	TOOLKIT.ALGR	ALGR.grpname

<i>Table 3. zSecure CICS Toolkit commands: Required authorization levels (continued)</i>		
<b>COMMAND</b>	<b>LEVEL</b>	<b>SUBSEQUENT LEVELS</b>
<b>ALTUSER</b>	TOOLKIT.AUSR  When using the subfunctions to manage segments, access to TOOLKIT.ACIC, TOOLKIT.ATSO, TOOLKIT.AOMV, or TOOLKIT.AWRK is also required.	AUSR. <i>dfltgrp</i>  When you assign a shared UID in an OMVS segment, you also need either System-SPECIAL or access to SHARED.IDS in the UNIXPRIV class.
<b>CONNECT</b>	TOOLKIT.CONN	CONN. <i>grpname</i>
<b>DELDSD</b>	TOOLKIT.DELED	DELD. <i>hlq</i>
<b>DELGROUP</b>	TOOLKIT.DELG	DELG. <i>grpname</i>
<b>DELUSER</b>	TOOLKIT.DELU	DELU. <i>dfltgrp</i>
<b>LISTDATASET</b>	TOOLKIT.LDSD	None
<b>LISTGROUP</b>	TOOLKIT.LGRP	LGRP. <i>grpname</i>
<b>LISTUSER</b>	TOOLKIT.LUSR	LUSR. <i>dfltgrp</i>
<b>PASSWORD</b>	None	PSWD. <i>grpname</i>  The <b>PASSWORD</b> command is available only through the API.
<b>PERMIT</b>	TOOLKIT.PEMT	PEMT. <i>grpname</i> / <i>dfltgrp</i>  If the PERMIT is for a GROUP, PEMT. <i>grpname</i> is used. If it is for a USERID, then PEMT. <i>dfltgrp</i> is used.  When issuing a PERMIT, the user also requires access to the resource that is being given access to.  If the resource is in a class that is not defined in the CICS SIT, the user also needs access to PEMX. <i>cdtclass</i> .
<b>RACLINK</b>	TOOLKIT.RACL	RACL. <i>dfltgrp</i>
<b>RALTER</b>	TOOLKIT.RALT	RALT. <i>cdtclass</i>
<b>RDEFINE</b>	TOOLKIT.RDEF	RDEF. <i>cdtclass</i>
<b>REMOVE</b>	TOOLKIT.REMV	REMV. <i>grpname</i>
<b>RDELETE</b>	TOOLKIT.RDEL	RDEL. <i>cdtclass</i>
<b>RLIST</b>	TOOLKIT.RLST	RLST. <i>cdtclass</i>
<b>USRDATA</b>	TOOLKIT.USRL  When using the subfunctions to Add/Update/Delete, or when accessing these functions directly from the API, access to TOOLKIT.USRA or TOOLKIT.USRD is required.	USRU. <i>grpname</i>  USRN. <i>usrdata-name</i>

Table 3. zSecure CICS Toolkit commands: Required authorization levels (continued)		
COMMAND	LEVEL	SUBSEQUENT LEVELS
VERIFY	None  VERIFY is available only through the API and allows applications to verify a user's ID and password without the need for the user to sign on.	None

The following list clarifies the variables that were used in the preceding definitions:

- *grpname* is the GROUP name.
- *dfltgrp* is the DEFAULT GROUP name of the user ID.
- *hlq* is the high-level-qualifier of the data set name.
- *cdtclass* is the GENERAL RESOURCE CLASS name that is defined in the CDT.

Each command is defined to RACF as a resource in the class that is specified by RSRCLASS in CQTPCNTL.

It is best to define the following generic names first, with a UACC of NONE. This ensures that users are not given access to commands through other generic definitions within the resource class.

Assuming that the RSRCLASS parameter in CQTPCNTL is TCICSTRN:

```
RDEFINE TCICSTRN (TOOLKIT.* ADGR.* ADUS.* ALGR.* AUSR.*
CONN.* DELD.* DELG.* DELU.* LDSD.* LGRP.* LUSR.* PEMT.*
PSWD.* RACL.* RALT.* RDEF.* RDEL.* REMV.* RLST.*
USRJ.* USRN.*) UACC(NONE)
```

Define the zSecure CICS Toolkit commands to RACF with the **RDEFINE** command. This example also assumes that TCICSTRN is the RSRCLASS parameter.

```
RDEFINE TCICSTRN (TOOLKIT.ADGR TOOLKIT.ADUS TOOLKIT.ALGR TOOLKIT.AUSR
TOOLKIT.CONN TOOLKIT.DELD TOOLKIT.DELG TOOLKIT.DELU TOOLKIT.LDSD TOOLKIT.LGRP
TOOLKIT.LUSR TOOLKIT.PEMT TOOLKIT.REMV TOOLKIT.RACL TOOLKIT.RALT TOOLKIT.RDEF
TOOLKIT.RDEL TOOLKIT.RLST TOOLKIT.USRL TOOLKIT.USRA TOOLKIT.USRD)
```

2. Give the users access to the commands that they are allowed to use.

Access must be given to the ID that is running the transaction.

Permit users to each command as required. Examples:

```
PERMIT TOOLKIT.LUSR CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.AUSR CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.LDSD CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.LGRP CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.CONN CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.REMV CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.ADUS CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT TOOLKIT.PEMT CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
```

When using the RTMM transaction, only the commands that a user has access to are displayed on the primary panel. For example, if a user has access to only the LUSR command, none of the other commands are displayed.

3. Define the subsequent levels of authority within those commands that the user can access.

For example, after you have given a user access to the ALTUSER command, you must specify **which** users they can alter.

Most commands require one or more subsequent levels of authority to be given to a user. These next levels determine which users, groups, and resources the user can access or control after you have given the user access to a command.

For a list of security resources, see [“Resource names used for command authorization”](#) on page 14.

For example, if a user is granted access to ALTUSER through the TOOLKIT .AUSR resource, the IDs to which the user has access must also be defined. This is done by defining the default group of those users, prefixed with AUSR, as a resource. A user can then be granted access to this resource.

Table 4 on page 14 shows examples of definitions that are required to give this type of capability.

<i>Table 4. Example resource definitions used within RACF commands</i>		
<b>USERID</b>	<b>DEFAULT GROUP</b>	<b>RSRCLASS</b>
USER01	TECHSUPP	TCICSTRN
USER02	USERSUPP	TCICSTRN
USER03	QUALCNTL	TCICSTRN
USER04	AUDIT	TCICSTRN

The RACF command in this example:

```
RDEFINE TCICSTRN (AUSR.TECHSUPP AUSR.USERSUPP AUSR.QUALCNTL AUSR.AUDIT)
```

Then, permit users to each group:

```
PERMIT AUSR.TECHSUPP CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT AUSR.QUALCNTL CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
PERMIT AUSR.AUDIT CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
```

With these definitions, USER01 can perform an ALTUSER on all user IDs whose default group is TECHSUPP, QUALCNTL, or AUDIT, but not on user IDs whose default group is USERSUPP, or any other group.

## Resource names used for command authorization

zSecure CICS Toolkit uses resource names to determine if a user is authorized for a command.

Table 5 on page 14 lists the resource names that zSecure CICS Toolkit uses to determine if a user is authorized for a command.

<i>Table 5. zSecure CICS Toolkit: Command security resource list</i>	
<b>Resource name</b>	<b>What it allows if a user has READ access</b>
TOOLKIT.ADGR	Allows a user to run the ADDGROUP command of zSecure CICS Toolkit.
TOOLKIT.ADUS	Allows a user to run the ADDUSER command of zSecure CICS Toolkit.
TOOLKIT.ALGR	Allows a user to run the ALTGROUP command of zSecure CICS Toolkit.
TOOLKIT.AUSR	Allows a user to run the ALTUSER command of zSecure CICS Toolkit.
TOOLKIT.ACIC	Allows a user to manage CICS segments through the ALTUSER command of zSecure CICS Toolkit.
TOOLKIT.ATSO	Allows a user to manage TSO segments through the ALTUSER command of zSecure CICS Toolkit.
TOOLKIT.AOMV	Allows a user to manage OMVS segments through the ALTUSER command of zSecure CICS Toolkit.
TOOLKIT.AWRK	Allows a user to manage WORKATTR segments through the ALTUSER command of zSecure CICS Toolkit.

Table 5. zSecure CICS Toolkit: Command security resource list (continued)

Resource name	What it allows if a user has READ access
TOOLKIT.CONN	Allows a user to run the CONNECT command of zSecure CICS Toolkit.
TOOLKIT.DELD	Allows a user to run the DELETE DATASET command of zSecure CICS Toolkit.
TOOLKIT.DELG	Allows a user to run the DELETE GROUP command of zSecure CICS Toolkit.
TOOLKIT.DELU	Allows a user to run the DELETE USER command of zSecure CICS Toolkit.
TOOLKIT.DUPE	Allows a user to sign on at a second terminal but forces a signoff at the original terminal. Any transaction that is currently attached at the original terminal is also purged.
TOOLKIT.GPID	Allows a user ID to be used as a group ID so that more than one user can use it to sign on to CICS.
TOOLKIT.LDSD	Allows a user to run the LISTDATASET command of zSecure CICS Toolkit.
TOOLKIT.LGRP	Allows a user to run the LISTGROUP command of zSecure CICS Toolkit.
TOOLKIT.LUSR	Allows a user to run the LISTUSER command of zSecure CICS Toolkit.
TOOLKIT.PEMT	Allows a user to run the PERMIT command of zSecure CICS Toolkit.
TOOLKIT.RACL	Allows a user to run the RACLINK command of zSecure CICS Toolkit.
TOOLKIT.RALT	Allows a user to run the RALTER command of zSecure CICS Toolkit.
TOOLKIT.RDEF	Allows a user to run the RDEFINE command of zSecure CICS Toolkit.
TOOLKIT.RDEL	Allows a user to run the RDELETE command of zSecure CICS Toolkit.
TOOLKIT.REMV	Allows a user to run the REMOVE command of zSecure CICS Toolkit.
TOOLKIT.RLST	Allows a user to run the RLIST command of zSecure CICS Toolkit.
TOOLKIT.USRL	Allows a user to list usrdata fields as part of the USRDAT command of zSecure CICS Toolkit.
TOOLKIT.USRA	Allows a user to add and update usrdata fields as part of the USRDAT command of zSecure CICS Toolkit.
TOOLKIT.USRD	Allows a user to delete usrdata fields as part of the USRDAT command of zSecure CICS Toolkit.
TOOLKIT.SPEC	Gives a user the equivalent of SPECIAL, when running RACF commands from zSecure CICS Toolkit. Users who have access to TOOLKIT.SPEC are allowed access to all resources within a specific command. For example, if users have access to the LISTUSER command and TOOLKIT.SPEC, they can list <i>any</i> user. They are not restricted by the LUSR. <i>dfltgrp</i> definitions. While TOOLKIT.SPEC gives a user access to <i>all</i> resources within a command, it does not give the user access to the command itself. In this example, for the user to use the LISTUSER command, the user still requires access to TOOLKIT.LUSR. This applies only to RACF commands that are issued by the zSecure CICS Toolkit interactive interface.

Table 5. zSecure CICS Toolkit: Command security resource list (continued)

Resource name	What it allows if a user has READ access
TOOLKIT.SVC	Allows a region to use the zSecure CICS Toolkit SVC.
ADGR. <i>grpname</i>	Defines the groups for which a user can issue an ADDGROUP.
ADUS. <i>dfltgrp</i>	Defines the DFLTGRPs for which a user can issue an ADDUSER.
ALGR. <i>grpname</i>	Defines the groups for which a user can issue an ALTGROUP.
AUSR. <i>dfltgrp</i>	Defines the DFLTGRPs for which a user can issue an ALTUSER.
CONN. <i>grpname</i>	Defines the groups for which a user can issue a CONNECT.
DELD. <i>hlq</i>	Defines the high-level-qualifier of data set names for which a user can issue a DELETE DATASET. See <a href="#">“Deleting a data set (DELETE DATASET command)”</a> on page 43 for more details.
DELG. <i>grpname</i>	Defines the groups for which a user can issue a DELETE GROUP.
DELU. <i>dfltgrp</i>	Defines the DFLTGRPs for which a user can issue a DELETE USER.
LGRP. <i>grpname</i>	Defines the groups for which a user can issue a LISTGROUP.
LUSR. <i>dfltgrp</i>	Defines the DFLTGRPs for which a user can issue a LISTUSER.
PEMT. <i>dfltgrp / grpname</i>	Defines the regular groups or users with the DFLTGRPs for which a user can issue a PERMIT.
PEMX. <i>cdtclass</i>	Defines the general resource classes, including the DATASET class, for which a user can issue a PERMIT. The PEMX resource is only checked for non-CICS resource classes.
PSWD. <i>dfltgrp</i>	Gives authority to change a user's PASSWORD within the specified default groups.
RACL. <i>dfltgrp</i>	Defines the groups for which a user can issue a RACLINK.
RALT. <i>cdtclass</i>	Defines the general resource classes for which a user can issue an RALTER.
RDEF. <i>cdtclass</i>	Defines the general resource classes for which a user can issue an RDEFINE.
RDEL. <i>cdtclass</i>	Defines the general resource classes for which a user can issue an RDELETE.
REMV. <i>grpname</i>	Defines the groups for which a user can issue a REMOVE.
RLIST. <i>cdtclass</i>	Defines the general resource classes for which a user can issue an RLIST.
SECL. <i>nnn</i>	Specifies the SECLEVEL that a user can specify for IDs for which the user is authorized. The <i>nnn</i> is the SECLEVEL number from 001-254.
USRU. <i>dfltgrp</i>	Defines the DFLTGRPs for which a user can display USRDATA fields.
USRN. <i>usrdata-name</i>	Defines the <i>usrdata-names</i> that can that the user can display or manage.

## Automatic assignment of UIDs (OMVS AUTOUID)

If you want to use the automatic assignment of unique OMVS UIDs, you must ensure that the following requirements are fulfilled.

- The RACF database must be enabled for Application Identity Mapping. The minimum stage that is required is stage 2.
- The profile BPX.NEXT.USER in the FACILITY class must be defined, with appropriate APPLDATA. The details are described in the *RACF Security Administrator's Guide*. See the chapter *RACF and z/OS UNIX*.
- RACF TSO command usage of AUTOUID also requires that profile SHARED.IDS is defined and that the UNIXPRIV resource class is active and RACLISTed.

## Automatic creation of home directories (OMVS MKDIR)

If you want to automatically create a home directory when you create an OMVS segment for a user, the following extra requirements must be fulfilled.

- Because the OMVS home directory is case sensitive, you must ensure that your terminal currently supports mixed case. If your terminal is using uppercase only, the OMVS home directory as specified in the OMVS segment and the actual directory that zSecure CICS Toolkit created both use uppercase characters.
- The CICS region user ID must have an OMVS segment that assigns a UID.
- The current group of the CICS region user ID must have an OMVS segment that assigns a GID.
- The CICS region user ID must have sufficient access to create the home directories. It can be implemented by one of the following methods:

### **UID=0**

This option gives the CICS region full control over the entire z/OS UNIX environment. It is acceptable during initial testing, but is not suitable for a regular production environment.

### **UNIXPRIV**

You can also grant CONTROL access to the UNIXPRIV profile SUPERUSER.FILESYS. Because it gives the CICS region READ/WRITE access to all files in the file system, it is also not suitable for use in a production environment.

### **WRITE access to the directory where user home directories are created.**

This option gives the CICS region the exact authorization that is required. It is the preferred option.

If you do not grant UID=0 to the CICS region user ID, you must give the CICS region the authority to also set the correct owner for the newly created home directories. Failure to do so might render the new home directories unusable to the intended users. Set the correct owner with the CHOWN command, which typically requires authorization:

### **UNIXPRIV SUPERUSER.FILESYS.CHOWN**

Granting READ access to this profile allows changing the owner for all files in the system. Because it is a rather powerful authorization, it is better not to use this approach.

### **UNIXPRIV CHOWN.UNRESTRICTED**

This discrete profile enables all users to change the owner of files and directories that they own. It is similar to the way RACF handles DATASET profiles. Because zSecure CICS Toolkit creates the home directories initially with the CICS region as owner, it is authorized to change the owner to the intended user.

## zSecure CICS Toolkit restart

---

Normally, after making all the required updates and definitions for the installation, you must restart the CICS system to activate all the changes. For the initial installation, the restart is required to activate, for example, the SRT definitions. You can combine this activation with the system IPL that is required to pick up the definition of the zSecure CICS Toolkit SVC.

zSecure CICS Toolkit internally uses MVS subtasks. Normally, these subtasks are started during CICS initialization by a PLT program. These MVS subtasks are detached again at CICS termination by a second PLT program. Restarting CICS is the preferred method for this part of the installation process.

If all the required definitions are in place, but restarting CICS is not possible, you can use the following alternative method instead.

**Attention:** If you use this process to do the initial activation of zSecure CICS Toolkit, you must also use this process to deactivate it before you shut down the CICS system. Failure to do so results in A03 abends, probably followed by a system memory dump.

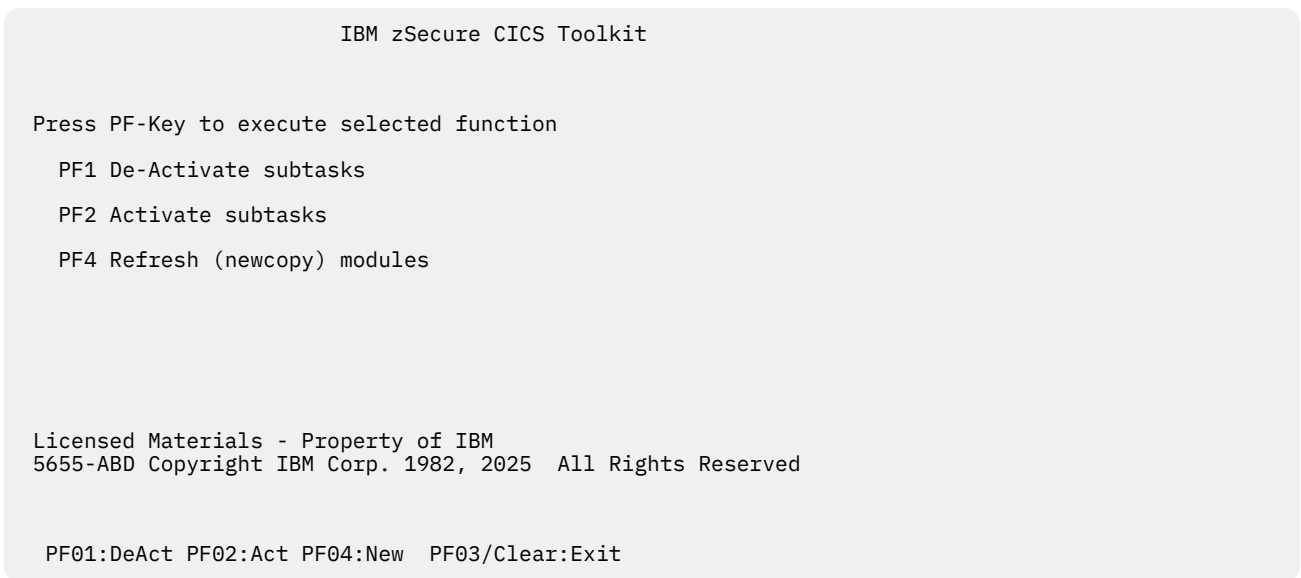
If the zSecure CICS Toolkit SVC is not installed, and the CICS SRT definition is not activated, attempts to install the software subtasks might result in a terminating abend of the CICS Started Task.

Sometimes, an error occurs during execution of the zSecure CICS Toolkit programs. Some of these errors result in the termination of one of the MVS subtasks that are used for zSecure CICS Toolkit processing. Current versions of the zSecure CICS Toolkit provide the RTST transaction for stopping and restarting the MVS subtasks. Previous versions require a manual process. This manual process is described in [“Manual restart of the zSecure CICS Toolkit subtasks” on page 19](#).

## RTST transaction definition

The RTST transaction can be defined to run the CRTKSTRT program. This program performs the necessary functions to stop and restart the zSecure CICS Toolkit subtasks. It also provides a function for refreshing the various zSecure CICS Toolkit programs, maps, and parameter modules.

When the RTST transaction is run, the following panel is displayed:



*Figure 1. RTST Transaction panel*

This panel provides the following functions:

### **PF1**

The currently active subtasks are terminated. Because this is done by a regular stop request to each task, it might take several seconds to run this function.

### **PF2**

Start the subtasks. Before starting the subtasks, the program verifies that the subtasks are not already active.

### **PF4**

Obtain a new copy of the zSecure CICS Toolkit programs, maps, and parameter modules. This process first ensures that the modules are no longer in use. It involves releasing some permanently resident modules. Also, the MVS subtasks are verified not to be active now. If any other terminal user

is concurrently using the zSecure CICS Toolkit interface, the user might experience unpredictable results.

Because the RTST transaction does not perform any internal authorization verification, access to the transaction must be controlled. Access must be restricted to those people who must be able to stop and start the zSecure CICS Toolkit subtasks, or refresh the modules.

CICS RACF class DCICSDCT is used to define and control access to CICS transient data queues and class MCICSPPT is used to control access to CICS application programs that are invoked by other programs.

While both MCICSPPT and DCICSDCT are RACF classes used for CICS security, they protect different types of resources related to program execution. The user ID associated with the RTST transaction might need resource access depending on the CICS settings, for more information see CICS Transaction Server for z/OS - Security for CICS programs.

## Manual restart of the zSecure CICS Toolkit subtasks

When the RTST transaction is not available, you might also use the manual process to stop and start the zSecure CICS Toolkit subtasks. This process involves the use of the CECI transaction.

Run the following two commands:

```
CECI LINK PROG(CQTPKDTCH)
CECI LINK PROG(CQTPLT00)
```

When running these transactions, the terminal user must have access to CSML in DCICSDCT. If you chose to configure a different DESTID in CQTPCNTL, CSML must be replaced with your selected DESTID.

## Additional considerations

There are several additional considerations for running zSecure CICS Toolkit. These are described in this section.

Be aware of the following specifications:

- The RSRCLASS parameter in CQTPCNTL must specify the correct RACF resource class. It does not default to the XTRAN parameter defined in the SIT.
- If you want to use the DUPEUSER capabilities of zSecure CICS Toolkit, it is best to start program CQTPSNP0. You can start this program in one of the following ways:
  - Perform an XCTL or LINK to the program.
  - Start the program as a transaction from your own signon program.
  - Start the program from the sign on exit point.

The major purpose for using the DUPEUSER support is the ability to automatically cancel an existing session when you log on to a second terminal.

**Note:** The new ID becomes effective only after termination of the current transaction. Module CQTPSNP0 has functionality to obtain the ID of the user that is signing on and use that to verify access to the TOOLKIT.DUPE and TOOLKIT.GPID resources. Other functions continue to use the user ID that started the sign on transaction.

## Globalization

The BMS mapsets that are used by zSecure CICS Toolkit are provided as samples in SCQTSAMP.

An installation can modify these BMS mapsets, if the new mapsets are compatible with the existing mapsets. The copybook (symbolic map) resulting from the modification must be identical to the unmodified copybook that is used by the zSecure CICS Toolkit program modules. The only parts that can be changed are field attributes (for example to suppress display of a certain field) or initial field values. All the fields must still be present and the field lengths cannot be changed. Although CICS might allow other

parts of the BMS maps to be changed, such changes are not supported in zSecure CICS Toolkit. Changed mapsets must be translated with the standard DFHMAPS procedure.

---

## Chapter 3. Parameters for zSecure CICS Toolkit

The parameter module CQTPCNTL is used to define the parameters that zSecure CICS Toolkit uses.

After the parameters are set, use the RTCK transaction to check them. Errors are displayed with an error message. Resolve all errors before you implement zSecure CICS Toolkit.

The following is an example of setting up the CQTPCNTL parameters:

```
CQTPCNTL CSECT
CQTPCNTL AMODE 31
CQTPCNTL RMODE ANY
*
EXITPGM DC CL8 ' '
DESTID DC CL4 'CSML '
CICSAPPL DC CL8 'IGNOREIT '
RSRCLASS DC CL8 'TCICSTRN '
CMNDPFX DC CL8 'TOOLKIT. '
SMFUID DC CL8 ' '
SVCNUM DC CL3 '222 '
DUPEUSER DC CL1 '2 '
RACFCMND DC CL1 'Y '
LOGGING DC CL1 'Y '
PEMTALL DC CL1 'Y '
LGDFLTU DC CL1 'N '
END
```

Use the supplied CQTCNTL sample job to apply the update from SMP/E. If that is not possible, you can also use the IBM supplied procedures DFHASMVS and DFHLNKVS to assemble and link the module. The parameters must be in the order as shown in the example. The definitions in the example are the defaults in the installation modules. You can customize the parameters for your installation.

---

### Parameter Descriptions

The following list describes the parameters present in CQTPCNTL.

#### **EXITPGM**

The name of a program that is to receive control whenever the main zSecure CICS Toolkit transaction (normally RTMM) terminates. If you do not want to use an exit program, specify blanks. For a complete description of the exit program features, see [Chapter 6, “zSecure CICS Toolkit exit points specifications,”](#) on page 75.

#### **DESTID**

The destination zSecure CICS Toolkit uses for writing run time messages. The default is CSML. It can be changed to any other entry but must conform to the definitions for CSML as specified in the CICS Resource Definition manual.

#### **CICSAPPL**

This parameter is used as a prefix for the transaction names when you use the RSRC API interface for application security. If IGNOREIT is specified, or the parameter is left blank, the parameter is ignored. If the parameter is coded, it can be up to eight bytes in length and must conform to RACF naming conventions. For more information, see [Chapter 4, “Application security management,”](#) on page 25.

#### **RSRCLASS**

The RACF resource class that is used by zSecure CICS Toolkit. zSecure CICS Toolkit uses this class when it checks resources. It can be any of the classes that are defined in the SIT to CICS so that it is RACLISTed by CICS. It must be the name of the MEMBER class, not the group class (for example, TCICSTRN and **not** GCICSTRN). If you leave it blank or specify an invalid class, zSecure CICS Toolkit fails to initialize. The resource class to be used by the API when performing resource access checking (extended) can be defined as a parameter being passed to the API and overrides this definition for those resource checks. See the API documentation for further information.

## CMNDPFX

The zSecure CICS Toolkit commands that a user can use, and that are displayed when the user enters the zSecure CICS Toolkit transaction (RTMM), are determined by the RACF definitions as outlined in step 1 in [“Define the RACF profiles”](#) on page 11. These definitions all have a prefix of TOOLKIT . . Using the CMNDPFX parameter, it is possible to specify a different prefix. However, this prefix is only in effect when the RTMM transaction is being used. When zSecure CICS Toolkit is being accessed through the API, a prefix of TOOLKIT . is always used.

For example, if CMNDPFX is CICSONE and a user wants to do an ADDUSER, the user must have the following access:

- Access to CICSONE . ADUS if they are using the RTMM transaction.
- Access to TOOLKIT . ADUS if they are doing the ADDUSER through the API.

This provides more flexibility to control functions that are performed through the API, while restricting functions that are performed through the RTMM transaction.

This parameter must be eight characters, must end with a period (.) and cannot contain any blanks. The default is TOOLKIT.

## SMFUID

When zSecure CICS Toolkit creates an SMF record that reflects a change to a RACF profile, the ID of the user that is logged on at the terminal is used in the SMF records. However, there might be situations where you want the ID in the SMF record to be different. In SMFUID, you can specify a different ID that is used in the SMF records the zSecure CICS Toolkit creates.

If this parameter is left blank, the ID of the terminal user is used in the SMF records.

**Note:** This value is different from the SMF80UID field. The SMF80UID field is always set to the value TOOLKIT\* to indicate that the record was produced as part of a zSecure CICS Toolkit function.

## SVCNUM

The SVC number that was assigned to the zSecure CICS Toolkit SVC.

## DUPEUSER

Use this parameter to control user sign on.

- If this parameter is coded as 0, no checking takes place when a user signs on.
- If it is a 1, zSecure CICS Toolkit checks to see whether the same RACF user ID is signed on at another terminal. If it is, the duplicate sign on is disallowed and the user ID is signed off.
- Coding this parameter as 2 has the same effect as 1, with the exception that the terminal is logged off as well (the equivalent of performing a CSSF LOGOFF).

Checking for duplicate user IDs is done only in the terminal-owning region when it is run in an MRO environment. If a user uses the CRTE transaction to route to an application region, no checking takes place in that region.

### Permitting users:

When the DUPEUSER parameter is specified as 1 or 2, you have the option of allowing specific user IDs to be used as group IDs, or you can specify that certain IDs can log on at a second terminal but will be logged off at the terminal at which they are currently signed on. To use this capability, define the following resources to RACF. (This example assumes that the XTRAN parameter in the SIT is CICSTRN):

```
RDEFINE TCICSTRN (TOOLKIT.GPID TOOLKIT.DUPE) UACC(NONE)
```

To allow a user ID to be used as a group ID (that is, it can be shared by multiple users), permit it access to TOOLKIT.GPID. For example:

```
PERMIT TOOLKIT.GPID CLASS(TCICSTRN) ID(GROUP01) ACCESS(READ)
```

This allows GROUP01 to be used by more than one user when they sign on to CICS.

To allow a user to log on at a second terminal, but to be forced off the first terminal, permit it access to TOOLKIT.DUPE. For example:

```
PERMIT TOOLKIT.DUPE CLASS(TCICSTRN) ID(USER01) ACCESS(READ)
```

This enables USER01 to sign on at a second terminal but forces a sign off at the first terminal at which the user was signed on.

If a user has access to both TOOLKIT.DUPE and TOOLKIT.GPID, TOOLKIT.GPID takes precedence.

