

Security Systems

This chapter covers the interfaces to the various Security Systems on the market as well as how they interface with the Com-plete Security System. A good understanding of the relevant system is essential as we can only discuss the Com-plete side of the interfaces here. For the purposes of this description, ACF2, RACF and TOP SECRET are known as "external security systems" and Com-plete Security is known as COMSEC. Com-plete also has an interface to the Natural Security system for logon validation.

This information is provided under the following headings:

- Modes of Operation
 - External Security System Operation
 - Com-plete Security Operation
 - External Security with COMSEC
 - Interface To Natural Security
 - Defining Com-plete to ACF2
 - Defining Com-plete to RACF
 - Defining Com-plete to TOP SECRET
-

Modes of Operation

Through the SECSYS sysparm, you can choose which security system is to be used. The currently available choices are RACF, ACF2, and TOP SECRET, and/or COMSEC.

External Security System Operation

Com-plete uses the System Authorization Facility (SAF) to interface to the external security system. All logons and logoffs are verified/notified via the external security system and access to data sets is also verified through the specified security system via the SAF interface. Com-plete uses this interface as it is common to all systems, therefore, except for a few small exceptions, the sysparm specification is only used where it is necessary to identify the external security system name.

Com-plete identifies itself as the caller via the SUBSYS keyword on the RACROUTE call. The format of the ID is as follows...

```
SAGCOMvr
```

where "vr" is the current Com-plete version release level. This has implications for the various external security systems which are discussed later.

As various users will run within the same address space, the external security system must be aware of that fact (for example, ACF2 must know the Com-plete address space as Multiple User Address Space "MUSASS") otherwise, requests will be given the authority of the actual address space which is normally too high for the general user.

The Com-plete module issuing the SAF requests runs with AMODE=31 and RMODE=ANY. This means that the ACEEs built by the security can exist above the 16 MB line if the external security system supports this.

Com-plete Security Operation

Com-plete Security holds all information on an Adabas file. When the security system is loaded, the data is stored in tables within the address space to be queried as to the access that a user may have to various resources. Refer to the Com-plete Security documentation for more details on defining access rules.

External Security with COMSEC

The only current duplication between these two is access to data sets and system entry validation. The access calls that are made are made to an internal security routine which then calls the various exits or products installed. The application therefore gets no indication of who fails the request, it simply knows that it failed. In the case where both are specified, one OR the other has the chance to fail the request. To avoid unnecessary duplication, you should allow anybody running under that Com-plete have access to the data sets, while using the other system to actually validate the access.

If an external security system is installed, you will have all user IDs defined there. Therefore, the logon request is ignored by Com-plete Security and issued through the external security system.

Interface To Natural Security

An interface is also available to the Natural Security System. In this case, if the user ID is not defined to Com-plete, Com-plete checks the user ID and password against the Natural Security System file. If found, the user is logged on with the entered user ID and with a model user ID of "SYSNAT" from the Com-plete user ID file. If the user ID exists, but the password check fails and an external security system has been specified at startup, the password violation is ignored and the password is verified via the external security system.

To use this feature of Com-plete, the following steps must be taken.

1. Add a model user ID SYSNAT using the Com-plete user ID maintenance utility.
2. Specify the Com-plete sysparms NATSECDB and NATSECFN to identify the Natural Security System file to be used.

Defining Com-plete to ACF2

As stated previously, Com-plete uses the SAF facility. Therefore, the ACF2 SAF exit must be installed and active on the system. This can be checked by entering the command T C(GSO) followed by LIST OPTS in the TSO ACF command. Options SAF and STC must be specified (they are not specified by default). Please refer to the ACF2 documentation for more information. The user ID assigned to the Com-plete must be defined with the following privileges.

```
JOBFROM MUSASS NO-SMC STC
```

For Job Submission, Com-plete inserts the /*JOBFROM control card in the second line to ensure that the Com-plete supplied card is seen first by ACF2. This means that the user does not need to supply a user ID and password in the JCL and it also means that Com-plete does not have to remember the password to insert it for the user.

