

Introduction

This chapter covers the following topics:

- Summary of Available Exits
- Areas of Exit Usage
- ULOG ON Security
- SYSCOM,SYSNAT
- Batch/TPF User IDs
- ULOGX1 Exit
- Program, SD File, File I/O Security
- Control Programs
- Message Switching and Printout Spooling
- Utility and Application Security
- ACCESS User Exits

Summary of Available Exits

The following table summarizes Com-plete's security and user exit facilities. Each of the facilities listed below is discussed later in this chapter.

Facility	Summary
ACSUUEX1	Intercepts all screen data that would normally be sent to the user's terminal for manipulation.*
ACSUUEX2	Passes data on to the target system.*
SDAMSEX1	Controls the use of SDAM API functions.
TUDUEX1	Allows user-defined tests and restrictions for use of the TUDUMP program.
UCOEX1	UCOPY exit. Allows user alteration of the destination supplied.
UDMPX1	Defines security restrictions on the use of UDUMP to control the access of dumps in the online dump library.
UDSEX1	Defines security restrictions on the use of UDS (MVS only).
UDVXSX0	Controls/restricts the use of UDS/UDVS VSAM SERVICES.
UDYEX1	Control dynamic allocation/Deallocation of datasets using UDYN (MVS only).
UEDTB1	Defines the library identification codes used to refer to user libraries.

Facility	Summary
ULHMX1	Allows user alteration or suppression of Com-plete's hello message, based on TID.
ULMSBTCH	Allows modification of parameters used by batch spool output routines to generate DYNALLOC/SEGMENT calls.
ULMSDISK	Allows modification of a dynamically allocated printer TIB entry by a user.
ULINUSER	Allows user processing during Com-plete initialization.
ULOGX1	Defines security restrictions on the use of ULOG prior to various events.
ULOPADAB	Allows user examination and/or alteration of Adabas call parameters.
ULSRMPEX	Allows modification of PF key codes in a MRCB.
ULSRSEC	Controls use of specific application functions, programs, modules, and Com-plete utility programs.
ULSRRJE	Examines and/or modifies the (RJE) input data submitted for background processing via the RJE function call.
ULSRSEC	Controls access to files.
UMSEX1	Controls the use of the message switching functions.
USTKX1	
USTRE1	Defines security restrictions on the use of operator command functions.
UTMEX1	Examines each new timer request to be added to the timer SD file by UTIMER.
UTMEX2	Is a timer monitor exit called every minute and for each request that is to be served.
UTMEX3	Is a timer monitor exit called at RJE job submission.
UUEDEX	Defines security restrictions on the use of UED.
UUMAX1	Defines security restrictions on the use of UMAP, and allows user modification of the global defaults to UMAP.
UUMAX2	Defines security restrictions on the use of the UMAP command functions.
UUMAX3	Defines security restrictions on the use of UMAP, forces the cleanup of SD files, and controls the termination of UMAP.
UUPDX1	Defines security restrictions on the use of UPDS (MVS only).
UUQEX1	Defines security restrictions on the use of UQ.
UUSEX1	Defines security restrictions on the use of USDLIB to control the access of SD files.
UUSPL0	Is the USPOOL command exit.
UUSVX1	Defines security restrictions on the use of USER (VSE only).
UTMEX1	Defines security restrictions on the use of UTIL functions.

Facility	Summary
UXEEX1	Defines security restrictions on the use of UEDIT and user ID access to specific libraries or members.
UXEEX2	Defines security restrictions on the use of UEDIT commands and UEDIT termination.
UXEEX3	Defines security restrictions on the use of UEDIT, and controls the job control conventions for submitted jobs from UEDIT and UPDS. (It is recommended that ULSRRJE be used for this function.)
UXEEX4	Defines security restrictions on the use of UEDIT and the interfaces to PANVALET and LIBRARIAN.
UXEEX5	Examines each LOCATE request to catalog management and allows the recall of migrated data sets.

* These exits only exist on the "host" side of an access request, for example the CICS from which the user is accessing.

Areas of Exit Usage

The Com-plete security and user exit facilities allow you to set restrictions on individuals or groups of individuals (departments) for accessing the various facilities, programs, and functions of Com-plete. Restrictions that can be imposed include:

- Requiring a password in order to gain access to the system;
- Disallowing specific users or groups from using certain application programs or Com-plete utilities;
- Disallowing specific users or groups from using various functions within an application program, while simultaneously allowing the use of other functions within the same program (for example, allowing the display of records for an application file, but disallowing updates);
- Disallowing specific users or groups from using certain control functions provided by some of the Com-plete online utility programs (for example, the K function of the UQ utility program);
- Restricting usage of the UQ functions H, R, C, DE, and S to terminal users who have submitted the specific job being accessed or to users who belong to a specific department;
- Disallowing specific users or groups from viewing certain messages or printout spooling data sets.