### RACFCMND

If zSecure CICS Toolkit is used only by applications for internal security checking, controlling sign on, or both, it does not require all of its subtasks in the region. These subtasks are required only if you use the RTMM transaction or the API to run RACF commands. It saves approximately 40K per CICS region.

Specify Y if you use the commands or N if you do not.

### LOGGING

When an application program uses the API to check resource access, zSecure CICS Toolkit creates SMF records based on the AUDIT parameters for the resource. In other words, when a user does not have access to the resource, and auditing for failures is turned on, or AUDIT is all, zSecure CICS Toolkit creates SMF records.

This can result in a large amount of unwanted SMF records being written. If you want zSecure CICS Toolkit to create these records, specify Y. If you want them to be suppressed, specify N. For the RSRC and RSRX functions, it is also possible to specify S. This results in suppression of possible access violation messages, while still creating SMF records about these violations. For all other functions, S is interpreted the same as Y.

This parameter setting does not apply to SMF records that are created by zSecure CICS Toolkit when a user modifies a RACF profile.

### PEMTAL

This parameter is used to control the scope of the PERMIT command. The PERMIT command can be restricted to giving access only to resources that are in a class that is specified in the SIT (for example: XDCT, XFCT, XJCT, SPPT, XTRAN), and is RACLISTED by CICS. In this case, specify N. To allow the PERMIT command to be used for ALL resource classes, including DATASET, specify Y. For more information, see the PEMX and PEMT definitions in the [“Resource names used for command authorization”](#) on page 14 and [“Granting or removing access to a resource \(PERMIT command\)”](#) on page 62.

### LGDFLTU

This parameter is used to control the display of USERIDs as a subfunction of the LISTGROUP function. If this value is set to N, all users that are connected to the specified GROUP are shown. If this value is set to Y, only users that are connected to the DFLTGRP of the terminal user are shown.

## CQTPCNTL parameter values verification

Each region can have its own version of CQTPCNTL. However, select the CICSAPPL value carefully to avoid errors.

After coding CQTPCNTL, use transaction **RTCK** to verify its parameters. Perform this action before zSecure CICS Toolkit is implemented.

While both MCICSPPT and DCICSDCT are RACF classes used for CICS security, they protect different types of resources related to program execution. Class DCICSDCT is used to define and control access to CICS transient data queues and class MCICSPPT is used to control access to CICS application programs that are invoked by other programs. The user ID associated with the RTCK transaction might need resource access depending on the CICS settings, for more information see CICS Transaction Server for z/OS - Security for CICS programs.

Display the RTCK transaction screen. The following screen is displayed and shows any errors that might have occurred.

IBM zSecure CICS Toolkit  
 CICS level = 0730 Toolkit level = HCQT320

Exit program		Has not been defined to CICS
Destination	CSML	Destination id for messages
Prefix (Appl security)	IGNOREIT	Application prefix for security
Resource class	TCICSTRN	Member class name for Toolkit
LG users in DFLTGRP only	N	N=All users, Y=Only matching DFLTGRP
Duplicate Signon	2	0=Yes,1=No(Signoff),2=No(Logoff)
Toolkit SVC	222	Required for RACF commands
RACF commands	Y	Region may issue RACF commands
Logging	Y	SMF Records if audit specified
PEMTALL	Y	Allow permits for all classes

PF03/Clear=Quit      Check Highlighted fields for error messages

Figure 2. RTCK transaction panel

Select the function for the task that you want to accomplish:

- Press PF01 from the main menu to view YOUR access to zSecure CICS Toolkit commands.
- Press PF02 from the main menu to view the zSecure CICS Toolkit programs, their status and PTF level.
- Press PF04 from the main menu to view the zSecure CICS Toolkit subtasks, their status and PTF level.
- Press CLEAR or PF03 to terminate the transaction. Any other key re-displays the main menu.

The following two screens show example output for the programs and subtasks.

**Sample partial screen showing the output for the program status:**

Program	PTFlevl	ST	Program	PTFlevl	ST	Program	PTFlevl	ST	Program	PTFlevl	ST
CQTPAPRM		OK	CQTPCNTL		OK	CQTPMSGE		OK	CQTPLT00	HCQT320	OK
CQTPATCH	HCQT320	OK	CQTPDTCB	HCQT320	OK	CQTPCHEK	HCQT320	OK	CQTPAPI0	HCQT320	OK
CQTP0000	HCQT320	OK	CQTP0010	HCQT320	OK	CQTP0020	HCQT320	OK	CQTP0030	HCQT320	OK
CQTP0040	HCQT320	OK	CQTP0041	HCQT320	OK	CQTP0042	HCQT320	OK	CQTP0043	HCQT320	OK
CQTP0044	HCQT320	OK	CQTP0050	HCQT320	OK	CQTP0055	HCQT320	OK	CQTP0056	HCQT320	OK
CQTP0058	HCQT320	OK	CQTP0059	HCQT320	OK	CQTP0060	HCQT320	OK	CQTP0070	HCQT320	OK
CQTP0080	HCQT320	OK	CQTP0081	HCQT320	OK	CQTP0082	HCQT320	OK	CQTP0083	HCQT320	OK
CQTP0084	HCQT320	OK	CQTP0086	HCQT320	OK	CQTP0090	HCQT320	OK	CQTP0091	HCQT320	OK
CQTP0100	HCQT320	OK	CQTP0110	HCQT320	OK	CQTP0111	HCQT320	OK	CQTP0112	HCQT320	OK
CQTP0113	HCQT320	OK	CQTP0114	HCQT320	OK	CQTP0120	HCQT320	OK	CQTP0130	HCQT320	OK
CQTP0131	HCQT320	OK	CQTP0132	HCQT320	OK	CQTP0133	HCQT320	OK	CQTP0134	HCQT320	OK
CQTP0140	HCQT320	OK	CQTP0160	HCQT320	OK	CQTP0161	HCQT320				
OK											

Figure 3. zSecure CICS Toolkit: Program status output

**Sample partial screen showing the output for the subtask status:**

Program	PTFlevl	ST	Program	PTFlevl	ST	Program	PTFlevl	ST	Program	PTFlevl	ST
CQTSUBS	HCQT320	AV	CQTS000	HCQT320	AV	CQTS010	HCQT320	AV	CQTS020	HCQT320	AV
CQTS030	HCQT320	AV	CQTS041	HCQT320	AV	CQTS042	HCQT320	AV	CQTS043	HCQT320	AV
CQTS044	HCQT320	AV	CQTS050	HCQT320	AV	CQTS055	HCQT320	AV	CQTS056	HCQT320	AV
CQTS058	HCQT320	AV	CQTS059	HCQT320	AV	CQTS060	HCQT320	AV	CQTS070	HCQT320	AV
CQTS081	HCQT320	AV	CQTS082	HCQT320	AV	CQTS083	HCQT320	AV	CQTS084	HCQT320	AV
CQTS086	HCQT320	AV	CQTS090	HCQT320	AV	CQTS100	HCQT320	AV	CQTS111	HCQT320	AV
CQTS112	HCQT320	AV	CQTS113	HCQT320	AV	CQTS114	HCQT320	AV	CQTS120	HCQT320	AV
CQTS131	HCQT320	AV	CQTS132	HCQT320	AV	CQTS133	HCQT320	AV	CQTS134	HCQT320	AV
CQTS135	HCQT320	AV	CQTS136	HCQT320	AV	CQTS140	HCQT320	AV	CQTS150	HCQT320	AV
CQTS160	HCQT320	AV									

Figure 4. zSecure CICS Toolkit: Subtask status output

---

## Chapter 4. Application security management

zSecure CICS Toolkit lets you request access to multiple resources with a single system call.

Traditionally, applications that run under CICS use some form of their own internal security. Even though CICS and the External Security Manager (ESM) might control access to the transactions, access to subfunctions of those transactions was often maintained by the application.

Since several years, applications also can use the EXEC CICS QUERY SECURITY function. However, if an application must establish authorization to many resources (for example, for determining which options to display on a selection panel), considerable time might be involved in requesting the authorization. Also, only a single resource can be specified on the QUERY SECURITY call. In that environment, zSecure CICS Toolkit provides advantages. Using the zSecure CICS Toolkit RSRC or RSRX functions, you can request access to multiple resources using a single API call.

---

### Operator ID or OPID check

The traditional method that is employed by various applications to do security checking is based on the 3-byte operator ID of a user. This ID is checked against a table or a file, which contains an array or matrix of functions that this user, or operator ID, can perform.

Such internal security methods leads to numerous exposures. CICS provides no capability to ensure that operator IDs are unique. And the three characters that are used for the OPID are often not sufficient to accommodate all users. By using zSecure CICS Toolkit for application security checking, you can overcome these exposures. Other added advantages are the centralization of security definitions, and one security system (RACF) being used by all applications.

---

### Application conversion

If your application uses internal authorizations, some conversion is needed to start using RACF for security. zSecure CICS Toolkit makes the conversion simpler.

This requires a coding change to the application that now checks security. If the application is a package, contact the vendor and create an exit point within the package, where the security checking takes place. Use the zSecure CICS Toolkit API for security checks to use RACF security facilities. With the API, more than 2000 resources can be checked with one call. For more information about using the API and its multiple functions and capabilities, see [Chapter 7, “Application programming interface \(API\),” on page 77](#). Application programs can link to CQTPAPI0, asking for access to a resource that represents the application function. CQTPAPI0 then performs the required checks and returns to the calling application with the appropriate return code. The following example shows how an application could use CQTPAPI0, the RACF profiles that could be defined, and the possible return codes from CQTPAPI0.

If the transaction that the user runs has multiple functions, it probably provides the user with a menu panel. The user can select one of those options. In the following example, the user starts transaction ABCD. The application then gives the user an option menu as follows:

```
OPTION DESCRIPTION
1      READ PAYROLL MASTER RECORDS
2      UPDATE PAYROLL MASTER RECORDS
3      ADD PAYROLL MASTER RECORDS
4      DELETE PAYROLL MASTER RECORDS

ENTER OPTION : _
```

*Figure 5. Option menu example*

The same transaction, ABCD, performs all the functions, but not all users must have access to all of them. There are several different approaches.

- Check access to a resource that is associated with the user's choice, and invoke the function if the choice is authorized.
- Before showing the selection panel, check access to all possible choices, and hide the options that are not authorized.

The individual functions can be associated with a RACF resource name through a simple mapping process. For example, READ for option one, UPDT for option two, ADDS for option three, and DELT for option four. The application program LINKs to CQTPAPI0 providing the parameters through a COMMAREA. The following example shows an assembler program to check access to the READ function. The return code is set by CQTPAPI0.

```

*
*           MVC  API_FUNC,=CL4'RSRC'           MOVE FUNCTION CODE FOR
*           MVC  API_RESOURCE_NAME,=CL13'READ' A RESOURCE CHECK
*           MVI  API_END,X'FF'                OPTION REQUESTED BY USER
*                                           END OF RESOURCE NAMES
*
*           EXEC CICS LINK PROGRAM('CQTPAPI0') COMMAREA(API-COMM)
*
*           CLI  API_RESOURCE_RC,X'00'        ACCESS ALLOWED ?
*           BE   ACCESSOK                     YES
*           B    ERROR                        NO
*
*
* API_COMM      DS 0CL99
* API_FUNC      DS CL4                       FUNCTION CODE
* API_RC        DS XL1                       RETURN CODE
* API_MSG       DS CL79                     MESSAGE AREA
*
* API_RESOURCE_NAME DS CL13                 RESOURCE NAME
* API_RESOURCE_RC  DS XL1                   RACF RETURN CODE
* API_END        DS XL1                   X'FF' END OF LIST
*

```

The return code is a one-byte hexadecimal value. See the following list for an explanation of the possible codes.

#### RETURN CODE MEANING:

##### **X '00'**

Access is allowed to resource

##### **X '04'**

The resource or classname is not defined to RACF

##### **X '08'**

The user or group is not authorized to use the resource

##### **X '0C'**

RACF is not active

##### **X '10'**

RACROUTE FASTAUTH installation exit error

##### **X '14'**

RACF is not installed or at the wrong level

If the COMMAREA is not large enough, the API\_RC field contains the value X '02'.

## Resource profile definitions

The resource profiles that are used in the previous example must be defined to in RACF. Because the example program uses the RSRC function, the resource profiles must be defined in the resource class that is specified for RSRCLASS in CQTPCNTL.

When access checking is done using the RSRC function, the resource names that are specified in the application can be automatically prefixed with the value that is defined for CICSAPPL in CQTPCNTL. If CICSAPPL is IGNOREIT or blank, the resource name is not automatically prefixed. The RACF profiles must match the resources and, therefore, must be defined using the same prefix. Another requirement is that

the profiles are defined in the same RACF class as the class that is used for zSecure CICS Toolkit. It is as specified in the RSRCLASS parameter of CQTPCNTL.

If the API\_FUNCTION is RSRX, the resource name can be up to 246 characters in length. However, it must not be greater than the maximum that is defined for the resource class in the Class Descriptor Table.

Assuming that the value that is coded for CICSAPPL was PRODAPPL, and the RSRCLASS value of TCICSTRN, the resource profiles would be defined as follows:

```
RDEFINE TCICSTRN (PRODAPPL.READ PRODAPPL.UPDT PRODAPPL.ADDS PRODAPPL.DELT)
```

Users would then be permitted to the resource as required:

```
PERMIT PRODAPPL.READ CLASS(TCICSTRN) ID(USER01) ACCESS (READ)
PERMIT PRODAPPL.UPDT CLASS(TCICSTRN) ID(USER02) ACCESS (READ)
PERMIT PRODAPPL.ADDS CLASS(TCICSTRN) ID(USER03) ACCESS (READ)
PERMIT PRODAPPL.DELT CLASS(TCICSTRN) ID(USER03) ACCESS (READ)
```

After the RACF profiles are created, zSecure CICS Toolkit is ready to check application security.

## Alternative simple application security interface

zSecure CICS Toolkit also provides a simple interface (CQTPAPPL) as alternative to the full API provided by CQTPAPI0. The full API is described in [Chapter 7, “Application programming interface \(API\),” on page 77](#).

The simple interface provides only two functions:

- Access the user profile, current group profile, and instdata of the currently signed on user
- Check access to a resource.

These two functions can also be accessed using current CICS services like EXEC CICS ADDRESS ACEE and EXEC CICS QUERY SECURITY. To assist existing customers in their migration to these standard CICS services, the CQTPAPPL interface is provided.

## User information retrieval

To use the CQTPAPPL user information retrieval function, you must provide a commarea of at least 22 bytes. If the commarea is larger than 286 bytes, the DFTLGRP and the INSTDATA for the user are returned as well.

To use this function, the first 4 bytes of the commarea must contain the value '????' (that is, four question marks). Here is an example of how to use this function:

```

MVI  COMMAREA,' '           Clear commarea
MVC  COMMAREA+1(L'COMMAREA-1),COMMAREA
MVC  COMM_FUNC,=CL4'????'   Move function code
EXEC  CICS LINK PROGRAM('CQTPAPPL')
      COMMAREA(COMMAREA)
      LENGTH(COMALEN)
      CLI  COMM_RC,X'00'     Ok?
*
*   Further processing
*
COMMAREA DS  0CL286         Space for COMMAREA
COMM_FUNC DS  CL4           Function code ????
COMM_RSVD DS  CL9           Unused
COMM_RC   DS  XL1           Return code
COMM_USER DS  CL8           Userid
COMM_GRP  DS  CL8           Group
COMM_IDL  DS  XL1           Length of instdata
COMM_IDA  DS  CL255         Instdata
COMALEN   DC  AL2(*-COMMAREA) Length of COMMAREA

```

The COMM\_RC has two possible values:

- X'00' user information is returned
- X'10' Invalid or no ACEE present.

If the commarea is too small, an asterisk (\*) is returned in the first byte of COMM\_FUNC. If the commarea has length zero, or is absent, no information is returned.

## Resource access verification

To use the resource access verification function, you must provide a commarea of at least 14 bytes, containing the name of a resource.

The access of the current user is verified to be at least READ and the COMM\_RC is set accordingly. The resource name must be left-aligned and padded with blanks. When processing the request, the name of the resource is prefixed with the value that is specified in CICSAPPL in CQTPCNTL. If the value of CICSAPPL is IGNOREIT or blank, no prefix is applied. The resource name as used in the access verification request is returned in the field COMM\_RESN. The following shows an example of how to use this function:

```

MVI  COMMAREA,' '           Clear commarea
MVC  COMMAREA+1(L'COMMAREA-1),COMMAREA
MVC  COMM_RESN,=CL13'PAYROLL' Move resource name
EXEC CICS LINK PROGRAM('CQTPAPPL')
      COMMAREA(COMMAREA)
      LENGTH(COMALEN)
      COMM_RC,X'00'           Access?
*
*   Further processing
*
COMMAREA DS 0CL14           Space for COMMAREA
COMM_RESN DS CL13           Resource name
COMM_RC   DS X11            Return code
COMALEN   DC AL2(*-COMMAREA) Length of COMMAREA

```

The COMM\_RC has three possible values:

- X'00' Access is allowed to resource.
- X'04' The resource or classname is not defined to RACF.
- X'08' The user is not authorized to use the resource.

If the commarea is too small, an asterisk (\*) is returned in the first byte of COMM\_RESN. If the commarea has length zero, or is absent, no information is returned.

# Chapter 5. The zSecure CICS Toolkit command interface

zSecure CICS Toolkit provides the capability of issuing RACF commands from CICS.

The commands that can be issued are: ADDGROUP (ADGRP), ADDUSER (ADUSER), ALTGROUP (ALTGRP), ALTUSER (ALUSER), CONNECT (CONNCT), manage CSDATA, DELETE GROUP (DELGRP), DELETE USER (DELUSER), LISTDSD (LDSO), LISTGRP (LGRP), LISTUSER (LUSER), PASSWORD, PERMIT, REMOVE, RALTER, RDEFINE, RDELETE, REMOVE, RLIST, RACLINK, and manage USRDATA.

For any option used to alter profiles, SMF records are produced, indicating the changes and who changed. These records show up in your regular RACF reports.

The SMF records all show the value TOOLKIT\* in the SMF80UID field. This special value is used to indicate that the record was produced as part of a zSecure CICS Toolkit function.

The **PASSWORD** and **VERIFY** commands are only available through the API. You can use the zSecure CICS Toolkit API to customize the panels for your installation. For more information, see the API documentation.

Before users can use zSecure CICS Toolkit, they must be given access to one or more zSecure CICS Toolkit commands, as described in [Chapter 2, “zSecure CICS Toolkit installation,”](#) on page 3.

## Navigating the Main menu

To view the command interface main menu, you must have access to the transaction to execute it. If you have not completed a signon to CICS with a valid RACF user ID, the transaction automatically terminates with message CQT006.

### Procedure

1. To view the command interface main menu, enter RTMM at a clear panel.

```
Termid = 0002          IBM zSecure CICS Toolkit          Date = 2021/243
Userid = CRMBVK1      MAIN MENU                          Time = 08:22:36
Name   = John Smith

PF01 ADGRP  PF02 ADUSER  PF03 ALTGRP  PF04 ALUSER  PF05 CONNCT  PF06 DELDSD
PF07 DELGRP  PF08 DELUSR  PF09 LDSO   PF10 LGRP   PF11 LUSER   PF12 PERMIT
PF13 RALTER  PF14 RACLNK  PF15 RDEFNE PF16 RDELTE PF17 REMOVE  PF18 RLIST
PF19 USRDAT  PF20 CSDATA

                          Number ==> __

Licensed Materials - Property of IBM
5655-ABD Copyright IBM Corp. 1988, 2025. All Rights Reserved.

Use PF key or enter NUMBER for desired command. Press CLEAR to exit
```

Figure 6. Main Menu

2. To make a selection, press the PF key, or type in the number of the command you want to use and press **Enter**.

When displaying a field within a profile (for example, the groups a user is connected to), you can use PF08 to page down if there is more than one panel of entries.

# Adding, altering, or deleting a group (ADDGROUP, ALTGROUP, or DELGROUP command)

Use the **ADDGROUP**, **ALTGROUP**, and **DELGROUP** commands to add a new group to the system, or to alter or delete an existing group.

## About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.ADGR / TOOLKIT.ALGR / TOOLKIT.DELG / TOOLKIT.LGRP, depending on the command that is performed) and the group (ADGR.grpname / ALGR.grpname / DELG.grpname / LGRP.grpname).

## Procedure

1. Access the **ADDGROUP**, **ALTGROUP**, and **DELGROUP** commands by pressing the designated **PF** key, as shown on the main menu.

```
Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1      GROUP =                          Time = 11:09:39

Owner =                Supgroup =                Termuacc = Y Universal = N

-----1-----2-----3-Installation data-5-----6-----7-----

                                     |<===
-----1-----2-----3-----4-----5-----6-----7-----

PF1=Addgroup 3=Delgroup 4=Altgroup ENTER=Listgroup CLEAR=Main menu
```

Figure 7. ADDGROUP / ALTGROUP / DELGROUP panel

2. Specify the values that are needed to perform the selected task. The different fields and their meanings are described under the LISTGROUP command.

The fields that are required when you perform the different commands are as follows:

### ADDGROUP

To define a new group, the GROUP name must be entered. This GROUP name must be unique and not currently exist as a group or user name. The OWNER, if not entered, defaults to your user ID. If a group name is entered as the owner, it must be the same name as the superior group (SUPGROUP). If you do not enter a SUPGROUP, it defaults to your current connect group. TERMUACC must be Y or N. UNIVERSAL must also be Y or N. The INSTALLATION DATA field is optional. After you entered the required information press PF01 to add the new group.

### ALTGROUP

To alter the GROUP profile. You can change any of the fields except the GROUP. After you entered the data that you want to change, press PF04 to update the profile.

### DELGROUP

To delete the GROUP profile. Enter the GROUP name that you want to delete, and press PF03. The group must not have any subgroups, users that are connected to it, or any group data sets. zSecure CICS Toolkit has no way to find all the users that might be connected to the group. Therefore, the group might not be a Universal group. zSecure CICS Toolkit checks for subgroups and users but not for group data sets.

## Adding a user profile (ADDUSER command)

Use the **ADDUSER** command to add a user profile to the system.

### About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.ADUS) and the default group of the user profile that is added (ADUS.dfltgrp).

### Procedure

1. Access the **ADDUSER** command by pressing the designated **PF** key, as shown on the main menu.

```
Termid = 4701          IBM zSecure CICS Toolkit          Date = 2024/335
Userid = CRMBPH1      Adduser =                          Time = 15:47:57

Name =                Dfltgrp =                Authority = U
Seclevel =
SMTWTF5 FROM TILL
YYYYYYY 0000 0000      Password =                Owner =
NoPhrase? (Y/N) = N    NoPassword? (Y/N) = N    PhrInt = 00000    PwInt = 000
Password Phrase =

                                |<===

-----+-----1-----+-----2-----+-----3-Installation data-5-----+-----6-----+-----7-----+-----

                                |<===

-----+-----1-----+-----2-----+-----3-----+-----4-----+-----5-----+-----6-----+-----7-----+-----

CQT020 -Enter details of user to be added
PF5=AddUser ENTER=Redisplay CLEAR=Main menu
```

Figure 8. ADDUSER panel

2. Enter information in these fields to add a user:

#### USERID

In the ADDUSER= field. USERID can be 1 - 8 characters.

#### NAME

Is normally the users name, 1- 20 characters.

#### DFLTGRP

The user default group. It must be a valid group name.

#### AUTHORITY

The authority of the user within the group. The default is U (use), but might be changed to C (create).

#### SECLEVEL

Specify the SECLEVEL for the user or leave blank. Available SECLEVELS can be displayed with the RLIST command and displaying class SECDATA, resource name SECLEVEL and then selecting the MEMBERS display.

#### LOGON DAYS

Enter a Y or N to indicate which days the user can access the system. Specifying N for any particular day prevents the user from accessing the system on that day.

#### LOGON TIME

LOGON TIME specifies the time of day the user might log on. Leave the FROM and TILL fields zero to allow the user to log on at any time. If a time is specified, it must be in the range 0001 through 2359.

**PASSWORD**

The initial password for the user. The initial password is always set as expired.

**OWNER**

The owner of the profile.

**NOPHRASE**

Specify Y to delete the password phrase.

**NOPASSWORD**

Specify Y to delete the password and set the PROTECTED attribute.

**PHRINT**

Specify the password phrase interval for the user. The value must be in the range 0-65534 days.

**PWINT**

Specify the password interval for the user-. RACF allows the interval to be- in the range of 1-254 days. If the password interval is zero 0, then the default interval is used.

**PASSWORD PHRASE**

The initial password phrase for the user. The initial password phrase is always set as expired. Trailing blanks are removed.

**Note:** Attempts to set a password phrase on z/OS levels that do not support them result in message CQT184. The user is defined as specified but without a password phrase.

**INSTALLATION DATA**

Information about the user can be entered in this field. If data is entered, the EOF key must be pressed after the last character was entered. This field is optional.

3. Press PF05 to add the user to the system.

The initial PASSWORD for the user, if not specified, can be the same as the name of the DEFAULT GROUP. Users must enter a new password the first time they log on.

4. To delete the password, specify NOPASSWORD.

The PROTECTED attribute is then set.

5. To delete the password phrase, specify NOPHRASE.

6. To change the password interval, specify a value in the range 1-254.

If you specify 0, then the global password interval is used.

7. To change the password phrase interval, specify a value in the range 0-65534.

## Changing a profile (ALTUSER command)

---

Use the **ALTUSER** command to change the profile for a specific user.

### About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.AUSR) and the users default group (AUSR.dfltgrp). SMF records are created any time that a profile is altered by any user.

### Procedure

1. Access the **ALTUSER** command by pressing the designated **PF** key, as shown on the main menu.

```

Termid = 4701          IBM zSecure CICS Toolkit          Date = 2024/335
Userid = CRMBPH1     ALTUSER =                          Time = 15:40:35

Password = ***** Resume user? (Y/N) = N Expire PW? (Y/N) = Y
NoPhrase? (Y/N) = N NoPassword? (Y/N) = N PhrInt = 00000 PwInt = 000
Name = ***** Revokedt = ***** Resumedt = *****

Password Phrase = *****
***** |<===

-----1-----2-----3-Installation data-5-----6-----7-----
*****
*****
*****
***** |<===
+++++
CLAuth =              NoCLauth =
Special = * Operations = * Auditor = * Restr = * Grpacc = * Adsp = *
Protected = * Uaudit   = * Dfltgrp = ***** Owner = *****

SMTWTF5 From Till
***** **** Model = *****
CQT009 -Enter userid to be updated
PF5=Update 6=CICS 7=TSO 8=OMVS 9=WORK ENTER=Redisplay CLEAR=Main menu

```

Figure 9. ALTUSER panel

2. Specify the user for whom you want to change the profile.

When you display a user, you are given the option to resume the user or not.

3. To reset a user password to the name of the DEFAULT GROUP, clear the PASSWORD field: place the cursor in the first position of the field, pressEOF, then press PF05.
4. To set a specific PASSWORD, clear the field, place the cursor in the first position of the field, enter the new password and press PF05.

By default the new password is set to expired. If you have the special attribute, you can indicate that the new password does not need to be changed immediately (set **Expire PW** to N).

If you must change a password phrase, specify the new value. Ensure that you remove excess characters at the end. zSecure CICS Toolkit strips trailing blanks, but trailing question marks (?) or asterisks (\*) are included as part of the password phrase. If you want to remove an existing password phrase, blank out or erase the entire password phrase field. If you want to retain the current value, leave all the question marks as shown.

5. You can REVOKE a user one of two ways by specifying REVOKEDT:
  - Set REVOKEDT to the current date, the equivalent of specifying ALTUSER *userid* REVOKE. The revoke flag is set and the REVOKE and RESUME dates are cleared.
  - Specify a REVOKEDT date other than current date. The user is revoked on that date.
6. Use RESUMEDT to resume a user.

You can use the special value 00000 (five zeros) to remove any REVOKE or RESUME date. Setting the field to blanks or empty, or leaving the value as shown, results in retaining the current value.

Specify **Y** for **Resume User** to resume a user immediately.

7. To update one of the supported segments, press the indicated PF key.
  - To modify CICS information for the user, press PF06.
  - To update the TSO segment, press PF07.
  - For the OMVS and WORKATTR segments, use PF08 and PF09.
8. Unless you have SPECIAL, or access to TOOLKIT.SPEC, you are not permitted to change any field below the delimiter line of \*\*\*\*\*.

There are exceptions for the DFLTGRP value the RESTRICTED attribute. Regular administrators can change these two fields without the need for SPECIAL. Another exception is the EXPIRED setting for a new password. The user needs system special or access to TOOLKIT.SPEC to set non-expired passwords. If you do have SPECIAL, you can alter and of the fields on the panel and press PF05 to update.

9. Specify an entry in the CLAUTH or NOCLAUTH to give or remove class authority in the specified class.  
zSecure CICS Toolkit does not verify that the specified class is valid.
10. To set no password, specify NOPASSWORD.  
The PROTECTED attribute is then set.
11. To set no password phrase, specify NOPHRASE.
12. To set the password interval, specify a value in the range 1-254.  
If you specify 0, then the global password interval is used.
13. To change the password phrase interval, specify a value in the range 0-65534.

## Altering the CICS segment for a user (ALTUSER CICS SEGMENT)

Use the **ALTUSER** command with the CICS SEGMENT option to alter the CICS segment for a specific user.

### About this task

The user must have the following authorizations:

- The user must have access to the zSecure CICS Toolkit command (TOOLKIT.AUSR) and the user default group (AUSR.dfltgrp).
- To manage the CICS segment, the user must have access to TOOLKIT.ACIC.