ACF2 v. 5.2 and lower:

Assuming that most installations run as advised by the ACF2 installation documentation, the "SAFSAFE" record lets all SAF requests through without checking, as with the following "SAFSAFE" definition.

```
CLASSES(-) CNTLPTS(-) SUBSYS(-)
```

the following "SAFPROT" definition is required for Com-plete:

```
CLASSES(-) CNTLPTS(THREAD-) SUBSYS(SAGCOMvr)
```

Where "vr" is the current version release for Com-plete.

ACF2 v. 6 and above:

The SAF interface in ACF2 has changed. You must use ACF2 conversion facilities to switch your old definitions to match the new version (the old definitions can remain, but will be ignored). The following SAFDEF definition is an example of what is required for Com-plete:

```
SAFDEF COMvr LAST CHANGED BY BHD ON 23/9/97-15:51
  FUNCRET(4) FUNCRSN(0) ID (COMvr) MODE(GLOBAL)
  RACROUTE(SUBSYS=SAGCOMvr REQSTOR=-) RETCODE(4)
```

Defining Com-plete to RACF

As stated previously, Com-plete uses the SAF facility. Standard RACF installation results in the installation of the RACF SAF routines.

No changes to the RACF definition are necessary for Com-plete.

For Job Submission, when the USERID and PASSWORD cards are not provided on the Job Card, Com-plete supplies both cards to identify the job submitter. However, this means that Com-plete must remember the password to insert it for the user, therefore applmod 83 is incompatible with the use of RACF on a system.

Defining Com-plete to TOP SECRET

The following describes the steps required to define Com-plete to a CA-TOP SECRET security system. For the sake of clarity, the following examples do not take advantage of techniques such as the defining of profiles, etc. Where examples are given, you are also referred to the relevant CA-TOP SECRET documentation where you will find more information.

Com-plete is defined as a system facility by CA-TOP SECRET by default. This is described in the TOP SECRET documentation CA-TOP SECRET Implementation: Other Interfaces Guide, section Com-plete. The modifications described in the subsection Required Modifications are no longer necessary, as Com-plete interfaces with TOP-SECRET via the SAF interface as described above. To avoid confusion, an update request for this section has been issued.

You must change this facility definition using the TSS MODIFY FACILITY command to set the following options:

```
NOABEND          TENV
```

For more information, see the CA-TOP SECRET MVS Control Options Guide.

You now must create an ACID to identify this Com-plete release and link this ACID to the Facility. The name we have chosen for this ACID is the same as that used for the subsystem name we use on the RACROUTE calls documented previously. This is simply as a naming convention and is not necessary for the operation of this interface. You can choose your own names if you so wish. For our example, the ACID we use is SAGCOMvr (where "vr" is the Com-plete Version and Release). The ACID is created with a TSS command as follows:

```
TSS CREATE(SAGCOMvr) TYPE(USER) NAME('COMPLETE vr')
      DEPT(RDDEPT) PASS(NOPW) FAC(ALL) MASTFAC(COMPLETE)
```

For more information, see the CA-TOP SECRET MVS Implementation documentation.

Each Com-plete startup procedure must use the relevant ACID. The ACID that should be used can be identified with the following TSS command:

```
TSS ADD(STC) PROC(pppppppp) ACID(SAGCOMvr)
```

where pppppppp is the procedure name.

For more information see the CA-TOP SECRET MVS Implementation documentation.

Users must then be authorized to logon to Com-plete. This can be done with the following TSS command:

```
TSS ADD(uuuuuuuu) FAC(COMPLETE)
```

where uuuuuu is the user ID.

For more information see the CA-TOP SECRET MVS Implementation documentation.

For Job Submission, Com-plete inserts the constant "x'FF',c'TSS'" followed by the address of the user's ACEE in columns 73-80 of the Job Card. In this way, the user does not have to supply a user ID and password in the JCL and it also means that Com-plete does not have to remember the password to insert it for the user.