In addition to the security checks that can be imposed, an installation can also restrict program execution to specific threads based upon their thread-lock number. For example, if a program is thread-locked to thread two, the installation may choose to force execution to thread one without recataloging the program. This restriction can be forced by program name, thread number, or both.

The areas where security can be defined in order to accomplish these objectives include:

- ULOG ON security;

- Program security;
- SD file security;
- File I/O security;
- Thread-scheduling control;
- Program timing (MVS only);
- Control user IDs;
- Message switching security;
- Printout spooling security;
- Utility security;
- Application security;
- Data manipulation using ACCESS.

Many of these security areas allow you to define and write subroutines to meet the needs of your installation. Their general purpose and function is presented in the following sections.

ULOG ON Security

Before accessing any application program or Com-plete utility, a terminal operator can be required to enter a "*ULOG ON" request as identification to Com-plete security and accounting routines. This logon requirement is an optional feature of Com-plete selected at initialization time (see the ACCOUNTING and PASSWORD sysparms).

When a user logs on, a user ID and a password, must be supplied. Com-plete verifies the information by invoking an external security package (for example, RACF) via the SAF interface, or by accessing the Com-plete system data set, which contains user ID information. For each user allowed to access the Com-plete system, this information consists of the following:

- A unique user ID that identifies the user;
- The account number (or group number) with which the user ID is associated;
- The password for the user ID;
- The control status to be assigned to the user ID. This status is used by various Com-plete utilities to restrict the use of certain privileged functions (e.g., the K function of the UQ utility);
- The authorization code for the user ID;
- The sending and receiving message and printout class codes for the user ID.

Each time a "*ULOG ON" request is entered, the user ID is accessed in the system data set and the password, if required, is validated. If the user ID is not found, or if the password is not verified, the ULOG ON request is aborted.

If the user ID is found and the password is verified, a control block for the user containing information from the user ID record is created, plus additional room for keeping track of the resources to be assigned to the user ID. This control block is called the user accounting block (UAB), see also the chapter Accounting.

If an external security system such as RACF, ACF2 or TOP SECRET is installed and specified in the Com-plete startup procedure, the user ID/password combination must pass the external security system verification rules. If the user ID/password combination is unknown, the request is rejected with the message returned from the security system.

SYSCOM,SYSNAT

If the user ID is not defined on the Com-plete system data set and the NATURAL Security Interface is active (sysparms with prefix NATSEC), the user ID and password combination is verified against the NATURAL Security File. If the user ID exists and the password is correct, the user ID is logged on with the entered user ID, and the Com-plete required information retrieved using the user ID model SYSNAT.

If the user ID is not defined to the Com-plete system data set, and the NATURAL Security interface is either not installed or rejects the logon, and APPLYMOD 57 is specified, the user ID is logged on irrespective of the specified password and given the Com-plete required information from the user ID model SYSCOM.

In both cases the model user ID must be defined to Com-plete. If an external security system is present, then the model user ID is also validated with the security system.

If the model user ID is defined, then the logon is allowed using the authorization obtained for the model user ID.

If the model user ID is not defined, then the logon is still allowed but no authorization is supplied, that is, any attempted access to items which would normally be protected by the external security system will fail.

Batch/TPF User IDs

For Batch and TPF users, a model user ID is always supplied by the host system in the logon data (SYSBAT and SYSTPF respectively). The logon then proceeds as above, the user IDs SYSBAT and SYSTPF must be defined on the Com-plete system data set and can also be defined to an external security system.

ULOGX1 Exit

In addition to Com-plete security, a user-written security exit, ULOGX1, is called to allow the installation to perform further security checking against passwords, time-of-day, etc. This routine can also change some items in the Logon Information Block that is assigned to the user ID. These items include:

- Control status ;
- Authorization code;

- Account number;
- Message class codes;
- COM-PASS model.

The ULOGX1 security exit is discussed later in this chapter.

Program, SD File, File I/O Security

The user-written security routine ULSRPSFS is called to allow security checks to be issued for any or all Com-plete application functions.

ULSRPSFS either allows or disallows the request by setting a return code. If the request is disallowed, the application program is abnormally terminated.