### Procedure

1. To access the ALTUSER CICS SEGMENT command, press the PF06 key in the main ALTUSER panel.

```

Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1      ALTUSER = BCSCGB2                Time = 11:10:47

OPIdent = 123
OPPrtty = 123
Timeout = 000
XRFSoff = NOFORCE
OPClass =

RSLKey =
TSLKey =

CQT074 -Command completed successfully
PF5=Update 6=User 11=Delete Enter=Redisplay CLEAR=Main menu

```

Figure 10. ALTUSER (CICS SEGMENT) panel

#### OPIDENT

The one-to-three character operator identification to assign to this user.

#### OPPRTY

The operator priority for this user. It can be in the range 000 - 255.

#### TIMEOUT

The number of minutes that must elapse since the user last used the terminal before CICS timeouts the terminal.

The valid range is 000 - 999. A value of zero means the terminal is not timed out.

## **XRFSOFF**

The CICS extended recovery facility sign-off option. Specify FORCE to sign off the operator in the event of XRF takeover, or NOFORCE to leave the operator signed on.

## **OPCLASS**

Operator classes are used by CICS when it routes basic mapping support messages. The valid classes are in the range 01 - 24. When you specify the operator classes, they must be separated by a comma (for example: 01,04,05,16,24).

## **RSLKEY**

The RSL keys are used by CICS on distributed platforms. Each CICS resource has one RSL key that is assigned to it. In order for a user to access a resource, the user must have the same RSL key as the RSL key assigned to the resource. The valid keys are in the range 01 - 24. The values 00 and 99 have special meaning. When you specify RSLKEYs, they must be separated by a comma, for example, 01,04,05,16,24.

**Note:** In the current release, zSecure CICS Toolkit provides space for only 22 RSLKEY values.

## **TSLKEY**

The TSL keys are used by CICS on distributed platforms. Each CICS transaction has one TSL key that is assigned to it. In order for a user to run a transaction, the user must have the same TSL key as the TSL key assigned to the transaction. The valid keys are in the range 01 - 64. The values 00 and 99 have special meaning. When you specify TSLKEYs, they must be separated by a comma, for example, 01,04,05,16,24.

**Note:** In the current release, zSecure CICS Toolkit provides space for only 22 TSLKEY values.

2. To display the current information in the CICS SEGMENT of a user, enter the userid, and press Enter.
3. To change any or all of the information, enter the new data and press PF5.  
If there are any errors, an error message displays, indicating the problem.
4. To remove the CICS SEGMENT, press PF11.

**Note:** Removing a CICS SEGMENT does not prevent a user from accessing CICS services. Access to CICS services might be controlled by profiles in the APPL resource class.

Without a CICS segment, CICS users inherit certain values from the CICS SEGMENT of the CICS Default User.

Whenever the OPCLASS, RSLKEY or TSLKEY parameter is updated, it completely replaces the prior values. For example, if a user has OPCLASS 01,02,03 defined, and you update the profile by specifying 02,05,06, the user only has 02, 05, and 06 defined. The prior values of 01,02, and 03 are deleted.

## **Altering the TSO segment for a user (ALTUSER TSO SEGMENT)**

Use the **ALTUSER** command with the TSO SEGMENT option to alter the TSO segment for a specific user.

### **About this task**

The user needs the following authorizations:

- The user must have access to the zSecure CICS Toolkit command (TOOLKIT.AUSR) and the user default group (AUSR.dfltgrp).
- To manage the TSO segment, the user must have access to TOOLKIT.ATSO.

### **FUNCTION**

### **AUTHORITY:**

### **Procedure**

1. To access the ALTUSER TSO SEGMENT command, press the PF07 key in the main ALTUSER panel.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      ALTUSER = BCSCGB2             Time = 11:11:05

Acctnum = *
Destid  =
HClass  =              JClass =                   MsgClass=           SClass =
Size    = 0000000     Maxsize = 0000000   Seclabl =
Proc    = ISPFPROC    Unit     =                   Udata  = 0000

```

```

CQT074 -Command completed successfully
PF5=Update 7=User 11=Delete Enter=Redisplay CLEAR=Main menu

```

Figure 11. ALTUSER (TSO SEGMENT) panel

### ACCTNUM

The users default TSO account number.

### DESTID

The default destination for dynamically allocated SYSOUT data sets.

### HCLASS

The default hold class of the user.

### JCLASS

The default job class of the user.

### MSGCLASS

The default message class of the user.

### SCLASS

The default sysout class of the user.

### SIZE

The minimum region size if the user does not request one at logon time.

### MAXSIZE

The maximum region size the user can request at logon time.

### SECLABL

The users security label.

### PROC

The name of the user default logon procedure.

### UNIT

Default name of a device or group of devices that a procedure uses for allocations.

### UDATA

Installation data for the user.

2. To display the current information in the TSO SEGMENT of a user, enter the userid, and press Enter.
3. To change any or all of the information, enter the new data and press PF5.

If there are any errors, an error message displays, indicating the problem. If a field is set to blanks, that parameter is deleted from the user TSO segment.

When the parameters ACCTNUM, PROC and SECLABL are specified, the user must have access to these definitions in the appropriate RACF resource class.

Refer to the RACF Command Language Reference for complete information and the other TSO segment fields.

4. To remove the TSO SEGMENT, press PF11.

**Note:** Removing a TSO SEGMENT prevents the user from accessing TSO interactive services.

## Altering the OMVS segment for a user (ALTUSER OMVS SEGMENT)

Use the **ALTUSER** command with the OMVS SEGMENT option to alter the OMVS segment for a specific user.

### About this task

The user needs the following authorizations:

- The user must have access to the zSecure CICS Toolkit command (TOOLKIT.AUSR) and the user default group (AUSR.dfltgrp).
- For managing the OMVS segment, the user must have access to TOOLKIT.AOMV.

### Procedure

1. To access the **ALTUSER OMVS SEGMENT** command, press the **PF08** key in the main ALTUSER panel.

```
Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      ALTUSER = BCSCGB2              Time = 11:11:22

UID      = 0000002009 (# or AUTOUID)  Shared = N    MKDIR   = N
Home     =
Program  =

ASSizeMax =
CPUTimeMax =
FileProcMax =
MMapAreaMax =
ProcUserMax =
ThreadsMax =
MemLimit =
SHMemMax =
```

```
CQT074 -Command completed successfully
PF5=Update 8=User 11=Delete  Enter=Redisplay CLEAR=Main menu
```

Figure 12. ALTUSER OMVS segment panel

#### UID

The OMVS UID of the user. When you change the UID to another value, it is possible to enter AUTOUID in this field. If the required profiles are defined, zSecure CICS Toolkit assigns the next available UID. When you change the UID into a value that is already assigned to another user, the command is rejected. For authorized users, it can be overridden by usage of the SHARED parameter.

#### Shared

When you assign a UID to a user, the UID must be unique. When the terminal user has the System-SPECIAL attribute or has access to SHARED.IDS in the UNIXPRIV class, the user might request that the UID value can be shared between multiple users. In other words, the UID value then does not need to be unique. If you want to assign a shared UID, enter Y in the SHARED field.

#### MKDIR

When you assign a HOME directory to a user, the directory must exist in the file system. By selecting option Y, the zSecure CICS Toolkit task attempts to create the directory, and set the

owner to the userid and dfltgrp. The authority to run the necessary USS commands is based on the CICS region user, and not on the authority of the CICS terminal user. If this function is not enabled in your installation, leave the value for this field as N.

**Home**

The home directory of the user. When you change the OMVS segment of the user, ensure that the case of this field is correct. Either do not update the OMVS segment at all, or ensure that your terminal uses mixed case. Or, verify that the actual home directory of the user is defined in ALL UPPERCASE. If the HOME directory (case sensitive) cannot be located, use of UNIX System Services might fail.

**Program**

The initial program (shell program) for the user. When you change the OMVS segment of the user, ensure that the case of this field is correct. Either do not update the OMVS segment at all, or ensure that your terminal uses mixed case. Or, verify that the program actually exists in ALL UPPERCASE. If you leave the field blank, USS normally uses the value */bin/sh* as default value.

**ASSizeMax**

The address-space-size that you define is a numeric value 10 485 760 - 2 147 483 647. The value that is specified overrides any value that is provided by the MAXASSIZE parameter of BPXPRMxx. If the system value is adequate, you must leave this field blank.

**CPUTimeMax**

The processor time that you define is a numeric value 7 - 2 147 483 647. The value that is specified overrides any value that is provided by the MAXCPU TIME parameter of BPXPRMxx. If the system value is adequate, you must leave this field blank.

**FileProcMax**

The files-per-process that you define is a numeric value 3 - 524287. Regular users can use the value 256. The value that is specified overrides any value that is provided by the MAXFILEPROC parameter of BPXPRMxx. If the system value is adequate, you must leave this field blank.

**MMapAreaMax**

The memory-map-size that you define is a numeric value 1 - 16 777 216. The value that is specified overrides any value that is provided by the MAXMMAPAREA parameter of BPXPRMxx. If the system value is adequate, you must leave this field blank.

**ProcUserMax**

The processes-per-UID that you define is a numeric value 3 - 32 767. The value that is specified overrides any value that is provided by the MAXPROCUSER parameter of BPXPRMxx. If the system value is adequate, you must leave this field blank.

**ThreadsMax**

The threads-per-process that you define is a numeric value 0 - 100 000. Specifying a value of 0 prevents applications that are run by this user from using the pthread\_create service. The value that is specified overrides any value that is provided by the MAXTHREADS parameter of BPXPRMxx. If the system value is adequate, you must leave this field blank.

**MemLimit**

The nonshared-memory-size that you define to RACF is a numeric value 0 - 16777215, followed by the letter M, G, T, or P.

**SHMemMax**

The shared-memory-size that you define to RACF is a numeric value 1 - 16777215, followed by the letter M, G, T, or P. The value that is specified for SHMEMMAX overrides any value that is provided by the IPCSHMNSEGS parameter of BPXPRMxx. If the system value is adequate, you must leave this field blank.

2. To display the current information in the OMVS SEGMENT of a user, enter the userid, and press Enter.
3. To change any or all of the information, enter the new data and press PF5.

If there are any errors, an error message displays, indicating the problem.

You can delete a field from the user's OMVS segment by setting the value to all blanks. For setting the UID to the value zero (0), the terminal user must have the RACF System-SPECIAL attribute. Access to TOOLKIT.SPEC is not applicable to this particular function.

Use the value AUTOUID whenever possible. The AUTOUID function is only available in z/OS 1.4 and higher. It requires definition of the BPX.NEXT.USER profile in the facility class. For more information, see Chapter 2, “zSecure CICS Toolkit installation,” on page 3.

4. To remove the OMVS SEGMENT, press PF11.

**Note:** Removing an OMVS SEGMENT prevents the user from accessing any UNIX System Services. Access to USS might also be provided by the default UID designated by BPX.DEFAULT.USER in the FACILITY class.

## Altering the WORKATTR segment for a user (ALTUSER WORKATTR SEGMENT)

Use the **ALTUSER** command with the WORKATTR SEGMENT option to alter the WORKATTR segment for a specific user.

### About this task

The user needs the following authorizations:

- The user must have access to the zSecure CICS Toolkit command (TOOLKIT.AUSR) and the user default group (AUSR.dfltgrp).
- For managing the WORKATTR segment, the user must have access to TOOLKIT.AWRK.

### Procedure

1. To access the ALTUSER WORKATTR SEGMENT command, press the PF09 key in the main ALTUSER panel.

```
Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      ALTUSER = BCSCGB2             Time = 11:11:32

Name      = John Smith
Account   =
Bldg      =
Dept      = CICS Toolkit Development
Room      = Annex-1
Addr1     = 't Zandt Labs
Addr2     = The Netherlands
Addr3     =
Addr4     =

CQT074 -Command completed successfully
PF5=Update 9=User 11=Delete  Enter=Redisplay CLEAR=Main menu
```

Figure 13. ALTUSER (WORKATTR SEGMENT) panel

#### Name

Specifies the name of the user SYSOUT information is to be delivered to.

#### Account

Specifies an account number for APPC/MVS processing. Although RACF accepts any string of up to 255 characters, the zSecure CICS Toolkit interface allows up to 60 characters.

**Bldg**

Specifies the building that SYSOUT information is to be delivered to.

**Dept**

Specifies the department that SYSOUT information is to be delivered to.

**Room**

Specifies the room SYSOUT information is to be delivered to.

**Addr1**

Address-line-1 specifies other address line for SYSOUT delivery.

**Addr2**

Address-line-2 specifies other address line for SYSOUT delivery.

**Addr3**

Address-line-3 specifies other address line for SYSOUT delivery.

**Addr4**

Address-line-4 specifies other address line for SYSOUT delivery.

2. To display the information in WORKATTR SEGMENT of a user, enter the userid, and press Enter.
3. To change any or all of the information, enter the new data and press PF5.

If there are any errors, an error message displays, indicating the problem. If a field is set to blanks, that parameter is deleted from the users WORKATTR segment.

When you change the WORKATTR segment of the user, ensure that the case of these fields is correct. If your installation requires mixed case values in these fields, you might refrain from updating the WORKATTR segment at all, or ensure that your terminal uses mixed case.

4. To remove the WORKATTR SEGMENT, press PF11.

**Note:** Removing a WORKATTR SEGMENT normally does not affect the users of their authorization to use any system services.

## Connecting a user or group to a group (CONNECT command)

---

Use the **CONNECT** command to connect a user or group to a group.

### About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.CONN) and to the target group (CONN.*grpname*).

### Procedure

1. To access the CONNECT command, press the designated PF key on the main menu.
2. To connect a user to a group, enter the user and group name as indicated and press PF05.  
If there are any errors, such as an invalid user or group name, an error message indicates the problem.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      CONNECT                    Time = 11:14:03

Connect =      Userid      Group =      Group      Authority = U      Owner = BCSCGB1
Special = N      Operations = N      Revokedt =      Resumedt =

```

CQT016 -Enter userid and group name  
PF5=Update ENTER=Redisplay CLEAR=Main menu

Figure 14. CONNECT panel

#### AUTHORITY

Defaults to U (use) but might be set to C<sup>®</sup> (create), N (connect), or J (join).

#### SPECIAL

Specify Y if the user must have the group-special attribute.

#### OPERATIONS

Specify Y if the user must have the group-operations attribute.

#### OWNER

Defaults to the ID of the person who is issuing the command, but any valid user ID or group can be entered.

#### REVOKEDT

The date (YYDDD) the user is prevented from connecting to the group. If today's date is specified, the connection is revoked immediately. In this case, the value of RESUMEDT is ignored, and both the RESUMEDT and the REVOKEDT are reset. The special value 00000 (five zeros) can be used to remove an existing REVOKEDT. Setting the field to blanks or empty, results in leaving the current value unchanged.

#### RESUMEDT

The date (YYDDD) the user can connect to the group. If today's date is specified, the connection is resumed immediately. In this case, the value of REVOKEDT is ignored, and both the RESUMEDT and the REVOKEDT are reset. The special value 00000 (five zeros) can be used to remove an existing RESUMEDT. Setting the field to blanks or empty, results in leaving the current value unchanged.

## Managing CSDATA fields (CSDATA command)

You can use the CSDATA command to list, add, update, or remove CSDATA fields. CSDATA fields are available for USERS and GROUPs. Starting with z/OS 2.4, CSDATA fields are also available for DATASET and General Resource profiles.

### About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.CSDL), the specified class and profile (CSDx.owner), and the CSDATA name (CSDN.csdata-name).

Class	Scope authorization
USER	CSDU.owner



```

Termid = CP03          IBM zSecure CICS Toolkit      Date = 2019/324
Userid = BCSCGB1      Custom Data Fields          Time = 05:05:52

Class = USER         Profile = BCSCGB3
Type = * (G/*)
Name = EMPNUM        Value = 788000001
|<===

```

PF5=Update 11=Delete ENTER=Refresh CLEAR=Back

*Figure 16. CSDATA Detail display panel*

3. To add CSDATA to a profile, enter the class, profile, *csdata-name* and *csdata-value* on the [CSDATA main panel](#). Next, enter an A in the field in front of the CLASS and press **PF05**.

You can also use this same method to delete or update CSDATA fields by using a D or U in this command field. For the D command, the field value is ignored. The methods described in [“4” on page 43](#) and [“5” on page 43](#) are preferred because they are simpler and less error prone.

4. To delete one of the displayed CSDATA name/value pairs, use either the D, L, or S line command.
  - On the [CSDATA main panel](#), type the D line command in front of the CSDATA that you want and press **PF05**.
  - On the [CSDATA main panel](#), type the S or L line command to display the CSDATA value and press **PF11**.
5. To update existing CSDATA values, enter the S (or L) line command in front of the listed CSDATA name to go to the detail panel. On the detail panel, type over the value with the new value and press **PF05**.

When entering new or updated CSDATA values, zSecure CICS Toolkit verifies only the maximum length of the CSDATA field. Other characteristics, like a minimum or maximum numerical value, are not verified. It is the responsibility of the user to provide valid values. Invalid HEX characters are replaced by zeros.

## Deleting a data set (DELETE DATASET command)

Use the **DELETE DATASET** command to delete a data set profile from the system.

### About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.DELD) and the high-level-qualifier of the data set profile name (DELD.hlq). If the user does not have access to the DELD.hlq, standard RACF authority checking is used. Refer to the RACF Command Language Reference manual for information about which data set profiles a user is authorized to delete.

### Procedure

To access the **DELETE DATASET** command, press the designated PF key on the main menu.

```
Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1                                           Time = 11:14:18

Delete = Dsname                                           Generic = Y

CQT144 -Enter dataset profile to be deleted. Specify Y if Generic, N if not
PF5=Update ENTER=Redisplay CLEAR=Main menu
```

Figure 17. DELETE DATASET panel

## Deleting a user profile

Use the **DELETE** command to delete a user profile from the system.

### About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.DELU) and the default group of the user (DELU.dfltgrp).

Before the user profile is deleted, it must be REMOVED from any groups it is connected to except its default group. No data set profiles that have this userid as a high-level qualifier can exist.

zSecure CICS Toolkit checks for group connections but not for data set profiles.

### Procedure

To access the DELETE command, press the designated PF key on the main menu.

```
Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1                                           Time = 11:14:35

Delete = Userid

PF5=Update ENTER=Redisplay CLEAR=Main menu
```

Figure 18. DELETE USER panel

# Listing the profile for one or more data sets (LISTDSET command)

Use the **LISTDSET** command to list the profile for a specific data set or multiple data sets.

## About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.LDSD).

## Procedure

1. To access the **LISTDSET** command, press the designated PF key on the main menu.

```
Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1      Listdset =                          Time = 11:14:47
G , D OR * *          -----
Owner = ***** Cre = ***** Last ref = ***** Last chg = ***** Uacc = *****
Alter acc = ***** Cntrl acc = ***** Updte acc = ***** Read acc = *****
Group ds = * WARN = * Cre grp = ***** Dataset type = **** Level = ***
Audit = * Aud Succ = * Aud Fail = * Glbl audit = * Gaud Succ = * Gaud Fail = *
Sec1 = *** Numctgy = **** NumPgms = **** NumUsrs = ****

-----+-----1-----+-----2-----+-----3-Installation data-5-----+-----6-----+-----7-----+-----
*****
*****
*****
***** |<===
-----+-----1-----+-----2-----+-----3-----+-----4-----+-----5-----+-----6-----+-----7-----+-----

PF1=Toggle 3=Chgopts 5=Userids 7=Programs 11=Search CLEAR=Main menu
```

Figure 19. LISTDSET panel

### LISTDSET

The ID of the data set to be displayed (if you perform a **listuser**). If a search is being done, this field can be bypassed, or any characters can be entered in any position as part of the search criteria.

**Note:** If you are doing a normal **listdset**, the following fields are not used for entry. These other fields are only used as entries if you are doing a search (PF11).

G,D, or \* Allows you to search for generic (G), discrete (D), or both (\*) types of profiles.

### OWNER

A user or group that was defined as the owner of the data set.

### CRE

The date the data set was created. The format is YYDDD.

### LAST REF

The date the data set was last referenced. The format is YYDDD.

### LAST CHG

The date the data set was last updated. The format is YYDDD.

### UACC

The universal access for the data set. This field can be *ALTER*, *CONTROL*, *UPDATE*, *READ*, or *NONE*.

### ALTER ACC

The number of times the data set was accessed with *ALTER*.

### CNTRL ACC

The number of times the data set was accessed with *CONTROL*.

**UPDTE ACC**

The number of times the data set was accessed with UPDATE.

**READ ACC**

The number of times the data set was accessed with READ.

**GROUP DS**

This field can be *Y* or *N*.

**WARN**

Indicates whether the data set is in warning mode. This field can be *Y* or *N*.

**CRE GROUP**

The current connect group of the user that created this data set.

**DATASET TYPE**

This field identifies the data set type. These first two characters in this field indicate a VSAM (*VS*), or Non-VSAM (*NV*) data set profile. The third character indicates whether the profile is a model profile (*M*) or not (*N*). Finally, the fourth character indicates whether the profile is for a tape data set (*T*) or not (*N*).

**LEVEL**

The level indicator for the data set. This field is a numeric field.

**AUDIT**

Indicates the audit flag for the data set. The settings can be: *A* to audit all accesses, *S* to audit successful accesses, *F* to audit failures, or *N* for no auditing.

**AUD SUCC**

The audit *SUCCESS* flag. The settings can be: *R* to audit successful reads, *U* to audit successful updates, *C* to audit successful control accesses, or *A* to audit successful alter accesses.

**AUD FAIL**

The audit *FAILURE* flag. The settings can be: *R* to audit unsuccessful reads, *U* to audit unsuccessful updates, *C* to audit unsuccessful control accesses, or *A* to audit unsuccessful alter accesses.

**GLBL AUDIT**

The Global audit options as specified by a user with the *AUDITOR* attribute. The settings can be: *A* to audit all accesses, *S* to audit successful accesses, *F* to audit failures, or *N* for no auditing.

**GAUD SUCC**

The GLOBAL audit *SUCCESS* flag. The setting can be: *R* to audit successful reads, *U* to audit successful updates, *C* to audit successful control accesses, or *A* to audit successful alter accesses.

**GAUD FAIL**

The GLOBAL audit *FAILURE* flag. The settings can be: *R* to audit unsuccessful reads, *U* to audit unsuccessful updates, *C* to audit unsuccessful control accesses, or *A* to audit unsuccessful alter accesses

**SECL**

The security level of the data set. This field is a numeric field.

**NUMCTGY**

The number of security categories to which the data set belongs.

**NUMPGMS**

The number of programs that are authorized to access the data set.

**NUMUSRS**

The number of users and groups authorized to access the data set.

**INSTALLATION DATA**

The information that is contained in the data sets *DATA* field. This installation data can be up to 255 characters.

2. Press PF05 to display the access list of this data set profile (the users and groups).
3. Press PF07 to display the programs in the conditional access list.
4. Press PF01 to toggle the display (if you are doing a search) and display all the data sets that match the criteria.

5. Press PF03 to clear the fields and enter new criteria for a search or LISTDSET.

## LISTDSET Display Example

You can view the programs in the conditional access list.

```
Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      Listdset =                    Time = 11:15:07
G , D OR * G        SYS1.**

Owner = SYS1      Cre = 05033 Last ref = 05033 Last chg = 05033 Uacc = READ
Alter acc = 000000 Cntrl acc = 000000 Updte acc = 000000 Read acc = 000000
Group ds = Y WARN = N Cre grp = SYS1      Dataset type = NVNN Level = 000
Audit = F Aud Succ = R Aud Fail = R Glbl audit = N Gaud Succ = R Gaud Fail = R
Secl = *** Numctgy = 0000 NumPgms = 0000 NumUsrs = 0003

-----1-----2-----3-Installation data-5-----6-----7-----

                                |<===
-----1-----2-----3-----4-----5-----6-----7-----
PF1=Toggle 3=Chgopts 5=Userids 7=Programs 11=Search CLEAR=Main menu
```

Figure 20. LISTDSET Display panel

Now you can choose to do one of the following:

- Display access list entries (PF05, "userids").
- Display conditional access list entries (PF07, "programs").
- Change the search or list options (PF03).
- Return to the main menu (CLEAR).
- If you are doing a search, display all data sets that meet the criteria (PF01).

## Toggling the LISTDSET panel

If you are doing a search, you can toggle the panel and display all the data sets that match the criteria.

### Procedure

- To do a search, press PF01.  
All data sets that match the criteria are displayed.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      Listdset =                   Time = 11:21:14
                               SYS1.ZTKTEST
G SYSAPPL.**
G SYS1.BROADCAST
G SYS1.MAN**.*
G SYS1.RACF**.*
G SYS1.ZTKTEST
G SYS1.**
D SYS1.ZTKTEST

```

```

CQT064 -End of entries matching this criteria
CQT015 -PF1=Toggle 3=Chgopts ENTER=Next CLEAR=Main Menu

```

Figure 21. LISTDSET Toggle panel

- Choose a PF key for the task you want to to:
  - Change the search or list options (PF03).
  - Return to the main menu (CLEAR).
  - If the panel is full with data sets, display the next panel (ENTER).
  - To perform a LISTDSET on any ID, enter the ID in the LISTDSET field and press PF01.

## Viewing the users authorized, their access authority and access count (LISTDSET USERIDS)

Use the LISTDSET user IDs option to display the users authorized to access the data set, the access authority of the user, and their access count.

### Procedure

- Press PF05 from a LISTDSET panel.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      Listdset = (USERIDS)          Time = 11:22:41
                               SYSAPPL.**
STCUSER /A/00000      C2POLICE/U/00000      BCSCGB1 /A/00000

```

```

PF3=Chgopts 5=Userids 7=Programs 8=Down 9=Datasets ENTER=Next CLR=Main menu

```

Figure 22. LISTDSET USERIDS panel

- Choose a PF key for the task you want to do:
  - Change the search or list options (PF03).
  - Display the programs that can access this data set (PF07).
  - Return to the LISTDSET panel (PF09).
  - Display the next data set if you are doing a search (ENTER).
  - Return to the main menu (CLEAR).

## Viewing the program/userid combination (LISTDSET Programs)

Use the LISTDSET panel to display the program/userid combination that is authorized to access the data set and to display the access authority.

### Procedure

- Press PF07 from a LISTDSET panel.

```

Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1     Listdset = (PROGRAMS)             Time = 11:23:23
                SYS1.RACF*.**
                C2RCARLA/*          /R

PF3=Chgopts 5=Userids 7=Programs 8=Down 9=Datasets ENTER=Next CLR=Main menu

```

Figure 23. LISTDSET Programs

- Choose a PF key for the task you want to do:
  - Change the search or list options (PF03).
  - Display the access list entries (PF05).
  - Return to the LISTDSET panel (PF09).
  - Display the next data set if you are doing a search (Enter).
  - Return to the main menu (CLEAR).

## Listing the profile for one or more groups (LISTGROUP command)

Use the **LISTGROUP** command to list the profile for a specific group or multiple groups.

### About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.LGRP) and the target group (LGRP.grpname).

### Procedure

1. To access the **LISTGROUP** command, press the designated PF key on the main menu.

```

Termid = CP24           IBM zSecure CICS Toolkit           Date = 2007/094
Userid = BCSCGB1       LISTGROUP = *****           Time = 11:23:38

Supgroup = ***** Owner = ***** Univ = * Cre = ***** Uacc = *****
Termuacc = * Number of subgroups = ***** Number of users = *****

Model = *****

-----1-----2-----3-Installation data-5-----6-----7-----
*****
*****
*****
***** |<===
-----1-----2-----3-----4-----5-----6-----7-----

PF1=Toggle 3=Chgopts 4=UserID 5=Users 6=Dfltu 7=Subgrps 11=Search CLR=Main menu

```

Figure 24. LISTGROUP panel

**LISTGROUP**

The ID of the group to be displayed (if performing a listgroup). If a search is being performed, this field can be bypassed, or any characters can be entered in any position as part of the search criteria.

**Note:** If you are performing a normal listgroup, the fields are not used for entries. These other fields are only used as entries if you are doing a search (PF11).

**SUPGROUP**

The superior group to this group.

**OWNER**

A user or group that has been defined as the owner of this group.

**UNIV**

An indicator if it is a Universal group. The list of users connected to a Universal group only shows those users that have non-standard authorizations within the group.

**CRE**

The date this profile was created. The format is YYDDD.

**UACC**

The authority of a user to the group if the user is not connected to the group. This field can be JOIN, CONNECT, CREATE, USE or NONE. This field cannot be set using any RACF command or zSecure CICS Toolkit. It must have a value NONE for all groups, except for the fixed group VSAMDSET.

**TERMUACC**

Indicates if a group or user must be explicitly authorized to access a terminal. This field can be Y or N.

**NUMBER OF SUBGROUPS**

The number of subgroups to this group. This field is a numeric field.

**NUMBER OF USERS**

The number of users connected to this group. This field is a numeric field. For a Universal group, it only reflects the number of users that have non-standard authorizations within the group.

**MODEL**

The name of a discrete data set profile to be used as a model for a new *groupname* data sets. This field is an alphanumeric field.

## INSTALLATION DATA

The information contained in the data sets DATA field. This information can be up to 255 characters.

2. You can either enter a specific group to perform a listgroup on that ID, or enter any character in the field as the search criteria.
  - After entering the search criteria, press **PF11** to start the search.
  - A normal listgroup is performed by entering the group name and pressing **Enter** to open the LISTGROUP panel.
3. Press **PF04** to display the users connected to this group with a DELETEUSER option.
4. Press **PF05** to display the users connected to this group.
5. Press **PF07** to display the subgroups.
6. Use **PF01** to toggle the display (if you are performing a search) and display all the groups that match the criteria.
7. Press **PF03** to clear the fields and enter new criteria for a search or LISTGROUP.

## LISTGROUP Display Example

Enter a group to be listed or initiate a search to display the panel.

```
Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      LISTGROUP = SYSPROG          Time = 11:24:02

Supgroup = SYS1      Owner = SYS1      Univ = N Cre = 05033 Uacc = NONE
Termuacc = Y Number of subgroups = 00000 Number of users = 00003

Model =

-----1-----2-----3-Installation data-5-----6-----7-----
SYSTEM PROGRAMMERS

          |<===
-----1-----2-----3-----4-----5-----6-----7-----

PF1=Toggle 3=Chgopts 4=UserD 5=Users 6=Dfltu 7=Subgrps 11=Search CLR=Main menu
```

Figure 25. LISTGROUP Display panel

Now you can choose to:

- Display users (PF05).
- Display only users that are also connected to your default group.
- Display subgroups (PF07).
- Change the search or list options (PF03).
- Return to the main menu (CLEAR).
- If you are performing a search, display all groups that meet the criteria (PF01).

## Toggle the LISTGROUP panel

If you are doing a search, you can toggle the LISTGROUP panel and displays all groups that match the criteria.

### Procedure

- To perform a search, press **PF01**.  
All groups that match the criteria are displayed.

```
Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      LISTGROUP = SYSADMA          Time = 11:24:21
SYSADMA  SYSAPPL  SYSAUDIT  SYSCTLG  SYSOPRA  SYSPROG  SYS1
```

```
CQT064 -End of entries matching this criteria
CQT015 -PF1=Toggle 3=Chgopts ENTER=Next CLEAR=Main Menu
```

*Figure 26. LISTGROUP Toggle panel*

- Choose a PF key for the task you want to perform:
  - Change the search or list options (PF03).
  - Return to the main menu (CLEAR).
  - If the panel is full with group names, display the next panel (press **Enter**).To perform a listgroup on any name, enter the name in the LISTGROUP field and press **PF01**.

## Listing users for a group (LISTGROUP command, USERIDS option)

You can use the **LISTGROUP** command with the **USERIDS** option to list all the users connected to a group.

### Procedure

- Press **PF05** from a LISTGROUP panel to display all the users connected to the group.

```
Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      LISTGROUP = SYSPROG (USERIDS)      Time = 11:24:47
BCSCGB1 BCSCWN1 BCSCWN2
```

```
PF3=Chgopts 4=UserD 5=Users 6=Dfltu 8=Down 9=Gtprs ENTER=Next CLEAR=Main menu
```

*Figure 27. LISTGROUP USERIDS panel*

- Choose a PF key for the task you want to perform:
  - Change the search or list options (PF03).
  - Display the alternate users display (PF04).
  - Display the subgroups (PF07).
  - Return to the LISTGROUP panel (PF09).
  - Display the next group if performing a search (ENTER).
  - Return to the main menu (CLEAR).

## Deleting user IDs from a LISTGROUP

You can use delete one or more user IDs from the list of user IDs connected to a group.

### Procedure

- Press **PF04** from a LISTGROUP panel to display all the users connected to the group and the option to delete one or more of them.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1     LISTGROUP = SYSPROG (USERS LIST)    Time = 11:25:05

S  Userid  Name                Created  Last signon
-  BCSCGB1  JOHN SMITH           05033   07094
-  BCSCWN1  #####             05033   03126
-  BCSCWN2  #####             05033   02338
-
-
-
-
-
-
-
-
-
-
-
-
-
-

PF3=Chgopts 5=Users 8=Down 9=Grips 11=Deluser ENTER=Next CLEAR=Main menu

```

Figure 28. LISTGROUP Userids Delete panel

- Choose a PF key for the task you want to perform:
  - Change the search or list options (PF03).
  - Display the users display (PF05).
  - Display the subgroups (PF07).
  - Return to the LISTGROUP panel (PF09).
  - Display the next group if performing a search (ENTER).
  - Return to the main menu (CLEAR).
- To delete selected users, enter a D next to the user profile you want to delete and then press **PF11**. Authority to delete the user profile is controlled by the standard zSecure CICS Toolkit DELUSER authorization.

## Listing the subgroups of a group

You can list all the subgroups of a group.

### Procedure

- Press **PF07** from a LISTGROUP panel to display all the subgroups of the group.

```

Termid = CP24           IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1       LISTGROUP = SYS1           (GROUPS)      Time = 11:25:21

SYSCTLG  VSAMDSET  TEST    OMVSGRP  IMWEB    EXTERNAL  EMPLOYEE  SPECIAL
DB2      DSN710    UUCPG   TTY      ADB210   ADCD      APS330    ASU
BP0110   CATALOG   CBC     CEE      CICSTS22 CICSTS23  CRMB      CSQ520
CSQ530   CSQ531    C2RSERVG DCF140   DIT130   DSNA      EOY       EUV
FAN130   FAN140    FMN410  FON210   GDDM     GIM       GLD       GLDGRP
HFS      HLA       ICQ     IGY310   IOE      ISF       ISP       P390
QMFA     QMF710   REVOKE  SCPTST   SMTP     STCGRP    SYSADMA   SYSAPPL
SYSAUDIT SYSOPRA   SYSPROG USER     USERCAT  #EMPLOY   #READ    AUT220
NETV     CDS       CIM     CMX      CSF      ECN       EPH       EUVF
GSK      ICA       IMO     IMW      ING      NFS       BIP210    BIP501
HPJ200   IEL330   IGY330  IXM140   JVA130   JVA140   AUT230    IXM160
NETV510  IXGLOGR  FMN510  IOA      EQA510   IPT110   FFST      AOP
IDI510   ITP110   OMVS    BCSC     ZTKQA    SLDMVSS  CRMA

```

PF3=Chgopts 4=UserD 5=Users 6=Dfltu 8=Down 9=Grips ENTER=Next CLEAR=Main menu

Figure 29. LISTGROUP (Subgroups) panel

- Choose a PF key for the task you want to perform:
  - Change the search or list options (PF03).
  - Display the alternate users display (PF04).
  - Display the users (PF05).
  - Display the users also connected to your default group (PF06).
  - Return to the LISTGROUP panel (PF09).
  - Display the next group if performing a search (ENTER).
  - Return to the main menu (CLEAR).

## Listing the profiles for a user ID (LISTUSER command)

You can use the **LISTUSER** command to list the profile for a specific user ID.

### About this task

#### Procedure

1. To access the LISTUSER command, press the designated PF key on the main menu.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2025/168
Userid = BCSCGB1      LISTUSER = *****      Time = 13:52:41

Name = ***** Owner = ***** Password = ***** Cre = *****
Dfltgrp = ***** Authority = ***** Uacc = ***** Classcnt = ****

Special = * Operations = * Auditor = * Restr = * Grpacc = * Adsp = *
Contained = * Nevercontain = *                               PhrInt = *****
Protected = * Uaudit = * Revoke = * Revokedt = ***** Resumedt = *****

Lastacc = ***** Passdate = ***** Passint = *** PwTry = ** Secl = ***

SMTWTFs From Till Pwdgen = *** Pwdcnt = *** NumCtgy = **** NumGrp = ****
***** ** Model = *****

-----1-----2-----3-Installation data-5-----6-----7-----
*****
*****
***** |<==
-----1-----2-----3-----4-----5-----6-----7-----

PF1=Toggle 3=Chgopts 5=Ctgy 6=Segments 7=Groups 11=Search CLEAR=Main menu

```

Figure 30. LISTUSER panel

**CONTAINED**

Indicates whether the CONTAIN attribute is set for the user (Y/N). A user ID that is quarantined loses privilege immediately; RACF "contains" this user ID.

**LISTUSER**

The ID of the user to be displayed (if performing a listuser). If a search is being performed, this field can be bypassed, or any characters can be entered in any position as part of the search criteria.

**Note:** If you are performing a normal listuser, the fields are not used for entries. These other fields are only used as entries if you are doing a search (PF11).

**NAME**

The user name. A maximum of 20 alphanumeric characters.

If you want to search for a name, or part of a name, anywhere within the name field, use the following format:

To search for, for example, SMITH anywhere in the name field, enter <>SMITH. It returns all profiles that include the characters SMITH anywhere in the name field. The <> characters indicate to zSecure CICS Toolkit that the criterion is a different search criterion for this field than if using wild-card characters (\*).

**NEVERCONTAIN**

Indicates whether the NEVERCONTAIN attribute is set for the user (Y/N). RACF can never quarantine this user ID.

**OWNER**

A user or group that has been defined as the owner of the user.

**PASSWORD**

Not used.

**PHRINT**

The password phrase interval is in effect. This is a numeric field.

**CRE**

The date this profile was created. The format is YYDDD.

**DFLTGRP**

The name of the default group for the user.

**AUTHORITY**

This is the user's authority within the default group. The possible entry for this field is ASORGGAT. The meanings of the subfields are: **A** indicates ADSP, **GA** indicates GROUP AUDITOR, and **T** indicates that terminal access is required.

**UACC**

The universal access of the user for the default group. This field can be **ALTER**, **CONTROL**, **UPDATE**, **READ** or **NONE**.

**CLASSCNT**

The number of classes in which the user is allowed to define profiles.

**SPECIAL**

Indicates whether the user has the SPECIAL attribute (Y/N).

**OPERATIONS**

Indicates whether the user has the OPERATIONS attribute (Y/N).

**AUDITOR**

Indicates whether the user has the AUDITOR attribute (Y/N).

**RESTR**

This field indicates whether the UACC, GAC, and ID(\*) apply for this user (Y/N).

**GRPACC**

Specifies whether group data sets created by this user are accessible to other users in the group (Y/N).

**ADSP**

Indicates that new data sets created by this user are automatically protected by discrete profiles. This field can be **c**.

**PROTECTED**

This field indicates whether the user ID can be used by specification of the password (Y/N). PROTECTED user IDs can only be propagated, started, or used through surrogate.

**UAUDIT**

Indicates whether all RACHECKs and RACDEFs issued for the user can be logged (Y/N).

**REVOKE**

Indicates whether the REVOKE attribute is set for the user (Y/N).

**REVOKEDT**

The date that the user is revoked. The format is *YYDDD*.

**RESUMEDT**

The date the user is resumed. The format is *YYDDD*.

**LASTACC**

The date and time the user last accessed the system by using RACINIT. The format is *YYDDD/HH:MM:SS*. If the user has never logged on, this field contains **?** in the first position.

**PASSDATE**

The date the users password was last changed. The format is *YYDDD* or the field is zero if it has been reset.

**PASSINT**

The interval that the users password is in effect. This field is a numeric field.

**PWTRY**

The number of unsuccessful password attempts by this user. This field is a numeric field.

**SECL**

The security level of the user. This field is a numeric field.

**SMTWTFS**

The days of the week that the user can logon. **Y** indicates that the user can logon for that day. **N** indicates that the user is restricted for that day.

**FROM**

If the user is restricted by time, FROM is the starting time that the user might log on at. The format is *HHMM*. If there are no time restrictions, both the FROM and TILL fields are **0000**.

**TILL**

The latest time the user can logon to the system. The format is *HHMM*.

**PWDGEN**

The current password generation number for the user. This field is a numeric field.

**PWDCNT**

The number of old passwords that are present for this user. This field is a numeric field.

**NUMCTGY**

The number of security categories the user has access to. This field is a numeric field.

**MODEL**

The data set profile model for this user. This field is an alphanumeric field.

**INSTALLATION DATA**

The information contained in the user's DATA field. This information can be up to 255 characters.

2. You can either enter a specific userid to perform a LISTUSER on that user, or enter any character in the field as the search criteria.
  - After entering the search criteria, press **PF11** to start the search.
  - A normal LISTUSER is performed by entering the userid and pressing **Enter**.
3. Press **PF05** to display the categories for this user.
4. Press **PF07** to display the groups.
5. Use **PF01** to toggle the display (if you are performing a search) and display all the users that match the criteria.
6. Press **PF03** to clear the fields and enter new criteria for a search or LISTUSER.

## LISTUSER Display Example

This example shows what might be displayed if you specify a user ID and press **Enter**, or enter different criteria and press **PF11** to initiate a search.

**Note:** If you enter a full user ID and click **PF11**, you obtain the same results as if you clicked **Enter** because there is only one profile with the specified user ID.

```

Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1      LISTUSER = BCSCGB2              Time = 11:25:55

Name = GUUS 2ND          Owner = BCSC          Password = ???????? Cre = 05033
Dfltgrp = BCSC          Authority =              Uacc = NONE          Classcnt = 0001
Special = N Operations = Y Auditor = N Restr = N Grpacc = N Adsp = N
Protected = N Uaudit = N Revoke = N Revokedt = ***** Resumedt = *****
Lastacc = 07089/09:17:57 Passdate = 07068 Passint = 180 PwTry = 00 Sec1 = ***
SMTWTFS From Till    Pwdgen = 006 Pwdcnt = 006 NumCtgy = 0000 NumGip = 0005
YYYYYYY 0000 0000    Model =

-----1-----2-----3-Installation data-5-----6-----7-----

                                |<===
-----1-----2-----3-----4-----5-----6-----7-----

PF1=Toggle 3=Chgopts 5=Ctgy 6=Segments 7=Groups 11=Search CLEAR=Main menu

```

Figure 31. LISTUSER Display panel

From this point, you can choose to:

- Display the categories (PF05).
- Display the groups (PF11).
- Change the search or list option (PF03).
- Return to the main menu (CLEAR).
- If you are performing a search, display all users that meet the criteria (PF01).

## Toggle the LISTUSER panel

You can use the LISTUSER panel to list all the users that match the criteria you enter.

### Procedure

- To perform a search, press PF01.  
All users that match the criteria are displayed.

```

Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1      LISTUSER = B8FU0142                Time = 11:32:50

B8FTEST  B8FU0000 B8FU0001 B8FU0002 B8FU0003 B8FU0004 B8FU0005 B8FU0006
B8FU0007 B8FU0008 B8FU0009 B8FU0010 B8FU0011 B8FU0012 B8FU0013 B8FU0014
B8FU0015 B8FU0016 B8FU0017 B8FU0018 B8FU0019 B8FU0020 B8FU0021 B8FU0022
B8FU0023 B8FU0024 B8FU0025 B8FU0026 B8FU0027 B8FU0028 B8FU0029 B8FU0030
B8FU0031 B8FU0032 B8FU0033 B8FU0034 B8FU0035 B8FU0036 B8FU0037 B8FU0038
B8FU0039 B8FU0040 B8FU0041 B8FU0042 B8FU0043 B8FU0044 B8FU0045 B8FU0046
B8FU0047 B8FU0048 B8FU0049 B8FU0050 B8FU0051 B8FU0052 B8FU0053 B8FU0054
B8FU0055 B8FU0056 B8FU0057 B8FU0058 B8FU0059 B8FU0060 B8FU0061 B8FU0062
B8FU0063 B8FU0064 B8FU0065 B8FU0066 B8FU0067 B8FU0068 B8FU0069 B8FU0070
B8FU0071 B8FU0072 B8FU0073 B8FU0074 B8FU0075 B8FU0076 B8FU0077 B8FU0078
B8FU0079 B8FU0080 B8FU0081 B8FU0082 B8FU0083 B8FU0084 B8FU0085 B8FU0086
B8FU0087 B8FU0088 B8FU0089 B8FU0090 B8FU0091 B8FU0092 B8FU0093 B8FU0094
B8FU0095 B8FU0096 B8FU0097 B8FU0098 B8FU0099 B8FU0100 B8FU0101 B8FU0102
B8FU0103 B8FU0104 B8FU0105 B8FU0106 B8FU0107 B8FU0108 B8FU0109 B8FU0110
B8FU0111 B8FU0112 B8FU0113 B8FU0114 B8FU0115 B8FU0116 B8FU0117 B8FU0118
B8FU0119 B8FU0120 B8FU0121 B8FU0122 B8FU0123 B8FU0124 B8FU0125 B8FU0126
B8FU0127 B8FU0128 B8FU0129 B8FU0130 B8FU0131 B8FU0132 B8FU0133 B8FU0134
B8FU0135 B8FU0136 B8FU0137 B8FU0138 B8FU0139 B8FU0140 B8FU0141 B8FU0142

CQT015 -PF1=Toggle 3=Chgopts ENTER=Next CLEAR=Main Menu

```

Figure 32. LISTUSER Toggle panel

- Choose a PF key for the task you want to perform:
  - Change the search or list options (PF03).
  - Return to the main menu (CLEAR).
  - If the panel is full with userids, display the next panel (ENTER).

To perform a LISTUSER on any ID, enter the ID in the **LISTUSER** field and press **PF01**.

## Listing groups for a user ID (LISTUSER command, GROUPS option)

You can use the **LISTUSER** command with the Groups option to display the groups that a user ID is connected to.

### Procedure

- Press **PF07** from a LISTUSER panel to display the groups that a user is connected to.

```

Termid = CP24           IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1       LISTUSER = BCSCGB1 (Groups)      Time = 11:33:30
BCSC      #READ      P390      SYSAUDIT SYSPROG  CRMA      CRMB

```

PF3=Chgopts 5=Ctgy 6=Segment 7=Group 8=Down 9=User ENTER=Next CLEAR=Main menu

*Figure 33. LISTUSER GROUPS panel*

- Choose a PF key for the task you want to perform:
  - Change the search or list options (PF03).
  - Display the categories for this user (PF05).
  - Return to the LISTUSER panel (PF09).
  - Display the next user if performing a search.
  - Return to the main menu (CLEAR).

## Listing categories for a user ID (LISTUSER command, Categories option)

You can use the LISTUSER command with the Categories option to list the categories that a user ID is connected to.

### Procedure

- Press PF05 from a LISTUSER panel to display the categories that a user is connected to.

```

Termid = CP24           IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1       LISTUSER = BCSCGB1 (Categories)  Time = 11:34:40
00000001

```

PF3=Chgopts 5=Ctgy 6=Segment 7=Group 8=Down 9=User ENTER=Next CLEAR=Main menu

*Figure 34. LISTUSER (Categories) panel*

- Choose a PF key for the task you want to perform:
  - Change the search or list options (PF03).
  - Display the groups for this user (PF07).
  - Return to the LISTUSER panel (PF09).
  - Display the next user if performing a search.
  - Return to the main menu (CLEAR).

## Listing the TSO and CICS segments for a user ID (LISTUSER command, Segments option)

You can use the **LISTUSER** command with the Segments option to list the TSO and CICS segments for a user ID.

### Procedure

- Press **PF06** from a LISTUSER panel to display the TSO and CICS segments for the user.

```

Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1      LISTUSER = BCSCGB2 (Segments-1)    Time = 11:34:54

TSO
Acctnum = *
Destid  =
HClass  =              JClass =              MsgClass=              SClass  =
Size    = 0000000      Maxsize = 0000000      Seclabl =
Proc    = ISPFPROC     Unit    =              Udata   = 0000

CICS
OPIdent = 123
OPPrty  = 123
Timeout = 0000
XRFSoff = NOFORCE
OPClass =

RSLKey  =
TSLKey  =

PF3=Chgopts 5=Ctgy 6=Segment 7=Group 8=Down 9=User ENTER=Next CLR=Main menu

```

Figure 35. LISTUSER (Segments)

- Press **PF08** to display the OMVS and WORKATTR segments. Pressing **PF08** again scrolls up to the previous segment display.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1     LISTUSER = BCSCGB2 (Segments-2)    Time = 11:35:00

OMVS
  UID      = 0000002009
  Home     =
  Program  =
  ASSizeMax =
  FileProcMax =
  ProcUserMax =
  MemLimit =
  CPUTimeMax =
  MMapAreaMax =
  ThreadsMax =
  SHMemMax =

WORKATTR
  Name     = JOHN SMITH
  Account  =
  Bldg     =
  Dept     = CICS TOOLKIT DEVELOPMENT
  Room     = ANNEX-1
  Addr1    = 'T ZANDT LABS
  Addr2    = THE NETHERLANDS
  Addr3    =
  Addr4    =

PF3=Chgopts 5=Ctgy 6=Segment 7=Group 8=Up 9=User ENTER=Next CLR=Main menu

```

Figure 36. LISTUSER: OMVS and WORKATTR panel

- Choose a PF key for the task you want to perform:
  - Change the search or list options (PF03).
  - Display the groups for this user (PF07).
  - Return to the LISTUSER panel (PF09).
  - Display the next user if performing a search.
  - Return to the main menu (CLEAR).

## Granting or removing access to a resource (PERMIT command)

You can use the **PERMIT** command to grant or remove access to a resource.

### About this task

The resource might be in:

1. One of the resource classes defined in the SIT for this run of CICS or
2. Any other general resource class or the DATASET class.

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.PEMT) and the default group of the user ID or group (PEMT.dfltgrp)

### and

If the resource is in a class defined in the SIT, the user must also have access to the resource, at a level equal to or higher than the level of access that is being given. After the PERMIT has been completed, the resource classes must be recreated in order to have immediate effect. zSecure CICS Toolkit does not provide a way for issuing the required **SETROPTS REFRESH** command.

If the resource is in any other class, the user must also have authority to issue **PERMIT** commands in that class (PEMX.classname), and also to the resource, at a level equal to or higher than the level of access that is being given.

### Procedure

1. To access the **PERMIT** command, press the designated **PF** key on the main menu.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1     Permit                          Time = 11:35:10

User/Grp =           Rsrcclass =

Resource =

<===

Delete = N      Access = R  (R=Read,N=None,U=Update,A=Alter,C=Control)
Specify "Delete = Y" to remove the user from the access list

CQT029 -Enter userid/group name and resource
PF5=Update ENTER=Redisplay CLEAR=Main menu

```

Figure 37. PERMIT panel

#### USERID

The name of the user or group to be granted access (or removed).

#### RESOURCE

The name of the resource (for example, CEMT if it was the transaction CEMT).

#### RSRCLASS

The resource class name. If blank, the value of the XTRAN parameter specified in the SIT is used.

#### DELETE

Specify Y in this field to remove a user or group from the access list for this resource.

#### ACCESS

Specify R for READ access or N for NONE, U for update, A for alter or C for control. If N is specified, the user must have a minimum of READ authority to issue the command.

2. Update or specify the information and press **PF5**.

The user executing the **PERMIT** command must have access to the resource that is being altered. For example, if access is being given to CEMT, the user must have access to CEMT. If **DELETE** is specified as **Y**, the user executing the command must still have access to the resource. The level of access required is whatever specified in the **ACCESS** field.

## Maintaining associations (RACLINK command)

You can use the **RACLINK** command to define, list, undefine, or approve user associations.

### About this task

The **RACLINK** command only works with local nodes. Independent of the value of the **NODE** specified on the panel, zSecure CICS Toolkit assumes it to be the name of the local node.

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.RACL). To issue a **RACLINK** for a different user, the user must have RACF Special, TOOLKIT.SPEC or access to the default group of the user (RACL.dfltgrp).

### Procedure

1. To access the **RACLINK** command, press the designated PF key on the main menu.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2017/199
Userid = BCSCGB1      RACLINK = BCSCGB1          Time = 08:17:09

D PEER      STRX      BCSCGB4  YES (          ) <= Password(optional)
  ---TYPE--- --NODE-- --USERID- PWD
                Sync   Status                Created by YYYY/MM/DD

- PEER OF    IDFX     IBMUSER  NO           ESTABLISHED      BCSCGB1    2007/04/04
- PEER OF    IDFX     BCSCGB2  NO           ESTABLISHED      BCSCGB1    2007/04/04
- PEER OF    OBLX     BCSCGB2  NO           ESTABLISHED      BCSCGB1    2007/04/04
-
-
-
-
-
-
-
-
-
-
-
-

PF5=Update 8=Down ENTER=List CLEAR=Main menu

```

Figure 38. RACLINK panel

**TYPE**

The type of association. It can be PEER or MANAGED.

**NODE**

The name of the node where the association is defined.

**USERID**

The user that the association is being defined for.

**PWD SYNC**

Specifies if the association has password synchronization or not (enter YES or NO)

**PASSWORD**

Optional parameter. The password for the user specified.

2. In the field RACLINK =, enter the user for which the command is being issued. Press **Enter** to list the associations for that user.
3. Enter a U to the left of an association and then press PF05 to cause it to be undefined.
  - The association needs to be for your own ID, or you need system special, TOOLKIT.SPEC or RACL.dfltgrp.
  - If the association is awaiting approval and it is your own ID (or you have system special or zSecure CICS Toolkit special), you can approve it by entering A to the left of it and pressing PF05.
  - In the preceding display, a new association is about to be defined. After the user presses the PF5 key, the new association is defined. The D must be present to indicate a DEFINE.
  - The association is implicitly approved if a valid PASSWORD was provided or the issuer of the command has RACF SPECIAL, TOOLKIT.SPEC or RACL.dfltgrp.
  - To define a new user association, you need access to the normal RACLINK authorizations as defined for the TSO RACLINK command. These authorizations are RACLINK.DEFINE.nodename and RACLINK.PWSYNC.nodename.

## Listing and maintaining profiles in a general resource class (RALTER / RDEFINE / RDELETE commands)

You can use the **RALTER**, **RDEFINE**, and **RDELETE** commands to list and maintain profiles in a general resource class defined in the CDT.

### About this task

The user must have access to the zSecure CICS Toolkit command (**TOOLKIT.RALT** / **TOOLKIT.RDEF** / **TOOLKIT.RDEL**, depending on the command being performed) and to the general resource class (RLST.cdtclass in addition to RALT.cdtclass / RDEF.cdtclass / RDEL.cdtclass).

### Procedure

1. To access the **RALTER** / **RDEFINE** / **RDELETE** command, press the designated **PF** key on the main menu.

```
Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1      RES Class =                      Type =          Time = 11:37:16
Profile

Member

Owner =                Notify =                Uacc = None      Warn = N Level = 000
Audit = F Aud succ = R Aud fail = R

-----1-----2-----3-Installation data-5-----6-----7-----

                                |<===
-----1-----2-----3-----4-----5-----6-----7-----

PF1=Rdef PF2=Addmem PF3=Rdel PF4=Delmem PF5=Updprof ENTER=Rlst CLEAR=Main menu
```

Figure 39. RALTER / RDEFINE / RDELETE panel

### RDEFINE

To define a new profile/resource, all fields are required, except for the installation data. After entering these information, press **PF01** to perform the **RDEFINE**.

### RDELETE

To delete a profile/resource, enter the CLASS and PROFILE names and press **PF03**.

### RALTER

Allows you to add a new member to a group (ADDMEM), delete a member from a group (DELMEM), or update the profile information (UPDPROF). The information required depends on the subcommand being performed.

#### ADDMEM

Requires the CLASS, PROFILE and MEMBER to be added. Press **PF02** to complete the ADDMEM.

#### DELMEM

Requires the CLASS, PROFILE and MEMBER to be deleted. Press **PF04** to delete the member.

#### UPDPROF

Requires all fields, except for the installation data. By entering the **CLASS** and **PROFILE** fields and pressing **Enter**, all the current entries for each field display. These entries can then be over stepped. Press **PF05** to complete the update.

2. Specify the values for the action you want to perform using the field descriptions in step 1, then press the corresponding **PF** key to initiate the change.

## Removing user IDs or groups from a group (REMOVE command)

You can use the **REMOVE** command to remove user IDs or groups from a group. User IDs cannot be removed from their default group.

### About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.REMV) and the target group (REMV.grpname).

### Procedure

1. To access the REMOVE command, press the designated PF key on the main menu.

```
Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1                                           Time = 11:37:31

Remove = Userid      Group =

CQT016 -Enter userid and group name
PF5=Update ENTER=Redisplay CLEAR=Main menu
```

Figure 40. REMOVE panel

2. To remove a user from a group, enter the user and group name as indicated and press **PF05**. Users cannot be removed from their default group.

## Listing the profiles for a general resource class (RLIST command)

You can use the **RLIST** command to list the profiles for a general resource class defined in the CDT.

### About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.RLST) and the general resource class (RLST.cdtclass).

### Procedure

1. To access the **RLIST** command, press the designated **PF** key on the main menu.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1     Rlist class =          Type =          Time = 11:37:41
                          Profile

```

```

-----
-----
-----
Owner = ***** Dte = ***** Last ref = ***** Last chg = ***** Uacc = *****
Audit = * Aud succ = * Aud fail = * Notify = ***** Warn = * Level = ***
Glbl Audit = * Gaud Succ = * Gaud Fail = * Secl = ***
Members = **** NumUsrs = **** Condacc = ****

----+----1----+----2----+----3-Installation data-5----+----6----+----7----+----
*****
*****
*****
***** |<===
-----1-----2-----3-----4-----5-----6-----7-----
PF1=Toggle 3=Chgopts 5=Members 7=Users 9=Condacc 11=Search CLEAR=Main menu

```

Figure 41. RLIST panel

### RLIST CLASS

This is the name of the resource class to be displayed. It must be a valid entry in the RACF Class Descriptor Table.

### TYPE

This defines the class as being a member (TYPE=M) or group (TYPE=G) class. It is provided as information only and is not used as input for a list or search.

### PROFILE

The name of the profile to be displayed. Enter the name of the profile to be displayed in this field. If a search is being performed, this field can be bypassed, or any characters can be entered in any position as part of the search criteria. This field can be up to 246 characters in length.

**Note:** If you are only performing an **RLIST**, the rest of the fields are ignored. The remaining fields are only used as input when doing a search (PF11).

### OWNER

A user or group that has been defined as the owner of the profile.

### DTE

The date this profile was created. The format is *YYDDD*.

### LAST REF

The date the data set was last referenced. The format is *YYDDD*.

### LAST CHG

The date the profile was last updated. The format is *YYDDD*.

### UACC

The universal access for the profile. This field can be ALTER, CONTROL, UPDATE, READ or NONE.

### AUDIT

Indicates the audit flag for the profile. The settings can be: A to audit all accesses, S to audit successful accesses, F to audit failures, or N for no auditing.

### AUD SUCC

This is the audit SUCCESS flag. The settings can be: R to audit successful reads, U to audit successful updates, C to audit control accesses, or A to audit successful alter accesses.

### AUD FAIL

This is the audit FAILURE flag. The settings can be: R to audit unsuccessful reads, U to audit unsuccessful updates, C to audit unsuccessful control accesses, or A to audit unsuccessful alter accesses.

**NOTIFY**

The user to be notified when access is denied to this profile.