Control Programs

Some of the functions afforded by the Com-plete utilities are restricted to user IDs that are assigned control status. These functions are listed in the following table:

Utility	unction
UDD	All commands
UDZAP	All commands
ULIB	CAT and DEL commands for PV programs
UM	SCLASS command RCLASS command PURGE command, using TID parameter* DELETE command, using TID parameter* ALT command, using TID parameter* RESET command, using TID parameter*
UQ	K command (see APPLYMOD=6 in Binary Modifications (APPLYMODS))
USTOR	All functions
UUTIL	For authorizations of UUTIL functions, see the Com-plete Utilities documentation

* See APPLYMOD=7 in Binary Modifications (APPLYMODS)

These utility programs and their privileged functions are discussed in more detail in the Com-plete Utilities documentation.

Message Switching and Printout Spooling

Each time an application program or Com-plete utility program makes a request to send a message or printout, Com-plete performs a security check to see if the class codes assigned to the message or printout correspond to the class codes assigned to the user ID using the sending terminal. If not, the message switch or printout request is aborted.

Com-plete also checks the class codes for the user ID of the receiving terminal. If they do not match the class codes of the message or printout, the message or printout is aborted.

If an attempt is made to send a message or printout to a terminal not in use, the default class codes for that terminal are used. This allows for sending messages and printouts to terminals to which no one has logged on (e.g., a 3286 line printer).

Default message switching and printout spooling class codes are normally set when TIBTAB is created and/or the user ID is defined. The creation of TIBTAB is defined in the chapter entitled TIBTAB - Terminal Information Block Table. User IDs are defined using the UUTIL utility program, which is described in the Com-plete Utilities documentation.

Utility and Application Security

Utility Security

Most of the Com-plete utilities described in the Com-plete Utilities documentation contain at least one exit point for exiting to a user-written routine. Each of these routines' functions and linkage conventions is discussed later in this chapter. These routines allow you to define your own security restrictions on the use of the utility programs.

In addition, the UQ utility program recognizes certain job control comment cards that can be used to restrict usage of the UQ functions H, R, C, DE, and S. These statements are:

xxxUQ USER ID	restricts user IDs
xxxUQ ACCOUNT	restricts account numbers
xxxUQ AUTHORIZE	restricts authorization codes
xxxUQ DISALLOW	restricts all access
xxxUQ ALLOW	removes access restrictions
xxxUQ USER	passes information to the exit

where xxx is "/*" in MVS, and "* *" in VSE.

Note that these job control comment statements must exist in the job stream preceding the first EXEC statement. Further information on their usage can be found in the Com-plete Utilities documentation.

Generally, if more than one of the comment statements are present, only one condition must be met to pass security checking. If none are present, UQ either disallows everyone using the indicated functions or allow everyone, depending upon the default Com-plete sysparm UQDEFAULT.

Application Security

If an application program needs to restrict some but not all of its functions, the GETCHR function can be used to establish the required authorization.

The GETCHR function enables the program to determine the user ID, account number, authorization code, and control status of the terminal user. This way, some functions can be restricted to certain user IDs.

The GETCHR function is fully described in the Com-plete Application Programmer's documentation.

COM-PASS Security System

All or parts of utility and application security can be accomplished through the use of the COM-PASS security system.

COM-PASS users are defined by a User Profile. A part of this profile is the User Transaction Profile. Every access the user attempts to make to a transaction is checked by COM-PASS. If the user is not allowed to use the transaction, either of the following messages are displayed:

```
OVL0007 (-) - ACCESS TO REQUESTED PROGRAM DISALLOWED
UMP0023 - SECURITY VIOLATION - ACCESS TO PROGRAM DISALLOWED
```

The COM-PASS User Profile is determined by:

- The COM-PASS security indicator. This defines the user to be checked by COM-PASS for transaction security within Com-plete.
- The COM-PASS menu transactions (A through I). These are the transactions that are defined for the user, which appear on the COM-PASS main menu as service programs.
- The COM-PASS startup program. This can be set to any valid COM-PASS, Com-plete, or user transaction program. To have the main menu appear first, set this parameter to USTACK.

The user is not allowed to change the transaction authority. When the security switch is set, the user is only allowed to use the defined transaction programs that appear on his/her main menu as service programs.

ACCESS User Exits

ACCESS provides user exits that enable user-written routines to be called by the ACCESS transaction. These user exit routines can examine and alter data at the following times:

- Before writing the data from the target node to the host terminal;
- Before the terminal input is sent to the target node.

Note:

All references to "target node" refer (currently) to a Com-plete system.

The names of these exits are ACSUUEX1 (writing) and ACSUUEX2 (reading). Each one is explained later in this section