**WARN**

Indicates if the profile is in warning mode. This field can be **Y** or **N**.

**LEVEL**

The level indicator for the data set. This field is a numeric field.

**GLBL AUDIT**

The Global audit options as specified as by a user with the AUDITOR attribute. The settings can be: A to audit all accessed, S to audit successful accesses, F to audit failures, or N for no auditing.

**GAUD SUCC**

This is the GLOBAL audit SUCCESS flag. The settings can be: R to audit successful reads, U to audit successful updates, C to audit successful control accesses, or A to audit successful alter accesses.

**GAUD FAIL**

This is the GLOBAL audit FAILURE flag. The settings can be: R to audit unsuccessful reads, U to audit unsuccessful updates, C to audit unsuccessful control accesses, or A to audit unsuccessful alter accesses.

**SECL**

The security level of the profile. This field is a numeric field.

**MEMBERS**

The number of members in this profile, if it is a group profile.

**NUMUSRS**

The number of users and groups authorized to access the profile. This field is a numeric field.

**CONDACC**

The number of user/groups on the conditional access list. This field is a numeric field.

**INSTALLATION DATA**

The information contained in the DATA field of the profile. It can be up to 255 characters.

2. You can choose to:

- Display the users/groups with access to the profile (PF07).
- Display users/groups on the conditional access list (PF09).
- If the resource class is a group class, as indicated by the **TYPE=** field, display the members in the profile (PF05).

When displaying members, users, or the conditional access list, you can use **PF08** page down if there is more than one panel to be displayed.

## **RLIST Display Example**

This example shows what is displayed when you enter a profile to be listed.

If you enter a profile to be listed, or initiate a search, the next panel is displayed as follows.

```

Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1      Rlist class = GCICSTRN Type = G          Time = 11:38:02
                                Profile
CICSA.CAT1

Owner = SYS1          Dte = 05033 Last ref = 05033 Last chg = 05033 Uacc = NONE
Audit = F Aud succ = R Aud fail = R Notify = ***** Warn = N Level = 000
Glbl Audit = N Gaud Succ = R Gaud Fail = R Sec1 = ***
Members = 0051 NumUsrs = 0003 Condacc = 0000
-----+-----1-----+-----2-----+-----3-Installation data-5-----+-----6-----+-----7-----+-----
|<===
-----+-----1-----+-----2-----+-----3-----+-----4-----+-----5-----+-----6-----+-----7-----+-----
PF1=Toggle 3=Chgopts 5=Members 7=Users 9=Condacc 11=Search CLEAR=Main menu

```

Figure 42. RLIST Display panel

From this point, you can choose to:

- Display the members (PF05).
- Display the users (PF07).
- Display the conditional access list (PF09).
- Change the search or list options (PF03).
- Return to the main menu (CLEAR).
- If you are performing a search, display all profiles that meet the criteria (PF01).

## Listing the members in a profile (RLIST command, MEMBERS option)

You can use the **RLIST** command with the Members option to list the members in a profile.

### Procedure

- Press **PF05** from an RLIST panel to display the members in profile.

```

Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1      Rlist      = (MEMBERS)          Time = 11:38:12
CICSA.CAT1

CICSA.CRTP
CICSA.CPIR
CICSA.CATA
CICSA.CATD
CICSA.CDBD
CICSA.CDBF
CICSA.CDBO
CICSA.CDBQ
CICSA.CDTS
CICSA.CESC
CICSA.CESD
CICSA.CEX2
CICSA.CFCL
CICSA.CFOR
CICSA.CFQR
CICSA.CFQS
CICSA.CFTL
CICSA.CFTS

PF1=Toggle 3=Chgopts 5=Memb 7=User 8=Down 9=Condacc ENTER=Next CLEAR=Main menu

```

Figure 43. RLIST Members panel

- From this point, you can choose to:
  - Display the users (PF07).
  - Display the conditional access list (PF09).
  - Change the search or list options (PF03).
  - Return to the main menu (CLEAR).
  - If you are performing a search, display the next profile (ENTER).

## Listing user IDs in a profile and the access they have (RLIST command, USERS option)

You can use the **RLIST** command with the Users option to list the user IDs in the profile and the access they have.

### Procedure

- Press **PF07** from an RLIST panel to display the users in the profile and the access they have.

```

Termid = CP24          IBM zSecure CICS Toolkit          Date = 2007/094
Userid = BCSCGB1      Rlist = (USERS)                 Time = 11:38:23
CICSA.CAT1

IBMUSER /A CICSA    /R CICSASTC/R

PF1=Toggle 3=Chgopts 5=Memb 7=User 8=Down 9=Condacc ENTER=Next CLEAR=Main menu

```

*Figure 44. RLIST Users panel*

- From this point, you can choose to:
  - Display the members (PF05).
  - Display the conditional access list (PF09).
  - Change the search or list options (PF03).
  - Return to the main menu (CLEAR).
  - If you are performing a search, display the next profile (ENTER).

## Listing users/groups in the conditional access list for a profile (RLIST command, CONDACC option)

You can use the **RLIST** command with the Conditional Access option to list the users/groups in the conditional access list for the profile.

### Procedure

- Press **PF09** from an RLIST panel to display the user/groups in the conditional access list for the profile.

```
Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      Rlist = (CONDACC)          Time = 11:39:04
CICSA.CAT1

BCSC /R-TERMINAL=D20AK021
```

```
PF1=Toggle 3=Chgopts 5=Memb 7=User 8=Down 9=Condacc ENTER=Next CLEAR=Main menu
```

*Figure 45. RLIST Conditional Access panel*

- From this point, you can choose to:
  - Display the members (PF05).
  - Display the users (PF07).
  - Change the search or list options (PF03).
  - Return to the main menu (CLEAR).
  - If you are performing a search, display the next profile (Enter).

## Managing USRDATA fields (USRDATA command)

---

You can use the **USRDATA** command to list, add, update, or remove the USRDATA fields from a user profile. For information about the special SMF record created for updates to USRDATA, see [“SMF records created by zSecure CICS Toolkit”](#) on page 77.

### About this task

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.USRL), the userid (USRU.dfltgrp), and the USRDATA name (USRN.*usrdata-name*). For the **ADD**, **UPDATE** and **DELETE** subfunctions, access to the corresponding command profile is required (TOOLKIT.USRA for **ADD** and **UPDATE** or TOOLKIT.USRD for **DELETE**).

### Procedure

1. To access the **USRDATA** command, press the designated **PF** key on the main menu.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      USRDATA                      Time = 11:39:16

Fill in Profile and ENTER. For Add, fill in fields, select A and PF5
_ Class = _____ Profile = _____
  Name = _____ Value = _____

_____ |<===
Name      Value      (Use S/L and ENTER for details, or D and PF5 for delete)
-
-
-
-
-
-
-
-
-
-
CQT018 -Enter userid
PF5=Update 8=Down ENTER=List CLEAR=Main menu

```

Figure 46. USRDATA panel

2. To display USRDATA of a user, enter the user ID and press **Enter**.
  - The USRDATA names and the first 64 characters of the corresponding values display on the bottom part of the panel.
  - If more USRDATA names are present than fit on the panel, press **PF8** to scroll down.
  - For an untruncated display of one USRDATA value, use the **S** (or **L**) command in front of the wanted USRDATA name/value and press **Enter**.

```

Termid = CP24          IBM zSecure CICS Toolkit      Date = 2007/094
Userid = BCSCGB1      USRDATA                      Time = 11:41:00

  Class = USER      Profile = BCSCGB2
  Name =  PHONE     Value = +1_123-456-7890

_____ |<===

PF5=Update 11=Delete ENTER=Refresh CLEAR=Back

```

Figure 47. USRDATA Display panel

3. To add USRDATA for a user, enter the name and value of the USRDATA, then enter an A in the field in front of the **CLASS** and press **PF5**.

You can also use this same method to delete or update USRDATA fields from selection of a D or U in this command field. This latter method is an alternative to the preferred methods described here.
4. To delete one of the displayed USRDATA name/value pairs, use either of the following methods:
  - Use the **D** command in front of the USRDATA you want, and press **PF5**.
  - Use the **S** or **L** line command to display the USRDATA value, followed by **PF11** on the detail panel.

5. To update existing USRDATA values, go to the detail panel obtained by using **S** (or **L**) in front of the listed USRDATA name. On the detail panel, type over the value with the new value and press **PF5**.



---

## Chapter 6. zSecure CICS Toolkit exit points specifications

In the EXITPGM parameter in CQTPCNTL, you can specify a program that is to receive control whenever the main zSecure CICS Toolkit transaction (normally RTMM) terminates and returns control to CICS.

Control is passed to the EXITPGM through the XCTL command. zSecure CICS Toolkit does not receive control again after the EXITPGM, which includes a return code and the data, if any, that was sent to the user's panel. The format of the COMMAREA is as follows:

EXITRC	DC CL1	Return Code 0 = CICS Toolkit transaction has terminated 1 = Signon transaction failed or was terminated with the clear key 3 = Signon completed. User was signed-on at a second terminal but was not authorized (did not have access to TOOLKIT.DUPE and DUPEUSER checking is in effect). 4 = Signon completed. Same as 3, but terminal logged off CICS. 5 = Signon completed. No CICS segment found for user. 6 = Signon completed. CICS segment was found for user. 7 = Signon completed. Error in installation data being used for operator information.
* EXITDATA	DC CL335	Data sent to users screen from signon or CICS Toolkit transaction termination. If the return code is 0, this field is only 79 bytes in length. For any other return code, this field will contain the data, if any, that was sent to the terminal user.

A sample EXITPG is provided in the SCQTSAMP pds as member CQTXSNEX.



## Chapter 7. Application programming interface (API)

The zSecure CICS Toolkit Applications Programming Interface allows users to access the RACF database directly from a CICS application program. No special knowledge of RACF or its database format is required and the applications do not need to run authorized.

Using the API, an installation can tailor the zSecure CICS Toolkit panels to suit their own requirements, or produce different types or reports. zSecure CICS Toolkit ensures that only authorized users access the RACF database. The same rules apply when using the API as for using zSecure CICS Toolkit. The user executing a transaction that is using the API must be authorized to the zSecure CICS Toolkit commands used. If requesting user information, the user must have access to the default group of the user profile being displayed. For more information about this subject, see Chapter 5, “The zSecure CICS Toolkit command interface,” on page 29.

Using the API is a procedure that only requires the CICS application program to call the interface module, CQTPAPI0, and pass certain parameters to it in a COMMAREA. These parameters inform zSecure CICS Toolkit of the command being requested and also provide the storage area where the requested information is returned.

For compatibility reasons, the CQTPAPI0 program has an alias CRTKAPI. Although both names refer to the same module, use the new name, CQTPAPI0, in all applications.

zSecure CICS Toolkit does not cause the CICS main task to wait while it is reading or updating the RACF database. All these commands are processed by the zSecure CICS Toolkit subtasks, leaving CICS free to continue with normal transaction processing. This CICS region does not run in an authorized state at any time, in keeping with the IBM statement of integrity.

### SMF records created by zSecure CICS Toolkit

All changes that zSecure CICS Toolkit makes to RACF profiles are recorded through SMF. The changes that directly correspond to RACF commands, like ALTUSER, are recorded using the same format as used by those RACF commands. These records also include the terminal user that requested the change and show up in your normal RACF reports. To distinguish these records from the SMF records that are created from TSO and batch jobs, the field SMF80UID has the value TOOLKIT\*. This special value is used to indicate that the record was produced as part of a zSecure CICS Toolkit function.

Changes to the USRDATA fields do not correspond to any regular RACF command. Therefore, it is not possible to use the same record format. A RACF General Audit event SMF record is used with the LOGSTR showing the changed data. The log string consists of 6 character strings that are separated by a single blank:

Field	Length	Content
Header	15	TOOLKIT USRDATA
Class	4	USER
Profile	8	userid
Action	6	{ADD, UPDATE, DELETE, LIST}
UserNm	8	Field name
UserData	max. 209	Field value (truncated)

## Command requests using the COMMAREA

The COMMAREA is the way zSecure CICS Toolkit is informed of the command being requested. The size of the COMMAREA varies depending upon the command being executed. In all cases, there is a common header, followed by specific information for the relevant command.

The format of the header is as follows:

API_FUNCT	DC	CL4	This field specifies the command being requested.
*			
*			
API_RC	DC	XL1	A one byte hexadecimal return code.
*			
*			
API_MSG	DC	CL79	The message that would normally be displayed on the terminal if the user was using the standard Toolkit transaction is returned in this field.
*			
*			
*			

The application program invokes the API using a standard CICS LINK command:

```
EXEC CICS LINK PROGRAM('CQTPAPI0') COMMAREA(APICOMM) LENGTH(APILEN)
```

If a COMMAREA is not passed, CTKAPI just returns to the caller without any further processing. If an error is detected in the COMMAREA layout, either the length or the command requested is invalid. Or, the user is not authorized to the zSecure CICS Toolkit COMMAND and the API sets API\_RC with a return code, indicating the nature of the error. The possible return codes are:

RETURN CODE

### **X'00'**

COMMAREA is correct

### **X'01'**

An invalid command was requested. Check the parameter specified in API\_FUNC and verify that it is correct.

### **X'02'**

The length of the COMMAREA is too small for the requested command.

### **X'03'**

The user is not authorized to use this zSecure CICS Toolkit COMMAND or is not signed on at the terminal.

### **X'04'**

There was no profile protecting the TOOLKIT.*function* resource. An authorization decision could not be made, and the API function was not executed.

### **X'05'**

Internal error, contact Technical Support

If the commarea passed to the API is correct, but the function fails for some other reason, the API\_RC contains the value x'00'. The function-specific return code field (typically called API\_*function*\_RC) contains an error indicator. Most API-functions use the value -1 as indicator that an error occurred. The field API\_MSG contains the error message describing the failure. Here are the examples of these messages:

- CQT039 is for the **ALTUSER** command if the specified ID does not exist.
- CQT080 is for the **LIST** commands if the requested profile cannot be found.

For the complete text of the error messages, see the *IBM zSecure: Messages Guide*.

All fields in the COMMAREA must be padded with blanks unless indicated otherwise in the documentation.

## Change the authorized user

To execute a command through the API, the userid associated with the task must be authorized to the zSecure CICS Toolkit command. This userid is normally the one for the user logged on at the terminal or the CICS default user. You might specify a different userid to be the authorized user.

To change the authorized user, make the following definition in the first 24 bytes of the API-MSG area before calling CQTPAPI0:

API Message Variable	Value	Description
API_MSG_USERAUTH	DC CL8'USERAUTH'	A constant of USERAUTH
API_MSG_USERID	DC CL8'USERAUTH'	The USERID to be used as the authorized user.
API_MSG_PASSWORD	DC CL8' <i>password</i> '	The PASSWORD for the user.

If the password is incorrect for the user, the command fails and the appropriate message is returned to the calling program.

## Perform a search

A search of the RACF database can be performed using the **LISTUSER**, **LISTGROUP**, **LISTDATASET**, and **RLIST** commands.

The COMMAREA for each of these commands contains a one-byte code field. It indicates whether a search is being performed, if the next profile must be retrieved, or if other information about the profile is required.

When a search is requested, the profile attribute fields in the COMMAREA must be padded with asterisks. The search mask can be any combination of valid characters or letters in any combination of fields. When zSecure CICS Toolkit finds a match, it returns the profile information into the COMMAREA. To retrieve the next profile that matches the search criteria, set the code field in the COMMAREA to N (next) and call the API. The profile itself must not be padded with asterisks, but instead must be padded with blanks (x'40'), nulls (x'00') or underscores (x'6D'). The reason for this exception to the general masking rule, is to allow a specific search for profiles containing generic characters.

As zSecure CICS Toolkit returns the profile information into the COMMAREA, you must build the search mask in working storage and move it to the COMMAREA before each call to the API. There is also an API\_RESERVED field used by the API during a search and the contents of this field must be preserved between calls.

To retrieve all profiles (for example, all user profiles), the search mask must be all asterisks. Initiate<sup>®</sup> the search by specifying S in the code field. You can then retrieve the rest of the profiles by setting the code field to N. Continue to call the API until a non-zero return code is returned. The API\_MSG field also contains a message indicating that there are no more profiles matching the criteria or that you have reached the end of the RACF database. Remember to recreate the search mask before each call.

## Implementing field or record level security

Field or record level security can be implemented by using the API resource authorization checking capabilities, especially when using resource names of up to 246 bytes.

### About this task

By defining resource names that represent a particular field or record within a file, access to those records/fields can be restricted. An application program can call the API to verify the access authority of a user and determine what action must be taken. The action includes updating the record, displaying the record, updating the field, blanking out the field, and so on.

An example might be for a file with a DDNAME of PAYFILE, whose keys are social security numbers.

## Procedure

1. Define the DDNAME and social security numbers to RACF:

```
RDEFINE RSRCLASS PAYFILE.999-99-999 UACC(NONE)
```

2. Permit the user to the record:

```
PERMIT PAYFILE.999-99-999 CLASS(RSRCLASS) ID(USERIDA) ACC(READ)
```

## What to do next

The application can now call the API to perform a resource access check and determine the users' level of access to the record/field.

## Access Authority Check function

You can use the Access Authority Check function to determine if a user has access to one or more resources. No authority is required.

### COMMAREA

Minimum size 99 bytes.

In your application, use the CQTMPIA or CQTMPIIC mapping macros (copybooks) provided in the SCQTMAC library. Example:

```
API_FUNC      DC  CL4'RSRC'  FUNCTION code for access check
API_RC        DC  XL01'00'  Return code
API_MSG       DC  CL79' '    Message area
*
API_RSRC_NAMES DC  XCL14    This is a list of resources for
*                          which the access authority of the user
*                          signed on at the terminal is to be checked.
*                          The size of this field depends on the
*                          number of resources being checked. Each
*                          resource name requires thirteen bytes,
*                          padded with blanks, followed by a one byte
*                          return code field.
*
*                          The return code field may also specify the
*                          level access to be checked. This may be
*                          'R' (read), 'U' (update), 'C' (control) or
*                          'A' (alter). Read is the default.
*
*                          For example to check the users access to
*                          AUDIT and PAYROLL the following
*                          entries could be coded.
*
*                          DC  CL13'AUDIT'  First resource name
*                          DC  XL1'00'    Return Code
*                          DC  CL13'PAYROLL' Next resource name
*                          DC  XL1'00'    Return Code
*
*                          DC  XL1'FF'    The last field in the COMMAREA
*                          must be a one byte field containing X'FF',
*                          indicating the end of the list of
*                          resource names.
```

The resource class used when making the access check is that specified in the RSRCLASS parameter in CQTPCNTL.

If a prefix has been specified for application resource names (see the CICSAPPL parameter of CQTPCNTL), it is used to prefix the resource names passed to CQTPAPI0. Refer to [Chapter 4, "Application security management,"](#) on page 25 for more information about application security and defining resources to RACF.



```

API_RSRX_ACC      EQU API_RSRX_NAMES+246,1
                   The access level
*
*                   For example to check the users access to
*                   AUDIT and PAYROLL the following entries
*                   could be coded.
                   DC CL246'AUDIT'      First resource name
                   DC XL1'00'          Return Code
                   DC CL246'PAYROLL'    Next resource name
                   DC XL1'00'          Return Code
*
                   DC XL1'FF'          The last field in the COMMAREA must be a
*                                       one byte field containing X'FF',
*                                       indicating the end of the list of
*                                       resource names.

```

The resource class used when making the access check is that specified in the RSRCLASS parameter in CQTPCNTL. If specified, the value in API\_RSRX\_RSRCLASS overrides that in CQTPCNTL.

If a prefix has been specified for application resource names (see the CICSAPPL parameter of CQTPCNTL), it is used to prefix the resource names passed to CQTPAPI0. Refer to [Chapter 4, “Application security management,”](#) on page 25 for more information about application security and defining resources to RACF.

SMF records are produced depending on the (GLOBAL)AUDIT parameters that are specified for the resources. If you want to suppress the ICH408I messages on the system console and the CICS log, you can specify the value S or N in the API\_RC field:

#### **S**

Overrides the LOGGING parameter value Y in CQTPCNTL. Also suppresses possible access violation messages, while still creating SMF records about these violations.

#### **N**

Overrides the LOGGING parameter value Y or S in CQTPCNTL. Also suppresses both the possible ICH408I messages and the SMF records for violations and successful access.

The resource return codes are a 1-byte hexadecimal field with the following meanings:

#### **RETURN CODE:**

##### **X'00'**

Access allowed to resource.

##### **X'04'**

The resource is not defined to RACF.

##### **X'08'**

The user is not authorized to use the resource.

##### **X'0C'**

RACF is not active.

##### **X'10'**

FRACHECK installation exit error.

##### **X'14'**

RACF is not installed or at the wrong level.

## Resource Profile List function

You can use the Resource Profile List function to provide a list of the profiles accessible to a user. No authorization is required.

You can use a function provided through the zSecure CICS Toolkit API for high-performance listing of all authorized profiles in a specified resource class. This API provides an alternative to the combined SEARCH and RLIST interfaces. You can use it to list all profiles in the specified resource class to which a user has access at a certain level. Internally, the API is based on high-performance RACF functions like the Profile Name List function (IRRPNL00) and the fast authorization checking function (RACROUTE REQUEST=FASTAUTH). This function is available only through the API.

## COMMAREA

Minimum size 146 bytes.

In your application, use the APICOMMA or APICOMMC mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'RSRL'	FUNCTION code for Resource List
API_RC	DC	XL1'00'	API Return code
API_MSG	DC	CL79' '	Message area
*			
API_RSRL_RETC	DS	XL1	Return code
API_RSRL_REAS	DS	XL1	Reason code
API_RSRL_CLASS	DS	CL8	CLASS
API_RSRL_USERID	DS	CL8	USERID or blank
API_RSRL_GROUP	DS	CL8	GROUPLD or blank
API_RSRL_TSQUEUE	DS	CL16	TSQUEUE name or blank
API_RSRL_Prefix	DS	CL16	Filter prefix or blank
API_RSRL_Retflag	DS	CL1	Processing flags
*			"C" Return data in Commarea
*			"T" Return data in TSQUEUE
*			"B" Return data in Comm/TSQ
*			"N" Don't return any data
API_RSRL_FL_PR	DS	CL1	Use filter prefix Y/N
API_RSRL_FL_AC	DS	CL1	Return all profiles Y/N
API_RSRL_ACCESS	DS	CL1	Requested Access
*			"R" Read
*			"U" Update
*			"C" Control
*			"A" Alter
API_RSRL_PROFCNT	DS	XL4	Returned number of entries
API_RSRL_PROFLST	DS	XL2	Length of the profile below (CLx)
	DS	CL1	Flag byte
*			Possible values for the flag byte
*			"A" Access to discrete profile
*			"N" READ to discrete profile
*			"B" Access to generic profile
*			"G" READ to generic profile
	DS	CLx	Profile

Output of this function consists of a list of profile names. The list is returned in the provided commarea or in the specified Temporary Storage Queue (TSQUEUE). The return option set in API\_RSRL\_RETFLAG determines which of the return areas is used. The list of profiles contains either all profiles to which the user has at least READ access or only those profiles to which the user has at least the access specified in API\_RSRL\_ACCESS. The API\_RSRL\_FL\_AC flag byte controls what the list of profiles contains. You can filter the list of profiles based on the first characters of the profile name. Specify the filter pattern in the field API\_RSRL\_Prefix. Filtering is activated by the API\_RSRL\_FL\_PR flag byte.

When profiles are to be returned in a CICS TSQUEUE, a non-recoverable MAIN-storage TSQUEUE must be specified. When using a recoverable TSQUEUE, the program might terminate with an ATSP ABEND. Using an AUXILIARY storage queue might involve I/O to auxiliary storage, impacting the application response time. If you want the associated system resources freed, the calling program must delete the TSQUEUE after processing the data.

When profiles are to be returned in the provided COMMAREA, be sure that the commarea is sufficiently large. If the output data does not fit in the provided space, the data is truncated and a message is issued. This RSRL API does not allow retrieval of the remainder of the truncated data. If additional data is required, the request must be re-issued providing a larger commarea, or requesting that output is returned in a TSQUEUE.

The specified resource class must have been RACLISTed using the RACF SETROPTS command. Globally RACLISTed resource classes, like the CICS resource class TCICSTRN, are not supported.

The following list describes the fields in the API commarea.

### API\_FUNC

Describes the function being called. For the List Authorized Resources function, it must contain 'RSRL'.

**API\_RC**

The API return code. This is the return code for the API interface. The return code from the RSRL function is provided in the API\_RSRL\_RETC field. Possible values for the API\_RETC are described in [“Command requests using the COMMAREA”](#) on page 78.

**API\_MSG**

A warning or error message.

**API\_RSRL\_RETC**

The return code from the RSRL function. See [“Return and Reason codes”](#) on page 86 for a description of the possible return codes.

**API\_RSRL\_REAS**

The reason code from the RSRL function. See [“Return and Reason codes”](#) on page 86 for a description of the possible reason codes.

**API\_RSRL\_CLASS**

The resource class for which the authorized profiles are required. This resource class must be RACLISTed using the SETROPTS RACLIST command. Globally RACLISTed resource classes, like the CICS resource class TCICSTRN, are not supported. If the resource class is not SETROPTS RACLIST, an error message is issued and execution stops. The class name must be specified in full. Abbreviations and generic characters are not supported.

**API\_RSRL\_USERID**

The user for which the list of authorized profiles is to be determined. If this field is empty, the list of authorized profiles is determined for the logged-on terminal user. The field is considered empty if the first position contains either a blank or a hexadecimal null.

**API\_RSRL\_GROUP**

The RACF group to be used for the user specified in API\_RSRL\_USERID. This field must either be empty or contain a valid non-revoked group connect for the specified user. This field is ignored if the API\_RSRL\_USERID field is empty.

**API\_RSRL\_TSQUEUE**

Specifies the CICS Temporary Storage Queue (TSQUEUE) to be used for the output data. The TSQUEUE name is up to 16 characters long, and must be padded with blanks or nulls. The name must be that of a non-recoverable MAIN-storage TSQUEUE. Recoverable TSQUEUEs are not supported. Using an AUXILIARY storage queue might involve I/O to auxiliary storage, impacting the application response time. If you want the associated system resources freed, the calling program must delete the TSQUEUE after processing the data. This field is ignored if the API\_RSRL\_RETFLAG has any value other than T or B.

**API\_RSRL\_PREFIX**

Specifies the prefix filter to be used for filtering the authorized profiles. The prefix is up to 16 characters long, and must be padded with blanks or nulls. The prefix is used to compare against the profiles, similar to the process used for the TSO SEARCH MASK keyword. The first characters of the profile name must match the characters specified for the prefix filter. If these characters do not match, the profile is skipped and is excluded from the list of profiles.

**API\_RSRL\_RETFLAG**

Specifies processing flags. The following values for the processing flags can be used:

**C**

The output data is returned in the COMMAREA. The number of entries located is shown in the API\_RSRL\_PROFCNT field. If the COMMAREA is too small, this number can be higher than the actual number of profiles in the COMMAREA.

**T**

The output data is returned in the specified TSQUEUE. The number of entries located is shown in the API\_RSRL\_PROFCNT field.

**B**

The output data is returned in the COMMAREA and the specified TSQUEUE. The number of entries located is shown in the API\_RSRL\_PROFCNT field.

## **N**

No output data is returned in either the COMMAREA or the specified TSQUEUE. The number of entries that might have been returned is still shown in the API\_RSRL\_PROFCNT field.

### **API\_RSRL\_FL\_PR**

The prefix filter is used to limit the profiles listed. Possible values are Y or N. Any other value is treated as if the value is N.

### **API\_RSRL\_FL\_AC**

The output data always includes only those profiles to which the user has at least READ access. Profiles to which the user has no access are never shown. The API\_RSRL\_FL\_AC flag can be used to reduce the profiles returned. Possible values for the flag are Y and N. Any other value is treated as if the value is N.

If this flag has the value N, only the profiles to which the user has at least the requested access are returned. If this flag has the value Y, all profiles to which the user has at least READ access are returned, and the profile flag shows whether the user has only READ access or the requested access.

### **API\_RSRL\_ACCESS**

Specifies the minimum required access of the user. Possible values are R for READ, U for UPDATE, C for CONTROL, or A for ALTER. If this field is empty or contains any other value, access is determined as if the value R was specified. If the user has access at the requested access level or higher, the profile flag has the value A or B. If the user does not have the requested access, the profile flag has the value N or G.

### **API\_RSRL\_PROFCNT**

This output field shows the number of entries listed. If the response area is large enough, it contains the number of profiles returned. If the response area is too small, it contains the number of profiles that would have been returned if the response area were large enough.

### **API\_RSRL\_PROFLST**

This part of the commarea contains the list of authorized profiles. It consists of an array of profiles using the following format:

#### **NAME LENGTH**

The 2-byte length of the profile name. This value does not include the length of the length field itself or the length of the FLAG byte.

#### **FLAG**

A 1-byte flag field. Possible values for this return flag are:

##### **A**

The user has access to the discrete profile at the requested access level or higher.

##### **B**

The user has access to the generic profile at the requested access level or higher.

##### **N**

The user does not have the requested access to the discrete profile. The user has READ access to the profile.

##### **G**

The user does not have the requested access to the generic profile. The user has READ access to the profile.

#### **PROFILE NAME**

A variable-length profile name

If the application requests to return those profiles to which the user has at least READ access, the profile flag for the returned profiles has the value A or B. In this situation the values N and G are not used. If the requested access is one of the other values, all four values for the profile flag are used.

## TSQUEUE usage for profiles

If the application specifies the value **T** or **B** in the **API\_RSRL\_RETFLAG** field, the profiles are returned in the TSQUEUE specified in the **API\_RSRL\_TSQUEUE** field.

The TSQUEUE must be a non-recoverable MAIN-storage TSQUEUE. Recoverable TSQUEUES are not supported. Using an AUXILIARY storage queue is discouraged because it might involve I/O to auxiliary storage, impacting the application response time. The API program clears the entire TSQUEUE before writing any records. If you want the associated system resources freed, the calling program must delete the TSQUEUE after processing the data.

Each of the requested profiles is written in a separate record. The layout of the record is identical to that of the API\_RSRL\_PROFLST shown in the preceding list.

## Return and Reason codes

Some of the return and reason codes returned by this API are specific ones for this function, and some are the ones used by RACF for the IRRPNL00 function.

The following list summarizes the specific return and reason codes. See *z/OS Security Server RACF Macros and Interfaces* for information about the return and reason codes for the IRRPNL00 function.

### **RC=00**

No error occurred. The requested profiles are provided in the specified areas.

### **RC=04**

See IRRPNL00 return and reason codes.

### **RC=08**

See IRRPNL00 return and reason codes.

### **RC=0C**

REAS=00 The internal work area used to process the authorized profiles is too small. Only profile list requests that need less than 128Kbyte of data can be processed.

REAS=04 Profile return in a TSQUEUE was requested, but no TSQUEUE name is given.

REAS=08 The terminal user does not have access to the specified TSQUEUE name.

REAS=0C The COMMAREA provided is not large enough to contain all authorized profiles.

### **RC=14 to RC=24**

See IRRPNL00 return and reason codes.

### **RC=32**

RACROUTE REQUEST=VERIFY for the specified user failed. See message CQT030 for the RACF return and reason codes.

## Access check and DATA retrieval (RSRD)

---

The RSRD function can be used to retrieve the USERDATA associated with the access specification for a user ID.

The user access can be granted through an individual permit, a group connection, access to ID(\*), or through the UACC. If matching entries are defined in the USERDATA fields in the appropriate profile, the associated DATA is returned to the caller of the API function.

## Retrieval of USERDATA

The USERDATA is retrieved for the alphabetically highest, best fitting ACL entry from the most specific or alphabetically highest member or grouping class profile that was used during the RACLIST processing of the resource profiles for the class.

In sequence, the following items are checked to determine where to retrieve the USERDATA:

1. A direct permit to the user ID.

2. An indirect permit through a group that the user ID is connected to.
3. If access is granted through multiple groups, the alphabetically highest group.
4. Access granted through ID(\*).
5. Access granted through the UACC.
6. If access is granted through a member-class profile and one or more grouping-class profiles, the member-class profile.
7. If access is granted through multiple grouping-class profiles, the alphabetically highest grouping-class profile.

This strategy is probably best illustrated by using an example. The purpose of this first example is mainly to show the profile from which the USERDATA is retrieved. Subsequent examples focus on determining which USERDATA entry is used to locate the requested DATA.

As an example, assume that the following profiles are defined in the resource classes \$GROUP and \$MEMBER:

```
$GROUP GRPA Addmem(MEMA, MEMB) READ(USER1, USER2, GROUP1)
$GROUP GRPB Addmem(MEMA, MEMC) READ(USER1, USER3, GROUP2)
$MEMBER MEMA READ(USER4)
USER1 CONNECT(GROUP1, GROUP2)
USER2 CONNECT(GROUP1)
USER3 CONNECT(GROUP2)
USER4 CONNECT(GROUP4)
USER5 CONNECT(GROUP1, GROUP2)
```

When the RSRD API is called for resource MEMA and user USER2, the API function checks that USER2 has access. Because the user has a direct permit, the USERDATA entry for USER2 is retrieved. Also, USER2 has access to only one profile. Therefore, the USERDATA is retrieved from that single profile \$GROUP GRPA.

When the API is called for MEMA and user USER1, the API function detects that USER1 has access through profiles \$GROUP GRPA and \$GROUP GRPB. The relevant ACL entry for both profiles is the same (USER1). In that case, the highest alphabetical profile is used. Therefore, USERDATA is retrieved from profile \$GROUP GRPB.

For USER5 accessing MEMA, access is granted through groups GROUP1 and GROUP2. Two different grouping-class profiles are involved and access is granted through two different GROUPs. When different GROUPs grant access, the alphabetically highest group (GROUP2) is used.

For the access of USER4 to MEMA, only one profile is relevant: \$MEMBER MEMA.

The following table shows the profiles that are used to retrieve the applicable USERDATA.

<i>Table 7. Profiles used to retrieve USERDATA</i>			
<b>User</b>	<b>MEMA</b>	<b>MEMB</b>	<b>MEMC</b>
USER1	GRPB/USER1	GRPA/USER1	GRPB/USER1
USER2	GRPA/USER2	GRPA/USER2	None
USER3	GRPB/USER3	None	GRPB/USER3
USER4	MEMA/USER4	None	None
USER5	GRPB/GROUP2	GRPA/GROUP1	GRPB/GROUP2

It is possible to specify in the API parameter list that access is to be checked at a certain level. This access level is used for the access verification process, but is not used to determine the most applicable USERDATA entry. So, if USER5 has UPDATE access through GROUP1 and READ access through GROUP2, the USERDATA is always retrieved for GROUP2, even though the actual access is granted through GROUP1.

## Definitions of USERDATA entries

USERDATA entries consist of two parts: the USRNM and the USRDATA. The USRNM is used as an index to locate the associated USRDATA.

In the remainder of this information, the term USRDATA is used to refer to the data-value field in the RACF database, and the term USERDATA is used to refer to the combination of the two fields.

The USERDATA can be entered into the RACF profiles, for example, by using the CKGRACF function of zSecure Admin. The correct implementation for the RSRD function requires that each ACL entry is mirrored by a USERDATA entry. Additional USERDATA entries can be defined for the UACC and access granted through ID(\*). Entries defined for the UACC are represented by a USRNM of -UACC-, and entries for access granted through ID(\*) are represented by a USRNM of -STAR-. ACL entries for users or groups that have ACCESS=NONE must *not* be represented in the USERDATA entries.

The USRDATA can contain any character that is supported by the tool that is used to add these values to the profile. The zSecure CICS Toolkit RSRD function does not impose any restrictions on the characters used. Embedded blanks are allowed. The maximum length of the USRDATA returned by RSRD to the application is 64 characters.

**Note:** As stated earlier, the correct implementation for the RSRD function *requires* that each ACL entry with access other than NONE is mirrored by a USERDATA entry. The RSRD function detects inconsistencies where information is missing. However, some types of inconsistencies are not detected, and might lead to unexpected results. For example, if a USERDATA entry is missing on the member-class profile that granted access, but is present on one of the applicable grouping-class profiles, the absence of the correct USERDATA entry might be undetected. Another example might be that DATA for ID(\*) is returned when data for a GROUP was expected.

## Additional considerations

When using the RSRD function, also consider the information in this topic.

Although the resource name can be up to 246 characters, the profiles used to define access to the resource have a maximum length of 40 characters. If longer profile names are used, they are truncated at 40 positions. If profile truncation occurs, the value returned for the USERDATA is undefined.

If grouping-class profiles are used, the RSRD function process must determine the name of that grouping-class profile. However, during the SETROPTS RACLIST processing, the name of the grouping-class profile is dropped and it is no longer available in memory. As a substitute for the grouping-class profile name, the RSRD function uses the APPLDATA of the profile. The APPLDATA is retained in the in-memory profiles built during SETROPTS RACLIST processing. To provide the profile name to the RSRD function, the name of the profile must be specified in the APPLDATA of the profile itself. Although not needed for member-class profiles, adding the profile name to the APPLDATA of member-class profiles is also supported. Examples of such definitions are:

```
RDEFINE $GROUP GRP1 ADDMEM(RES1,RES2) APPLDATA('GRP1')
RDEFINE $GROUP GRP2 ADDMEM(RES3,RES4) APPLDATA('GRP2')
RDEFINE $MEMBER RES5 APPLDATA('RES5')
```

As a result of these definitions, the following in-memory logical profiles are built during RACLIST processing:

```
$MEMBER RES1 APPLDATA(GRP1)
$MEMBER RES2 APPLDATA(GRP1)
$MEMBER RES3 APPLDATA(GRP2)
$MEMBER RES4 APPLDATA(GRP2)
$MEMBER RES5 APPLDATA(RES5)
```

Using this approach, the RSRD function can use the APPLDATA to locate the correct grouping-class profile. For example, the data for resource RES1 can be retrieved from profile GRP1 in class \$GROUP.

Using the APPLDATA is insufficient if the same resource is defined as a member in multiple grouping-class profiles. During RACLIST processing, profiles are combined into in-memory (logical) profiles. However,

only one value for the APPLDATA is retained. Using the example profiles introduced in [“Retrieval of USERDATA”](#) on page 86, the following in-memory profiles are built:

```
$MEMBER MEMA APPLDATA(MEMA) READ(USER1,USER2,USER3,USER4,GROUP1,GROUP2)
$MEMBER MEMB APPLDATA(GRPA) READ(USER1,USER2,GROUP1)
$MEMBER MEMC APPLDATA(GRPB) READ(USER1,USER3,GROUP2)
```

During the RACLIST processing, only one APPLDATA value is retained. For example, the in-memory logical profile for MEMA only has the APPLDATA value for MEMA, and the information from GRPA and GRPB is no longer available. This situation can be remedied by implementing the RACLIST exits. See [“Use of RACLIST exits”](#) on page 89.

## Use of RACLIST exits

To accommodate members that are defined in multiple grouping-class profiles, RACLIST exits can be exploited.

(For an example of accommodating members that are defined in multiple grouping-class profiles, see [“Retrieval of USERDATA”](#) on page 86 .)

zSecure CICS Toolkit provides two RACLIST exits for this purpose.

### ICHRLX01

The RACLIST preprocessing and postprocessing exit. It is used to determine whether special processing is needed for the resource class being RACLISTed. A resource class is eligible for special RACLIST processing if the class name is included in the APPLDATA of profile ICHRLX02.PROCESS.CLASS in the XFACILIT resource class. An example of the profile is:

```
RDEFINE XFACILIT ICHRLX02.PROCESS.CLASS APPLDATA('$MEMBER')
```

### ICHRLX02

The RACLIST selection or processing exit. In this implementation, the APPLDATA of the in-memory profile is updated to contain a list of all profiles that contributed to the resulting in-memory logical profile. Profiles in the RACF database itself are unaffected by this exit.

If both exits are active at the time of the RACLIST or the SETROPTS REFRESH RACLIST command, the following in-memory logical profiles are created:

```
$MEMBER MEMA APPLDATA(MEMA GRPB GRPA) READ(USER1,USER2,USER3,USER4,GROUP1,GROUP2)
$MEMBER MEMB APPLDATA(GRPA) READ(USER1,USER2,GROUP1)
$MEMBER MEMC APPLDATA(GRPB) READ(USER1,USER3,GROUP2)
```

Notice that the only difference is the value of the in-memory APPLDATA. It now has a list of *all* the contributing profiles.

If these RACLIST exits are used, it is no longer necessary to specify any APPLDATA value on the profiles in the RACF database. The exit will use the profile names directly to build the in-memory list that the RSRD function uses.

## Restrictions

When using the provided RACLIST exits to support definition of the same member as part of multiple grouping or member class profiles, the following limitations apply:

- The total length of the profile names that contribute to the in-memory profile for a resource cannot exceed 255 bytes. If more characters are needed, some profile names are truncated.
- A maximum of 16 grouping and member class profiles can be used to define the effective protection of a single resource. If more profiles are used, some profile names are ignored.
- Each profile name can have a maximum length of 40 characters. If profile names have more characters, the profile name is truncated.

## API specification

This section describes the COMMAREA as required for the RSRD API function.

### FUNCTION

Check whether a user has access to a resource, and retrieve the associated value of the USERDATA.

### AUTHORITY

None required.

### COMMAREA

Minimum size 412 bytes.

In your application, use the CQTMPIA or CQTMPIIC mapping macros (copybooks) provided in the SCQTSAMP library.

API_FUNC	DC	CL4'RSRD'	Function code for access check
API_RC	DC	XL01'00'	Return code
*			On input, the following values are supported
*			"S" Suppress ICH408I messages for violations
*			"N" Suppress ICH408I messages and SMF Audit
API_MSG	DC	CL79' '	Message area
*			
API_RSRD_USERID	DC	CL8	Userid for which the access must be checked and for which the associated USRDATA must be retrieved.
*			If blank, the ACEE of the userid signed on at the terminal is used. On return, this field contains the id that was used to retrieve the associated USRDATA.
*			
API_RSRD_ACC	DC	C11	The required access level. Valid values are 'R' (read), 'U' (update), 'C' (control) or 'A' (alter). Read is the default. On return, this field contains the return code from the function.
*			
API_RSRD_CLASS	DC	CL8	This field specifies the resource class for the resource. This class must be RACLISTed through SETROPTS RACLIST. On return this field contains the resource class of the matching profile.
*			
API_RSRD_NAME1	DS	XL1	Length of the resource name. The specified length can be greater than the actual resource name, provided it is padded with blanks up to the specified length.
*			
API_RSRD_NAME	DS	CL246	Name of the resource. On return, this field contains the name of the profile used.
*			
API_RSRD_DATA	DS	CL64	On return, this field contains the USRDATA associated with the userid.
*			

Most fields in the COMMAREA are used for input and output. On output, the API\_RSRD\_CLASS and API\_RSRD\_NAME reflect the profile used for the retrieval of the API\_RSRD\_DATA. Also, the API\_RSRD\_USERID contains the value of the USRNM index in the USERDATA used to retrieve the API\_RSRD\_DATA. Because most fields are updated as part of the process, you must reinitialize the entire COMMAREA on each call.

Auditing the access verification through SMF records is done based on the AUDIT settings of the RACF profiles or through RACF SETROPTS LOGOPTIONS. If you want to suppress ICH408I resource access violation messages on the system console and in the CICS log, you can specify the value "S" in the API\_RC field. Specifying this value results in suppression of possible access violation messages, while still creating SMF records about these violations. It is also possible to specify the value "N" in the API\_RC field. In that case, both ICH408I resource access violation messages and SMF auditing are suppressed. If you do not specify an "S" or an "N" character, messages and SMF records can be suppressed according to the settings in CQTPCNTL.

## Return codes

The return codes are returned in the field API\_RSRD\_ACC.

In the following list, the return codes are shown as 1-byte hexadecimal fields with the following meanings:

### **X'00'**

Access to the resource is allowed. The API COMMAREA is updated with the information retrieved for the associated USRDATA.

### **X'04'**

The resource is not defined to RACF.

### **X'08'**

The user is not authorized to use the resource at the specified access level.

### **X'0C'**

USRDATA specification error. The user has access to the specified resource, but no associated USRDATA value could be found.

### **X'10'**

USERID specification error. The user ID specified in the API COMMAREA could not be used. Check the system log for the corresponding ICH408I message for additional information about why setting up the security environment for this user ID failed.

### **X'14'**

Profile consistency error. The RSRD function uses the information in the in-storage APPLDATA field to determine the name of grouping class profiles that contribute to the RACLISTed in-memory profile. The APPLDATA information is incorrect and contains profile names that do not exist.

### **X'18'**

CLASS specification error. The resource class specified in the API COMMAREA could not be found in the system.

## Installation considerations

When using the RACLIST exits, these exits must be active at the time that an initial RACLIST or a SETROPTS RACLIST REFRESH is done.

To make these exits active at the correct time, either install the provided exits in a SYSTEM library using the RACF names ICHRLXnn, or use the zSecure Exit Activator function (program C2XACTV), followed by a SETROPTS RACLIST REFRESH command. The C2XACTV program is provided as part of the zSecure Admin, zSecure Audit, and zSecure Alert products.

If the same resource class is used in multiple LPARs and RACF sysplex communication is enabled, the RACLIST exits must be installed and active on all systems in the sysplex.

The ICHRLX01 exit uses the word at offset 48 (X'30') in the exit parameter list to communicate to the ICHRLX02 exit if the current resource class must be processed. If you have your own RACLIST exits in place, they cannot use that same communication area.

Using the provided exits as regular RACF exits is only supported if you currently do not have any RACLIST exits active. If you have, your exits cannot use the communication area mentioned before and you must modify your exits to call the exits provided with zSecure CICS Toolkit. Also, your ICHRLX01 exit cannot specify non-default RACLIST merge rules for the UACC, UADIT, GLOBALAUDIT, INSTDATA, and APPLDATA fields.

To install as a regular RACF exit, follow these steps:

1. Rename the supplied exit routines from CQTRLX01 and CQTRLX02 into ICHRLX01 and ICHRLX02. The C2XRLZxx routines are not used.
2. Copy exit routines ICHRLX01 and ICHRLX02 to an LPALIST data set; for example, zSecure CICS Toolkit SCQTLPA.
3. IPL your system with CLPA.

4. Ensure that the required resource classes are set up as RACLISTed.

To install the exits using the zSecure Exit Activator program, follow these steps:

1. Run a job similar to the following one, using a concatenation of the zSecure Admin and zSecure CICS Toolkit load libraries as steplib.

```
//C2XACTV EXEC PGM=C2XACTV
//STEPLIB DD DISP=SHR,DSN=<ZSECURE.SCQTLOAD>
//          DD DISP=SHR,DSN=<ZSECURE.SCKRLOAD>
//SYSTSPRT DD SYSOUT=*
//C2XPRINT DD SYSOUT=*
//C2XIN DD *
DYNEXIT DEACTIVATE ICHRLX01 DIRECT
DYNEXIT RECOVER ICHRLX01 DIRECT
DYNEXIT ACTIVATE ICHRLX01 DIRECT
DYNEXIT DEACTIVATE ICHRLX02 DIRECT
DYNEXIT RECOVER ICHRLX02 DIRECT
DYNEXIT ACTIVATE ICHRLX02 DIRECT
```

The user ID running this job must have UPDATE access to the following profiles:

```
XFACILIT C2X.ICHLX01
XFACILIT C2X.ICHLX02
```

2. Issue a SETROPTS RACLIST or SETROPTS RACLIST REFRESH for the required resource classes.

The provided RACLIST exits perform no processing unless a profile has been defined in the XFACILIT resource class. The APPLDATA of the profile specifies for which resources classes the exit must create in-memory APPLDATA values for use by the zSecure CICS Toolkit RSRD function. An example of the profile follows:

```
RDEFINE XFACILIT ICHRLX02.PROCESS.CLASS APPLDATA('$MEMBER')
```

## ADDGROUP / ALTGROUP / DELGROUP function (add, alter, or delete a group)

Use the ADDGROUP, ALTGROUP, and DELGROUP function to add a new group to the system or to alter or delete an existing group.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (**TOOLKIT.ADGR / TOOLKIT.ALGR / TOOLKIT.DELG / TOOLKIT.LGRP**, depending in the command being performed) and the group (ADGR.grpname / ALGR.grpname / DELG.grpname / LGRP.grpname).

### COMMAREA

Minimum size for this function is 370 bytes in order to support Universal groups.

In your application, use the CQTMPIA or CQTMPIA mapping macros (copybooks) provided in the SCQTMAC library.

```
API_FUNC          DC  CL4'ADGR'  Function code
API_RC            DC  XL01'00'  Return code
API_MSG          DC  CL79' '    Message area
*
API_AGRP_RC      DC  XL1      Return code from requested command
*                  If non-zero the command failed.
*                  API_MSG will give the reason for the failure.
*
API_AGRP_CODE1   DC  CL4"xxxx" 'ADGR' for ADDGROUP
*                  'ALGR' for ALTGROUP
*                  'DELG' for DELGROUP
*                  'LGRP' for LISTGROUP
*
*API_AGRP_GROUP  DC  CL8      Group name.
*
API_AGRP_OWNER   DC  CL8      Owner name
*
API_AGRP_SUPGRUP DC  CL8      Superior Group name
*
```

API_AGRP_TERMUAC	DC	CL1	Terminal UACC ('Y' or 'N')
*			
API_AGRP_INSTDATA	DC	CL255	Installation data
*			
API_AGRP_UNIVERS	DC	CL1	Universal Group ('Y' or 'N')
*			

To retrieve information about the group, enter LGRP in the **API\_AGRP\_CODE1** field. When altering data, blank fields are ignored and are not updated. To DELETE the installation data field, set the first byte to binary zeros (X'00').

## ADDUSER function (add user profile)

Use the ADDUSER function to add a new user profile to the system.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.ADUS) and the default group of the user being added (ADUS.dfltgrp).

### COMMAREA

Minimum size 408 bytes.

If your application reserves space for the no longer supported automatic create of a CICS segment, the required size would be 495 bytes.

If you need to specify a password phrase, the required size is 595 bytes.

In your application, use the CQTMPIA or CQTMPIA mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4	'ADUS'	Function code for ADDUSER
API_RC	DC	XL01	'00'	Return code
API_MSG	DC	CL79	' '	Message area
*				
API_ADUS_RC	DC	XL1		Return code from ADDUSER.
*				If non-zero the command failed.
*				API_MSG will give the reason for the failure.
*				
API_ADUS_USERID	DC	CL8		Userid being added.
API_ADUS_PGMRNAME	DC	CL20		Users name.
*				
API_ADUS_DFLTGRP	DC	CL8		The users default group.
*				
API_ADUS_AUTHRTY	DC	CL1		Authority in the default group.
*				Must be 'U' (use)
				or 'C' (create).
*				
API_ADUS_SMTWTFS	DC	CL7		The days of the week the user can logon.
*				Specify 'Y' for each
*				day the user may logon and 'N'
*				for the days they may not.
*				
API_ADUS_FROM	DC	CL4		The time of day the user can logon
*				from (24 hour clock).
*				
API_ADUS_TILL	DC	CL4		The time of day the user can logon
*				till (24 hour clock).
*				
API_ADUS_INSTDATA	DC	CL255		Installation data field.
*				
API_ADUS_PASSWORD	DC	CL8		Initial password for the user.
*				If it is omitted, the password
				defaults to the users default
				group.
*				
API_ADUS_OWNER	DC	CL8		The owner of the profile.
*				
* THE FOLLOWING FIVE FIELDS WERE USED FOR AUTOMATIC ADD * OF A CICS SEGMENT. THIS IS NO				
LONGER SUPPORTED. THE FIELDS * SHOULD BE BLANKS OR NULLS. API_ADUS_OPIDENT DC CL3				
Retained for compatibility API_ADUS_OPPRTY DC CL3 Retained for compatibility				
API_ADUS_TIMEOUT DC CL3 Retained for compatibility API_ADUS_XRFSOFF DC CL7				
Retained for compatibility API_ADUS_OPCLASS DC CL71 Retained for compatibility *				

API_ADUS_PHRASE	DC	CL100	The password phrase of the userid.
* API_ADUS_NOPHRSE	DS	CL01	No Passphrase
API_ADUS_NOPASSW	DS	CL01	No Password
API_ADUS_PHRINT	DS	CL05	PassPhrase Interval
API_ADUS_PWINT	DS	CL03	Password Interval

If you do not specify a value when creating the user profile, the initial PASSWORD for the user is set to the value of the DEFAULT GROUP.

The first time users log on, they are required to enter a new password.

## ALTUSER function (changing a profile)

Use the ALTUSER function to change the profile for a specific user.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.AUSR) and the users default group (AUSR.dfltgrp).

For several fields, the user must also have system special, or access to TOOLKIT.SPEC. These fields are flagged with an asterisk (\*).

### COMMAREA

Minimum size 487 bytes.

If you need to specify a password phrase, the required size is 587 bytes.

In your application, use the CQTMPIA or CQTMPIA mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'AUSR'	Function code for ALTUSER
API_RC	DC	XL01'00'	Return code
API_MSG	DC	CL79' '	Message area
*			
API_ALUS_RC	DC	XL1	Return code from ALTUSER
*			If non-zero the command failed.
*			API_MSG will give the reason for the failure.
*			
*			
API_ALUS_USERID	DC	CL8	The userid to be altered.
API_ALUS_PASSWRD	DC	CL8	Password
API_ALUS_RESUME	DC	CL1	Resume the userid (Y or N)
API_ALUS_PGMNAME	DC	CL20	Name
API_ALUS_INSTDATA	DC	CL255	Installation data field.
API_ALUS_DFLTGRP	DC	CL8	Default group.
API_ALUS_REVOKED	DC	CL5	Revoke Date(YYDDD).
API_ALUS_RESUMED	DC	CL5	Resume Date(YYDDD).
API_ALUS_AUTHOR	DS	CL8	* OWNER
API_ALUS_GRPACC	DC	CL1	* Group access.
API_ALUS_ADSP	DC	CL1	* ADSP.
API_ALUS_SPEC	DC	CL1	* Special
API_ALUS_OPER	DC	CL1	* Operations
API_ALUS_AUDITOR	DC	CL1	* Auditor
API_ALUS_RESTR	DC	CL1	* UACC and similar not used.
API_ALUS_PROTECT	DC	CL1	* Password cannot be used.
API_ALUS_UAUDIT	DC	CL1	* Audit all RACHECK's/RACDEF's.
API_ALUS_LOGDAY	DC	CL7	* Days user can logon.
API_ALUS_LOGFROM	DC	CL4	* Starting time for logon.
API_ALUS_LOGTILL	DC	CL4	* Latest time for logon.
API_ALUS_MODEL	DC	CL44	* Dataset profile model.
API_ALUS_CLAUTH	DC	CL8	* Give class authority.
*API-ALUS-AUTH			Name used in COBOL copybook
API_ALUS_NOCLAUTH	DC	CL8	* Remove class authority.
*API-ALUS-NAUTH			Name used in COBOL copybook
API_ALUS_PASSEXP	DC	CL1	* New password is expired (Y or N).
API_ALUS_PHRASE	DC	CL100	The password phrase of the userid.
API_ALUS_NOPHRSE	DS	CL01	No Passphrase
API_ALUS_NOPASSW	DS	CL01	No Password
API_ALUS_PHRINT	DS	CL05	PassPhrase Interval
API_ALUS_PWINT	DS	CL03	Password Interval

The fields in the commarea must be initialized to BINARY ZEROES. Only fields that are to be altered need to contain data. Refer to [Chapter 5, "The zSecure CICS Toolkit command interface,"](#) on page 29 for a

description of the fields and the restrictions on who can update which fields. After linking to CQTPAPI0, the users profile will be updated with the information contained in any field that was not binary zeros.

To specify that the password phrase must be removed, specify a value of 100 blanks. Any other value results in the password phrase being changed into the specified value, or be retained at its current value.

You can use the special date zeros (c'00000' = x'F0F0F0F0F0') to remove the Revoke/Resume date. Using this special value, you might implement a function like the NOREVOKE and NORESUME keywords of the RACF **ALTUSER** command.

## ALTUSER (CICS SEGMENT) function (alter CICS segment)

Use the ALTUSER (CICS SEGMENT) function to change the CICS segment for a specific user.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.AUSR) and the default group of the user (AUSR.*dfltgrp*). In addition, for managing the CICS segment, the user must have access to TOOLKIT.ACIC. In version 1.4 of Consul zToolkit, this requirement was only enforced if the TOOLKIT.ACIC profile has been defined or is covered by a generic profile. In version 1.8.1 and higher of zSecure CICS Toolkit, access to resource TOOLKIT.ACIC is required.

### COMMAREA

Minimum size is 184 bytes. If your application requires access to the TSLKEY and RSLKEY, the required minimum size is 316 bytes.

In your application, use the CQTMAPIA or CQTMATIC mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'ACIC'	Function code for CICS segment.
*			For compatibility reasons, ACSG is also accepted
API_RC	DC	XL01'00'	Return code
API_MSG	DC	CL79' '	Message area
*			
API_ACSG_RC	DC	XL1	Return code from ALTUSER. If non-zero the command failed.
*			API_MSG will give the reason for the failure.
*			
API_ACSG_CODE	DC	CL4	Specify LIST to retrieve the current specifications for the user. See LISTUSER (TSO/CICS)
*			UPDT to update the CICS segment
*			with the values in the COMMAREA.
*			DELT to delete the CICS segment.
*			The userid to be listed/updated.
API_ACSG_USERID	DC	CL8	
API_ACSG_OPIDENT	DC	CL3	Three character opident
API_ACSG_OPPRTY	DC	CL3	Operator priority (000-255)
API_ACSG_TIMEOUT	DC	CL3	Minutes before signoff
API_ACSG_XRFSOFF	DC	CL7	FORCE or NOFORCE
API_ACSG_OPCLASS	DC	CL71	Operator classes (01-24, separated by a comma, e.g.; 01,03,04)
*			
API_ACSG_TSLKEY	DS	CL66	TSL KEYS (00, 99, or 01-64, separated by a comma, e.g.; 01,03,04)
*			
API_ACSG_RSLKEY	DS	CL66	RSL KEYS (00, 99, or 01-24, separated by a comma, e.g.; 01,03,04)
*			

When the CICS segment is updated, all fields in the CICS segment are replaced. For this reason, valid data must be supplied for all parameters.

**Note:** In the current release, zSecure CICS Toolkit does not verify that each TSLKEY and RSLKEY value only provides space for 22 TSLKEY and RSLKEY values.

## ALTUSER (TSO SEGMENT) function (change TSO segment)

Use the ALTUSER (TSO SEGMENT) function to change the TSO segment for a specific user.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.AUSR) and the default group of the user (AUSR.*dfltgrp*). In addition, for managing the TSO segment, the user must have

access to TOOLKIT.ATSO. In version 1.4 of Consul zToolkit, this requirement was only enforced if the TOOLKIT.ATSO profile has been defined (or is covered by a generic profile). In version 1.8.1 and higher of zSecure CICS Toolkit, access to resource TOOLKIT.ATSO is required.

#### COMMAREA

Minimum size 191 bytes.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'ATSO'	Function code for TSO segment.
*			For compatibility reasons, ATSG is also accepted
API_RC	DC	XL01'00'	Return code
API_MSG	DC	CL79' '	Message area
*			
API_ATSG_RC	DC	XL1	Return code from ALTUSER. If non-zero the command failed.
*			API_MSG will give the reason for the failure.
*			
API_ATSG_CODE	DC	CL4	Specify LIST to retrieve the current specifications for the user.
*			See LISTUSER (TSO/CICS)
*			UPDT to update the TSO segment with the values in the COMMAREA.
*			DELT to delete the TSO segment.
API_ATSG_USERID	DC	CL8	The userid to be listed/updated.
API_ATSG_ACCTNUM	DC	CL40	The account number
API_ATSG_DESTID	DC	CL8	The destination id.
API_ATSG_HCLASS	DC	CL1	The hold class.
API_ATSG_JCLASS	DC	CL1	The job class.
API_ATSG_MSGCLASS	DC	CL1	The message class.
API_ATSG_SCLASS	DC	CL1	The sysout class.
API_ATSG_SECLABL	DC	CL8	The security label.
API_ATSG_SIZE	DC	CL7	The region size.
API_ATSG_MAXSIZE	DC	CL7	The maximum region size.
API_ATSG_PROC	DC	CL8	The logon proc.
API_ATSG_UNIT	DC	CL8	The allocation device.
API_ATSG_UDATA	DC	CL4	The installation data.

When the TSO segment is updated, all fields in the TSO segment are replaced. For this reason, valid data must be supplied for all parameters. Leaving a field empty (blanks or nulls) results in the corresponding field in the TSO segment to be deleted.

## ALTUSER (OMVS SEGMENT) function (change OMVS segment)

Use the ALTUSER (OMVS SEGMENT) function to change the OMVS segment for a specific user.

#### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.AUSR) and the default group of the user (AUSR.dfltgrp). In addition, for managing the OMVS segment, the user must have access to TOOLKIT.AOMV.

#### COMMAREA

Minimum size 273 bytes. If your applications access to the MEMLIM and SHMMAX fields, the minimum size is 291 bytes.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'AOMV'	Function code for OMVS segment.
API_RC	DC	XL01'00'	Return code
API_MSG	DC	CL79' '	Message area
*			
API_AOMV_RC	DS	XL01	Return code from command
*			
API_AOMV_CODE	DS	CL04	UPDT = Update segment
*			LIST = Retrieve segment
*			DELT = Delete segment
API_AOMV_USERID	DS	CL08	The userid
API_AOMV_UID	DS	CL10	UID (1-10# Left align, AUTOUID)
API_AOMV_SHARED	DS	CL01	Shared UID N/Y
API_AOMV_MKDIR	DS	CL01	MKDIR N/Y

API_AOMV_HOME	DS	CL60	HOME (1-60 CHARS) mixed case
API_AOMV_PROGRAM	DS	CL60	SHELL PROGRAM (1-60 CHARS)
API_AOMV_ASSIZE	DS	CL10	ASSIZEMAX (1-10 Digits left al)
API_AOMV_CPUTIME	DS	CL10	CPUTIMEMAX (1-10 Idem)
API_AOMV_FILEPROC	DS	CL06	FILEPROCMAX (1-6 Idem)
API_AOMV_MMAPAREA	DS	CL08	MMAPAREA (1-8 Idem)
API_AOMV_PROCUER	DS	CL05	PROCUER (1-5 Idem)
API_AOMV_THREADS	DS	CL06	THREADS (1-6 Idem)
API_AOMV_MEMLIM	DS	CL09	MEMLIMIT (1-8 DIGITS + M/G/T/P)
API_AOMV_SHMMAX	DS	CL09	SHMEMMAX (1-8 DIGITS + M/G/T/P)

When the OMVS segment is updated, all fields in the OMVS segment are replaced. For this reason, valid data should be supplied for all parameters. Leaving a field empty (blanks or nulls) results in the corresponding field in the OMVS segment to be deleted.

## ALTUSER (WORKATTR SEGMENT) function (change WORKATTR segment)

Use the ALTUSER (WORKATTR SEGMENT) function to change the WORKATTR segment for a specific user.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.AUSR) and the default group of the user (AUSR.dfltgrp). In addition, for managing the OMVS segment, the user must have access to TOOLKIT.AWRK.

### COMMAREA

Minimum size 637 bytes.

In your application, use the CQTMPIA or CQTMPIB mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'AWRK'	Function code for WORKATTR segment.
API_RC	DC	XL01'00'	Return code
API_MSG	DC	CL79' '	Message area
*			
API_AWRK_RC	DS	XL01	Return code from command
*			
API_AWRK_CODE	DS	CL04	UPDT = Update segment
*			LIST = Retrieve segment
*			DELT = Delete segment
API_AWRK_USERID	DS	CL08	The userid
API_AWRK_NAME	DS	CL60	WANAME (1-60 Chars)
API_AWRK_ACCNT	DS	CL60	WAACCNT (1-60 Chars)
API_AWRK_BLDG	DS	CL60	WABLDG (1-60 Chars)
API_AWRK_DEPT	DS	CL60	WADEPT (1-60 Chars)
API_AWRK_ROOM	DS	CL60	WAROOM (1-60 Chars)
API_AWRK_ADDR1	DS	CL60	WAADDR1 (1-60 Chars)
API_AWRK_ADDR2	DS	CL60	WAADDR2 (1-60 Chars)
API_AWRK_ADDR3	DS	CL60	WAADDR3 (1-60 Chars)
API_AWRK_ADDR4	DS	CL60	WAADDR4 (1-60 Chars)

When the WORKATTR segment is updated, all fields in the WORKATTR segment are replaced. For this reason, valid data must be supplied for all parameters. Leaving a field empty (blanks or nulls) results in the corresponding field in the WORKATTR segment to be deleted.

## CONNECT function (connect a user or group to a group)

Use the CONNECT function to connect a user or group to a group.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.CONN) and the target group (CONN.dfltgrp)

### COMMAREA

Minimum size 112 bytes. If your application requires access to the REVOKE and RESUME dates, the minimum length is 122 bytes.

In your application, use the CQTMPIA or CQTMPIB mapping macros (copybooks) provided in the SCQTMAC library.

```

API_FUNC      DC  CL4'CONN'  Function code for CONNECT
API_RC        DC  XL01'00'  Return code
API_MSG       DC  CL79' '   Message area
API_CONN_RC   DC  XL1      Return code from CONNECT. If
*              non-zero the command failed.
*              API_MSG will give the reason for
*              the failure.
*
API_CONN_USERID DC  CL8      Userid/group being connected.
*
API_CONN_GROUP DC  CL8      Group being connected to.
*
API_CONN_AUTH  DC  CL1      Connect authority
*              Must be 'U' (use),
*              'C' (create)
*              'N' (connect) or
*              'J' (join).
*
API_CONN_OWNER DC  CL8      Owner of the connect profile. It
*              must be a valid userid or group.
*
API_CONN_SPEC  DC  CL1      Specify 'Y' if the user should have the
*              group-special attribute otherwise
*              specify 'N'.
*
API_CONN_OPER  DC  CL1      Specify 'Y' if the user should have the
*              group-operations attribute otherwise
*              specify 'N:'.
*
API_CONN_REVOKE DC  CL5      The date (YYDDD) the user is to be REVOKED
*
API_CONN_RESUME DC  CL5      The date (YYDDD) the user is to be RESUMED

```

The **API\_CONN\_REVOKE** and **API\_CONN\_RESUME** fields can be used to set or remove the REVOKE and RESUME dates for the connection. If you use the value blanks (x'4040404040'), the revoke and resume dates are left at their current value. If you use the special date zeros (c'00000' = x'F0F0F0F0F0'), the current Revoke/Resume date is removed. Using this last special value, you can implement a function like the NOREVOKE and NORESUME keywords of the RACF **CONNECT** command. If you specify today's date for either the REVOKEDT or the RESUMEDT, the revoke-status for the user is updated immediately and the other date value is ignored. Both the RESUMEDT and the REVOKEDT are reset.

## CSDATA function (list and maintain CSDATA fields)

Use the CSDATA function to list, add, update, or remove the CSDATA fields in USER, GROUP, DATASET and General Resource profiles.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command. The resource name depends on the function requested, as shown in the following table:

Function	Authorization through
List	TOOLKIT.CSDL
Add	TOOLKIT.CSDA
Update	TOOLKIT.CSDA
Delete	TOOLKIT.CSDD

The user must also have at least READ access to the CSDN.*csdata-name* profile. If a single field is accessed, and the user is not authorized for the field, message CQT194 is issued: "You are not authorized for this CSDATA field". If the list function is used for all fields, message CQT198 can be issued: "CSDATA entries outside scope suppressed".

The target profiles must be within the scope of the command user. In contrast to other zSecure CICS Toolkit functions, this authorization is not controlled through the DFLTGRP, but through the OWNER of the target profile. The user must have at least READ access to the indicated resource. The following table lists the scope related resources:

Class	Scope authorization
USER	CSDU.owner
GROUP	CSDG.owner
DATASET	CSDD.owner
General Resources	CSDR.owner

## COMMAREA

Minimum size 605 bytes.

In your application, use the CQTMPIA or CQTMPIB mapping macros (copybooks) provided in the SCQTMAC library.

```

API_FUNC      DC  CL4'CSDA'  Function code for CSDATA management
API_RC        DC  XL01'00'   Return code
API_MSG       DC  CL79' '    Message area
*
API_CSDA_RC   DS  XL01      Return code from command
*
API_CSDA_CODE1 DS XL01      "A" Add
*                          "D" Delete
*                          "U" Update
*                          "L" List
*
API_CSDA_CLASS DS CL08      Class
API_CSDA_PROF DS CL248     Profile
API_CSDA_GENERIC DS CL01    Generic (G or anything else)
API_CSDA_CSDN DS CL08      CSDATA field name (at x'157')
API_CSDA_CSDV DS CL255     CSDATA field value
API_CSDA_CSDLST DS XL265   Space for returned CSDATA
*                          XL2      Length of data entry that
*                          follows. 0 to indicate end.
*                          CL8      CSDATA field name
*                          CLx     CSDATA field value

```

The API provides two methods of listing the CSDATA of the indicated profile. If you specify a value only for CLASS and PROF, all CSDATA fields for which you are authorized are returned in CSDLST. If you also specify a value for CSDN, the value for the specified CSDATA field is returned in CSDV, and CSDLST is not used.

The GENERIC field is used as input only. It can be used to indicate that a DATASET profile is a fully qualified generic. It is ignored for all other resource classes. zSecure CICS Toolkit does not support multiple discrete DATASET profiles (for example, for identically named data sets on different volumes).

When using the LIST function, only those CSDATA names or values are returned for which you are authorized by CSDN.csdname. If you request all CSDATA names/values, the returned list excludes those items for which you are not authorized.

If you request a LIST of all CSDATA names/values, only those names and values that fit completely within the supplied commarea are provided. In addition, the API\_CSDA\_RC is set to indicate the overflow condition. If you need all values, you must provide a sufficiently large commarea.

Flag fields are shown as a single Y or N character.

When processing CSDATA values through fields CSDN and CSDV, the length of the field value is always limited to 255 characters. This applies to all functions. If the current value of the field is longer than 255 characters, it is truncated. The full, non-truncated values of all fields are available in CSDLST when using the LIST function for all fields (that is, leaving CSDN blanks). If the field is truncated, API\_MSG field shows message CQT202: "CSDATA value truncated".

CSDATA fields for DATASET and General Resource profiles are only available on z/OS 2.4 and higher. If you use the zSecure CICS Toolkit interface to manage CSDATA fields for profiles in these resource classes, message CQT193 is returned if the z/OS level does not support CSDATA fields: "CSDATA field not found".

## DELETE DATASET function (delete data set profile)

---

Use the DELETE DATASET function to delete a data set profile from the system.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.DELD) and the high-level-qualifier of the data set profile name (DELD.hlq). If the user does not have access to the DELD.hlq, standard RACF authority checking is used. Refer to the RACF Command Language Reference manual for information about which data set profiles a user is authorized to delete.

### COMMAREA

Minimum size 130 bytes.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

```
API_FUNC      DC  CL4'DELD'  Function code for DELDSD
API_RC        DC  XL01'00'  Return code
API_MSG       DC  CL79' '    Message area
API_DELD_RC   DC  XL01'00'  Return code from DELDSD.
*             *             If non-zero the command
*             *             failed. API_MSG will give the reason for
*             *             the failure.
*             *
API_DELD_DSNAME DC CL44'DS-Profile'
*             *             The dataset profile to be deleted.
*             *
API_DELD_GENERIC DC CL01'Y'  Specify 'Y' if the profile is Generic
*             *             or 'N' if it is not.
*             *
```

## DELETE USERID function (delete user profile)

---

Use the DELETE USERID function to delete a user ID from the system.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.DELU) and the default group of the user ID (DELU.dfltgrp)

### COMMAREA

Minimum size 93 bytes.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

```
API_FUNC      DC  CL4'DELU'  Function code for DELUSER
API_RC        DC  XL01'00'  Return code
API_MSG       DC  CL79' '    Message area
API_DELU_RC   DC  XL01'00'  Return code from DELUSER.
*             *             If non-zero the command
*             *             failed. API_MSG will give the
*             *             reason for the failure.
*             *
API_DELU_USERID DC CL8'USERID' The userid to be deleted.
*             *
```

The user ID must be REMOVED from all groups, except the default group, and no data set profiles using this user ID as a high-level qualifier must exist, before the DELETE is issued.

zSecure CICS Toolkit checks for group connections but not for data set profiles.

## LISTDATASET function (list profile for one or more data sets)

---

Use the LISTDATASET function to list the profile for a specific data set or data sets.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.LDSD)

## COMMAREA

Minimum size 524 bytes to display the data set profile or 2374 if requesting the users or programs.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

**Note:** If you want to perform a SEARCH, initialize all fields according to your search pattern. Use asterisks for all field padding except for the **DSETID** field, which must be padded with nulls, blanks, or underscores.

API_FUNC	DC	CL4'LDSD'	Function code for LISTDATASET
API_RC	DC	XL01'00'	Return code
API_MSGDC	DC	CL79' '	Message area
*			
API_LDSD_RC	DC	XL1	Return code from LISTDATASET.
*			If non-zero the command failed.
*			API_MSG will give the reason for
*			the failure.
*			
API_LDSD_CODE1	DC	CL1	Request code.
*			'S' = start search
*			'N' = get next profile
*			'L' = retrieve this profile
*			'U' = retrieve users
*			'P' = retrieve programs
*			
API_LDSD_RESERVED	DC	CL46	This field is reserved for the
*			API and must be preserved between
*			calls.
*			
API_LDSD_DTYPE	DC	CL1	Profile type (generic or discrete).
*			
API_LDSD_DSETID	DC	CL44	The dataset to be retrieved.
*			Only required when the CODE
*			field is L, U or P; otherwise it is
*			used as part of the search criteria.
*			
API_LDSD_AUTHOR	DC	CL8	Owner of the profile.
API_LDSD_CREADAT	DC	CL5	Creation date.
API_LDSD_LREFDAT	DC	CL5	Last reference date.
API_LDSD_LCHGDAT	DC	CL5	Last update date.
API_LDSD_ACSALTR	DC	CL6	# of alter accesses.
API_LDSD_ACSCNTL	DC	CL6	# of control accesses.
API_LDSD_ACSUPDT	DC	CL6	# of update accesses.
API_LDSD_ACSREAD	DC	CL6	# of read accesses.
API_LDSD_UACC	DC	CL7	Universal access to the dataset.
API_LDSD_GRPDST	DC	CL1	Group dataset.
API_LDSD_AUDIT	DC	CL1	Audit flag.
API_LDSD_GROUPNM	DC	CL8	Current connect group.
API_LDSD_DSTYPE	DC	CL4	Dataset type.
API_LDSD_LEVEL	DC	CL3	Level indicator.
API_LDSD_GAUDIT	DC	CL1	Global audit option.
API_LDSD_AUDITQS	DC	CL1	Audit success flag.
API_LDSD_AUDITQF	DC	CL1	Audit failure flag.
API_LDSD_GAUDQS	DC	CL1	Global audit success flag.
API_LDSD_GAUDQF	DC	CL1	Global audit failure flag.
API_LDSD_WARNING	DC	CL1	Warning mode.
API_LDSD_SECLEVEL	DC	CL3	Security level.
API_LDSD_NUMCTGY	DC	CL4	Number of categories.
API_LDSD_NUMPGMS	DC	CL4	Number of programs.
API_LDSD_NUMUSER	DC	CL4	Number of users/groups.
API_LDSD_INSTDATA	DC	CL255	Installation data field.
	ORG	API_LDSD_RESERVED	
API_LDSD_USERPGMS	DC	CL???	When the users or programs
*			are requested they will be returned
*			into this area.

When the list of programs is returned, the format of the output is as follows:

Description	Length
Length of program name	4 bytes
Program name	8 bytes
Length of userid	4 bytes
userid	8 bytes
Length of access field	4 bytes
Access	1 byte X'80' Alter access X'40' Control access

```

X'20' Update access
X'10' Read access
X'08' Execute access
X'01' None

```

When the list of users is returned, the format of the output is as follows:

Description	Length
Length of Userid	4 bytes
Userid	8 bytes
Length of access field	4 bytes
Access	1 byte
	X'80' Alter access
	X'40' Control access
	X'20' Update access
	X'10' Read access
	X'08' Execute access
	X'01' None
Length of access count	4 bytes
Access count	2 bytes (binary)

In all cases, when the first field is zero (x'00000000'), it indicates the end of the data.

## LISTGROUP function (list profile for a group)

Use the LISTGROUP function to list the profile for a specific group or groups.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.LGRP) and the group name (LGRP.*grpname*)

### COMMAREA

Minimum size 441 bytes to display the group profile or 2374 if requesting the users of subgroups. To enable Universal group support, the minimum size is 442 bytes.

In your application, use the CQTMPIA or CQTMPIB mapping macros (copybooks) provided in the SCQTMAC library.

**Note:** If you want to perform a SEARCH, remember to initialize all fields according to your search pattern. Use asterisks for all field padding except for the **GROUP** field, which must be padded with nulls, blanks, or underscores.

```

API_FUNC      DC  CL4'LGRP'  Function code for LISTGROUP
API_RC        DC  XL01'00'  Return code
API_MSG       DC  CL79' '   Message area
*
API_LGRP_RC   DC  XL1      Return code from LISTGROUP.
*                If non-zero the command failed.
*                API_MSG will give the reason for
*                the failure.
*
API_LGRP_CODE1 DC  CL1      Request code.
*                'S' = start search
*                'N' = get next profile
*                'L' = retrieve this profile
*                'G' = retrieve subgroups
*                'U' = retrieve users
*
API_LGRP_RESERVED DC CL9    This field is reserved for the
*                API and must be preserved between
*                calls.
*
API_LGRP_GROUP DC  CL8      The group to be retrieved.
*                Only required when the CODE field
*                is L, G or U otherwise it is used
*                as part of the search criteria.
*
API_LGRP_SUPGRP DC  CL8      This groups superior group.
API_LGRP_OWNER DC  CL8      Owner of this group.
API_LGRP_DTE  DC  CL5      Date this profile was created.
API_LGRP_UACC DC  CL7      Authority of a user to the group
*                if the user is not connected to
*                the group.

```

```

*
API_LGRP_TERMACC      DC  CL1      Authority to access a terminal* required.
*
API_LGRP_SUBGRPS     DC  CL5      Number of subgroups.
*
API_LGRP_USERS       DC  CL5      Number of users.
*
API_LGRP_MODEL       DC  CL44     Name of a profile to be used as
*                               model for new group-name
*                               datasets.
*
API_LGRP_INSTDATA    DC  CL255   Installation data field.
*
API_LGRP_UNIVERS     DC  CL1      Universal Group ('Y' or 'N')
*
API_LGRP_USERSUBG    DC  CL????   ORG API_LGRP_RESERVED
*                               When the users or subgroups are
*                               requested they will be returned
*                               into this area.

```

When the list of users or subgroups is returned, the format of the output is as follows:

Description	Length
Length of member	4 bytes
User/Subgroup name	8 bytes

In all cases, when the first length field is zero (x'00000000'), this indicates the end of the data.

## LISTUSER function (list profile for a user ID)

Use the LISTUSER function to list the profile for a specific user or user IDs.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.LUSR) and the users default group (LUSR.*dfltgrp*).

### COMMAREA

Minimum size 544 bytes to display the group profile or 2374 if requesting the groups or categories.

In your application, use the CQTMPIA or CQTMPIB mapping macros (copybooks) provided in the SCQTMAC library.

**Note:** If you want to perform a SEARCH, you need to initialize all fields according to your search pattern. Use asterisks for all field padding except for the **USERID** field, which must be padded with nulls, blanks, or underscores.

```

API_FUNC      DC  CL4'LUSR'  Function code for LISTUSER.
API_RC       DC  XL01'00'   Return code
API_MSG      DC  CL79' '    Message area
*
API_LUSR_RC   DC  XL1      Return code from LISTUSER.
*                               If non-zero the command failed.
*                               API_MSG will give the reason for
*                               the failure.
*
API_LUSR_CODE1 DC  CL1      Request code.
*                               'S' = start search
*                               'N' = get next profile
*                               'L' = retrieve this profile
*                               'G' = retrieve groups
*                               'A' = retrieve groups and authority to groups
*                               'C' = retrieve categories
*
API_LUSR_RESERVED DC  CL9   This field is reserved for the
*                               API and must be preserved between
*                               calls.
API_LUSR_USERID DC  CL8     The userid to be retrieved.
*                               Only required when the CODE field
*                               is L, G or C otherwise it is used
*                               as part of the search criteria.
*
API_LUSR_PGMNAME DC  CL20   Users name.
API_LUSR_AUTHOR DC  CL8     Owner of the profile.

```

```

API_LUSR_PASSWRD DC CL8 Password field (will contain ?)
API_LUSR_AUTHDTE DC CL5 Creation date.
API_LUSR_DFLTGRP DC CL8 Default group.
API_LUSR_AUTHRTY DC CL7 Authority.
API_LUSR_UACC DC CL7 Universal access.
API_LUSR_CLASCNT DC CL5 Number of classes.
API_LUSR_ADSP DC CL1 ADSP.
API_LUSR_SPEC DC CL1 Special.
API_LUSR_OPER DC CL1 Operations.
API_LUSR_REVOKE DC CL1 Revoke.
API_LUSR_GRPACC DC CL1 GRPACC.
API_LUSR_AUDITOR DC CL1 Auditor.
API_LUSR_PROTECT DC CL1 Password cannot be used.
API_LUSR_RESTR DC CL1 UACC and similar not used.
API_LUSR_UAUDIT DC CL1 Audit all RACHECK's/RACDEF's.
API_LUSR_REVOKEC DC CL2 # unsuccessful pwd attempts.
API_LUSR_REVOKED DC CL5 Date user will be revoked.
API_LUSR_SECL DC CL2 Security level. This is a binary field that
* represents the security level. Eg.:
* X'00FE' would be a security level of 254.
API_LUSR_RESUMED DC CL5 Date user will be resumed.
API_LUSR_LASTACC DC CL14 Last access date and time.
API_LUSR_PASSDTE DC CL5 Date password last changed.
API_LUSR_PASSINT DC CL3 Password interval.
API_LUSR_PWDGEN DC CL3 Current password generation #.
API_LUSR_PWDCNT DC CL3 Number of old passwords.
API_LUSR_NUMCTGY DC CL4 Number of categories.
API_LUSR_NUMGRP DC CL4 Number of groups.
API_LUSR_LOGDAY DC CL7 Days user can logon.
API_LUSR_LOGFROM DC CL4 Starting time for logon.
API_LUSR_LOGTILL DC CL4 Latest time for logon.
API_LUSR_MODEL DC CL44 Dataset profile model.
API_LUSR_INSTDATA DC CL255 Installation data field.
API_LUSR_PHRINT DS CL05
API_LUSR_CONTAIN DS CL01
API_LUSR_NEVERCO DS CL01
ORG API_LUSR_RESERVED
API_LUSR_GRPCTGY DC CL??? When the groups or categories are
* requested they will be returned
* into this area.

```

When the list of groups is returned, the format of the output is as follows:

Description	Length
Length of group name	4 bytes
Group name	8 bytes

When the list of groups and authority is returned, the format of the output is as follows:

Description	Length
Combined length of the following 'group length/names'	4 bytes
Length of group name	4 bytes
Group name	8 bytes

For each of the following fields, there is a one-to-one relationship to the groups. If the user was connected to two groups, there are two ADSP flags, two SPECIAL flags, two OPERATIONS flags, two REVOKE flags, two GRPACC flags, and two GROUP AUDITOR flags. If bit 0 in the flag is turned on (X'80'), the user has that attribute in the group.

Combined length of the ADSP lengths/flags	4 bytes
Length of the ADSP flag	4 bytes
ADSP flag	1 byte
Combined length of the SPECIAL lengths/flags	4 bytes
Length of SPECIAL flag	4 bytes
SPECIAL flag	1 bytes
Combined length of the OPERATIONS lengths/flags	4 bytes
Length of OPERATIONS flag	4 bytes
OPERATIONS flag	1 byte

Combined length of the REVOKE lengths/flags	4 bytes
Length of the REVOKE flag	4 bytes
REVOKE REVOKE flag	1 byte
Combined length of the GRPACC lengths/flags	4 bytes
Length of GRPACC flag	4 bytes
GRPACC flag	1 byte
Combined length of the GROUP AUDITOR lengths/flags	4 bytes
Length of GROUP AUDITOR flag	4 bytes
GROUP AUDITOR flag	1 byte

When the list of categories is returned, the format of the output is as follows:

Description	Length
Length of category	4 bytes
Category number	2 bytes (binary)

In all cases, when the first length field is zero (x'00000000'), it indicates the end of the data.

## PASSWORD function (change password)

Use the PASSWORD function to change the password of a user.

### AUTHORITY

NONE, unless you are specifying a value of 255 for the interval value (which corresponds to NOINTERVAL), or changing the INTERVAL value for a user ID other than your own. It requires you to have SPECIAL, or to have access to TOOLKIT.SPEC or PSWD.*dfltgrp* (*dfltgrp* is the default group of the user ID that is being altered). If you are using the **PASSWORD** command on a user ID different from your own, you can only change the INTERVAL value. To change another user's password, use the **ALTUSER** command.

### COMMAREA

Minimum size 112 bytes.

In your application, use the CQTMPIA or CQTMPIB mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'PSWD'	Function code for PASSWORD.
API_RC	DC	XL01'00'	Return code
API_MSG	DC	CL79' '	Message area
*			
API_PSWD_RC	DC	XL01'00'	Return code from PASSWORD.
*			If non-zero the command failed.
*			API_MSG will give the reason for the failure.
*			
API_PSWD_USERID	DC	CL08'USERID '	The userid being altered.
*			
API_PSWD_PASSWORD	DC	CL08'PASSWORD'	The password for this userid.
*			
API_PSWD_NEWPASS	DC	CL08'NEWPSWD'	The new password for this userid.
API_PSWD_PASSINT	DC	CL03'060'	The new password interval for this userid.

PASSWORD does not perform a signon for the user. It only verifies that the password entered for this user ID is correct and then changes the password to the new specification and changes the password interval.

Multiple failures to change the password of a user might result in the user ID being revoked, depending on your system parameters.

The password interval of the user might also be changed. The new interval might be 001 - 254, but might not exceed the global maximum specified. If it does, it can be set to the maximum allowed. If the value specified for the interval is invalid, the parameter is ignored. When only changing the password interval, it is not necessary to provide the password. However, if the interval is invalid and ignored, zSecure CICS Toolkit treats the operation as if it is a request to change passwords and it checks for a password and new

password. If a new password has not been supplied, the error message returned reflect it as the error, rather than the password interval being incorrect.

This command is only available through the API.

## PERMIT function (grant or remove access)

Use the PERMIT function to grant access to or remove access from a CICS resource. The resource must be in one of the resource classes defined in the SIT for this run of CICS.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.PEMT), the default group of the user ID or group that is being granted access (PEMT.*dfltgrp*), and must also have access to the resource. If the access is granted to a group, the resource used is PEMT.*group*. After the PERMIT has been completed, the resource classes must be refreshed in order to have immediate effect. Use the RACF **SETROPTS REFRESH** command to accomplish it.

### COMMAREA

Minimum size 116 bytes.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'PEMT'	Function code for PERMIT.
API_RC	DC	XL01'00	Return code
API_MSG	DC	CL79' '	Message area
*			
API_PEMT_RC	DC	XL01'00'	Return code from PERMIT
*			If non-zero the command failed
*			API_MSG will give the reason for the failure
*			
API_PEMT_USERID	DC	CL08'USERID'	The userid or group.
*			
API_PEMT_RSRC	DC	CL13'CEMT '	The name of the CICS resource.
*			
API_PEMT_CLASS	DC	CL08'TCICSTRN'	
*			The resource classname.
*			If blank the value of the XTRAN parameter
*			specified in the SIT is used.
*			
API_PEMT_DELT	DC	CL01'Y'	Specify 'Y' in this field to remove
*			a person from the access list for
*			this resource. The user or group
*			will no longer have access to the resource.
*			
API_PEMT_ACC	DC	CL01'R'	Access allowed to the resource
*			Specify 'R' for read,
*			'N' for none,
*			'U' for update,
*			'A' for alter or
*			'C' for control.
*			Read is the default

## PERMITX function (grant or remove access - any resource)

Use the PERMITX function to grant access to or remove access from any resource. It can also be used to grant access to DATASET profiles.

### AUTHORITY:

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.PEMT), the default group of the user ID or group that is being granted access (PEMT.*dfltgrp*), and the target resource itself. If the access is granted to a group, the CICS Toolkit resource is PEMT.*group*. If the class is a non-CICS class, the user must also have access to the PEMX.*classname* resource. After the PERMIT has completed, use the RACF SETROPTS REFRESH command to refresh the resource classes.

For the PERMITX function to be available, it must have been enabled in CQTPCNTL by specifying PENTALL=Y.

## COMMAREA

Minimum size 349 bytes.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) that are provided in the SCQTMAC library.

```
API_FUNC      DC  CL4'PEMX'  Function code for PERMITX
API_RC        DC  XL01'00  Return code
API_MSG       DC  CL79'  '  Message area
*
API_PEMX_RC   DC  XL01'00'  Return code from PERMIT
*              If non-zero the command failed
*              API_MSG will give the reason for the failure.
*
API_PEMX_USERID DC CL08'USERID' The userid or group.
*
API_PEMX_RSRC DC  CL246'CEMT ' The name of the resource.
*
API_PEMX_CLASS DC  CL08'TCICSTRN' The resource class name.
*              If blank the value of the
*              XTRAN parameter.
*              specified in the SIT is used
API_PEMX_DELT DC  CL01'Y'  Specify 'Y' in this field
*              to remove a person from the access
*              list for this resource. The user
*              or group will no longer have access.
*              access to the resource.
API_PEMX_ACC   DC  CL01'R'  Access allowed to the resource.
*              Specify 'R' for read,
*              'N' for none,
*              'U' for update,
*              'A' for alter,
*              'C' for control.
*              Read is the default
*
```

## RACLINK function (define, list, undefine, or approve user associations)

Use the RACLINK function to list, define, approve, and undefine RRSF user ID associations on the local system.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.RACL) and the default group of the user ID (PEMT.*dfltgrp*) and for the DEFINE function must also have access to the RACLINK.DEFINE.*nodename* and RACLINK.PWSYNC.*nodename* profiles in the RRSFDATA resource class.

## COMMAREA

Minimum size 1150 bytes.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

```
API_FUNC      DC  CL4'RACL '  Function code for RACLINK
API_RC        DC  XL01'00  Return code
API_MSG       DC  CL79'  '  Message area
*
API_RACL_RC   DS  XL01      Return code from command
API_RACL_CODE1 DS  XL01      'D' DEFINE
*              'U' UNDEFINE
*              'A' APPROVE
*              'L' LIST ASSOCIATIONS
*
API_RACL_USERID DC CL8'userid '  Userid on whose behalf
API_RACL_ATYPE  DC CL8'PEER '  Assoc. type (PEER/MANAGED)
)
API_RACL_ANODE  DC CL8'nodename'  Assoc. node
API_RACL_AUSERID DC CL8'ibmuser '  Assoc. Userid
API_RACL_PWSYNC DC CL4'yes '  yes/no
API_RACL_APSWD  DC CL8'sys1 '  Assoc. Userid Password
API_RACL ASSOCLST DS 15CL68      List of 15 associations
*
```

The list of associations for the user has the following format:

API_RACL ASSOCTYPE	DC	CL10	PEER/MANAG
API_RACL ASSOCCNODE	DC	CL8	node
API_RACL ASSOCCUSER	DC	CL8	USER
API_RACL ASSOCCPWSYNC	DC	CL4	pwsync
API_RACL ASSOCCSTAT	DC	CL20	status
API_RACL ASSOCCCREAT	DC	CL8	creator
API_RACL ASSOCCDATE	DC	CL10	date

The end of the list of associations is indicated by an entry consisting of blanks.

## REMOVE function (remove user IDs or groups from a group)

Use the REMOVE function to remove a user or group from group.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.REMV) and the target group (REMV.grpname)

### COMMAREA

Minimum size 101 bytes.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'REMV'	Function code for REMOVE
API_RC	DC	XL01'00'	Return code
API_MSG	DC	CL79' '	Message area
*			
API_REMV_RC	DC	XL1	Return code from REMOVE.
*			If non-zero the command failed.
*			API_MSG will give the reason for the failure.
*			
API_REMV_USERID	DC	CL8	Userid/group being removed.
*			
API_REMV_GROUP	DC	CL8	Group being removed from.

Users might not be removed from their default group.

## RALTER/RDEFINE/RDELETE function (list and maintain profiles)

Use the RALTER, RDEFINE, and RDELETE function to list and maintain profiles in a general resource class defined in the CDT.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.RALT / TOOLKIT.RDEF / TOOLKIT.RDEL depending on the command being performed) and the general resource class (RALT.cdtclass / RDEF.cdtclass / RDEL.cdtclass / RLST.cdtclass)

### COMMAREA

Minimum size 875 bytes.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'Rxxx'	Function code:
*			RALT for RALTER
*			RDEF for RDEFINE
*			RDEL for RDELETE
API_RC	DC	XL01'00'	Return code
API_MSG	DC	CL79' '	Message area
*			
API_RUPD_RC	DC	XL1	Return code.
*			If non-zero the command failed.
*			API_MSG will give the reason for* the failure.
*			
API_RUPD_CODE1	DC	CL4	Type of command being performed
*			'RDEF to define a profile

```

*          'RDEL' to delete a profile
*          'AMEM' to add a member
*          'DMEM' to delete a member
*          'UPDP' to update fields in the profile
*
API_RUPD_CLASS    DC  CL8      The class containing the profile
API_RUPD_CTYPE   DC  CL1      Profile type (not used as input to the API).
API_RUPD_ENTRY   DC  CL246    The profile name
API_RUPD_MEMBER  DC  CL246    The member name
*
API_RUPD_OWNER   DC  CL8      Owner of the profile.
API_RUPD_NOTIFY  DC  CL8      User to be notified.
API_RUPD_UNIVACS DC  CL7      Universal access to the dataset.
API_RUPD_WARNING DC  CL1      Warning mode.
API_RUPD_LEVEL   DC  CL3      Level indicator.
API_RUPD_AUDIT   DC  CL1      Audit flag.
API_RUPD_AUDITQS DC  CL1      Audit success flag.
API_RUPD_AUDITQF DC  CL1      Audit failure flag.
API_RUPD_INSTDATA DC CL255    Installation data field.

```

## RLIST function (list profiles for general resource class)

Use the RLIST function to list the profile details for a general resource class defined in the CDT.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command (TOOLKIT.RLIST) and the general resource class (RLIST.cdtclass).

### COMMAREA

Minimum size 907 bytes to display the profile. If the request is for the members, users or condacc, the commarea must be large enough to hold all the data returned. If it is not, the **API\_RLST\_RC** is non-zero and the message indicates it as the error.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

**Note:** If you want to perform a SEARCH, you need to initialize all fields according to your search pattern. Use asterisks for all field padding except for the **ENTRY** field, which must be padded with nulls, blanks, or underscores.

```

API_FUNC          DC  CL4'RLST'  Function code for RLIST
API_RC            DC  XL01'00'    Return code
API_MSG           DC  CL79' '     Message area
*
API_RLST_RC       DC  XL1         Return code from RLIST.
*                               If non-zero the command failed.
*                               API_MSG will give the reason for
*                               the failure.
*
API_RLST_CODE1    DC  CL1         Request code.
*                               'S' = start search
*                               'N' = get next profile
*                               'L' = retrieve this profile
*                               'C' = retrieve conditional access list
*                               'M' = retrieve members
*                               'U' = retrieve users
*
API_RLST_RESERVED DC  CL248      This field is reserved for the
*                               API and must be preserved between calls.
*
API_RLST_CLASS    DC  CL8         The class containing the profile to be
*                               retrieved. This field is always required
*
API_RLST_CTYPE    DC  CL1         Profile type (not used as input to the API).
*
API_RLST_ENTRY    DC  CL246      The profile to be retrieved. Only
*                               required when the CODE field is L, U, C
*                               or M otherwise it is used as part of the
*                               search criteria.
*
API_RLST_OWNER    DC  CL8         Owner of the profile.
API_RLST_DEFDATE  DC  CL5         Creation date.
API_RLST_LREFDAT  DC  CL5         Last reference date.
API_RLST_LCHGDAT  DC  CL5         Last update date.
API_RLST_UACC     DC  CL7         Universal access to the dataset.

```

API_RLST_AUDIT	DC	CL1	Audit flag.
API_RLST_AUDITQS	DC	CL1	Audit success flag.
API_RLST_AUDITQF	DC	CL1	Audit failure flag.
API_RLST_NOTIFY	DC	CL8	User to be notified.
API_RLST_WARNING	DC	CL1	Warning mode.
API_RLST_LEVEL	DC	CL3	Level indicator.
API_RLST_GAUDIT	DC	CL1	Global audit option.
API_RLST_GAUDQS	DC	CL1	Global audit success flag.
API_RLST_GAUDQF	DC	CL1	Global audit failure flag.
API_RLST_SECLEVEL	DC	CL3	Security level.
API_RLST_NUMMEM	DC	CL4	Number of members.
API_RLST_NUMUSER	DC	CL4	Number of users/groups.
API_RLST_NUMPGMS	DC	CL4	Number of programs.
API_RLST_INSTDATA	DC	CL255	Installation data field.
		ORG	API_RLST_RESERVED
API_RLST_MEMBUSRS	DC	???XL1	When the members, users or conditional
*			access list is requested the data will be
*			returned into this area.

When a profile or member name is returned, it might be generic. It cannot be converted to a displayable format. To do so, you must be aware of the RACF naming conventions for generic characters.

Generic Character	Converted To
The first '.'	X'02'
Ending double asterisks	X'FD'
Ending single asterisks	X'FC'
Internal double asterisks	X'FBFC90' (when a general resource class)
	X'FCFC' (when not a general resource class)
Internal single asterisk	X'FBFC80'
Percent sign	X'FB'
Ampersand	X'FA70'

When the list of members is returned, the format of the output is as follows:

Description	Length
Length of member	4 bytes
Member name	? bytes (length determined by length field)

When the list of users is returned, the format of the output is as follows:

Description	Length
Length of userid	4 bytes
Userid	8 bytes
Length of access field	4 bytes
Access	1 byte
	X'80' Alter access
	X'40' Control access
	X'20' Update access
	X'10' Read access
	X'01' None

When the conditional access list is returned, the format is the output is as follows:

Description	Length
Length	14 bytes
Filler	8 bytes
Length of userid	4 bytes
Userid	8 bytes
Length of access field	4 bytes
Access	1 byte
	X'80' Alter access
	X'40' Control access
	X'20' Update access
	X'10' Read access
	X'01' None
Device type length	3 bytes
Device type	8 bytes
Device name length	3 bytes
Device name	? bytes (length determined by length field)

In all cases, when the first length field is zero (x'00000000'), it indicates the end of the data.

## USRDATA function (list and maintain users' USRDATA fields)

Use the USRDATA function to list, add, update, or remove the USRDATA fields of a user profile. For information about the special SMF record created for updates to USRDATA, see “SMF records created by zSecure CICS Toolkit” on page 77.

### AUTHORITY

The user must have access to the zSecure CICS Toolkit command. Depending on the function requested, the profile is TOOLKIT.USRL for the list function, TOOLKIT.USRA for the ADD and UPDATE function, and TOOLKIT.USRD for the DELETE function. The user must also have access to the USRN.*usrdata-name* profile. The affected USERID must be within scope for USRDATA management functions. This means that the user must have access to USRU.*dfltgrp*.

### COMMAREA

Minimum size 365 bytes.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'USRD'	Function code for USRDATA management
API_RC	DC	XL01'00'	Return code
API_MSG	DC	CL79' '	Message area
*			
API_USRD_RC	DC	XL1	Return code.
*			01 Invalid function in CODE1 below
*			03 Data from L(ist) function does
*			not fit in commarea
*			
API_USRD_CODE1	DC	CL1	Type of command being performed
*			'L' to list all or one USRDATA field
*			'A' to add a USRDATA field
*			'U' to update a USRDATA field
*			'D' to delete a USRDATA field
*			
API_USRD_CLASS	DC	CL8	Must be 'USER' followed by four blanks
API_USRD_PROF	DC	CL8	Profile (=USERID)
API_USRD_USRN	DC	CL8	The name of the USRDATA field
API_USRD_USRV	DC	CL255	The value for the USRDATA field
*			
API_USRD_USRDLS	DC	CL8	Space for returned USRDATA
	DC	CL255	names and values

The API provides three methods of listing the USRDATA of the indicated USER. If you select L for CODE1 and specify a value only for **PROF**, all **USRDATA** fields are returned in USRDLS. If you also specify a value for **USRN**, the value for the specified USRDATA name is returned in USRV. If a value is present in the **USRV** field, it is used as the first few characters for the requested USRDATA value. For this last function, zSecure CICS Toolkit supplements USRV with additional characters from the first matching USRDATA Name/Value pair.

Except for the LIST and DELETE functions, zSecure CICS Toolkit does not support duplicate USRDATA names. If you have multiple USRDATA name/value pairs with the same name, you might only inspect and delete them, until the name becomes unique.

When using the LIST function, only those USRDATA names or values are returned for which you are authorized by USRN.*usrdata-name*. If you request all USRDATA names/values, the returned list excludes those items for which you are not authorized.

If you request a LIST of all USRDATA names/values, only those names and values that fit completely within the supplied commarea are provided. In addition, the **API\_USRD\_RC** is set to indicate the overflow condition. If you need all values, you must provide a sufficiently large commarea.

**Note:** The space reserved for each USRDATA value is 255 bytes, irrespective of the actual length of the data.

## VERIFY function (verify user ID and password or phrase)

Use the VERIFY function to verify a user ID and password or password phrase.

### AUTHORITY

NONE

### COMMAREA

Minimum size is 101 bytes. If you are using Newpass, Termid, or APPL, the minimum size is 125 bytes. To verify using a password phrase a minimum of 226 bytes is needed, and when specifying a new password phrase 327 bytes are needed.

In your application, use the CQTMAPIA or CQTMAPIC mapping macros (copybooks) provided in the SCQTMAC library.

API_FUNC	DC	CL4'VERF'	Function code for VERIFY.
API_RC	DC	XL01'00'	Return code
API_MSG	DC	CL79' '	Message area
*			
API_VERF_RC	DC	XL01'00'	Return code from VERIFY.
*			If non-zero the command failed.
*			API_MSG will give the reason
*			for the failure.
*			
API_VERF_USERID	DC	CL08'USERID '	The userid being verified.
*			
API_VERF_PASSWORD	DC	CL08'PASSWORD'	The password for this userid.
*			
API_VERF_NEWPASS	DC	CL08'NEWPASS'	The new password for this userid.
*			
API_VERF_TERMID	DC	CL08'TERMINAL'	A terminal id.
*			
API_VERF_APPL	DC	CL08'APPLNAME'	An application name.
* Next fields only if length=>226			
API_VERF_PHRASE_LEN	DC	XL1'09'	Length of phrase
API_VERF_PHRASE	DC	CL100'ABCDEFGHI'	Password phrase
* Next fields only if length=>327			
API_VERF_NPHRASE_LEN	DC	XL1'00'	Length of new phrase
API_VERF_NPHRASE	DC	CL100' '	New password phrase

he VERIFY function does not perform a CICS signon for the user. It only verifies that the password or phrase entered for this user ID is correct. Internally it uses a RACROUTE REQUEST=VERIFY with LOG=ASIS, resulting in SMF records and messages in case of an invalid password or phrase.

Multiple failures to verify a user ID and password or phrase can result in the user ID being revoked, depending on your system parameters.

You can also specify the following optional parameters:

### API\_VERF\_NEWPASS

Specifying a new password changes the users password to the specified new password. The **API\_VERF\_PASSWORD** field has to contain the valid current password for the user before the new password works.

### API\_VERF\_TERMID

If a terminal ID is present and TERMINAL checking is turned on in RACF, it verifies the users authority to use this terminal at the current time and date.

### API\_VERF\_APPL

If an application name is present and APPL checking is turned on in RACF, this will verify the users authority to use this application.

This command is only available through the API.

### API\_VERF\_PHRASE\_LEN and API\_VERF\_PHRASE

If you specify a **API\_VERF\_PASSWORD** field containing only blanks, you can use a phrase for the verify function. If the **API\_VERF\_PASSWORD** field has any non-blank character, the **API\_VERF\_PHRASE** field is ignored. To use a phrase for verification, the **API\_VERF\_PHRASE\_LEN** field must specify the exact length of the password phrase. and the **API\_VERF\_PHRASE** field must contain the current phrase of the user, padded with blanks.

## API\_VERF\_NPHRASE\_LEN and API\_VERF\_NPHRASE

If you use a phrase for the verify function, you can also specify a new phrase. If you use a password to verify, the new phrase is ignored. To specify the new phrase, the API\_VERF\_NPHRASE\_LEN field must specify the exact length of the new password phrase, and the API\_VERF\_NPHRASE field must contain the current password phrase of the user, padded with blanks. If the length API commarea is 327 bytes or more, the presence of a new phrase is assumed, unless API\_VERF\_NPHRASE\_LEN has the value zero.

## Sample programs

---

Several example programs are provided for your use as part of the product.

The example described in “Simple API interface” on page 113 is a general example showing how to use the API interface. The example in “Resource Profile List Interface” on page 113 is a simple program showing the use of the Resource Profile List API.

### Simple API interface

A sample program that demonstrates how the API might be used is provided in the SCQTSAMP data set. This program shows how a resource check might be performed using the RSRX API interface.

The user interface of these programs is simple, and does not perform any validation or additional processing. The examples are intended only to demonstrate the use of the CQTMPIA area for passing information back and forth between the API and your application program.

To install the sample programs, translate and compile the mapset and the program, and define the resources to CICS. See the following example resource definitions:

```
DEFINE PROG(CQTXAPIR) L(ASSEMBLER) EXECKEY(USER) DA(ANY) GROUP(CQTSAMP)
DEFINE TRANSACTION(XAPI)  PROG(CQTXAPIR)
                        PROFILE(CQTSAMP) GROUP(CQTSAMP) TASKDATALOC(ANY)
DEFINE MAPSET(CQTXAMP)  GROUP(CQTSAMP)
```

Program CQTXAPIR allows you to enter resource names and resource classes. It then checks to see if you have access to the resource. Alternatively, you might enter a user ID, other than your own, against which to perform the access check.

You can tailor this example to suit your own environment or to do specific editing on any of the fields.

### Resource Profile List Interface

An example program that demonstrates how to use the Resource Profile List interface is provided in members CQTXAPIL, CQTXAML, CQTXCPIL, and CQTXCML in SCQTSAMP. The same program is provided in both assembler and COBOL form.

#### About this task

The programs use a BMS map to display an initial panel, where the user can fill in some filters and options for the RSRL (Resource Profile List) API interface. The source for the BMS map is provided twice to generate different include members, but the two source members are otherwise identical. The programs call the API and show some relevant parts of the output. The programs serve no practical purpose, aside from illustrating how the API can be used, and verifying that the installation has completed successfully.

#### Procedure

To install the samples programs:

1. Translate, compile and linkedit the mapset and the program.
2. Define the resulting modules to CICS.

## Results

See the following example resource definitions:

```
DEFINE PROG(CQTXCPIL)      L(COBOL)          EXECKEY(USER)  DA(ANY)  GROUP(CQTSAMP)
DEFINE TRANSACTION(RSRC)  PROG(CQTXCPIL)
                           PROFILE(CQTSAMP)  GROUP(CQTSAMP)  TASKDATALOC(ANY)
DEFINE PROG(CQTXAPIL)     L(ASSEMBLER)     EXECKEY(USER)  DA(ANY)  GROUP(CQTSAMP)
DEFINE TRANSACTION(RSRA)  PROG(CQTXAPIL)
                           PROFILE(CQTSAMP)  GROUP(CQTSAMP)  TASKDATALOC(ANY)
DEFINE MAPSET(CQTXAML)    GROUP(CQTSAMP)
```

### Note:

- To use the example programs, install the group CQTSAMP as shown, and run the transaction RSRA or RSRC.
- To view the output, you might need to use CEBR to view the entire TSQUEUE that is created as part of this program.
- It is the responsibility of the calling program to remove the TSQUEUE after it has been created.
- The example programs do not delete the TSQUEUE after usage, so that you can inspect the data after the transaction has ended.
- After completing your testing, manually delete the TSQUEUE.

## Notices

---

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan, Ltd.  
1623-14, Shimotsuruma, Yamato-shi  
Kanagawa 242-8502 Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
2Z4A/101

11400 Burnet Road  
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

## Trademarks

---

IBM, the IBM logo, and [ibm.com](http://ibm.com)<sup>®</sup> are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on [ibm.com/legal/copytrade](http://ibm.com/legal/copytrade).

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are registered trademarks of Hewlett Packard Enterprise, International Business Machines Corporation and Quantum Corporation in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.



# Index

## A

- ADDGROUP command [30](#)
- ADDUSER command
  - panel [31](#)
- ALTGROUP command [30](#)
- ALTUSER command
  - CICS segment option [34](#)
  - OMVS segment option [37](#)
  - panel [32](#)
  - TSO segment option [35](#)
  - WORKATTR segment option [39](#)
- API
  - Access Authority Check (Extended) function [81](#)
  - Access Authority Check function [80](#)
  - ADDGROUP / ALTGROUP / DELGROUP function [92](#)
  - ADDUSER function [93](#)
  - ALTUSER (CICS SEGMENT) function [95](#)
  - ALTUSER (OMVS SEGMENT) function [96](#)
  - ALTUSER (TSO SEGMENT) function [95](#)
  - ALTUSER (WORKATTR SEGMENT) function [97](#)
  - ALTUSER function [94](#)
  - CONNECT function [97](#)
  - CSDATA function [98](#)
  - DELETE DATASET function [100](#)
  - DELETE USERID function [100](#)
  - implementing field or record level security [79](#)
  - LISTDATASET function [100](#)
  - LISTGROUP function [102](#)
  - LISTUSER function [103](#)
  - PASSWORD function [105](#)
  - PERMIT function [106](#)
  - PERMITX function [106](#)
  - RACLINK function [107](#)
  - RALTER/RDEFINE/RDELETE function [108](#)
  - REMOVE function [108](#)
  - Resource Profile List function [82](#)
  - RLIST function [109](#)
  - Sample programs [113](#)
  - searching the RACF database [79](#)
  - simple interface [113](#)
  - VERIFY function [112](#)
- API functions
  - Changing the authorized user [79](#)
  - using the COMMAREA [78](#)
- Application interface
  - overview [1](#)
- Application security check
  - application conversion [25](#)
- Application security checking
  - checking the OP-ID [25](#)
  - resource definitions [26](#)
  - with zSecure CICS Toolkit [25](#)

## B

- BMS mapsets [19](#)

## C

- checklist
  - installation [3](#)
  - post-installation [3](#)
- CICS
  - application security checking for [25](#)
  - defining programs, mapsets and transactions to [9](#)
  - Transaction Server [19](#)
  - updating tables [10](#)
- Command interface
  - overview [1](#)
- Command interface overview [29](#)
- commands
  - ADDGROUP [30](#)
  - ADDUSER [31](#)
  - ALTUSER
    - CICS segment option [34](#)
    - OMVS SEGMENT option [37](#)
    - TSO segment option [35](#)
    - WORKATTR segment option [39](#)
  - Command interface overview [29](#)
  - CONNECT [40](#)
  - CSDATA [41](#)
  - DELETE [44](#)
  - handling API requests [78](#)
  - LISTDSET
    - panel [47](#)
    - toggle option [47](#)
  - LISTGROUP [49](#)
  - LISTUSER [55](#)
  - Main menu [29](#)
  - PERMIT [62](#)
  - RACLINK [63](#)
  - RALTER [65](#)
  - RDEFINE [65](#)
  - RDELETE [65](#)
  - REMOVE [66](#)
  - RLIST [66](#)
- CONNECT command [40](#)
- Control [75](#)
- CQTJACC [7](#)
- CQTJALL [6](#)
- CQTJAPP [7](#)
- CQTJDDD [6](#)
- CQTJRDO [9](#)
- CQTJREC [7](#)
- CQTJSMPA [6](#)
- CQTJSMPB [6](#)
- CQTJSMPC [6](#)
- CQTPCNTL
  - parameter definitions [9](#)
  - parameter descriptions [21](#)
  - parameters for zSecure CICS Toolkit [21](#)
  - parameters verification [23](#)
- CSDATA command [41](#)
- CSI

## CSI (continued)

- defining Global [6](#)
- defining Product [6](#)

## D

- data set profile
  - listing [100](#)
- DATASET profiles
  - granting access to [106](#)
  - removing access to [106](#)
- date formatting [2](#)
- DELETE command [44](#)
- DELGROUP command [30](#)

## E

- education [xi](#)
- Exit points
  - transferring control from zSecure CICS Toolkit [75](#)

## F

- Field
  - implementing security for [79](#)

## G

- Group
  - adding [92](#)
  - altering [92](#)
  - connecting a user or group to [97](#)
  - deleting [92](#)
  - list and maintain CSDATA fields [98](#)
  - listing profile [102](#)
  - removing a user or group from [108](#)

## I

- IBM
  - Software Support [xi](#)
  - Support Assistant [xi](#)
- IEASVCxx
  - update [7](#)
- information retrieval [27](#)
- installation
  - allocating TARGET and DLIB data sets [6](#)
  - applying the product [7](#)
  - checklist [4](#)
  - creating and initializing SMP/E zones [5](#)
  - defining options [6](#)
  - protecting the SVC [8](#)
  - receiving the product [7](#)
  - SMP/E [3](#)
  - updating SMP/E DDDEFS [6](#)
- Installation
  - automatically assigning UIDs [17](#)
  - automatically create home directories [17](#)
  - defining programs, mapsets and transactions to CICS [9](#)
  - defining SCQTLLOAD as APF-authorized [8](#)
  - Enabling/Disabling zSecure CICS Toolkit [9](#)
  - installing the SVC [7](#)
  - making the RACF definitions [11](#)

## Installation (continued)

- updating CICS tables [10](#)
- updating the CICS startup JCL [8](#)
- installation checklist [3](#)
- introduction
  - installation [3](#)
- IPL
  - update [7](#)
- IRRPNL00 function [86](#)

## J

- JCL
  - for installation [4](#)

## L

- LISTDSET command
  - display option [47](#)
  - Programs option
    - panel [49](#)
  - toggle option [47](#)
  - Userids option
    - panel [48](#)
- LISTGROUP command
  - Display option
    - panel [51](#)
  - panel [49](#)
  - Subgroups option
    - panel [54](#)
  - Toggle option
    - panel [52](#)
  - USERIDS Delete option
    - panel [53](#)
  - USERIDS option
    - panel [52](#)
- LISTUSER command
  - Categories option
    - panel [60](#)
  - Display option
    - panel [58](#)
  - Groups option
    - panel [59](#)
  - OMVS option
    - panel [61](#)
  - panel [55](#)
  - Segments option
    - panel [61](#)
  - Toggle option
    - panel [59](#)
  - WORKATTR option
    - panel [61](#)
- LPALSTxx
  - update [7](#)

## N

- National Language Support [19](#)

## O

- OMVS
  - assigning UIDs automatically [17](#)

OMVS (*continued*)  
    automatically create home directories [17](#)  
Operator ID check [25](#)

## P

parameters  
    CQTPCNTL values verification [23](#)  
Parameters  
    descriptions of CQTPCNTL parameters for zSecure CICS Toolkit [21](#)  
Parameters for [21](#)  
PARMLIB [9](#)  
Password  
    changing [105](#)  
    verifying [112](#)  
PERMIT command  
    panel [62](#)  
post-installation checklist [3](#)  
problem-determination [xi](#)  
Profile  
    delete [100](#)  
    listing and maintaining [108](#)  
    view details of [109](#)  
Program directories [vii](#)  
publications  
    zSecure [vii](#)  
    zSecure Manager for RACF z/VM [vii](#)

## R

RACF  
    defining zSecure CICS Toolkit commands to [11](#)  
RACF database  
    searching [79](#)  
RACF profiles changed [77](#)  
RACLINK command  
    panel [63](#)  
RALTER command [65](#)  
RDEFINE command [65](#)  
RDELETE command [65](#)  
reason codes, IRRPNL00 function [86](#)  
Record  
    implementing security for [79](#)  
REMOVE command [66](#)  
Resource  
    checking user access [80](#), [81](#)  
    granting access to [106](#)  
    removing access to [106](#)  
resource access verification [28](#)  
Resource check  
    application conversion [25](#)  
Resource Profile List [113](#)  
Restart  
    manually [19](#)  
return codes, IRRPNL00 function [86](#)  
RLIST command  
    Conditional access option  
        panel [70](#)  
    Display option  
        panel [68](#)  
    Members option  
        panel [69](#)

RLIST command (*continued*)

    Users  
        panel [70](#)  
        Users option [70](#)  
RRSF [2](#)  
RRSF userid associations  
    approving [107](#)  
    defining [107](#)  
    listing [107](#)  
    removing [107](#)  
RSRC / RSRX functions [25](#)  
RTCK transaction  
    verifying CQTPCNTL parameters [23](#)  
RTST transaction [18](#)

## S

SCQTLOAD [8](#)  
Security checking  
    single point [25](#)  
simple  
    application security interface [27](#)  
simple application security interface [27](#)  
SMF records [77](#)  
SMP/E Modification Control Statements [7](#)  
SVC  
    unauthorized use [8](#)

## T

toggle option, LISTDSET command [47](#)  
training [xi](#)  
Translating BMS mapsets [19](#)  
troubleshooting [xi](#)  
TSQUEUE for profiles [86](#)

## U

User  
    adding a profile for [93](#)  
    authorization for RACF commands [11](#)  
    changing password [105](#)  
    changing the authorized user [79](#)  
    changing the CICS segment [95](#)  
    changing the OMVS segment [96](#)  
    changing the profile for [94](#)  
    changing the TSO segment [95](#)  
    changing the WORKATTR segment [97](#)  
    check access to resources [80](#), [81](#)  
    delete id [100](#)  
    listing profile [103](#)  
    user information retrieval [27](#)  
USRDATA command [71](#)  
USRDATA fields changed [77](#)  
USRDATA function [111](#)

## V

verifying resource access [28](#)

## Z

zSecure CICS Toolkit

zSecure CICS Toolkit (*continued*)  
manual restart [19](#)  
Security resources [14](#)





Part Number:

(1P) P/N: