# CA SYSVIEW® Performance Management

## Security Guide

Version 14.0

# CA Technologies Product References

This document references the following CA Technologies products:

- CA SYSVIEW® Performance Management (CA SYSVIEW)
- CA ACF2™ for z/OS (CA ACF2)
- CA Insight™ Database Performance Monitor for DB2 for z/OS (CA Insight DPM for DB2)
- CA Top Secret® for z/OS (CA Top Secret)

# Contact CA Technologies

**Contact CA Support**

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

**Providing Feedback About Product Documentation**

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

# Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Updated the Initial Settings for User Groups (see page 22): Revised the User-defined description.
- Updated the Resource Calls by Command (see page 74):
  - Added XSCONN
  - Removed XSYSDEST and XSYSORIG
- Updated the Resource-Value Field Values for Basic Resource Types (see page 83): Added XSDATA to the list of basic resources.
- Updated the Resource-Value Field Values for Other Resource Types (see page 93): Edited the XSYSDEST and XSYSORIG descriptions.
- Updated the FACILITY Class (see page 127): Removed the CSVAPF.** resource, which let the main task run GSVXINST.

# Contents

## Chapter 3: Printing Security Definitions 31

## Chapter 4: Security Displays 45

## Chapter 5: Interfacing with External Security 115

## Chapter 6: Controlling Access Using SAF 131

## Chapter 7: Preparing the SAFSAMPX Sample Exit 153

# Chapter 1: Security Basics

This section contains the following topics:

## Product Security Overview

The Administrators provide security for CA SYSVIEW because they control access to and use of the product. They define user groups that include a global group and a default group.

The Administrator does the following:

- Limit CA SYSVIEW command and subcommand usage
- Define what is shown on a display
- Limit MVS command usage
- Display a message on the system console when a user issues a command
- Interface with your system security through an exit
- Limit access to jobs and changes to job information
- Limit the output destinations accessible by members of a security group
- Limit the resources available to members of a security group

## User Groups

User groups contain the security definitions for lists of users who have similar security requirements for the product. CA SYSVIEW reviews these groups to determine what security privileges a user can exercise. You can define any number of user groups.

## Types of User Groups

CA SYSVIEW has four types of user groups. The following list describes each of the user groups:

**GLOBAL**

The GLOBAL group definitions apply to all CA SYSVIEW users.

**ADMIN**

The ADMIN group definitions apply only to the CA SYSVIEW administrators.

**User-defined**

The user-defined group definitions apply to users. The administrators define the definitions. The definitions for these security groups reflect the restricted use of the SECURITY command.

**DEFAULT**

The DEFAULT group definitions apply to users who are not defined in any security group. This group does not need User IDs defined. If a user ID is not found in any other security group, the DEFAULT security group is used.

**More information:**

Defining Security (see page 17)

## Who Defines User Groups

Administrators define user groups. An administrator is a user who has the authority to create and modify all user groups and perform all user functions.

## Administrator Privileges

The first CA SYSVIEW administrator is created during the installation of the product. That administrator creates additional administrators.

## Administrator Capabilities

The administrator performs the following functions:

- Creates administrators
- Changes the ADMIN, GLOBAL, and DEFAULT security user groups
- Defines a security user group and all security definitions for the group
- Defines a security user group, the members belonging to that group, and the commands they can use
- Defines a security user group, the members belonging to that group, and the command groups they can use
- Defines command groups
- Views all security user groups
- Changes the default user profile

## How User Groups Are Checked

CA SYSVIEW reviews the user groups to determine security privileges. When a user issues a CA SYSVIEW command, CA SYSVIEW verifies whether the user is allowed to use the command.

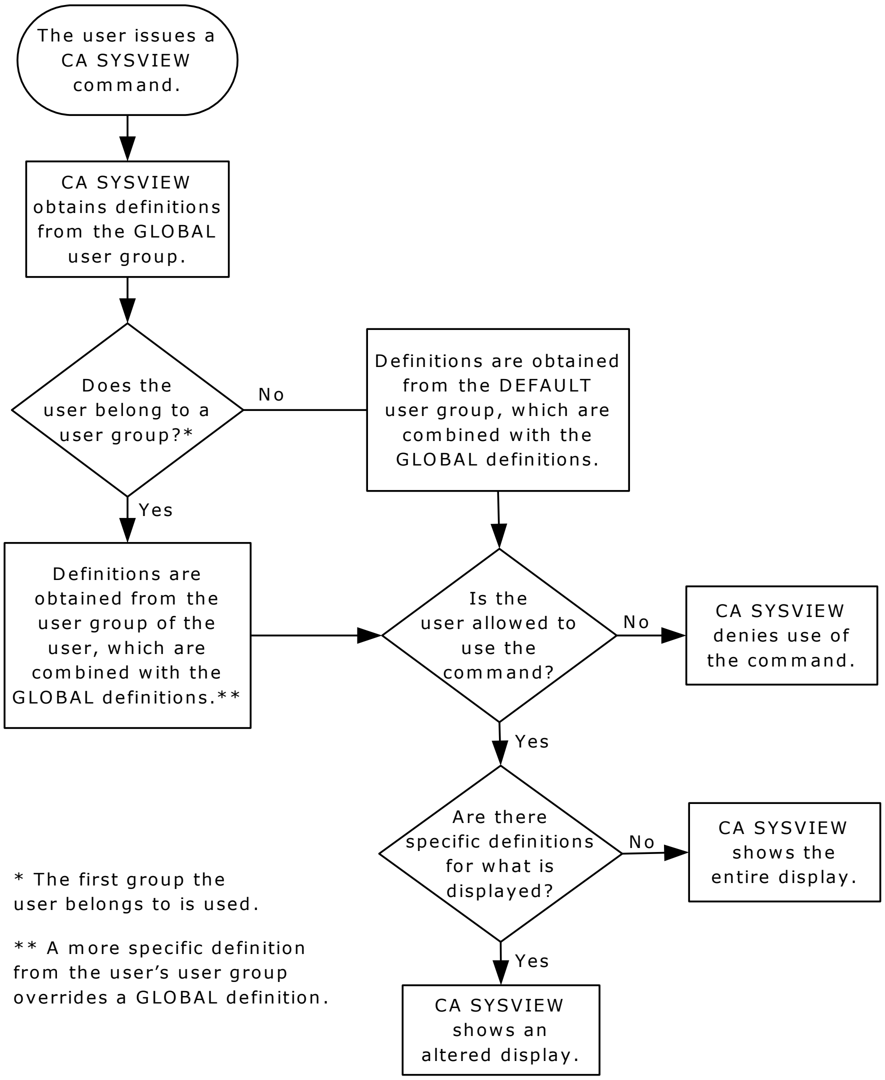
CA SYSVIEW uses the following process to verify the command against the user security:

1. Reviews the GLOBAL user group first for definitions that apply to every user of the product.
2. Checks to see what user-defined security group the user belongs to and reviews those definitions.
3. Uses the more specific definition in the user-defined group when a definition from a user-defined group is more specific or equivalent to a GLOBAL definition.

   The definition in the user-defined group overrides the GLOBAL group definition.
4. Uses the DEFAULT user group if a user ID is *not* found in any other user group.

## How Security Checks Work

The following diagram shows the order in which CA SYSVIEW verifies security groups:


The user issues a CA SYSVIEW command.
CA SYSVIEW obtains definitions from the GLOBAL user group.
Does the user belong to a user group?*
No
Definitions are obtained from the DEFAULT user group, which are combined with the GLOBAL definitions.
Yes
Definitions are obtained from the user group of the user, which are combined with the GLOBAL definitions.**
Is the user allowed to use the command?
No
CA SYSVIEW denies use of the command.
Yes
Are there specific definitions for what is displayed?
No
CA SYSVIEW shows the entire display.
Yes
CA SYSVIEW shows an altered display.

* The first group the user belongs to is used.

** A more specific definition from the user’s user group overrides a GLOBAL definition.

# Command Groups (Optional)

Command groups are groups that contain selected CA SYSVIEW commands. The administrator defines the command groups and then assigns them as either allowed or failed to one or more user groups.

For instance, to give all users in the group access to all of the commands in the CICS command group, the administrator:

1. Defines a command group named ALLCICS that contains all of the CICS commands.
2. Assigns this ALLCICS group to a user group with an action of allow.

Using command groups simplifies assigning which commands a group can use instead of setting the commands individually through the Commands Section.

## Types of Command Groups

CA SYSVIEW provides default command groups, which start with the letters GSV. The supplied command groups contain commonly grouped commands. For example, the GSVCICS group contains all of the CICS commands. You can assign the command groups to user groups or can copy them to make new command groups.

Only the administrator can modify the GSV groups.

To modify a GSV group when you do not have administrator privileges, do the following:

1. Copy the group that you want to modify to another group.
2. Assign a name that does not start with GSV.

The GSV groups are automatically updated with new commands. You can optionally update your site modified command groups with any of the new commands that are shipped in the GSV groups.

## Who Defines Command Groups

Administrators define the command groups. An administrator is a user who has the authority to create and modify all command groups and perform all command functions.

## Administrator Privileges

The first CA SYSVIEW administrator is created during the installation of the product. That administrator creates additional administrators.

## How Command Groups Are Checked

Using command groups significantly reduces the calls necessary to determine which commands are authorized for the user.

CA SYSVIEW verifies the security of command groups as follows:

1. Reviews the command groups during the initialization of a CA SYSVIEW user session to determine whether command groups are assigned to a user group.
2. When command groups are assigned to a user group, then CA SYSVIEW initiates a call to the security exit. This call determines whether the command group is authorized. The call is made during the session initialization with a resource type of CMDGROUP and a resource value of the command group name.

   **Note:** When internal security forbids a command group, the security exit cannot override this setting.
3. Marks the command included in the command group as allowed or not allowed, depending on the group authorization.
4. Verifies all the command groups.
5. Reviews the remaining commands that were not included in a command group that is assigned to the user group as the user references each command.

# Chapter 2: Defining Security

This section contains the following topics:

## Available Security

CA SYSVIEW gives you the ability to define security to users as follows:

**Users**

Define who can use CA SYSVIEW

**Commands**

Define which commands the user is allowed to use

**Command Groups**

Define which command groups are defined to the user group

**Command Capabilities**

Define which command capabilities the user can use

**Display**

Define what a user sees on the display of a command

**Other Users**

Create and change the profiles of other users

### Available Security Categories

The following table lists the security categories that can be available for a user group. These categories are options on the User Group Detail display.

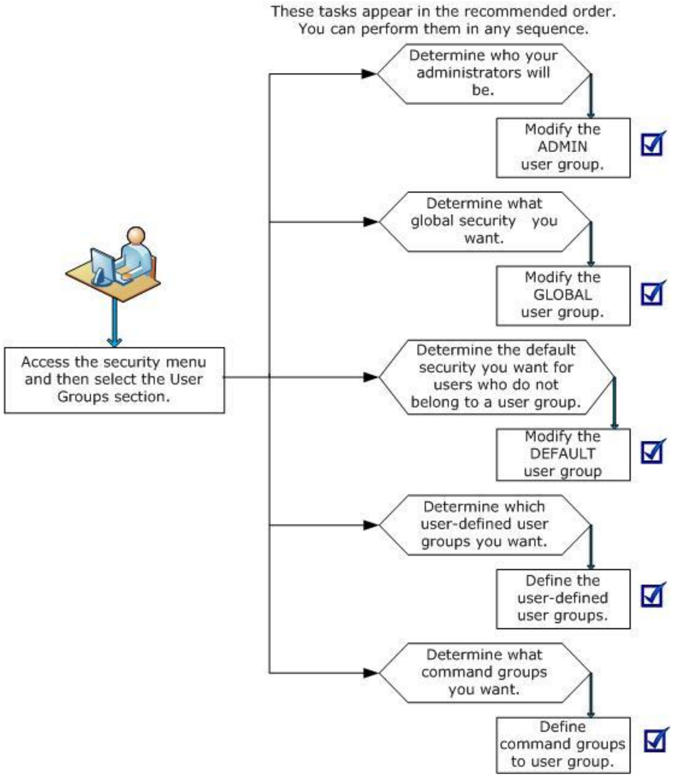
| Security Categories | What You Define |
|---|---|
| User IDs | The members of the user group |

| Security Categories | What You Define |
|---|---|
| Commands | The commands that the user group can use |
| Command Groups | Command groups that are defined to the user group |
| Command Fields | The fields on the CA SYSVIEW displays that the user group can see and change |
| Jobnames | The jobs that the user group can access or the ones for which definitions apply |
| Resources | The resources defined for the user group that the group can access |

**Note:** If the user group does not use a category, that category is not shown on the User Group Detail display for the group. For example, the GLOBAL user group does not use the User IDs Section or Commands Sections, so those categories do not appear on the display.

# How You Define Security

The following illustration describes the overall process to define security for CA SYSVIEW. The remainder of this chapter describes how to define each type of security group.


These tasks appear in the recommended order.
You can perform them in any sequence.
Access the security menu and then select the User Groups section.
Determine who your administrators will be.
Modify the ADMIN user group.
Determine what global security you want.
Modify the GLOBAL user group.
Determine the default security you want for users who do not belong to a user group.
Modify the DEFAULT user group
Determine which user-defined user groups you want.
Define the user-defined user groups.
Determine what command groups you want.
Define command groups to user group.

# How Administrators Are Defined

The first administrator for CA SYSVIEW is created during the installation of the product. The user ID of the first administrator is specified on the Administrator-Userid parameter in the Systems Configuration Member. You can specify more than one user ID on this parameter.

The administrator defined during installation creates additional administrators for the product by adding user IDs to the ADMIN user group. Any administrators can specify definitions for administrators in the ADMIN user group.

**Note:** For a description of the Systems Configuration Option, see the *Installation Guide*.

## Initial Settings for the ADMIN User Group

The installation provides the initial settings for the ADMIN user group definitions. Initially, the ADMIN user group can perform all functions for the CA SYSVIEW product.

## Define Additional Administrators

You can receive requests to add additional administrators to the system due to personnel changes.

**Follow these steps:**

1. Log on with an administrator ID.
2. Enter **SECURITY** after any CA SYSVIEW prompt and select the User Groups.

   The User Groups display is shown.
3. Enter **S** to the left of the group name ADMIN and press Enter.

   The User Group Detail display is shown.
4. Enter **S** to the left of the User IDs Section field and press Enter.

   The User IDs Section display is shown.
5. Enter the user IDs of the additional administrators in the user IDs column.
6. Issue the RETURN command and completely exit the SECURITY command.

   When you exit the SECURITY command, the changes are made permanent. If a user is logged on, the new definitions do not take effect immediately; the changes take effect the next time the user logs on.

**More information:**

Defining Security (see page 17)

## Specify or Change Definitions for Administrators

You can receive requests to change the definitions of the administrators. Specifying or changing the definitions affects all administrators, including the administrator making the specification or change.

**Follow these steps:**

1. Enter **SECURITY** after any CA SYSVIEW prompt and select the User Groups.

   The User Groups menu displays.

2. Enter **S** to the left of the group name ADMIN and press Enter.

   The User Group Detail menu displays.

3. Enter **S** to the left of one of the sections and press Enter.

   The section menu displays.

4. Specify or change the definitions and then issue the RETURN command.

5. Repeat Steps 4 and 5 until all of the changes are made and then completely exit the SECURITY command.

   When you exit the SECURITY command, the changes are permanent. If a user is logged on, the new definitions take effect the next time the user logs on.

## Delete an Administrator

You can receive requests to remove administrators from the system due to personnel changes.

**Follow these steps:**

1. Enter **SECURITY** after any CA SYSVIEW prompt and select the User Groups.

   The User Groups display is shown.

2. Enter **S** to the left of the group name ADMIN and press Enter.

   The User Group Detail display is shown.

3. Enter **S** to the left of the User IDs Section field and press Enter.

   The User IDs Section display is shown.

4. Remove the user IDs of the administrators you want to delete by erasing the line or spacing over the User ID.

5. Issue the **RETURN** command and completely exit the SECURITY command.

   The changes become permanent when you exit the SECURITY command. If a user is logged on, the new definitions take effect the next time the user logs on.

# Control Access with User Groups

The purpose of defining user groups is to control the use of CA SYSVIEW. Often, the members of a user group are the members of a department. For example, employees in the payroll department could be placed in a user group of their own.

This section applies to defining the following kinds of user groups:

- User-defined
- GLOBAL
- DEFAULT

**More information:**

Security Displays (see page 45)

## Initial Settings for User Groups

The installation provides initial settings for the following user group definitions:

- User-defined

  Provides initial setting for a user-defined group. All commands are initially allowed. So, minimally update the Commands Section to fail any commands that you do not want the new User Group to access.

- GLOBAL

  Provides initial settings for the GLOBAL group. Initially, each section in the GLOBAL user group grants access to all CA SYSVIEW commands and resources.

- DEFAULT

  Provides initial settings for the DEFAULT group. Initially, the DEFAULT user group grants access to all commands (except SECURITY).

## Define a User Group

You can receive requests to add new user groups. The following steps define your security for the new user groups. Repeat these steps for each user group you want to create.

**Follow these steps:**

1. Enter **SECURITY** after any CA SYSVIEW prompt and select the User Groups.

   The User Groups display is shown.

2. Enter **S** to the left of the AddGroup field, enter the new group name in the group field, and press Enter.

   The User Group Detail display is shown.

3. Enter **S** to the left of the Miscellaneous section field and press enter.

   The miscellaneous values display for your review.

4. Enter **S** to the left of the User IDs Section field and press Enter.

   The User IDs Section display is shown.

5. Enter the user IDs of the users you want to specify as members of this group and issue the RETURN command.

   The User Group Detail display is shown.

6. Enter **S** to the left of another section and press Enter.

   The display for this section is shown.

7. Specify the desired definitions and issue the RETURN command.

   The User Group Detail display is shown.

8. Repeat Steps 6 and 7 until you specify all the definitions you want and then completely exit the SECURITY command.

   The changes are made permanent. If a user is logged on, the new definitions do not take effect immediately; the changes take effect the next time the user logs in.

## Copy a User Group

You can receive requests to copy a user group. Repeat these steps for each security group you want to copy.

**Follow these steps:**

1. Enter **SECURITY** after any CA SYSVIEW prompt and select the User Groups.

   The User Groups display is shown.

2. Enter the **ADD** subcommand and its parameters to the right of the command prompt and press Enter.

   The new security group is created.

3. Completely exit the SECURITY command.

   The changes are made permanent. If a user is logged on, the new definitions take effect the next time the user logs in.

A batch utility is available to copy selected User Groups from one security data set to another. See the member GSVUSECC in the CNM4BSAM SMP/E target library for a sample JCL for executing the utility.

## Delete a User Group

You can receive requests to delete a user group.

**Follow these steps:**

1. Enter **SECURITY** after any CA SYSVIEW prompt and select the User Groups.

   The User Groups menu displays.

2. Enter **D** to the left of the security group you want to delete and press Enter.

   The security group is deleted.

   When you have the delete confirmation in effect, the User Group Detail display is shown and you are asked to confirm the deletion. Enter **YES** to delete the group. Press PF3 or enter **RETURN** to cancel the request.

3. Completely exit the SECURITY command.

   The changes are made permanent. If a user is logged on, the new definitions do not take effect immediately; the changes take effect the next time the user logs in.

## Change Definitions for User Groups

You can receive requests to change a user group.

**Follow these steps:**

1. Enter **SECURITY** after any CA SYSVIEW prompt and select the User Groups.

   The User Groups menu displays.

2. Enter **S** to the left of the security group you want to alter and press Enter.

   The User Group Detail menu displays.

3. Enter **S** to the left of a section and press Enter.

   The display for this section is shown.

4. Change the desired definitions and issue the RETURN command.

   You are returned to the User Group Detail display.

5. Repeat Steps 3 and 4 until you make all the changes you want.

6. Completely exit the SECURITY command.

   The changes are made permanent. If a user is logged on, the new definitions do not take effect immediately; the changes take effect the next time the user logs in.

## Delete a Member of a User Group

You can receive requests to delete a member of a user group.

**Follow these steps:**

1. Enter **SECURITY** after any CA SYSVIEW prompt and select the User Groups.

   The User Groups display is shown.

2. Enter **S** to the left of the security group to which the user you want to delete belongs and press Enter.

   The User Group Detail display is shown.

3. Enter **S** to the left of the User IDs Section field and press Enter.

   The User IDs Section display is shown.

4. Remove the user IDs of the members you want to delete by erasing the line or spacing over the user ID. Issue the RETURN command and completely exit the SECURITY command.

   The changes are made permanent. If a user is logged on, the new definitions do not take effect immediately; the changes take effect the next time the user logs in.

# Types of Profiles

CA SYSVIEW controls access by providing the following three types of profiles:

- Global

  Contains the default values for the profile settings. You cannot change these settings.

- Default

  Used to set default values for your site. You can change these settings. Changes made to the default profile override the global values.

- User

  Used to set override values for a user. You can change these settings. Changes made to the user profile override the default values.

**Note:** For more information about the displays you see when you change or create profiles, see the *User Guide*.

# DEFAULT Profile Contents

CA SYSVIEW uses the DEFAULT profile when a user does not have a profile defined. Administrators can change the DEFAULT profile to meet the needs of your site.

The DEFAULT profile contains the following information:

- Default PF key settings
- Default synonyms
- Other information used by the CA SYSVIEW commands

## Change the DEFAULT Profile

Only CA SYSVIEW administrators can change the DEFAULT profile.

**Follow these steps:**

1. Issue the following command:

   ```
   PROFILE CHANGE,DEFAULT
   ```

   The Profile Selection displays.

2. Enter **S** to the left of the section (either General or a specific command) you want to change and press Enter.

   The new selection displays.

3. Enter **S** on the next selection screen to the left of the section you want to change and press Enter.

   The section you selected displays.

4. Complete your updates and issue the RETURN command.

   You are returned to the previous display.

# User Profile Contents

The individual users define their profile using the PROFILE command. If a user does not have a profile, the PROFILE command automatically creates one from the DEFAULT profile.

The user profile contains the following information:

- PF key settings
- Synonyms
- Other information used by the CA SYSVIEW commands

## Create a User Profile

Only CA SYSVIEW administrators can create a user profile.

**To create a User Profile**

1. Issue the following command:

   ```
   PROFILE CREATE,u1,u2
   ```

   ***u1***

   Specifies the user ID of the user whose profile you want to create.

   ***u2***

   Specifies the profile to use when the new profile is created.

   The DEFAULT profile member is used to create the new profile when *u2* is not specified.

2. Enter **S** to the left of the option you want to change and press Enter.

   The menu for that option displays.

3. Enter **S** to the left of the section you want to change and press Enter.

   The menu for that section displays.

4. Complete your changes issue the RETURN command.

   You are returned to the previous display.

**Important!** Two members in a partitioned data set cannot have the same name. If a profile exists for the user ID supplied on the PROFILE CREATE command, it is overlaid.

## Change the Profile of a User

Only CA SYSVIEW administrators can change a profile of a user.

**To change a user profile**

1. Issue the following command:

   ```
   PROFILE CHANGE,userid
   ```

   ***userid***

   Specifies the user ID of the user whose profile you want to change.

   The Profile Selection menu displays.

2. Enter **S** to the left of the option you want to change and press Enter.

   The menu for that option displays.

3. Enter **S** to the left of the section you want to change and press Enter.

   The menu for that section displays.

4. Complete your changes and issue the RETURN command.

   You are returned to the previous display.

# Chapter 3: Printing Security Definitions

This section contains the following topics:

## Print Security Definition Reports

You can print three reports that list in various ways the information in your security data set. The security data set contains your security definitions.

The following reports are available for printing:

- Group/User ID Cross-Reference Report

  This report lists the names of the security groups defined in the security data set and the user IDs defined in each group.

- User ID/Group Cross-Reference Report

  This report lists each defined user ID and the name of the group or groups in which it is defined.

- Group Detail Report

  This report lists all the information from the definitions of the security group.

To print these reports, use the provided sample JCL to execute the GSVXSECL batch utility. This utility prints the contents of the security data set. The sample JCL is in the EXECSECL member of the *sysview*.CNM4BSAM data set.

# Group and User ID Cross-Reference Report

The Group and User ID Cross-Reference Report lists the following:

- Names of the security groups defined in the security data set
- User IDs defined in each group

Groups are listed in the order in which they occur in the security data set. This order is the same order used by CA SYSVIEW when determining what group a user belongs to. User IDs are sorted alphabetically in ascending order.

### Example: Sample Group and User ID Cross-Reference Report

```
CA SYSVIEW              Security Data set Report              Page 1
mm/dd/yy 11:22    Security Dataset Name: SYSVIEW.CNM4BSEC
                                           Group/User ID Cross-Reference
Group    User IDs
DEFAULT  None
ADMIN    APM      CRS  DCD   DTC   JFS   KSD   MKC   PBOJKO   RGF   RWM
CRSTES   CRSTEST
DTCTEST  DEMO1
BWWTEST  ASDF     BWW
PBOJKOT  PBOJKXX
RGFTEST  RGFTEST
MKCTEST  CRSTEST
```

The Group/User ID Cross-Reference Report contains the following fields:

**Group**

Identifies the name of a group.

**User IDs**

Indicates the user IDs that belong to the group.

# User ID/Group Cross-Reference Report

The User ID/Group Cross-Reference Report lists the following:

- Each defined user ID
- Name of the group or groups in which it is defined

This report is helpful in identifying users who are in multiple groups.

User IDs are sorted alphabetically in ascending order. User IDs belonging to multiple groups are flagged with a message in the SYSOUT report.

### Example: Sample User ID/Group Cross-Reference Report

```
CA SYSVIEW              Security Dataset Report            Page 1

mm/dd/yy 11:22                  Security Dataset Name: SYSVIEW.CNM4BSEC
                                          User ID/Group Cross-Reference
User ID  Group(s)
APM      ADMIN
ASDF     BWWTEST
BWW      BWWTEST
CRS      ADMIN
CRSTEST  CRSTEST  MKCTEST
DCD      ADMIN
DEMO1    DTCTEST
DTC      ADMIN
JFS      ADMIN
KSD      ADMIN
MKC      ADMIN
PBOJKO   ADMIN
PBOJKXX  PBOJKOT
RGF      ADMIN
RGFTEST  RGFTEST
RWM      ADMIN
```

The User ID/Group Cross-Reference Report contains the following fields:

**Group**

Identifies the name of a group.

**User IDs**

Indicates the user IDs that belong to the group.

# Group Detail Report

The Group Detail Report lists all the information for each selected security group. By default, all defined groups are reported in alphabetically by Group Name in ascending order. The provided control statements let you do the following:

- Select specific groups to print
- Select a group record for a specific user ID

### Example: Sample Group Detail Report

```
CA SYSVIEW                                    Security Data set Report                     Page 1

01/05/yy 11:30:27                 Security Dataset Name:  SYSVIEW.CNM4BSEC

                  Group Name:  GROUP1    Group Owner:   ADMIN      Description:  Group 1

Miscellaneous section:                                          Last Update:
Interfaces ...... ..........All
Default Profile.............DEFAULT                             Date .. 01/05/yy
Timeout Value ... ..........0000 (Minutes)                      Time .. 11:30:01
Update Minimum .. ..........0002 (Seconds)                      Userid  JOE01JOE
Update Duration... .........0000 (Minutes)
Display unauthorized jobs...NO
Display unauthorized help...NO
Debug user ID...............(blank)
Fail command if failed
in any CMDGroup............YES

User ID Section
JOE

Commands Section
Command  Sub-Cmd  Access CmdGroup Command  Sub-Cmd  Access CmdGroup Command  Sub-Cmd  Access CmdGroup
ABENDX            A               ACTIVITY          A               ACTJOB            A
ACTSUM            A               AGENTS            A               ALERTS            A
ALLFILES          A               ALLIST            A               ALLOCAS           A
ALLOCDS           A               APFLIST           A               APFLIST  ADD      A
APFLIST  DELETE   A               APFLIST  VERIFY   A               APPCOUTQ          A
CAIDS             F      CICS     CAILMP            A               CAIRIM            A
CAISMF            A               CALENDAR          A               CALERTS           F      CICS
CAPNOTE           A               CAPOPEN           A               CAPPARMS          A
CARTM             F      CICS     CATALOG           A               CCONFIG           F      CICS
CDBCTL            F      CICS     CDB2CONN          F      CICS     CDB2CSUB          F      CICS
CDB2ENTR          F      CICS     CDIR              F      CICS     CDOCTEMP          F      CICS
CDOMAINS          F      CICS     CDSAS             F      CICS     CDSAX             F      CICS
CDUMPMGT          F      CICS     CDUMPS            F      CICS     CEDA              F      CICS
CICSLOGR          F      CICS     CICSSET           F      CICS     CICSTEST          F      CICS
CJINFO            F      CICS     CJMODEL           F      CICS     CKTCB             F      CICS
CLIFE             F      CICS     CLIST             A               CLISTLIB          A
CLOCKMGR          F      CICS     CMCT              F      CICS     CMODES            F      CICS
CMONITOR          F      CICS     CMQCONN           F      CICS     CMQTASKS          F      CICS
.
.
.
```

```
CA SYSVIEW                                    Security Data set Report                     Page 2

01/05/yy 11:30:27              Security Dataset Name:  SYSVIEW.CNM4BSEC

                  Group Name:  GROUP1    Group Owner:   ADMIN      Description:  Group 1
Command Fields Section

Command Fields Section for ABENDX
Field-Name       Display  Input   Field-Name       Display  Input   Field-Name       Display  Input
TCB                Yes     n/a    Own-TCB            Yes     n/a    Own-RB             Yes     n/a
Type               Yes     n/a    Exit               Yes     n/a    Region             Yes     n/a
Module             Yes     n/a    Offset             Yes     n/a    Parm               Yes     n/a
Token              Yes     n/a    Asynch             Yes     n/a    Purge              Yes     n/a
Term               Yes     n/a    Xctl               Yes     n/a    Mode               Yes     n/a
Key                Yes     n/a    Cancel             Yes     n/a    Record             Yes     n/a
Interruptions      Yes     n/a

Jobnames Section

Refer to GLOBAL  Group

Resources Section

Resource  Resource-Value                               Access  Actions
EMAIL     KARL.PAUL@CA.COM                             FM
EMAIL     SUSAN.MA=                                    A       ALTER
LIBCACHE  CAPLIB                                       A
LIBCACHE  ALL                                          A
MENUKWD   SFASDFS                                      F
MVSVAR    2NDRES                                       A
```

```
CA SYSVIEW                                    Security Data set Report                               Page 3

01/05/06 11:30:27              Security Dataset Name:  SYSVIEW.CNM4BSEC

                  Group Name:  GROUP1    Group Owner:   ADMIN      Description:  Group 1

Resources Section (cont)
Resource  Resource-Value                                  Access  Actions
STGSSID   0041                                            F
STGSSID   0042                                            F
```

```
CA SYSVIEW                                         Security Data set Report                          Page 4

01/05/yy 11:30:27              Security Dataset Name:  SYSVIEW.CNM4BSEC

                                                           Report Index

         Report Name                     Page
Security Group Detail                       1
   Detail Report for GROUP1                 1
SECL001I Security report ended - completion code=00
```

The Group Detail Report contains the following fields:

**Group Name**

Specifies the group name that applies to the report information.

**Group Owner**

Specifies the group name that the user who created this group belongs to.

**Description**

Provides the description given to the group when it was created.

**Group Detail**

Provides the general information defined for the security group on the User Group Detail display.

**Last Update**

Indicates the date and time the group definition was last changed and the user ID of the person who changed it.

**User ID Section**

Specifies a list of the user IDs that belong to the group as defined on the User IDs Section display.

**Commands Section**

Specifies a list of commands that this group can access. This section has the following fields:

**Command**

Specifies the command name.

**Access**

Indicates if the command is authorized (A) or forbidden (F). If an M is displayed in this field, then a message is displayed in the system log when the command is used. An L displayed in this field indicates the command usage is logged in the Audit Log.

**Command Groups Section**

Specifies the commands that are defined to command groups and the command groups are defined to user groups. For example, all CICS commands are defined to the CICS Command Group and only the CICS users can access the CICS Command Group.

**Command Fields Section**

Specifies a list of the commands that this group can access and control. The display for each command has its own section on the report. Only displays that differ from the defaults or the GLOBAL group are listed. This section has the following fields:

**Field-Name**

Indicates the field name on the display.

**Display**

Indicates if the field can be displayed. Values are YES and NO.

**Input**

Indicates if the user can update the field. Values are YES and NO.

### Jobnames Section

Provides a list of jobs (or masks) that have been allowed or failed for this group. These jobs are defined on the Jobnames Section and Detail Jobnames Sections displays. If there are no specifications, the Refer to GLOBAL Group message is displayed. For definitions that apply to this section, see the GLOBAL Security Group on the report.

This section has the following fields:

**Jobname**

Specifies the job name or a partial name (specified with * or =).

**Access**

Specifies if access is allowed (A), allowed and issue a message (AM), forbidden (F), or forbidden and issue a message (FM).

**Function**

Specifies a CA SYSVIEW function.

### Resources Section

A list of the resources allowed for the group as defined on the Resources Section display. If there are no specifications, the GLOBAL group message is displayed. For definitions that apply to this section, see the GLOBAL security group on the report.

This section has the following fields:

**Resource**

Name of the resource.

**Resource-Value**

Value associated with the resource, either an exact resource name or a partial name (specified with * or =).

**Access**

Resource is either allowed (A) or forbidden (F). M indicates that a message is written to the system log when a group member uses the resource.

**Actions**

Valid actions for the resource.

### Report Index

An index of the major divisions in the report.

### Completion Code

The code with which the job ended.

**More infomation:**

How to Produce Reports (see page 38)
GSVXSECL Completion Codes (see page 43)

# How to Produce Reports

This section describes the JCL used to run the job and the control statements available to produce the reports.

## Report Types

CA SYSVIEW provides a sample job in the EXECSECL member of the data set *sysview*.CNM4BSAM. This sample job produces the following reports:

- Group/User ID Cross-Reference Report for all security groups
- User ID/Group Cross-Reference Report for all security groups
- Group Detail Report for the GLOBAL, ADMIN, and DEFAULT security groups

The Group Detail Report includes only the Jobnames Section for each selected group.

## Run Your Reports

To run your reports, use the GSVXSECL batch utility.

### Example: The EXECSECL job

```
//EXECSECL JOB ,,USER=
//STEP0001 EXEC PGM=GSVXSECL,PARM='LINECNT=60,'
//SYSOUT   DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//SYSIN    DD  *
  SECTIONS=JOBS,
  REPORTS=(USRXREF,GRPXREF,GRPDET=(GLOBAL,
                                   ADMIN,
                                   DEFAULT))
```

The JCL used to produce the reports contain the following job statements. In addition to the JCL discussed, you can add your company-specific JCL.

**JOB**

(Required) JOB statement for the job. The CA SYSVIEW user ID used to run the security report program is taken from either of the following:

- USER= value from the JOB statement
- Job name of the job

If USER= is not supplied on the JOB statement, the job name is used. This user ID must be authorized to use the batch interface.

**EXEC**

(Required) Executes the job.

**SYSOUT**

(Required) Prints the input control statements and messages. The required DCB attributes are RECFM=FBA (or FA) and LRECL=133. BLKSIZE is optional and defaults to 133.

**SYSPRINT**

(Required) Defines the output report data set. The required DCB attributes are RECFM=FBA (or FA) and LRECL=133. BLKSIZE is optional and defaults to 133.

**SYSIN**

(Optional) Designates the input control statements. The required DCB attributes are RECFM=FB (or F) and LRECL=80. BLKSIZE is optional and defaults to 80.

**SYSLIB**

(Optional) Specifies the name of the security data set from which to produce the reports. If omitted, the security data set name is obtained from the Systems Configuration Options member.

## LINECNT Control Statement

Specifies the number of lines printed per page of the report. You can specify 20 through 99 lines.

The LINECNT control statement has the following format:

LINECNT=*nn*

***nn***

Defines the number of lines per page.

**Default:** 66 lines per page

## REPORTS Control Statement

The REPORTS control statement specifies which reports are produced for which groups or users.

The REPORTS control statement has the following format:

```
REPORTS=rpt
REPORTS=(rpt,...rpt)
```

**Default Format:**

```
REPORTS=(GRPXREF,USRXREF,GRPDET)
```

The following parameters are available for *rpt*:

**GRPXREF**

Produces a Group/User ID Cross-Reference report.

**USRXREF**

Produces a User ID/Group Cross-Reference report.

**GRPDET**

Produces a Group Detail report of all defined groups.

**GRPDET=*group or* GRPDET=(*group,group*)**

Produces a Group Detail report for *groups* where *group* is a group name in a security file. ADMIN, GLOBAL, and DEFAULT are groups supplied with the default security file.

**USER=*userid***

Produces reports for the group belonging to this user ID. The GLOBAL group is also reported on.

**USER=(*userid,....userid*)**

Produces reports for the groups belonging to these user IDs. The GLOBAL group is also reported on.

## SECTIONS Control Statement

The SECTIONS control statement specifies which Group Detail Report sections to print. Specify no sections to print all available sections. If you specify one section, then only that section prints. Use the ALL parameter as the first parameter to select all sections. Prefix section names with the NO prefix to exclude that section.

The SECTIONS control statement has the following format:

```
SECTIONS=secname
SECTIONS=(secname,...secname)
SECTIONS=(ALL,NOsecname,...NOsecname)
```

The following parameters are available for *secname*:

**ALL**

Specifies all sections. ALL can only be specified as the first parameter and was designed to be used with the NO prefix on the following parameters.

**USERID**

Specifies the User ID section.

**CMDS**

Specifies the Commands section.

**CMDG**

Specifies the Command Groups section.

**CMDFLDS**

Specifies the Command Fields section.

**JOBS**

Specifies the Jobnames section.

**RESOURCE**

Specifies the Resources section.

**EXTERNAL**

Specifies the External Security section.

### Examples: Group Detail Report

- This example produces a Group Detail report with the User ID and Jobnames sections:

  ```
  SECTIONS=(USERID,JOBS)
  ```

- This example produces a Group Detail report with all sections except the CMDFLDS section:

  ```
  SECTIONS=(ALL,NOCMDFLDS)
  ```

## Usage and Processing Rules

The following rules pertain to global usage and processing:

- The GRPDET and USER control statements cannot be used during the same run of the GSVXSECL job.
- Include the control statements in any order you want.
- Separate control statements with a comma. The GSVXSECL job scans for parameters until it encounters a blank delimiter.
- Shorten the control statement name and parameter names to any length you want as long as the result is a unique specification.
- Place an asterisk (*) in column 1 of SYSIN records to ignore the remainder of the record.
- The EXEC statement parameters and the control statements from the SYSIN DD statement, if present, are concatenated.
- Input parameters are printed to the SYSOUT DD statement, if present.

## GSVXSECL Completion Codes

The following are GSVXSECL job completion codes and their explanations. For details, see the SECL001I message in the CA SYSVIEW online help.

**0**

The job completed typically.

**4**

A nonfatal error occurred while the report was running. All the reports you requested might not print.

**8**

A parameter processing error occurred.

**12**

The report job was not set up correctly or CA SYSVIEW was not installed correctly.

**16**

A SYSPRINT DD statement was not present in your job.

**20**

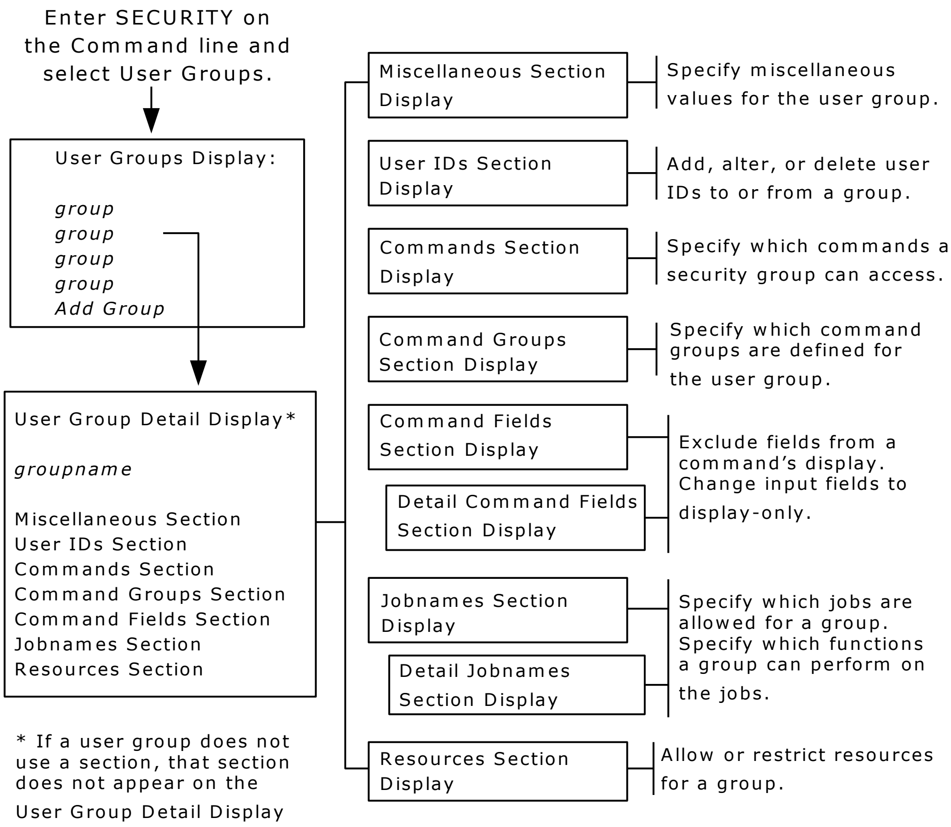
An OPEN for SYSPRINT failed.

# Chapter 4: Security Displays

This section contains the following topics:

# How to Access the Displays

The following illustration shows how to access security displays, and what tasks they perform.


Enter SECURITY on the Command line and select User Groups.
User Groups Display:
group
group
group
group
Add Group
User Group Detail Display*
groupname
Miscellaneous Section
User IDs Section
Commands Section
Command Groups Section
Command Fields Section
Jobnames Section
Resources Section
* If a user group does not use a section, that section does not appear on the User Group Detail Display
Miscellaneous Section Display
Specify miscellaneous values for the user group.
User IDs Section Display
Add, alter, or delete user IDs to or from a group.
Commands Section Display
Specify which commands a security group can access.
Command Groups Section Display
Specify which command groups are defined for the user group.
Command Fields Section Display
Detail Command Fields Section Display
Exclude fields from a command's display. Change input fields to display-only.
Jobnames Section Display
Detail Jobnames Section Display
Specify which jobs are allowed for a group. Specify which functions a group can perform on the jobs.
Resources Section Display
Allow or restrict resources for a group.

# Primary Security Menu

The Primary Security Menu is the first display presented when you enter the Security command.

This menu provides the following two selections:

**User Groups**

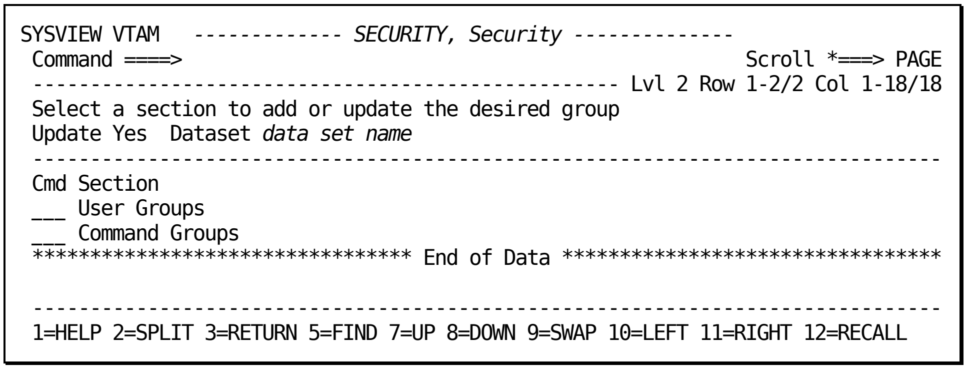
Contains a list all of the user groups you have permission to see.

**Command Groups**

Contains a list all of the command groups.

You can select a group by entering **S** to the left of the group and then pressing Enter.

### Example: Sample Security Menu



```
SYSVIEW VTAM   ------------- SECURITY, Security -------------
 Command ====>                                              Scroll *===> PAGE
 --------------------------------------------------- Lvl 2 Row 1-2/2 Col 1-18/18
 Select a section to add or update the desired group
 Update Yes  Dataset data set name
 -------------------------------------------------------------------------------
 Cmd Section
 ___ User Groups
 ___ Command Groups
 ******************************** End of Data ********************************

 -------------------------------------------------------------------------------
 1=HELP 2=SPLIT 3=RETURN 5=FIND 7=UP 8=DOWN 9=SWAP 10=LEFT 11=RIGHT 12=RECALL
```

# User Groups Display

The User Groups display is presented when you select the User Groups entry from the primary Security Menu. This display lists all the security groups you are allowed to see.

The display also serves as a menu. Select a user group to show the User Group Detail display.

You cannot change the group name of an existing security group. If you are adding the group, specify a new group name using the following guidelines:

- The name cannot be the same as another security group name
- The name cannot contain blanks
- The name cannot be longer than eight characters

The User Groups display has the following fields:

**Cmd**

Enter the following commands in this area:

- **S** to select a security group. Use with AddGroup to add a new security group.
- **D** to delete a security group.

**Group**

Specifies the name of a security group. Group names are shown in the order they were created.

**Note:** AddGroup is a special group name used to add a security group.

**Count**

Specifies the number of users belonging to the security group.

**Upd-Date**

The date the security group was last updated.

**Upd-Time**

Specifies the time the security group was last updated. This field uses the hh:mm:ss format. *hh* is the hour, *mm* is the minute, and *ss* is the second.

**Userid**

Specifies the user ID of the user who last updated the security group.

**Description**

Provides a brief description of the security group.

## Add Subcommand—Copy an Existing User Group

Use the ADD subcommand to copy an existing security group to a new group name.

The ADD subcommand has the following format:

```
ADD ngname,cgname
```

***ngname***

Specifies the name given to the created group.

***cgname***

Specifies the name of the existing group you want to copy.

## Delete User Groups

You can delete user-defined security groups by typing a **D** before each security group you want to delete.

You cannot delete the following security groups:

- GLOBAL
- DEFAULT
- ADMIN
- AddGroup

## Select User Groups

To select more than one user group at a time, enter an **S** before each security group you want to select and press Enter.

When you exit one of the selected user groups, the next one you selected is shown.

## WHERE Subcommand—Verify the User Group

To verify which user group a user will use when logging on to CA SYSVIEW, specify the WHERE subcommand after the command prompt.

This command has the following format:

```
WHERE userid
```

***userid***

Specifies the CA SYSVIEW user ID you want to verify as belonging to a particular user group.

The WHERE subcommand has the following features:

- You can enter the WHERE subcommand from the User Groups display and the User IDs display.
- The results you get when you issue the WHERE command reflect any user IDs coded in the Systems Configuration Options member. The user ID is included in the ADMIN group when coded in the Systems Configuration Options member. and not in any other user group.
- If a nonadministrator user ID is not coded in any user group, it is included in the DEFAULT group.

# User Group Detail Display

The User Group Detail display is presented when you select a user group from the User Groups Display. Use the User Group Detail display to access displays for a selected group.

Access the following displays by entering **S** to the left of the section and then pressing Enter:

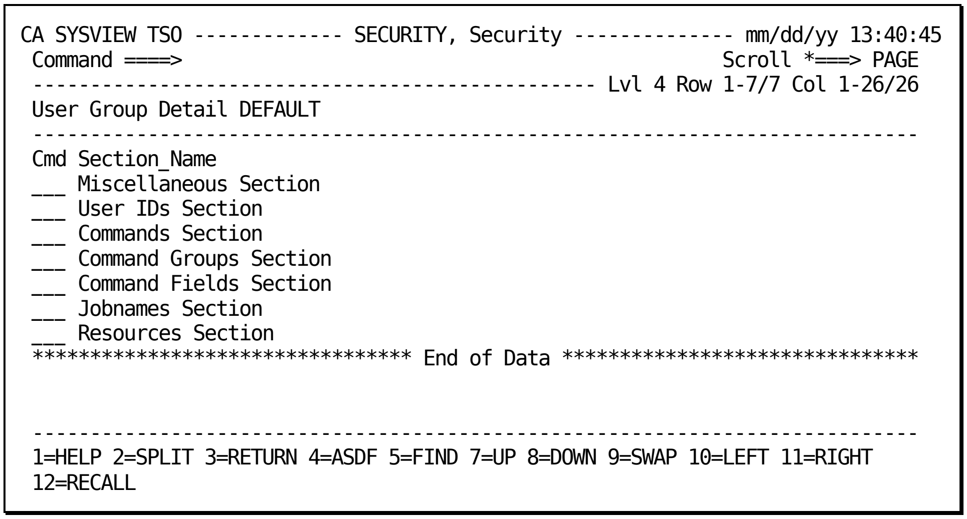
- Miscellaneous Section
- User IDs Section
- Commands Section
- Command Groups Section
- Command Fields Section
- Jobnames Section
- Resources Section

If the user group does not use a section, then that section is not shown. For example, the GLOBAL user group does not use the User IDs Section or Commands section. Therefore, these sections are not displayed when you select that user group.

You can use this display to change the description of a user group.

You can cancel any changes and return to the previous display by issuing the CANCEL command.

### Example: User Group Detail display



```
CA SYSVIEW TSO ------------- SECURITY, Security -------------- mm/dd/yy 13:40:45
 Command ====>                                                 Scroll *===> PAGE
 ------------------------------------------------ Lvl 4 Row 1-7/7 Col 1-26/26
 User Group Detail DEFAULT
 ------------------------------------------------------------------------------
 Cmd Section_Name
 ___ Miscellaneous Section
 ___ User IDs Section
 ___ Commands Section
 ___ Command Groups Section
 ___ Command Fields Section
 ___ Jobnames Section
 ___ Resources Section
 ********************************* End of Data ******************************


 ------------------------------------------------------------------------------
 1=HELP 2=SPLIT 3=RETURN 4=ASDF 5=FIND 7=UP 8=DOWN 9=SWAP 10=LEFT 11=RIGHT
 12=RECALL
```

The User Group Detail display contains the following selectable sections:

**Miscellaneous**

Indicates the Miscellaneous Section display, which lists miscellaneous values for the user group.

**User IDs**

Indicates the User IDs Section display, which lists the user IDs that belong to the user group.

**Commands**

Indicates the Commands Section display, which lists the commands that are allowed or forbidden for the user group.

**Command Groups**

Indicates the Command Groups Section display, which lists the command groups assigned to the user group.

**Command Fields**

Indicates the Command Fields Section display, which lists the fields you can control on a display.

**Jobnames**

Indicates the Jobnames Section display, which lists the jobs that are allowed or forbidden for the user group.

**Resources**

Indicates the Resources Section display, which lists resources that are allowed or forbidden for the user group.

# User Group Miscellaneous Fields

The User Group Miscellaneous fields display information about the user group.

This display has the following fields:

**Description**

Provides a general description of the group. You can update this field.

**Interfaces**

Specifies the interfaces the security group can use to access CA SYSVIEW. The valid interfaces are:

- ALL
- NONE
- TSO
- BATCH
- ISPF
- ETSO (CA ROSCOE/ETSO)
- VTAM
- CICS
- API

**Default Profile**

Specifies the default profile member to use for members in this group. Typically, the DEFAULT profile member is used for users without a profile.

**Note:** For information about creating profiles for other users, see the PROFILE command online help or Changing Profiles in the chapter "Defining Security" in this guide.

**Timeout Value**

Specifies the amount of time a CICS or VTAM session can be idle before CA SYSVIEW terminates the session. The value is in minutes. A value of 0 (zero) specifies there is no time limit.

For example, suppose the timeout value is 5. If a user in this group logs on and does not enter any input for 5 minutes, CA SYSVIEW terminates the session.

The DEAULT profile is distributed with a timeout value of 240 minutes.

**Update Minimum**

Specifies the minimum value a user in the group can specify as the update interval on the UPDATE command. Values can be from 2 to 9999 seconds.

**Update Duration**

Specifies the maximum amount of time specified in minutes that a user in the group could stay in update mode. Values can be from 0 to 9999 minutes. Values of 0 and 9999 mean that a user can stay in update mode indefinitely. Use this field to set an update mode limit on users.

**Display Unauthorized Jobs**

Controls whether unauthorized jobs are included in the list of jobs for a display. Enter YES to include unauthorized jobs or NO to exclude them. When you specify YES, security checks made when building a display for a command are bypassed. Using the SAF security exit can significantly reduce the amount of processing required to build the display. If one of the unauthorized jobs is selected from a display, a security check is made, and access is denied.

**Display Unauthorized Help**

Controls whether online help information for unauthorized commands can be displayed. Valid values are YES and NO. YES displays unauthorized online help and NO does not display the online help information.

**Debug Userid**

Used for debugging. When the user ID for a member in this group is entered in this field, tracing information is written to a SYSOUT file within the address space that invoked CA SYSVIEW. For job name and resource validation calls, the information shows which rule failed an access attempt. Only failed access attempts are traced. Remember to clear this field after debugging the problem.

# User IDs Section Display

The User IDs Section display lists the user IDs that belong to the security group. Use the display to add user IDs to the group, alter user IDs in the group, and delete user IDs from the group. The user IDs are sorted in ascending order.

The following field is on the User IDs Section display:

**User IDs**

Specifies a full user ID or a partial user ID. Place an = (equal sign) after a user ID to specify a partial user ID. Or, use an asterisk (*) to match any single character. Any user ID that begins with the characters before the = belongs to the group. = by itself is not permitted.

### Example: Specify User IDs

- XYZ= specifies user IDs that start with *XYZ*
- ******CD specifies user IDs that are eight characters long ending in CD. The first six characters of the user ID can be any characters.

# Commands Section Display

The Commands Section display lists the available commands. You can use the display to specify which commands the user group can access. The action for the commands contained in command groups assigned to the user group cannot be changed. The actions for these commands are based on the action assigned to the command group.

The fields on the Commands Section display are as follows:

**Command**

Specifies the name of the commands available to the user group.

**Sub-Cmd**

Specifies the name of a subcommand for the command in the Command field.

**Access**

Designates the definitions for the command or subcommand. The following can appear:

**A**

Allows the use of the command or subcommand.

**F**

Forbids the use of the command or subcommand.

**L**

Logs the use of the command in the Audit Log.

**M**

Displays a message on the system log whenever a member of the group enters the command. If defined for the z/OS command, and a z/OS REPLY command is issued, the reply is suppressed from the message. This suppression preserves the integrity of confidential replies. Use with the A or F definition.

**Alter**

Specifies whether the command is considered to be a command that can alter or update the system.

**CmdGroup**

Specifies the name of the command group that contains the command and is assigned to the user group. If the command is not in a command group, this field is blank. The Access field is set based on the access assigned to the command group for the user group. The Access field cannot be changed for commands in a command group assigned to the user group.

**Description**

Provides a description of the command.

# Command Groups Section Display

The Command Groups Section display lists the CA SYSVIEW command groups assigned to the user group. Use this display to assign command groups to the user group.

The Command Groups Section display has the following fields:

**Group**

Specifies the name of the command group.

**Access**

Specifies whether the command group is allowed or forbidden:

**A**

Allows the use of the commands or subcommands included in the command group.

**F**

Forbids the use of the commands or subcommands included in the command group.

**Description**

Describes the command group.

# Command Fields Section Display

The Command Fields Section display lists the commands whose displays you can control. This display also serves as a menu. Select an option (a command) to show a Command Fields Section Detail display. All product commands are displayed whether they are currently allowed or forbidden.

The Command Fields Section display has the following fields:

**Cmd**

Displays the area in which you select a command. Enter **S** to select a command. The Detail Command Fields Section display is shown for the command.

**Command-Name**

Displays the name of the command.

**Defined**

Indicates whether the command field section has been altered. YES is displayed if an alteration has occurred.

**Description**

Describes the command group.

# Detail Command Fields Section Display

The Detail Command Fields Section display lists the fields that are displayed when you issue the selected command. With this display, you can exclude fields from the display, and you can change input fields to display-only fields.

For example, suppose a command creates a display that has four possible fields, one is an input field. You can specify that all four fields be displayed, or that only two of the fields be displayed. You can also change an input field so that it is display-only.

The Detail Command Fields Section display has the following fields:

**Field-Name**

Specifies the name of the fields that can be displayed after issuing the selected command.

**Display**

Indicates whether the field is displayed. The values are YES and NO.

**Input**

Indicates whether the input field accepts input. You can only specify Input for fields that are designated as input fields. The values are YES and NO.

# Jobnames Section Display

The Jobnames Section display lists the jobs the security group can access or for which definitions apply.

The Jobnames Section display has the following fields:

**Cmd**

Displays the area where you enter a line command to perform actions on a job name.

The following are valid values:

**S**

Selects a job name. The Detail Jobnames Section display is shown for the job name. AddJob adds a new job name.

**D**

Deletes a job name.

**Jobname**

Specifies the name of a job. The job name can be an exact job name, or can use special qualifiers or masking characters. AddJob is a special job name used to add a job to the list.

Specify an exact job name, or use one of the following:

**=**

Indicates a partial job name. Matches any number of characters at the end of a job name. Used alone, specifies all jobs. For example, *XYZ=* specifies jobs that start with *XYZ*.

*****

Indicates a partial job name. Matches one character. For example, *******N2* specifies jobs that are eight characters long ending in *N2*. The first six characters of the job name can be any characters.

**USERID**

Indicates a job name that matches the user ID. This rule also applies when the security user ID field for the job matches the user ID of the user.

**USERID:*n***

Indicates a job name that starts with a portion of the user ID. This rule also applies when the security user ID field for the job matches a portion of the user ID of the user.

***n***

Specifies the number of characters to compare.

**USERID=**

Indicates a job name that starts with the user ID. This rule also applies when the security user ID field for the job starts with the user ID or the user.

**NOTIFY**

Indicates the NOTIFY field on the JOB statement matches the user ID.

**NOTIFY:*n***

Indicates the NOTIFY field on the JOB statement starts with the user ID.

***n***

Specifies the number of characters to compare.

**NOTIFY=**

Indicates the NOTIFY field on the JOB statement must start with the user ID.

**Additional Information**

- If a job matches the USERID rule and the security user ID for the job matches the user ID of the user, CA SYSVIEW does not validate the following:
  - Job class
  - Output class
  - Destination

  If the user tries to change the job class, output class, or destination, the new value is searched for authorization.

- If a job matches the NOTIFY rule (that is, the NOTIFY value on the JOB statement for the job matches the user ID of the user), CA SYSVIEW does not validate the job class, output class, and destination for the job.

**Access**

Specifies the display action for the job name.

The following are valid values:

**A**

The job is allowed for the group.

**F**

The job is forbidden for the group.

## Add Subcommand—Add a New Job Name Rule

Use the ADD subcommand to add a new job name rule by copying an existing job name rule.

The ADD subcommand has the following format:

```
ADD newjobname,currentjobname,currentjobgroup
```

**newjobname**

Specifies the name of the new job name rule.

**currentjobname**

Specifies the name of an existing job name rule.

**currentjobgroup**

(Optional) Specifies the user group name for the existing job rule.

**Default:** The current group

## Job Name Restrictions Affect On Displays

If a job name is restricted for a group, it does not appear in the following list of jobs. You can override this restriction by specifying YES on the display unauthorized jobs field on the User Group Detail display.

- APPC Output Queue
- Exception Log Summary
- Held Output Queue
- Initiators
- Input Queue
- Internal Readers
- Job Queue
- Job Summary
- NJE and RJE Lines
- Output Queue
- Printer
- Punch
- Readers
- System Activity
- WTOR Replies Required

## How Job Names Are Validated

You validate job names on a best-fit basis. For example, suppose a job name section contains the following entries:

```
  Jobname Access
_ A=      F
_ ABC=    A
```

If the job name ABCD is validated, the ABC= rule would apply because it has more characters that match. All job names in the job name section are verified when a job name is validated. Therefore, the order in which the job names are entered is not important.

# Detail Jobnames Section Display

The Detail Jobnames Section display lists certain functions that you can perform on jobs that appear on CA SYSVIEW displays. You can restrict the use of any of this information. For example, you can allow users in a security group to alter input attributes for a job, but not output attributes.

The Detail Jobnames Section display has the following fields:

**Description**

Lists the actions that can be taken against a job.

**Display**

Specifies whether the job is displayed at all. If this field is F, no other fields are verified. The message designator (M) is not valid for this field.

**Alter input**

Specifies whether the user can alter input attributes for the job. The following displays are affected:

- Job Summary
- Input Queue
- System Activity
- Job Queue

**Alter output**

Specifies whether the user can alter output attributes for the job. The following displays are affected:

- Held Output
- Job Queue
- Output File
- Output Queue

**Alter storage**

Specifies whether the user can alter storage for the job.

**Cancel**

Specifies whether the user can cancel the job. The following displays are affected:

- System Activity
- Initiator
- Job Summary
- NJE and RJE Lines

- Printer
- Punch
- Task
- Offloaders
- Internal Readers
- Readers
- Address Space List

**Copy**

Specifies whether the user can copy the output of the job.

**Datasets allocated**

Specifies whether the user can use the DSALLOC command for this job.

**Delete**

Specifies whether the user can delete the output of the job.

**Force**

Specifies whether the user can force a job. The following displays are affected:

- System activity
- Address Space List

**Hold**

Specifies whether the user can hold the job.

**Kill**

Specifies whether the user can kill the job.

**List output files**

Specifies whether the user can list the output files for the job. The following displays are affected:

- Output Descriptors
- Output Files
- Step Summary

**Make it nonswappable**

Specifies whether the user can use the nonswap (NS) line command for the job. The following displays are affected:

- System Activity
- Initiator
- Address Space List

**Make it swappable**

Specifies whether the user can use the swap (SW) line command for the job. The following displays are affected:

- System Activity
- Initiator
- Address Space List

**Modules loaded**

Specifies whether the user can use the following commands for the job:

- JPA
- LISTLOAD
- MODULES

**Private region info**

Specifies whether the user can use the following commands for the job:

- ABENDX
- ATTNX
- CELLPOOL
- DUMP
- FRAMES
- PAGES
- PLOT
- PLOTLIST
- PRIVATE
- SEGMENTS
- SYMBOLS
- TASK
- TIMERS

**Quiesce**

Specifies whether the user can quiesce the job.

**Release**

Specifies whether the user can release a job. If the job is on the input queue, the user must also have alter input authority to release the job.

**Reply to WTORs**

Specifies whether the user can reply to WTORs issued by the job. This field applies only to the WTOR command.

**Restart**

Specifies whether the user can restart a job. The following displays are affected:

- Initiator
- NJE and RJE Lines
- Printer
- Punch
- System Activity

**Resume**

Specifies whether the user can resume the job.

**Select output**

Specifies whether the user can display the output of the job. The following displays are affected:

- Output
- Step Summary

**DDname**

Specifies the DD names of the output files that are allowed or restricted. Use the Name field to enter the DDname. Use = to specify a partial DDname. For example, to specify all DD names that start with the character $, enter **$=**.

If no DD names are specified, all DD names are allowed. Once one DDname is specified, all other unspecified DD names are restricted. To allow all other DD names again, make a new entry of = in the Name field and A in the Access field.

**Access**

Lists the access to the action against the job name. The following can appear:

**A**

Allows use of the action against the job.

**F**

Forbids the use of the action against the job.

**M**

Displays a message on the system log whenever a member of the group uses the action against the job. This access is used with the A or F definition.

**Name**

Lists the DD names that are allowed or restricted. This field is only valid for the DDname action.

# Resources Section Display

The Resources Section display lists all resources that are allowed or restricted for the security group. To select a section, type **S** in the input field next to the desired resource and press Enter.

The Resources Section display has the following fields:

**Cmd**

Displays the command field area. Select a resource section by entering **S**.

**Resource**

Specifies the resource name that is allowed or restricted. For the list of resource types, see the following section.

**Description**

Provides a brief description of the resource section.

# Resources Section Detail Display

The Resources Section Detail Display allows resources to be controlled on displays. You can specify line commands and alter authority.

The following values are available:

**Resource-Value**

Specifies the value for a resource. To add a new resource value, use the newresource line. To delete a resource value, erase it or space over it and press enter.

For more information, see the Resource-Value Field Values (see page 82) section in this chapter.

**Access**

Specifies the action to take for the resource value. Valid values are:

**A**

Allows the use of the resource.

**F**

Forbids the use of the resource.

**M**

Displays a message on the system log when a group member uses the resource. Use this value with the A or F definition.

**Actions**

Specifies authorized actions for the resource. Enter ALL as the first action to include all valid actions. Enter NONE as the first action to clear the actions.

**Note:** For more information, see the Actions Field Description section that follows.

## Actions Field Description

The Actions field indicates which actions are valid for the resource rule. When entering actions in the Actions field, enter only enough characters to identify uniquely the action. For instance, CL can be entered for CLEAR but CLO must be entered for CLOSE. ALL can be entered as the first value to include all valid actions for the resource. NONE can be entered as the first value to clear all of the actions.

The actions are as follows:

**ACTIVATE**

Activates the resource

**ADD**

Adds the resource

**ADVANCE**

Advances a journal

**ALLOCATE**

Allocates the resource

**ALTER**

Alters the resource

**BACK**

Backspaces the output

**CANCEL**

Cancels a resource

**CHECKPT**

Checkpoints the resource

**CLEAR**

Clears the resource

**CLOSE**

Closes the resource

**CLSDEST**

Closes the destination

**DEACT**

Deactivates the resource

**DEFINE**

Defines a resource

**DELETE**

Deletes the resource

**DEQUEUE**

Dequeues the resource

**DISABLE**

Disables the resource

**DRAIN**

Drains the resource

**DUMP**

Dumps the resource

**ENABLE**

Enables the resource

**EXCLUSIV**

Restricts use of the resource

**FORCE**

Forces the resource

**FORMAT**

Formats a spool volume

**FORWARD**

Advances the output

**FREE**

Frees the resource

**HALT**

Halts the resource

**HOLD**

Holds the resource

**IDLE**

Makes the resource idle.

**IMSDBD**

Uses a line command that issues an IMS DBD command

**IMSDBR**

Uses a line command that issues an IMS DBR command

**IMSERE**

Uses a line command that issues an IMS ERE command

**IMSNRE**

Uses a line command that issues an IMS NRE command

**INIT**

Initializes the resource

**INTERRUP**

Interrupts the resource

**IOVF**

Uses the IOVF line command

**KILL**

Terminates a resource immediately

**LOCK**

Locks the resource

**MASTER**

Assigns master status to the resource

**MOUNT**

Mounts the resource

**NEW**

Loads a new copy of the resource

**OPEN**

Opens the resource

**PURGE**

Purges the resource

**QUIESCE**

Quiesces the resource.

**RELEASE**

Releases the resource

**REQUEUE**

Requeues the resource

**REPEAT**

Repeats the resource

**RESTART**

Stops and restarts the resource

**RESUME**

Resumes the resource

**SCFW**

Initiates a SETCACHE CACHEFASTWRITE against the resource

**SDEV**

Initiates a SETCACHE DEVICE against the resource

**SDFW**

Initiates a SETCACHE DASDFASTWRITE against the resource

**SEND**

Sends the resource

**SHUTDOWN**

Shuts down the resource

**SNVS**

Initiates a SETCACHE NVS against the resource

**SSUB**

Initiates a SETCACHE SUBSYSTEM against the resource

**START**

Starts the resource

**STOP**

Stops the resource

**SWITCH**

Switches a journal or IMS region

**TERM**

Terminates data collection

**TRACEOFF**

Turns off a trace for the resource

**TRACEON**

Turns on a trace for the resource

**UNLOAD**

Unloads the resource

**UNLOCK**

Unlocks the resource

**VARYOFF**

Varies the resource offline

**VARYON**

Varies the resource online

**XSCON**

Connects cross system to the resource

## Valid Actions by Resource

The following provides a list of resources and the valid actions you can perform for each resource.

**CATALOG**

ALTER, ALLOCATE, CLOSE, FREE, OPEN

**CICSAID**

ALTER, PURGE

**CICSDCT**

ALTER, CLOSE, DISABLE, ENABLE, OPEN

**CICSFILE**

ALTER, CLOSE, DISABLE, ENABLE, OPEN

**CICSGRPS**

ALTER, ADD

**CICSICD**

ALTER, PURGE

**CICSJOBN**

ALTER

**CICSJRNL**

ALTER

**CICSPROG**

ALTER, DISABLE, ENABLE, NEW

**CICSTCLS**

ALTER

**CICSTERM**

ALTER, CANCEL, FORCE, KILL, PURGE

**CICSTOPT**

ALTER, ADD, DELETE

**CICSTRAN**

ALTER, CANCEL, DISABLE, ENABLE, FORCE, KILL, PURGE

**CICSTSQ**

ALTER, DELETE

**CICSVAR**

ALTER, ADD, DELETE

**CONSOLE**

ALTER, ACTIVATE, DEACT, DELETE, MASTER, RELEASE, VARYOFF, VARYON

**CPU**

ALTER, VARYOFF, VARYON

**DEST**

ALTER

**DEVICE**

ALTER, BACK, FORWARD, HALT, INTERRUP, REPEAT, RESTART, START, STOP

**DUMPDS**

ALTER, ADD, CLEAR, DELETE

**EMAIL**

SEND

**GROUPS**

ALTER, ADD, DELETE

**IMSCLASS**

ALTER, START, STOP

**IMSCMD**

ALTER

**IMSDBASE**

ALTER, DELETE, IMSDBD, IMSDBR, LOCK, START, STOP, UNLOCK

**IMSID**

ALTER, SHUTDOWN, START, STOP, SWITCH

**IMSJOBN**

ALTER, CANCEL, CHECKPT, IMSERE, IMSNRE, PURGE, RESTART, START, STOP, SHUTDOWN, SWITCH, UNLOCK

**IMSLINE**

ALTER, IDLE, PURGE, START, STOP, TRACEOFF, TRACEON

**IMSLTERM**

ALTER, DEQUEUE, LOCK, PURGE, START, STOP, TRACEOFF, TRACEON, UNLOCK

**IMSNODE**

ALTER, ACTIVATE, CLSDEST, DEQUEUE, EXCLUSIV, IDLE, QUIESCE, RESTART, START, STOP, TRACEOFF, TRACEON

**IMSPROG**

ALTER, DELETE, LOCK, START, STOP, TRACEOFF, TRACEON, UNLOCK

**IMSPSB**

ALTER, TRACEOFF, TRACEON

**IMSTMEM**

START, STOP, TRACEOFF, TRACEON

**IMSTPIPE**

START, STOP, TRACEOFF, TRACEON

**IMSTRACE**

ALTER, TRACEOFF, TRACEON

**IMSTRAN**

ALTER, DUMP, LOCK, PURGE, START, STOP, TRACEOFF, TRACEON, UNLOCK

**IMSUSER**

ALTER, DEQUEUE, START, STOP

**IMSVAR**

ALTER, ADD, DELETE

**INIT**

ALTER, HALT, STOP, START

**INVOKEKW**

No valid commands

**JOBCLASS**

ALTER, HOLD, RELEASE

**LGSTREAM**

ALTER

**LIBCACHE**

ALTER

**MENUKWD**

No valid commands

**MQSVAR**

ALTER, ADD, DELETE

**MVSCMD**

No valid commands

**MVSVAR**

ALTER, ADD, DELETE

**NODE**

ALTER, START

**OUTCLASS**

ALTER

**PAGEDS**

ALTER, ADD, DELETE, DRAIN

**SCHEDULE**

ALTER, ADD, DELETE, DISABLE, ENABLE

**SETKWD**

No valid commands

**SMFDATA**

ALTER

**SMFDS**

ALTER, DUMP, SWITCH

**SPOOL**

ALTER, CANCEL, FORMAT, HALT, START, STOP

**STGSSID**

ALTER, SCFW, SDEV, SDFW, SNVS, SSUB

**SYSTEM**

ALTER, RESTART

**TCPVAR**

ALTER, ADD, DELETE

**UNIT**

ALTER, FREE, MOUNT, UNLOAD, VARYOFF, VARYON

**VOLSER**

ALTER, FREE, MOUNT, SDEV, SDFW, UNLOAD, VARYOFF

**WMAPLENV**

ALTER

**WMSCHENV**

ALTER

**XSYSDEST**

ALTER, XSCON.

**XSYSORIG**

ALTER, XSCON

**ZAP**

ALTER

## Resource Calls by Command

The following provides a list of commands and the resources they call.

**ACTIVITY**

Calls for the JOBCLASS resource.

**ALLOCAS**

Calls for the UNIT and VOLSER resources.

**ALLOCDS**

Calls for the UNIT and VOLSER resources.

**APPCOUTQ**

Calls for the DEST, JOBCLASS, and OUTCLASS resources.

**CACHECTL**

Calls for the STGSSID resource.

**CACHEDEV**

Calls for the STGSSID and VOLSER resources.

**CAIDS**

Calls for the CICSAID and CICSJOBN resources.

**CALERTS**

Calls for the CICSJOBN resource.

**CARTM**

Calls for the CICSJOBN and CICSTRAN resources.

**CATALOG**

Calls for the CATALOG resource.

**CDUMPMGT**

Calls for the CICSJOBN resource.

**CENQPOOL**

Calls for the CICSJOBN resource.

**CENQUEUE**

Calls for the CICSJOBN resource.

**CFILES**

Calls for the CICSFILE and CICSJOBN resources.

**CGROUPS**

Calls for the CICSGRPS and CICSJOBN resources.

**CICE**

Calls for the CICSICE and CICSJOBN resources.

**CICSLIST**

Calls for the CICSJOBN resource.

**CJINFO**

Calls for the CICSJOBN and CICSJRNL resources.

**CJMODEL**

Calls for the CICSJOBN and CICSJRNL resources.

**CONSOLE**

Calls for the CONSOLE resource.

**CPROGRAM**

Calls for the CICSJOBN and CICSPROG resources.

**CPU**

Calls for the CPU resource.

**CREMOTE**

Calls for the CICSJOBN and CICSTERM resources.

**CSFTASKS**

Calls for the CICSJOBN and CICSTRAN resources.

**CSTATES**

Calls for the CICSJOBN and CICSVAR resources.

**CSTATUS**

Calls for the CICSJOBN and CICSVAR resources.

**CSYSDATA**

Calls for the CICSJOBN resource.

**CTASKENT**

Calls for the CICSJOBN and CICSTRAN resources.

**CTASKS**

Calls for the CICSJOBN and CICSTRAN resources.

**CTCLASS**

Calls for the CICSJOBN and CICSTCLS resources.

**CTDATA**

Calls for the CICSDCT and CICSJOBN resources.

**CTERMS**

Calls for the CICSJOBN and CICSTERM resources.

**CTHRESH**

Calls for the CICSJOBN and CICSVAR resources.

**CTRANLOG**

Calls for the CICSJOBN and CICSTRAN resources.

**CTRANOPT**

Calls for the CICSJOBN and CICSTOPT resources.

**CTRANS**

Calls for the CICSJOBN and CICSTRAN resources.

**CTRANSUM**

Calls for the CICSJOBN and CICSTRAN resources.

**CTSMODEL**

Calls for the CICSJOBN resource.

**CTSPOOLS**

Calls for the CICSJOBN resource.

**CTSQUEUE**

Calls for the CICSJOBN and CICSTSQ resources.

**CUOW**

Calls for the CICSJOBN and CICSTRAN resources.

**DASD**

Calls for the UNIT and VOLSER resources.

**DESTID**

Calls for the DEST resource.

**DEVPATH**

Calls for the UNIT and VOLSER resources.

**DEVSERV**

Calls for the UNIT and VOLSER resources.

**DUMPDS**

Calls for the DUMPDS resource.

**EXTENTS**

Calls for the UNIT and VOLSER resources.

**GROUPS**

Calls for the GROUPS resource.

**IMS**

Calls for the IMSID resource.

**IMSCLASS**

Calls for the IMSCLASS and IMSID resources.

**IMSCMD**

Calls for the IMSCMD and IMSID resources.

**IMSDBASE**

Calls for the IMSDBASE and IMSID resources.

**IMSLINES**

Calls for the IMSLINE and IMSID resources.

**IMSLIST**

Calls for the IMSID and IMSJOBN resources.

**IMSLTERM**

Calls for the IMSID, IMSLTERM, and IMSNODE resources.

**IMSMON**

Calls for the IMSVAR resource.

**IMSNODES**

Calls for the IMSID and IMSNODE resources.

**IMSOSAM**

Calls for the IMSID and IMSTRACE resources.

**IMSOTMA**

Calls for the IMSID, IMSTPIPE, and IMSTMEM resources.

**IMSPI**

Calls for the IMSID and IMSTRACE resources.

**IMSPROGS**

Calls for the IMSID and IMSPROG resources.

**IMSPSBS**

Calls for the IMSID and IMSPSB resources.

**IMSREGNS**

Calls for the IMSID, IMSJOBN, and IMSTRAN resources.

**IMSTATE**

Calls for the IMSVAR resource.

**IMSTEXIT**

Calls for the IMSID and IMSTRACE resources.

**IMSTHRSH**

Calls for the IMSVAR resource.

**IMSTRANS**

Calls for the IMSID and IMSTRAN resources.

**IMSTTABL**

Calls for the IMSID and IMSTRACE resources.

**IMSUSERS**

Calls for the IMSID and IMSUSER resources.

**INTRDR**

Calls for the DEVICE and JOBCLASS resources.

**INVOKE**

Calls the INVOKEKW resource.

**JCOPYOUT**

Calls for the DEST and OUTCLASS resources.

**JHELDQUE**

Calls for the DEST, JOBCLASS, and OUTCLASS resources.

**JINIT**

Calls for the INIT and JOBCLASS resources.

**JINPRTY**

Calls for the JOBCLASS resource.

**JJOBQUE**

Calls for the DEST, JOBCLASS, and OUTCLASS resources.

**JOBCLASS**

Calls for the JOBCLASS resource.

**JOBSUM**

Calls for the DEST and JOBCLASS resources.

**JOUTQUE**

Calls for the DEST, JOBCLASS, and OUTCLASS resources.

**JPATHS**

Calls for the NODE resource.

**JPLEX**

Calls for the SYSTEM resource.

**JSPOOLS**

Calls for the SPOOL resource.

**LGDRO**

Calls for the LGSTREAM resource.

**LGEMPTY**

Calls for the LGSTREAM resource.

**LIBCACHE**

Calls for the LIBCACHE resource.

**LINES**

Calls for the DEVICE, JOBCLASS, and OUTCLASS resources.

**LISTCONS**

Calls for the CONSOLE resource.

**LISTFILE**

Calls for the DEST, JOBCLASS, and OUTCLASS resources.

**LISTINP**

Calls for the DEST, and JOBCLASS resources.

**MONITOR**

Calls for the MVSVAR resource.

**MQMON**

Calls for the MQSVAR resource.

**MQSTATES**

Calls for the MQSVAR resource.

**MQTHRESH**

Calls for the MQSVAR resource.

**MVS**

Calls the MVSCMD resource.

**NODES**

Calls for the NODE resource.

**OFFLOAD**

Calls for the DEST, DEVICE, JOBCLASS, and OUTCLASS resources.

**OUTCLASS**

Calls for the OUTCLASS resource.

**OUTDES**

Calls for the JOBCLASS and OUTCLASS resources.

**PAGEDS**

Calls for the PAGEDS resource.

**PRINTER**

Calls for the DEST, DEVICE, JOBCLASS, and OUTCLASS resources.

**PRISM**

Calls for the CPU resource.

**PROFILE**

Calls for the DEST resource.

**PUNCH**

Calls for the DEST, DEVICE, JOBCLASS, and OUTCLASS resources.

**READER**

Calls for the DEVICE, DEST, JOBCLASS, and OUTCLASS resources.

**SCHEDULE**

Calls for the SCHEDULE resource.

**SENDMAIL**

Calls for the EMAIL resource.

**SET**

Calls for the DEST, SETKWD, and OUTCLASS resources.

**SMF**

Calls for the SMFDS resource.

**SMFDATA**

Calls for the SMFDATA resource.

**SPACE**

Calls for the UNIT and VOLSER resources.

**STATES**

Calls for the MVSVAR resource.

**SUBCHAN**

Calls for the UNIT and VOLSER resources.

**TAPE**

Calls for the UNIT resource.

**TCPMON**

Calls for the TCPVAR resource.

**TCPSTATE**

Calls the TCPVAR resource.

**TCPTHRSH**

Calls for the TCPVAR resource.

**THRESH**

Calls for the MVSVAR resource.

**UNIT**

Calls for the UNIT and VOLSER resources.

**VOLSER**

Calls for the UNIT and VOLSER resources.

**VTAM**

Calls the MVSCMD resource.

**WMAPPENV**

Calls for the WMAPLENV resource.

**WMSCHENV**

Calls for the WMSCHENV resource.

**XLOG**

Calls for the CICSJOBN resource.

**XSCONN**

Calls for the XSYSDEST and XSYSORIG resources.

**ZAP**

Calls for the ZAP resource.

## Resource-Value Field Values

To specify a resource value, overtype the newresource field on the first line. Enter either an exact resource value or a partial value using an asterisk (*) or an equal sign (=). The asterisk matches one character. For example, to specify all resources that have ABC as their fourth, fifth, and sixth characters, enter ****ABC*=. An equal sign (=) matches any number of characters at the end of the value. For example, to specify all resources with values that start with the characters XYZ, enter XYZ=. Use = alone to specify all resources.

**More information:**

Resource-Value Field Values for the CICS Option (see page 85)
Resource-Value Field Values for the IMS Option (see page 89)

## Resource-Value Field Values for Basic Resource Types

The basic resources are either allowed or restricted. No actions can be specified for the resource.

The following lists the basic resources:

**INVOKEKW**

Specifies the allowed or restricted INVOKE command keywords. Specify an exact keyword or use an equal sign (=) at the end to specify a partial keyword.

The INVOKE command calls for the INVOKEKW resource to validate the external application that the user is trying to invoke. If the resource is not allowed, the user cannot invoke the application.

**MENUKWD**

Specifies the allowed or restricted menu panel names. Specify an exact keyword or use an equal sign (=) at the end of the value to specify a partial keyword.

The MENU member in the *sysview*.CNM4BPRM data set associates the name of a menu with a member name in the *sysview*.CNM4BPNL data set. For more details, see the MENU member in the data set *sysview*.CNM4BPRM.

If the menu panel is not authorized, it is not displayed as a selectable item on the Primary Option Menu.

**MVSCMD**

Specifies the allowed or restricted z/OS or JES commands. You can either specify an exact command or specify a partial command using * or =. For example, to specify all JES2 display commands, type $D=. To specify all commands, use = by itself. The z/OS and VTAM commands use this resource.

**Command Validation**

- For JES commands, all spaces are removed from the command before they are validated. For example, if a user enters the command $P JES2, then the command is changed to $PJES2 before validation. The space between the P and the J is removed.
- For MVS commands, multiple consecutive spaces are changed to one space before validation.

**SETKWD**

Specifies the allowed or restricted SET command keywords. Specify an exact keyword or use an equal sign (=) on the end to specify a partial keyword.

The SET command calls for the SETKWD resource.

The PROFILE command also calls for the SETKWD resource. Access to profile sections is controlled by validating access to the following SETKWD resources:

**PROFGENPFKS**

Displays the general PF key section

**PROFGENMSCS**

Displays the general miscellaneous section

**PROFCMDSYNS**

Displays the command synonym section

**PROFCMDPFKS**

Displays the command PF key section

**PROFCMDMSCS**

Displays the command miscellaneous section

**PROFCMDFMTS**

Displays the command format section

If the resource is not allowed, then the section is not displayed on the profile display. Individual fields within a profile section can also be controlled with the SETKWD resource. If the corresponding SETKWD resource for a field is restricted, then the field is displayed on the profile display, but it cannot be changed.

The PROFILE command also calls for the following SETKWD resources to control profile formats:

**FORMATCREATE**

Creates a format

**FORMATMODIFY**

Modifies an existing format

**FORMATDELETE**

Deletes a format

If the FORMATCREATE resource is not authorized, then formats cannot be created. However, the existing formats can be displayed. If the FORMATMODIFY resource is not authorized, then existing formats can be displayed but not modified. If the FORMATDELETE resource is not authorized, then formats cannot be deleted.

**XSDATA**

Specifies the allowed or restricted cross-system data commands. The complete list of cross-system eligible commands is shown on the XSCMDS display. Specify the exact command name (no synonyms or abbreviated command names). Masking is allowed in the command name. This resource call is only applicable if:

- The cross-system command has XSDATA set to YES.
- The command specified the XSDATA keyword when it was issued.

## Resource-Value Field Values for the CICS Option

The following are the possible values for the Resource-Value field of the CA SYSVIEW Option for CICS:

**CICSAID**

Specifies the CICS automatic initiate descriptor IDs.

Use this section to control the authorized descriptor IDs displayed with the following command, which calls for the CICSAID resource:

**CAIDS**-Calls for a descriptors ID and for the PUR line command.

**CICSDCT**

Specifies the CICS transient data queue names.

Use this section to control transient data queues displayed with the following command, which calls for the CICSDCT resource:

**CTDATA**-Calls for the queue name and for the CLOSE, DISABLE, ENABLE, and OPEN line commands.

**CICSFILE**

Specifies the CICS file names.

Use this section to control the authorized file names displayed with the CFILES command. The following command, which calls for the CICSFILE resource:

**CFILES**-Calls for the file name and for the CLOSE, DISABLE, ENABLE, and OPEN line commands.

**CICSGRPS**

Specifies the CICS group names.

Use this section to control the authorized group names displayed with the following command, which calls for the CICSGRPS resource:

**CGROUPS**-Calls for the group name, for alter access when group attributes can be changed, and for alter access when the ADD line command is used.

**CICSICE**

Specifies the CICS interval control element IDs.

Use this section to control the authorized element IDs displayed with the following command, which calls for the CICSICE resource:

**CICE**-Calls for the element ID and for the PUR line command.

**CICSJOBN**

Specifies the CICS job names.

Use this section to control the authorized CICS job names displayed with the following command, which calls for the CICSJOBN resource:

**CICSLIST**-Calls for the job name and for the ALTER line command.

The following commands calls for the CICSJOBN resource to validate a job name for the display: CAIDS, CALERTS, CARTM, CDUMPMGT, CENQPOOL, CENQUEUE, CFILES, CGROUPS, CICE, CICSLIST, CJINFO, CJMODEL, CPROGRAM, CREMOTE, CSFTASKS, CSTATES, CSTATUS, CSYSDATA, CTASKENT, CTCLASS, CTASKS, CTDATA, CTERMS, CTHRESH, CTRANLOG, CTRANOPT, CTRANS, CTRANSUM, CTSMODEL, CTSPOOLS, CTSQUEUE, CUOW, and XLOG

**CICSJRNL**

Specifies the CICS journal names.

The CJINFO and CJMODEL commands calls for the CICSJRNL resource to validate a name for display.

**CICSPROG**

Specifies the CICS program names.

The following command calls for the CICSPROG resource:

**CPROGRAM**-Calls for the program name and for the DISABLE, ENABLE, NEWCOPY, and PHASEIN line commands.

**CICSTCLS**

Specifies the CICS transaction class names.

Use this section to control the authorized classes displayed with the following command, which calls for the CICSTCLS resource:

**CTCLASS**-Calls for the class name and for alter access when class attributes are changed.

**CICSTERM**

Specifies the CICS terminal names.

Use this section to control the authorized terminals displayed with the following command, which calls for the CICSTERM resource:

**CREMOTE**

The ALTER access is required to change an attribute of the remote connection.

**CTERMS**

Calls for the following:

- Terminal name
- Alter access when terminal attributes can be changed
- Alter access when the Acquire, Inserv, Outserv, and Release line commands are used
- C, FOR, KIL, and PUR line commands

**CICSTRAN**

Specifies the CICS transaction names.

Use this section to control the authorized transactions displayed with the following commands, which calls for the CICSTRAN resource:

**CARTM**

Calls for the transaction name and for alter access when transaction attributes can be changed.

**CSFTASKS**

Calls for the transaction name and for the C, FOR, KIL, and PUR line commands.

**CTASKS**

Calls for the transaction name and for the C, FOR, KIL, and PUR line commands.

**CTASKENT**

Calls for the transaction name and for the C, FOR, KIL, and PUR line commands.

**CTRANLOG**

Calls to validate the authority to display a transaction.

**CTRANS**

Calls for the transaction name, for alter access when transaction attributes can be changed, and for the DIS and ENA line commands.

**CTRANSUM**

Calls to validate the authority to display a transaction.

**CUOW**

Calls for the transaction name and for alter access when transaction attributes can be changed.

**CICSTSQ**

Specifies the CICS temporary storage queue IDs.

Use this section to control the authorized queues displayed with the following command, which calls for the CICSTSQ resource:

**CTSQUEUE**

Calls for the queue ID and for the DELETE line command.

**CICSTOPS**

Specifies the CICS transaction options.

Use this section to control the authorized transactions displayed with the following command, which calls for the CICSTOPS resource:

**CTRANOPT**

Calls for the transaction name and for alter access when attributes can be changed, and for the Add, Delete, and Reset line commands.

**CICSVAR**

Specifies the CICS resource variable names.

Use this section to control the authorized variables and thresholds displayed with the following commands, which calls for the CICSVAR resource:

**CSTATUS**

Calls for the variable name, for alter access when group attributes can be changed, and for alter access when the Add line command is used.

**CSTATES**

Calls for the resource name. Calls for alter access when group attributes can be changed, and for alter access when the Add and Delete line command is used.

**CTHRESH**

Calls for the threshold name. Calls for alter access when group attributes can be changed, and for alter access for the Add, Delete, and Reset line commands.

## Resource-Value Field Values for the IMS Option

The following are the resource types and describes the possible values for the Resource-Value field of the CA SYSVIEW Option for IMS:

**IMSCLASS**

Specifies the IMS class number.

The IMSCLASS command calls for alter access to the IMSCLASS resource when the class state is changed.

**IMSCMD**

Specifies the IMS command name.

The following commands call for ALTER access to the IMSCMD resource when an IMS command is issued:

- IMSCLASS
- IMSCMD
- IMSLIST
- IMSLTERM
- IMSNODE
- IMSPROG
- IMSPSB
- IMSREGN
- IMSTRAN
- IMSUSER

**IMSDBASE**

Specifies the IMS database name.

The IMSDBASE command calls for database name to the IMSDBASE resource, and to the following line commands: ARECOV, ARNFEOV, DBDUMP, DBDNFEOV, DBRECOV, DBRNFEOV, DELETE, GARECOV, GARNFEOV, GPDB, GSDB, LOCK, PAREA, SAREA, START, STOP, and UNLOCK.

**IMSID**

Specifies the IMS subsystem ID.

If NOQUAL was specified for the GSVXGEN SECEXIT parameter, the following commands call for ALTER access to the IMSID resource. This call prevents any line commands from being issued that result in a MODIFY console command against the IMS control region:

- IMSCLASS
- IMSCMD
- IMSDBASE
- IMSLINES
- IMSLIST
- IMSLTERM
- IMSNODES
- IMSOSAM
- IMSPI
- IMSOTMA
- IMSPROGS
- IMSPSBS
- IMSREGNS
- IMSTEXIT
- IMSTRANS
- IMSTTABL
- IMSUSER

The following command makes READ access calls to the IMSID resource. This call prevents the IMS from being display on a list of active IMS control regions:

**IMSLIST**

Verifies READ access to the IMSID before displaying the IMS in the list.

**IMSJOBN**

Specifies the IMS job names.

The following commands call for ALTER access to the IMSJOBN resource. This call prevents any line commands from being issued that alter the state of the IMS control region or dependent region:

**IMSLIST**

Verifies ALTER access to the IMSJOBN before issuing any commands that can alter the state of the IMS control region.

**IMSREGN**

Verifies ALTER access to the IMSJOBN before issuing any commands that can alter the state of the IMS-dependent region.

The following commands call for access to the IMSJOBN resource before letting the IMS to be listed on a list of active IMS job names:

**IMSLIST**

Verifies READ access to the IMSJOBN before displaying an IMS job name in the list of IMS control regions.

**IMSREGN**

Verifies READ access to the IMSJOBN before displaying an IMS job in the region list.

**IMSLINE**

Specifies the IMS line number.

The IMSLINE command calls for the line number, and for the following line commands: IDLE, PURGE, START, STOP, TROFF, and TRON.

**IMSLTERM**

Specifies the IMS logical terminal name.

The IMSLTERM command calls for the terminal name and for the following line commands: DEQALL, DEQFIRST, LOCK, PSTOP, PURGE, START, STOP, TROFF, TRON, and UNLOCK.

**IMSNODE**

Specifies the IMS node name.

**IMSLTERM**

Calls for the node name and for the TROFF and TRON line commands.

**IMSNODES**

Calls for the node name and for the following line commands: TROFF, TRON, ACTIVATE, CLSDST, DEQUEUE, EXCLUSIV, IDLE, QUIESCE, RSTART, START, STOP, TROFF and TRON.

**IMSPROG**

Specifies the IMS program name.

The IMSPROG command calls for program name and for the following line commands: DELETE, LOCK, START, STOP, TROFF, TRON, and UNLOCK.

**IMSPSB**

Specifies the IMS program status block name.

The IMSPSB command calls for PSB name and of the TROFF and TRON line commands.

**IMSTMEM**

Specifies the IMS TMEMBER name.

The IMSOTMA command calls for the TMEMBER name and for the following line commands: TMTS, TMTP, TPTS, TPTP, TPS, and TPP.

**IMSTPIPE**

Specifies the IMS TPIPE name.

The IMSOTMA command calls for the TPIPE name and for the following line commands: TMTS, TMTP, TPTS, TPTP, TPS, and TPP.

**IMSTRACE**

Specifies the IMS trace type.

The following lists the calls made for the IMSTRACE resource:

**IMSOSAM**

Calls for the OSAM GTF trace status be set to active or inactive.

**IMSPI**

Calls for the program isolation trace status.

**IMSTTABL**

Calls for the trace type and for the TROFF, TRON, TRONLO, TRONME, TRONHI, TRONLLO, TRONLME, and, TRONLHI line commands

**IMSTEXIT**

Calls for the trace type and for the TROFF and TRON line commands.

**IMSTRAN**

Specifies the IMS transaction name.

**IMSREGNS**

Calls for alter access to the IMSREGNS resource when the IMS regions attributes are changed.

**IMSTRANS**

Calls for alter access to the IMSTRANS resource when the IMS transaction attributes are changed.

**IMSUSER**

Specifies the IMS USER ID

The IMSUSER command calls for alter access to the IMSUSER resource when the user state is changed.

**IMSVAR**

Specifies the IMS variables.

The IMSVAR resource is checked when trying to define or alter the attributes of an IMSVAR definition such as a threshold definition.

The following commands require alter access to the IMSVAR resource when a definition is created or altered: IMSTHRSH, IMSSTATE, and IMSMON.

## Resource-Value Field Values for Other Resource Types

Values for the Resource-Value field for other resource types are listed in this section.

The following are the values for the Resource-Value field:

**CATALOG**

Indicates the catalog data set name that is allowed or restricted. Specify an exact data set or use an equal sign (=) at the end to specify a partial data set.

The CATALOG command calls for the CATALOG resource to validate the catalog data set name. If the catalog data set is not allowed, the catalog is not displayed.

The CATALOG command also calls for alter access when the ISC, NOISC, VLF, and NOVLF line commands are used. Calls are also made for the AL, CL, FRE, and OP line commands.

**CONSOLE**

Indicates the console name that is allowed or restricted. Specify an exact name or use an equal sign (=) at the end to specify a partial name.

The following commands call for the CONSOLE resource:

**CONSOLE**

Calls for a console name, for the RELEASE subcommand, and for the D line command.

**LISTCONS**

Calls for a console name, for alter access, and for the AC, D, DE, MAS, OFF, ON, and R line commands.

**CPU**

Indicates the CPU address that is allowed or restricted.

**CPU**

Calls for the CPU resource to validate the CPU address. If the CPU is not allowed, it is not displayed. The CPU command also calls for the CPU resource to validate the line commands OFF and ON.

**PRISM**

Calls for the CPU resource to validate the VARYOFF and VARYON line commands.

**DEST**

Indicates the execution or output destination that is allowed or restricted. DEST can be an exact destination, a partial destination, or one of the following:

**USERID -**

Specifies a destination that matches the user ID of the user.

**USERID:*n***

Specifies a destination that starts with a portion of the user ID of the user.

**USERID=**

Specifies a destination that starts with the user ID of the user.

If use of the destination is allowed (the Act field value is A) and alteration is authorized (the Alt field value is YES), this destination can be used when you change the destination of a job or the selection criteria of a device. If use of the resource is allowed and alter authority is not allowed, you can see jobs associated with the destination, but you cannot use this destination when specifying a new destination for a job.

You can specify no line commands for the DEST resource. The following commands call for the DEST resource:

**APPCOUTQ**

Calls for the APPC initiators and transactions and for alter access to the new destination when the destination of the output file changes.

**DESTID**

Calls for the destination ID.

**JCOPYOUT**

Calls to copy the output to a new output file and for alter access to the new destination.

**JHELDQUE**

Calls for the destination of a job and for alter access to the new destination when the job destination is changed.

**JJOBQUE**

Calls for the destination of a job and for alter access to the new destination when the job destination changes.

**JOBSUM**

Calls for the destination of a job and for alter access to the new destination when the job destination changes.

**JOUTQUE**

Calls for the destination of a job and for alter access to the new destination when a job destination is changed.

**LISTFILE**

Calls for the destination of a file and for alter access to the new destination when the output file destination changes.

**LISTINP**

Calls for the destination of a job and for alter access to the new destination when the job destination changes.

**OFFLOAD**

Calls for the destination of a job and for alter access to the new destination when a job destination is changed.

**PRINTER**

Calls for the destination of a printer and for alter access to the new destination when the printer selection destination changes.

**PROFILE**

Calls for the destination of the profile and for alter access to the new destination when the profile selection destination changes.

**PUNCH**

Calls for the destination of a punch and for alter access to the new destination when the punch selection destination changes.

**READERS**

Calls for the destination of a reader and for alter access to the new destination when a job destination is changed.

**SET**

Calls for the destination of a job and for alter access to the new destination when a job destination is changed.

**DEVICE**

Specifies the device name for a JES line, offloader, printer, punch, or reader.

The following commands call for the DEVICE resource:

**INTRDR**

Calls for the device name of a reader and for alter access when a reader is changed.

**LINES**

Calls for the device name of a line, for alter access when a line is changed, and for the E, I, N, S, and Z line commands.

**OFFLOAD**

Calls for the device name of an offloader, for alter access when an offloader is changed, and for the P, S, and Z line commands.

**PRINTER**

Calls for the device name of a printer, for alter access when a printer is changed, and for the B, E, F, I, N, P, S, and Z line commands.

**PUNCH**

Calls for the device name of a punch, for alter access when a punch is changed, and for the B, E, F, I, N, P, S, and Z line commands.

**READER**

Calls for the device name of a reader, for alter access when a reader is changed, and for the P, S, and Z line commands.

**DUMPDS**

Specifies the dump data set that is allowed or restricted. Specify an exact data set or use an equal sign (=) at the end to specify a partial data set.

The DUMPDS command calls for the DUMPDS resource to validate the dump data set name. If the dump data set is not allowed, the dump data set is not displayed.

The DUMPDS command also calls for the AD, CLR, and D line commands.

**EMAIL**

Specifies the valid email address of users.

The following command calls to the EMAIL resource:

**SENDMAIL**

Initiates calls to validate the “From” email address with the SEN line command.

**GROUPS**

Specifies the allowed or restricted groups. Specify an exact name or use an equal sign (=) at the end to specify a partial group name.

The GROUPS command calls for the group name, for the AD and D line commands, and the ADDGRP, ADDMBR, DELGRP, and DELMBR subcommands.

**JINIT**

Specifies the initiator ID. Use = instead of an ID to specify all initiators. The JINIT command is the only command that uses this resource. JINIT calls for the ID of the initiator, for alter access when an initiator is changed, and for the P, S, and Z line commands.

**JOBCLASS**

Specifies the job class that is allowed or restricted. Values are A-Z, 0-9, $, and @. You can specify no line commands for the JOBCLASS resource.

You can use the ALT field with JOBCLASS, which works like the DEST resource described earlier in this table.

These commands call for the JOBCLASS resource:

**ACTIVITY**

Calls for job class data display.

**APPCOUTQ**

Calls for job class display and the APPC initiators and transactions data.

**JINIT**

Calls for job class data display.

**INTRDR**

Calls for job classes displayed and for alter access when a job class is changed.

**JHELDQUE**

Calls for the class of a job.

**JINPRTY**

Calls for job class data display.

**JJOBQUE**

Calls for the class of a job and for alter access to the new job class when the class of a job changes.

**JOBCLASS**

Calls for job classes displayed and for alter access when a job class is changed or the H or R line command is used.

**JOBSUM**

Calls for the class of a job and for alter access to the new job class when the class of a job changes.

**JOUTDES**

Calls for the class of a job.

**JOUTQUE**

Calls for the class of a job.

**LINES**

Calls for the class of a job when lines are active.

**LISTINP**

Calls for the class of a job and for alter access to the new job class when the class of a job changes.

**OFFLOAD**

Calls for the class of a job.

**PRINTER**

Calls for the class of a job when printers are active.

**PUNCH**

Calls for the class of a job when punches are active.

**READERS**

Calls for the class of a job and for alter access to the new job class when the class of a job changes.

**LGSTREAM**

Specifies the log stream name. The LGDRO and LGEMPTY commands use this resource with alter access to validate the log stream name.

### LIBCACHE

Specifies the library cache type. Valid resource values are CAPLIB, CLISTLIB, HELPLIB, MAPLIB, MIBLIB, PANELLIB, PANELLIB and PARMLIB.

The LIBCACHE command uses this resource to look for alter access to the library type when the following line commands and subcommands are used:

- The DELETE or RELOAD line command
- The COMPRESS, DELETE, RELOAD, or SETCACHE subcommand

When the EMPTY subcommand is used, a call is made for alter access with a resource value of ALL.

### MQSVAR

Specifies the WebSphere MQ monitor variable name.

The following commands call for the MQSVAR resource:

#### MQMON

Calls for alter access when adding, changing, or deleting a variable definition. Makes a check for the resource value ?ADD to determine whether to display the line for adding a variable.

#### MQSTATES

Calls for alter access when adding, changing, or deleting a variable definition. Makes a check for the resource value ?ADD to determine whether to display the line for adding a variable.

#### MQTHRESH

Calls for alter access when adding, changing, or deleting a variable definition. Makes a check for the resource value ?ADD to determine whether to display the line for adding a variable.

**MVSVAR**

Specifies the MVS monitor variable name.

The following commands call for the MVSVAR resource:

**MONITORS**

Calls for alter access when adding, changing, or deleting a variable definition. Makes a check for the resource value ?ADD to determine whether to display the line for adding a variable.

**STATES**

Calls for alter access when adding, changing, or deleting a variable definition. Makes a check for the resource value ?ADD to determine whether to display the line for adding a variable.

**THRESH**

Calls for alter access when adding, changing, or deleting a variable definition. Makes a check for the resource value ?ADD to determine whether to display the line for adding a variable.

**NODE**

Specifies the node name.

**JPATHS**

Calls for the JES network paths.

**NODES**

Calls for the node name of a node, for alter access when a node is changed, and for the S line command.

**OUTCLASS**

Specifies the Output class that is allowed or restricted. Values are A-Z or 0-9. You can specify no line commands for the OUTCLASS resource.

You can use the ALT field with OUTCLASS, which works like the JOBCLASS and DEST resources described earlier in this table.

These commands call for the OUTCLASS resource:

**APPCOUTQ**

Calls for a file output class and for alter access to the new output class when a file output class is changed.

**COPYOUTP**

Calls to copy output to a new output file and for alter access to the new destination.

**JHELDQUE**

Calls for a job output class and for alter access to the new output class when a file output class is changed.

**JJOBQUE**

Calls for a job output class and for alter access to the new output class when a file output class is changed.

**JOUTDES**

Calls for the class of a job.

**JOUTQUE**

Calls for a job output class and for alter access to the new output class when a file output class is changed.

**LINES**

Calls for the class of a job when lines are active.

**LISTFILE**

Calls for a file output class and for alter access to the new output class when a file output class is changed.

**OFFLOAD**

Calls for the class of a job and for alter access to the new output class when a file output class is changed.

**OUTCLASS**

Calls for output classes displayed and for alter access when an output class is changed.

**PRINTER**

Calls for the class of a job when printers are active.

**PUNCH**

Calls for the class of a job when punches are active.

**READERS**

Calls for the class of a job and for alter access to the new job class when the class of a job changes.

**SET**

Calls for the destination of a job and for alter access to the new destination when a job destination is changed.

**PAGEDS**

Specifies the Page data set that is allowed or restricted. Specify an exact data set or use an equal sign (=) at the end to specify a partial data set.

The PAGEDS command calls for the PAGEDS resource to validate the page data set name. If the page data set is not allowed, the page data set is not displayed.

The PAGEDS command also calls for the AD, D, and DR line commands.

**SCHEDULE**

Specifies the schedule name that is allowed or restricted. Specify an exact name or use an equal sign (=) at the end to specify a partial data set name.

The SCHEDULE command calls for:

- The schedule name to determine whether to display the schedule.
- Alter access when the Add, Delete, Enable, and Disable line commands are used and when a schedule field is changed.

A call is also made for read access for the name ?Add to see whether to display the line to add a schedule.

**SMFDATA**

Specifies the SMF record type that is allowed or restricted.

The SMFDATA command calls for alter access when, and the LOG, NOLOG, SUPRESS and NOSUPRES line commands are used.

**SMFDS**

Specifies the SMF data set that is allowed or restricted. Specify an exact data set or use an equal sign (=) at the end to specify a partial data set.

The SMF command calls for the SMFDS resource to validate the DU and SW line commands.

**SPOOL**

Specifies the last two characters of a spool volume name. The JSPOOLS command is the only command that uses this resource.

The JSPOOLS command makes a resource call to determine whether to present a line on the display that lets spool volumes be added. To authorize this line, define a resource value of XX with the S line command. If the XX resource value is not defined, you cannot add spool volumes.

Calls are also made to validate the C, FMT, P, S, and Z line commands.

**STGSSID**

Specifies the subsystem storage IDs.

These commands calls for the STGSSID resource:

**CACHECTL**

When you enter the line command:

- CACHEON or CACHEOFF, a call is made for the SSUB line command.
- CFWON or CFWOFF, a call is made for the SCFW line command.
- NVSON or NVSOFF, a call is made for the SNVS line command.

**CACHEDEV**

When you enter the line command:

- CACHEON or CACHEOFF, a call is made for the SDEV line command.
- DFWON or DFWOFF, a call is made for the SDFW line command.

**SYSTEM**

Specifies the system name. The LISTSYS command is the only command that uses this resource. It calls for the system ID, for alter access when a system is changed, and for the E line command.

**TCPVAR**

Specifies the TCP/IP monitor variable name.

The following commands call for the TCPVAR resource:

**TCPMON**

Calls for alter access when adding, changing, or deleting a variable definition. Makes a check for the resource value ?ADD to determine whether to display the line for adding a variable.

**TCPSTATE**

Calls for alter access when adding, changing, or deleting a variable definition. Makes a check for the resource value ?ADD to determine whether to display the line for adding a variable.

**TCPTHRSH**

Calls for alter access when adding, changing, or deleting a variable definition. Makes a check for the resource value ?ADD to determine whether to display the line for adding a variable.

**UNIT**

Specifies the Unit device address.

The following commands call for the UNIT resource:

**ALLOCAS**

Calls for the ON, OFF, and FRE line commands.

**ALLOCDS**

Calls for the FREE line command.

**DASD**

Calls for the DASD device address, for alter access when volume attributes can be changed, and for the MNT, OFF, ON, and UNL line commands.

**DEVPATH**

Calls for the DEVPATH device number, for alter access when volume attributes can be changed, and for the line commands OFF and ON.

**DEVSERV**

Calls for the DEVSERV device number and for the FREE, MNT, OFF, ON, and UNL line commands.

**EXTENTS**

Calls for the EXTENTS device number.

**SPACE**

Calls for the SPACE device number.

**SUBCHAN**

Calls for the subchannel device number.

**TAPE**

Calls for the tape device address, for alter access when volume attributes can be changed, and for the MNT, OFF, ON, and UNL line commands.

**UNIT**

Calls for the unit device address, for alter access when volume attributes can be changed, and for the MNT, OFF, ON, and UNL line commands.

**VOLSER**

Calls for the volser device number.

**VOLSER**

Specifies the DASD volume serial numbers allowed or restricted.

The following commands call for the VOLSER resource:

**ALLOCAS**

Calls for the OFF, and FRE line commands.

**ALLOCDS**

Calls for the FREE line command.

**CACHEDEV**

Calls for volser name.

SDEV initiates a call to CACHEON and CACHEOFF line commands.

SDFW initiates a call to DFWON and DFWOFF line commands.

**DASD**

Calls for the volser of a DASD and for the MOUNT, OFF, and UNLOAD line commands.

**DEVSERV**

Calls for the device service volser name and for the FREE, MNT, OFF, ON, and UNL line commands.

**DEVPATH**

Calls for the device path volser name and for the FREE, MNT, OFF, ON, and UNL line commands.

**EXTENTS**

Calls for the volser of a DASD.

**SPACE**

Calls for the volser of a DASD.

**SUBCHAN**

Calls for the subchannel volser name.

**UNIT**

Calls for the device address of a DASD. Calls for alter access when volume attributes can be changed, and for the MNT, OFF, and UNL line commands.

**VOLSER**

Calls for the volser name.

**WMAPLENV**

Specifies the WLM application environments.

The WMAPPENV command calls for alter access to this resource when the REFresh, RESume and QUIesce line commands are used.

**WMSCHENV**

Specifies the WLM scheduling environment names.

The WMSCHENV command requests ALTER access for this resource when the OFF, ON, or RESET line commands are used.

**XSYSDEST**

Specifies the destination system names allowed or restricted when connecting to another system. Specify an exact system name or use an equal sign (=) at the end to specify a partial system name.

The XSCONN command calls for the destination system name.

**XSYSORIG**

Specifies the originating system names allowed or restricted when connecting to another system. Specify an exact system name or use an equal sign (=) at the end to specify a partial system name.

The XSCONN command calls for the originating system name.

**ZAP**

Specifies the ZAP command resource that is allowed or restricted. Specify an exact resource value or use an equal sign (=) at the end to specify a partial resource value.

The ZAP command calls for the ZAP resource to validate access to the following resource values:

**LABEL.*volser***

*volser* is the volume serial number for the LABEL to be zapped. A call is made for this resource value when the ZAP LABEL command is entered.

**SPOOL.*jesname***

*jesname* is the JES subsystem name for the spool to be zapped. A call is made for this resource value when the ZAP SPOOL command is entered.

**VOLSER.*volser***

*volser* is the volume serial number for the volume to be zapped. A call is made for this resource value when the ZAP VOLUME command is entered.

**VTOC.*volser***

*volser* is the volume serial number for the VTOC to be zapped. A call is made for this resource value when the ZAP VTOC command is entered.

**Note:** External security covers the zapping data sets, members of data sets, and CSECTs through normal data set access.

# External Security Section Display

The External Security Section display shows the System Authorization Facility (SAF) definitions that are used to interface with external security products.

The External Security Section display has the following fields:

**SAF Entity Class Name**

Specifies the SAF resource class name to use when you want external security to validate commands and other resources.

Specify NONE to use internal security definitions to validate all commands and resources and thus bypass the SAF authorization calls.

**Default:** NONE

Suggested SAF resource class names:

- CAGSVX for CA Top Secret
- SYSVIEW for CA ACF2
- FACILITY for IBM RACF

Specifying a class name in the security group overrides any specified value in the GLOBAL group.

**Bypass Internal Security Call**

Specify a value of YES if you want only your external security determining access. CA SYSVIEW calls the external security before calling the internal security. Normally, access that internal security failed external security cannot override and allow. This option lets you use the external security exclusively without having to allow all access in the DEFAULT internal security group.

**Note:** When you set this option, Command Groups that are defined in internal security do not participate in determining command and subcommand access.

**Default:** NO

**SAF Entity Name Prefix**

The prefix, or first node name, used to build the entity names for SAF calls. The prefix is only used when a SAF entity class is defined.

**Default:** SV

**Call SAF if failed internally**

Specify a value of YES to call SAF to validate access to the resource when internal security already failed the access. External security cannot grant access to a resource that internal security failed. Setting this value to YES lets you log violations in the external security database that would otherwise not be recorded.

**Default:** NO

**Use JESSPOOL for Job Validation**

Specify a value of YES if you want to use the JESSPOOL resources for all job name validation calls. All other resource checks (CMND, SUBC, RESN, and so on) continue to use resources that are defined for the SAF Entity Class Name.

SAF only verifies the JESSPOOL resources (no SAF calls for CMND, SUBC, RESN, and so on) when JESSPOOL is the SAF Entity Class Name.

**Default:** NO

**Use System SMFID in Entity Name**

Specifies whether the SAF entity name contains the system SMFID as the third node when a SAF entity class is defined.

**Default:** YES

**Use System QUAL in Entity Name**

Specifies whether the SAF entity name contains a qualifier following the resource type when a SAF entity class is defined. Some example qualifiers would be JES2 for JES resource types, or the subsystem ID for IMS resources.

**Default:** YES

**SAF Exit Name**

Specifies the name of an optional user exit to invoke before SAF. The entity class and entity name is passed to the exit.

**Default:** NONE

**Pass JES JCT addr to the SAF exit**

Specify a value of YES to pass the address of the JES JCT to the SAF exit. This value only applies if an exit is coded.

**Default:** YES

**Access Entity Table Size**

Specifies the initial size of the SAF Access Entity Table (AET). The AET is used to cache responses to SAF calls so subsequent calls for the same entity name can retrieve the responses. The size of the AET is specified in KB. AET storage is allocated above the 2-GB bar. A value of zero uses no AET.

**Default:** 256

**Maximum:** 1024

# Command Groups Display

The Command Groups display is presented when you select the Command Groups entry from the primary Security Menu. This display lists all the command groups that you are allowed to see.

The display also serves as a menu. Select a command group to show the Command Group Access Detail display.

The Command Groups display has the following fields:

**Cmd**

Specifies the area in which you enter a command. Use the following commands:

- **S**-Selects a command group. Use with AddGroup to add a new command group. Specify the new command group name in the Group field.

  The group name cannot:

  - Be the same as another group name
  - Contain blanks
  - Be longer than eight characters

- **D**-Deletes a command group.

  - Command groups starting with GSV cannot be deleted.
  - A deleted command group is *not* automatically removed from the Command Groups Section of the user groups.

**Group**

Specifies the name of a command group.

AddGroup is a special group name used to add a command group.

**Count**

Specifies the number of commands included in the command group.

**Upd-Date**

Specifies the date the command group was last updated.

**Upd-Time**

Specifies the time the command group was last updated.

**Userid**

Specifies the user ID of the user who last updated the command group.

**Description**

Specifies a brief description of the command group.

## Add Subcommand-Copy an Existing Command Group

Use the ADD subcommand to copy an existing command group to a new group name.

The ADD subcommand has the following format:

```
ADD ngname,cgname
```

**ngname**

The name given to the created group.

**cgname**

The name of the existing group you want to copy.

## Select Command Groups

To select multiple command groups, enter an **S** before each command group you want to select and press Enter.

When you exit one of the selected command groups, the next one you selected is shown.

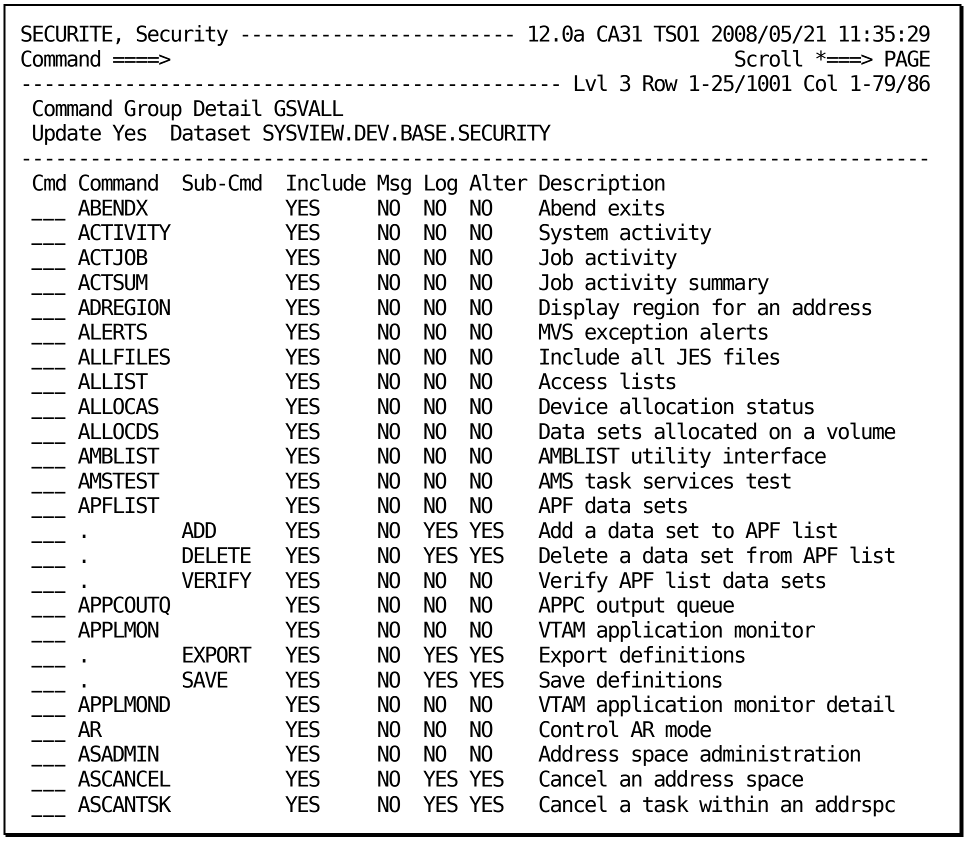
## Delete Command Groups

You can delete user-defined command groups by typing a **D** before each command group you want to delete. However, you cannot delete command groups that start with the letters GSV.

# Command Group Detail Display

The Command Group Detail display is presented when you select a command group entry from the Command Groups display. This display lists all the commands available in the product. You can use the display to specify which commands are included in the command group.

The following is a sample Command Group Detail display:



```
SECURITE, Security ----------------------- 12.0a CA31 TSO1 2008/05/21 11:35:29
Command ====>                                                 Scroll *===> PAGE
----------------------------------------------- Lvl 3 Row 1-25/1001 Col 1-79/86
 Command Group Detail GSVALL
 Update Yes  Dataset SYSVIEW.DEV.BASE.SECURITY
-------------------------------------------------------------------------------
 Cmd Command  Sub-Cmd  Include Msg Log Alter Description
 ___ ABENDX            YES     NO  NO  NO    Abend exits
 ___ ACTIVITY          YES     NO  NO  NO    System activity
 ___ ACTJOB            YES     NO  NO  NO    Job activity
 ___ ACTSUM            YES     NO  NO  NO    Job activity summary
 ___ ADREGION          YES     NO  NO  NO    Display region for an address
 ___ ALERTS            YES     NO  NO  NO    MVS exception alerts
 ___ ALLFILES          YES     NO  NO  NO    Include all JES files
 ___ ALLIST            YES     NO  NO  NO    Access lists
 ___ ALLOCAS           YES     NO  NO  NO    Device allocation status
 ___ ALLOCDS           YES     NO  NO  NO    Data sets allocated on a volume
 ___ AMBLIST           YES     NO  NO  NO    AMBLIST utility interface
 ___ AMSTEST           YES     NO  NO  NO    AMS task services test
 ___ APFLIST           YES     NO  NO  NO    APF data sets
 ___ .        ADD      YES     NO  YES YES   Add a data set to APF list
 ___ .        DELETE   YES     NO  YES YES   Delete a data set from APF list
 ___ .        VERIFY   YES     NO  NO  NO    Verify APF list data sets
 ___ APPCOUTQ          YES     NO  NO  NO    APPC output queue
 ___ APPLMON           YES     NO  NO  NO    VTAM application monitor
 ___ .        EXPORT   YES     NO  YES YES   Export definitions
 ___ .        SAVE     YES     NO  YES YES   Save definitions
 ___ APPLMOND          YES     NO  NO  NO    VTAM application monitor detail
 ___ AR                YES     NO  NO  NO    Control AR mode
 ___ ASADMIN           YES     NO  NO  NO    Address space administration
 ___ ASCANCEL          YES     NO  YES YES   Cancel an address space
 ___ ASCANTSK          YES     NO  YES YES   Cancel a task within an addrspc
```

The following are the Command Group Detail display sections:

**cmd**

Specifies the area in which you enter a command. Use the following commands:

**S**

Selects a command to include it in the group.

**I**

Includes the command in the group.

**E**

Excludes the command from the group.

**L**

Toggles whether the command is logged to the Audit Log when the command is entered.

**M**

Toggles whether a message is displayed when the command is entered.

**Command**

Specifies the name of the command in the command group.

**Sub-Cmd**

Specifies the name of a subcommand for the command.

**Include**

Shows whether the command is included in the command group.

**Msg**

Shows whether a message is displayed when the command is entered.

**Log**

Specifies whether to log the command.

**Alter**

Shows whether the command can alter or update the system.

**Description**

Shows the command description.

# Chapter 5: Interfacing with External Security

This section contains the following topics:

## Purpose of External Security

All CA SYSVIEW started tasks must be defined to the external security product at your site:

- CA Top Secret
- CA ACF2
- RACF

This chapter documents the external security requirements for both the CA SYSVIEW started tasks, as well as security requirements for individual user IDs.

## Customize CA Top Secret

CA Top Secret must be customized before you can activate the CA SYSVIEW interface.

**Follow these steps:**

1. Define a task as a facility to CA Top Secret in the Facilities Matrix by adding the following commands to the CA Top Secret parameter file:

   ```
   FAC(USERn=NAME=GSVX)
   FAC(GSVX=PGM=GSV,MULTIUSER,SHRPRF,KEY=8,NOLUMSG,NOSTMSG)
   FAC(GSVX=MODE=FAIL,LOG(NONE),ACTIVE,NOABEND)
   FAC(GSVX=SIGN(M),NOTRACE,AUTHINIT)
   FAC(GSVX=NOAUDIT,ASUBM,DEFACID(*NONE*))
   FAC(GSVX=UIDACID=8)
   ```

   **USER*n***

   Must be a valid Facility Matrix Table entry.

2. Create a master facility ACID for CA SYSVIEW

   ```
   TSS CREATE(SYSVIEW) NAME('SYSVIEW ACID') FACILITY(STC)
      MASTFAC(GSVX) PASSWORD(NOPW,0) DEPT(owningdept)
      NOLCFCHK NORESCHK NODSNCHK NOVOLCHK NOSUBCHK
   ```

   Specifying a password is recommended for the CA SYSVIEW acid and OPTION(4) be set in the CA Top Secret Control Option file. When these passwords are set, the started task does not get prompted on the console for a password.

3. Define the CA SYSVIEW address spaces as started tasks in the STC record using the master facility ACID you created in Step 2.

   ```
   TSS ADDTO(STC) PROCNAME(SYSVIEW) ACID(SYSVIEW)
   TSS ADDTO(STC) PROCNAME(SYSVUSER) ACID(SYSVIEW)
   TSS ADDTO(STC) PROCNAME(SYSVAAST) ACID(SYSVIEW)
   ```

4. Add OMVS segment to the ACID.

   ```
   TSS ADDTO(SYSVIEW) UID(0) GROUP(OMVSGRP) DFLTGRP(OMVSGRP)
         HOME(/) OMVSPGM(/bin/sh)
   ```

   CA Top Secret is customized. You can activate the CA SYSVIEW interface.

## Customize CA ACF2

CA ACF2 must be customized to activate the CA SYSVIEW interface.

**Follow these steps:**

1. Define security requirements for the CA SYSVIEW address space by using the following CA ACF2 commands to create an STC logon ID:

   ```
   READY
   ACF
   INSERT SYSVIEW NAME(SYSVIEW) STC
   ```

2. Be sure that the SYSVIEW address space has access to needed resources by granting access to the NON-CNCL logon ID permission.

   Use the following commands:

   ```
   ACF
   CHANGE SYSVIEW NON-CNCL
   CHANGE SYSVUSER NON-CNCL
   ```

3. Add OMVS segment to the SYSVIEW and SYSVUSER logon ID.

   ```
   ACF
   CHANGE SYSVIEW GROUP(OMVSGRP) UID(0) HOME(/) OMVSPGM(/bin/sh)
   CHANGE SYSVUSER GROUP(OMVSGRP) UID(0) HOME(/) OMVSPGM(/bin/sh)
   ```

4. (Optional) Define the optional system access requirements through the MUSID option of the SYSVIEW logon ID record. When specified in the SYSVIEW logon ID, users are required to have a special permission bit in their logon ID record before accessing CA SYSVIEW. The name of the field is arbitrary. Be sure that the name conforms to site definitions for naming logon ID fields.

   a. ADD the MUSID permission to the SYSVIEW logon ID as follows:

      ```
      ACF
      SET LID
      CHANGE SYSVIEW MUSID(SYSVIEW)
      ```

   b. Create a bit field in the logon ID record named SYSVIEW using the following CA ACF2 macro named CFDE:

      ```
      @CFDE   SYSVIEW,LIDI1FLG,BIT.ALTER=SECURITY+ACCOUNT,
      LIST=ALL,FLAGS=NULL,GROUP=2,BITMAP=LIDI1F1
      ```

   The user access requirements are defined, which completes your CA ACF2 security system customization.

**Note:** For more information about how to write data set and resource rules and information related to the CFDE macro, see the *CA ACF2* documentation.

## Customize RACF

RACF must be customized before you can activate the CA SYSVIEW interface.

**Follow these steps:**

1. Create a RACF group and a user ID for CA SYSVIEW.

   ```
   ADDGROUP STCGROUP DATA('started task group')
   ADDUSER SYSVIEW NAME(‘SYSVIEW user ID’) DFLTGRP(STCGROUP)
       OWNER(STCADMIN) NOPASSWORD
   ```

2. Define the CA SYSVIEW address spaces as started tasks in the class named STARTED using the user ID defined in step 1.

   ```
   RDEFINE STARTED SYSVIEW.SYSVIEW STDATA(USER(SYSVIEW)
   GROUP(STCGROUP)TRUSTED(YES))
   RDEFINE STARTED SYSVUSER.SYSVUSER STDATA(USER(SYSVIEW) GROUP(STCGROUP)
   TRUSTED(YES))
   RDEFINE STARTED SYSVAAST.SYSVAAST STDATA(USER(SYSVIEW) GROUP(STCGROUP)
   TRUSTED(YES))
   ```

3. Add OMVS segment to the SYSVIEW user ID.

   ```
   ADDUSER SYSVIEW OMVS(UID(0) HOME(/) PROG(‘/bin/sh’))
   ```

The RACF security is customized. You can activate the CA SYSVIEW interface.

# PassTicket Configuration

The PassTicket configuration is required for the CA SYSVIEW for CA Insight DPM for DB2 component. This CA SYSVIEW component acquires data from CA Insight Database Performance Monitor for DB2 for z/OS (CA Insight DPM for DB2), by establishing connections to CA Insight DPM for DB2 on behalf of users who are requesting the information. Although this connection is transparent to the user of CA SYSVIEW for CA Insight DPM for DB2, the connection setup to CA Insight DPM for DB2 is analogous to a logon into that product and the user must be authenticated by that product before access is allowed. The authentication mechanism for this interface is a PassTicket.

A *PassTicket* is a temporary encoded and encrypted substitute for the user password that can be used to access a specific application.

Using PassTickets enables the z/OS components and products to provide the user ID authentication without saving z/OS passwords and sending them through the network. Instead, the users are authenticated once using their real password when they first log in to CA SYSVIEW. The following process occurs when the user selects a function that accesses a z/OS component or product that must also authenticate the user:

- The CA SYSVIEW component calls the z/OS security product to generate a PassTicket for the user verification.
- The PassTicket is sent with the user request to the component.
- The component calls the z/OS security product to authenticate the user using the PassTicket as a password substitute before processing the request.

PassTickets must be generated for CA SYSVIEW for CA Insight DPM for DB2 users to connect to the CA Insight DPM product. The connection is made through the CA DB2 Tools Xnet component. The Xnet component performs the user authentication before forwarding requests to CA Insight DPM.

Sample CA ACF2, CA Top Secret, and IBM RACF commands to generate PassTickets are provided as a guideline.

**Note:** Some of the sample commands refer to the variable *xnet_applid*. The PassTickets generated using this configuration can only be used for access to the application that identifies itself as *xnet_applid* during the user authentication process. The recommended *xnet_applid* is DB2TOOLS but the name is configurable (any uppercase string of eight characters or less is permitted). If a different value is used for the application ID, update the sample commands to use the same value.

## PassTicket Configuration for CA SYSVIEW for CA Insight DPM for DB2 Component

CA SYSVIEW for CA Insight DPM for DB2 component generates a PassTicket that permits the user to access the CA Insight DPM back-end product that the CA SYSVIEW for CA Insight DPM for DB2 component uses.

The PassTicket configuration for the z/OS security product must be done on each z/OS system where the CA SYSVIEW for CA Insight DPM for DB2 component will be used to display DB2 data. Configuring PassTickets in your z/OS security products enables the proper user authentication in the back-end products that CA SYSVIEW accesses.

Note the following tips:

- When all security products in your z/OS configuration use the same shared security database, configure the PassTicket once from one of the z/OS systems.
- When there are z/OS systems in your configuration *not* using a shared security database, perform the PassTicket configuration on each of those z/OS systems.

## Sample: Use CA ACF2 to Configure CA SYSVIEW for CA Insight DPM for DB2 PassTickets

You can use CA ACF2 to configure specific CA SYSVIEW for CA Insight DPM for DB2 component PassTickets for validating access.

**Note:** These examples are provided as a guideline. Only a security administrator familiar with PassTicket configuration should execute this process. For detailed information about using these commands, see the *CA ACF2 for z/OS Administration Guide*.

### Example: Use CA ACF2 to Configure PassTickets for CA SYSVIEW for CA Insight DPM for DB2 Systems.

**Follow these steps:**

1. Define the application session keys by entering the following commands:

   ```
   SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
   INSERT xnet_applid SSKEY(0123456789ABCDEF)
   F ACF2,REBUILD(PTK),CLASS(P)
   ```

   ***xnet_applid***

   Defines the application ID used for the PassTicket validation. This value is specified in the CA DB2 Tools Xnet INITPARM data set parameter PASSNAME and subsequently in the CA SYSVIEW DB2 PARMLIB XNET-PassTicketApplId parameter.

   **SSKEY**

   Defines an encryption key for the application using values that are different from the values in the sample syntax.

   **Note:** The sample syntax demonstrates a complete key value of 16 hexadecimal digits (creating an 8-byte or 64-bit key). Each application key must be the same on all systems in the configuration and the values must be kept "secret."

   The CA Insight DPM for DB2 (CA DB2 Tools Xnet) session keys are defined.

2. Permit access to the xnet_applid application for each user that is allowed to access the CA Database Management Solutions for DB2 for z/OS (CA DB2 Tools Xnet):

   **Note:** Complete this step only if you have already defined the xnet_applid application resources. If you inserted a GSO CLASMAP record to change the type code for the APPL class to APL, use APL instead of SAF for TYPE in the following commands.

   ```
   ACF
   SET RESOURCE(SAF)
   RECKEY xnet_applid ADD(useridn UID(uid-of-useridn) SERVICE(READ)
   ALLOW)
   F ACF2,REBUILD(SAF)
   ```

## Sample: Use CA Top Secret to Configure CA SYSVIEW for CA Insight DPM for DB2 PassTickets

You can use CA Top Secret to configure specific CA SYSVIEW for CA Insight DPM for DB2 PassTickets for validating access.

**Note:** These examples are provided as a guideline. Only a security administrator familiar with PassTicket configuration should execute this process. For detailed information about using these commands, see the *CA Top Secret for z/OS Control Options Guide*.

**Note:** This procedure assumes that the PTKTDATA class and IRRPTAUTH resource ownership have been defined.

### Example: Use CA Top Secret to Configure PassTickets for CA SYSVIEW for CA Insight DPM for DB2 Systems.

**Follow these steps:**

1. Define the application resources used by CA SYSVIEW for CA Insight DPM for DB2 component and assign ownership:
   `TSS ADDTO(`*`department`*`) APPLICATION(`*`xnet_applid`*`)`

   ***department***

   Identifies a preexisting department. The application is defined to this department. This ownership lets a department administrator (or higher) define permissions for PassTicket generation and validation.

   ***xnet_applid***

   Defines the application ID used for the PassTicket validation. This value is specified in the CA DB2 Tools Xnet INITPARM data set parameter PASSNAME and subsequently in the CA SYSVIEW DB2 PARMLIB XNET-PassTicketApplId parameter.

   The application is defined and owned.

2. Update the Node Descriptor Table (NDT) to define the application IDs and assign session keys using the following command:
   `TSS ADDTO(NDT) PSTKAPPL(`*`xnet_applid`*`) SESSKEY(0123456789ABCDEF)`

   **Note:** The session key defines an encryption key for the application in the format of 16 hexadecimal digits (creating an 8-byte or 64-bit key). Use a session key value that is different from what is shown in the sample syntax. Each application key must be the same on all systems in the configuration and the value must be kept "secret."

   The host system is set up to accept PassTickets.

   All systems using Passtickets must have identical application names and session keys for all nodes on the network.

3. Permit access to the *xnet_applid* application for each user that is allowed to access the CA Database Management Solutions for DB2 for z/OS (CA Insight DPM for DB2 using CA DB2 Tools Xnet):
   ```
   TSS PERMIT(useridn) APPLICATION(xnet_applid)
   ```

## Sample: Use RACF to Configure CA SYSVIEW for CA Insight DPM for DB2 Component PassTickets

You can use IBM RACF to configure specific CA SYSVIEW for CA Insight DPM for DB2 PassTickets for validating access.

**Note:** These examples are provided as a guideline. Only a security administrator familiar with PassTicket configuration should execute this process. For detailed information about using these commands, see the IBM RACF product documentation.

**Note:** Before you begin Passticket configuration, verify that the PTKTDATA class and ownership for the PassTicket resource IRRPTAUTH have not been defined. If they have been defined, skip Step 1 and Step 2 in the following procedure.

### Example: Use IBM RACF to Configure PassTickets for CA SYSVIEW for CA Insight DPM for DB2 Systems.

**Follow these steps:**

1. Define the *xnet_applid* application by entering the following commands:

   ```
   RDEFINE APPL xnet_applid UACC(NONE)
   SETROPTS CLASSACT(APPL)
   ```

   **Note:** If you want to implement a generic user ID, specify the following additional command:

   ```
   SETROPTS GENERIC(PTKTDATA)
   ```

   ***xnet_applid***

   Defines the application ID used for the PassTicket validation. This value is specified in the CA DB2 Tools Xnet INITPARM data set parameter PASSNAME and subsequently in the CA SYSVIEW DB2 PARMLIB XNET-PassTicketApplId parameter.

2. Activate the PassTicket class if it is not currently active:

   ```
   SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
   ```

3. Define profiles for the applications and specify the session keys:

   ```
   RDEFINE PTKTDATA xnet_applid
   SSIGNON(KEYMASKED(FEDCBA9876543210))
   ```

   ***xnet_applid***

   Defines the application ID used for the PassTicket validation. This value is specified in the CA DB2 Tools Xnet INITPARM data set parameter PASSNAME and subsequently in the CA SYSVIEW DB2 PARMLIB XNET-PassTicketApplId parameter.

   **KEYMASKED**

   Defines an encryption key for the application using values that are different from the values in the sample syntax.

   **Note:** The sample syntax demonstrates a complete key value of 16 hexadecimal digits (creating an 8-byte or 64-bit key). Each application key must be the same on all systems in the configuration and the values must be kept "secret."

   The profiles and session keys are defined.

4. Permit access to the *xnet_applid* application for each CA SYSVIEW for CA Insight DPM for DB2 component user that is permitted to access the CA SYSVIEW for CA Insight DPM for DB2 component data from CA Insight DPM for DB2 using CA DB2 Tools Xnet:

   ```
   PERMIT xnet_applid CLASS(APPL) ID(useridn)
   ```

   ***useridn***

   Specifies the user ID of the users requesting access.

5. Refresh the APPL and PTKTDATA classes with the following commands if they are RACLISTed:

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

## User Access Requirements to Resources

Individual user IDs require access to various resources depending on the CA SYSVIEW component being accessed. All users will require access to the CA SYSVIEW run-time libraries.

The following table provides the data set and the access requirements:

| Data Set | Access Level |
|---|---|
| sysview.CNM4BLOD | Read access for all users |
| sysview.CNM4BSEC | Read access for all users, update for ADMIN |

| Data Set | Access Level |
|---|---|
| sysview.CNM4BPRF | Update access for all users |
| sysview.CNM4BPRM | Read access for all users, update for ADMIN |
| sysview.CNM4BREX | Read access for all users |
| sysview.CNM4BCAP | Read access to users permitted to do a CAPTURE |
| sysview.CAPINDEX.smfid | Update access to users permitted to do CAPTURE |
| sysview.CNM4BCLS | Read access for all users |
| sysview.CNM4BHLP | Read access for all users |
| sysview.CNM4BISP | Read access for all users |
| sysview.CNM4BMAP | Read access for all users |
| sysview.CNM4BMIB | Read access for all users |
| sysview.CNM4BPNL | Read access for all users |
| sysview.CNM4BPLT | Read access for all users |
| sysview.CNM4BTMP | Read access for all users |
| sysview.CNM4BDAT | Update access for ADMIN |

## User Validation for CA Top Secret

User validation is performed when you log in to the VTAM interface.

Provide the following CA Top Secret settings:

- Set the Security-Validation to the default value of USER in the System Configuration Options member.
- Create a master facility for CA SYSVIEW, that is GSVX.
- Provide the user with access to the facility as follows:

```
TSS ADDTO(useracid) FACILITY(GSVX)
```

**More information:**

SECC Access Field and Equates (see page 157)

## User Validation for CA ACF2

User validation is performed when you log in to the VTAM interface.

Provide the following CA ACF2 settings:

- Create a MUSID for CA SYSVIEW:

  ```
  SYSVIEW
  ```

- Provide the user with access as follows:

  ```
  ACF
  SET LID
  CHANGE userid SYSVIEW
  ```

## Add OMVS Segment to User IDs

When user IDs have an OMVS segment defined, they can issue any of the USS, TCP/IP, or CSM (Communications Storage Manager) commands.

Some USS commands, like UPROCESS, only display processes belonging to the USS UID and GID of a user.

To add OMVS segment to user IDs, see the Security Requirement section in the HELPLIB member for the command.

### Example: Help Command

Issue the following Help command to retrieve security requirements information for a specific USS, TCP/IP, or CSM:

```
HELP UPROCESS
```

# SAF Requirements

The following sections list SAF authorizations that are required for both the CA SYSVIEW address spaces and for individual user IDs. The SAF authorizations depend on what features and components are implemented at your site.

## JESSPOOL Class

The JESSPOOL class is used to protect JES spool data from unauthorized access. If the JESSPOOL class is active in your external security product, the SYSLOG, OUTPUT, and JJCL commands make SAF calls in the JESSPOOL class for the resources shown.

**JESSPOOL Class (if active)**

- This resource requires all users have Read access when permitted access to the SYSLOG command:

  `jesnode.+MASTER+.SYSLOG.SYSTEM.sysname`

- This resource requires all users have Read access when selecting a job on spool, or issuing the OUTPUT command directly:

  `jesnode.userid.jobname.jobid.jesdsname.ddname`

- This resource requires all users have Read access when selecting the execution JCL using the JJCL command:

  `jesnode.userid.jobname.jobid.JCL`

## FACILITY Class

Access is required to the following FACILITY class resources so you can:

- Define MVS log streams
- Allow the dynamic install utility to APF authorize load libraries
- Permit access to various MQSeries Queue Managers
- Allow access to USS commands

**FACILITY Class**

- The administrator, or user defining the CA SYSVIEW log streams, requires ALTER authority to the following resource:

  `MVSADMIN.LOGR`

- The administrator, or user defining the CA SYSVIEW log streams requires ALTER authority to the following resource:

  `MVSADMIN.XCF.CFRM`

- The administrator, or user defining the CA SYSVIEW log streams requires ALTER authority to the following resource:

  `XLSTR.`*`cf_structure_name`*

- The CA SYSVIEW started tasks and any individual user IDs requiring access to data from MQ needs READ authority to the specific MQ subsystem.

  *`ssid`*`.MQM`

- Grant READ authority to users in lieu of a default UID(0) to let them switch in and out of SUPERUSER.

  `BPX.SUPERUSER`

## LOGSTRM Class

The LOGSTRM class is used to secure access to MVS log streams.

**LOGSTRM Class**

- The CA SYSVIEW main address space requires UPDATE authority to write records to the log streams.

  *`log.stream.name`*

- The administrator, or user defining the CA SYSVIEW log streams, requires ALTER authority to change or alter the characteristics of the log stream.

  *`log.stream.name`*

- All users require READ authority to read data from the log stream.

  *`log.stream.name`*

## OPERCMDS Class

The OPERCMDS class is used to secure access to MVS operator commands.

**OPERCMDS Class**

- The user requires UPDATE authority to issue the STOP command for any of the CA SYSVIEW started tasks.

  ```
  MVS.STOP.STC.**
  ```

- The user requires UPDATE authority to issue the START command for any of the CA SYSVIEW started tasks.

  ```
  MVS.START.STC.**
  ```

- The user requires UPDATE authority to issue the MODIFY command for any of the CA SYSVIEW started tasks.

  ```
  MVS.MODIFY.STC.**
  ```

- The user requires UPDATE authority to issue the MVS or XMVS command. Access to the appropriate resource in the OPERCMDS class will also be checked.

  MVS.*mvscommand*.**

## UNIXPRIV Class

The UNIXPRIV class is used to secure access to Unix System Services (USS) commands.

**UNIXPRIV Class**

- Users require READ authority to see all USS processes from the UPROCESS display.

  ```
  SUPERUSER.PROCESS.GETPSENT
  ```

  **Note:** Use this resource in place of granting the user access to BPX.SUPERUSER in the FACILITY class, or having a default UID of 0. By default, you will only see processes running with the same UID/GID as your user ID.

- Grant READ authority to users that issue the UFILESYS command to view USS file systems. This prevents any security errors.

  ```
  SUPERUSER.FILESYS
  ```

  **Note:** Use this resource in place of granting the user access to BPX.SUPERUSER in the FACILITY class, or having a default UID of 0.

- Grant users READ authority to use the UKILL command to terminate any USS process.

  ```
  SUPERUSER.PROCESS.KILL
  ```

  **Note:** This could be done in place of granting the user access to BPX.SUPERUSER in the FACILITY class, or having a default UID of 0. By default, you will only be able to kill USS processes owned by your UID/GID.

## MQCONN Class

The MQCONN class is used to secure access to MQSeries connections.

**MQCONN Class**

- The CA SYSVIEW started task and individual user IDs require READ authority to the following resource to connect to WebSphere MQ.

  *ssid*.BATCH

## MQQUEUE Class

The MQQUEUE class is used to secure access to MQSeries queues.

**MQQUEUE Class**

- The CA SYSVIEW started task and individual user IDs require UPDATE authority to issue commands to WebSphere MQ through the system command queue.

  *ssid*.SYSTEM.COMMAND.**

- The CA SYSVIEW started task and individual user IDs require UPDATE authority to create temporary dynamic queues in which the queue manager puts replies from the display commands issued to the system command queue.

  *ssid*.SSID.**

## MQCMDS Class

The MQCMDS class is used to secure access to MQSeries commands.

**MQCMDS Class**

- The CA SYSVIEW started task and individual user IDs require READ authority to the following resource to issue display commands to WebSphere MQ.

  Resource:

  *ssid*.DISPLAY.**

# SERVAUTH Class

The SERVAUTH class is used to secure access to TCP/IP stacks.

**SERVAUTH Class**

- This resource allows access to the TCP/IP stacks. The CA SYSVIEW started task and individual user IDs requiring access to TCP/IP or CSM (Communications Storage Manager) commands will need READ authority to this resource.

  ```
  EZB.STACKACCESS.**
  ```

- This resource allows access to the NETSTAT commands. The CA SYSVIEW started task and individual user IDs requiring access to NETSTAT commands will need READ access to this resource.

  ```
  EZB.NETSTAT.**
  ```

- CSM commands use the Communications Server Network Management Interface to gather CSM data. READ authority to this resource is required for CSM monitoring, or the ability to issue any CSM commands. If the resource is not defined, then SUPERUSER access, or access to BPX.SUPERUSER in the FACILITY class, is required.

  ```
  IST.NETMGMT.mvsname.SNAMGMT
  ```

  ***mvsname***

  Represents the z/OS system name.

  **Note:** Superuser authority is either a UID of 0 or READ access to the BPX.SUPERUSER entity of the FACILITY class.

  **Note:** The VTAM start option, SNAMGMT, must be set to YES, so that the ISTMGCEH subtask will be attached to open the Network Management Interface.

# Chapter 6: Controlling Access Using SAF

This section contains the following topics:

## Overview of SAF

You can use your external security in lieu of the internal security to provide access to commands, subcommands, job names, and resources.

SAF calls made for various CA SYSVIEW entities determine whether to permit access.

Review the following external security guidelines:

- CA SYSVIEW always checks the internal security first unless 'Bypass internal security call' is set to YES in the External Security Section (see page 108) of the User Group.
- If the internal security fails the access, external security cannot override the failed access by permitting access to the resource.
- Grant external security full control using one of the following settings:
  - Set all internal security rules to allow access to all commands, job names, and resource.
  - Set the ‘Bypass internal security call’ to YES.
- If SAF is unavailable, access is granted to only users in the ADMIN group while your external security is not active.
- The following special characters are translated to a dash (‘-‘) in the Entity Name that is used for the SAF call:

  !`~#%¬&*()_+=¦\{}¢|<>:;"'?/,

**Note:** For more information, see the online Help topic Implementing External Security from the TOPICS command.

# Enable  SAF Entity Checking

SAF calls determine whether to permit access to various CA SYSVIEW entities.

**Follow these steps:**

1. Access the External Security Section of the group definition.
2. Define a SAF entity class in the internal security group or specify a SAF entity class in the GLOBAL group to have it apply to all users.

   **Note:** Defining a class name for the internal group of the user (DEFAULT) overrides the class name defined in the GLOBAL group.

SAF entity checking is enabled.

**More information:**

External Security Section Display (see page 108)

# SAF Entity Types

The security entity format used when calling SAF varies depending on the type of entity to validate. Each entity always starts with the SAF entity name prefix defined in the external security section of internal user group, where the default is SV.

The following descriptions require you to set the default of Yes in the external security section of internal user group for:

- Use System SMFID in Entity Name
- Use System QUAL in Entity Name

**More information:**

External Security Section Display (see page 108)

## ENV—Control Interfaces

The ENV entity controls which interfaces you can use for logging on to CA SYSVIEW.

The ENV entity has the following format:

SV.ENV.*system*.*interface*

***system***

Specifies the SMF system ID.

***interface***

Specifies API, BATCH, CICS, ETSO, ISPF and VTAM.

Read access is required to verify the interface.

## CMND—Control Primary Command Access

The CMND entity controls access to CA SYSVIEW primary commands.

The CMND entity has the following format:

SV.CMND.*system*.*command*

***system***

Specifies the SMF system ID.

***command***

Specifies the CA SYSVIEW primary command.

Read access is required to verify a command.

## SUBC—Control Subcommand Access

The SUBC entity controls access to CA SYSVIEW subcommands.

The CMND entity has the following format:

SV.SUBC.*system.command.subcommand*

***system***

Specifies the SMF system ID.

***command***

Specifies the CA SYSVIEW primary command.

***subcommand***

Specifies the subcommand of the primary command.

Read access is required to verify a subcommand.

## JOBN—Control Job Access and Action

The JOBN entity controls access to jobs, actions taken against jobs, and access to output files based on the job name.

- The JOBN entity to control job access has the following format:

  SV.JOBN.*system.qualifier.jobname*

  ***system***

  Specifies the SMF system ID.

  ***qualifier***

  Specifies the JES subsystem name.

  ***jobname***

  Specifies the job name of the job.

  Read access is required for this format of the JOBN entity.

- The JOBN entity used to control actions taken against jobs.

  This JOBN entity has the following format:

  SV.JOBN.*system.qualifier.jobname*.AC.*action*

  ***system***

  Specifies the SMF system ID.

  ***qualifier***

  Specifies the JES subsystem name.

***jobname***

Specifies the job name of the job.

The following are valid actions and access requirements:

- DSAL shows the allocated data sets.

  **Access:** Read

- MODL shows the loaded modules.

  **Access:** Read

- NSWP makes a job not swappable.

  **Access:** Update

- PRIV shows the private storage usage.

  **Access:** Read

- RPLY replies to a WTOR.

  **Access:** Read

- SWAP makes a job swappable.

  **Access:** Update

***action***

Specifies the action the user is taking against the job.

The following are valid actions and access requirements:

- ALTI alters a job on the input queue.

  **Access:** Update

- ALTO alters a job on the output queue.

  **Access:** Update

- ALTS alters storage for an executing job.

  **Access:** Update

- CANC cancels a job.

  **Access:** Update

- COPY copies the output of a job.

  **Access:** Read

- DEL deletes a job or the job output.

  **Access:** Update

- HOLD holds a job or the job output.

  **Access:** Update

  - LIST lists the output files for a job.

    **Access:** Read

  - REL releases a job or the job output.

    **Access:** Update

  - REST restarts a job.

    **Access:** Update

  - SEL selects a job to display the output.

    **Access:** Read

  - FORC Forces a job from the system.

    **Access:** Update

  - QUIE quiesces an executing job.

    **Access:** Update

  - RESU resumes an executing job.

    **Access:** Update

  - KILL kills a job.

    **Access:** Update

- The JOBN entity used to control access to output files for a job.

  This JOBN entity has the following format:

  `SV.JOBN.`*`system.qualifier.jobname`*`.DDNM.`*`ddname`*

  ***system***

  Specifies the SMF system ID.

  ***qualifier***

  Specifies the JES subsystem name.

  ***jobname***

  Specifies the job name of the job.

  ***ddname***

  Specifies the ddname for the output file.

  Read access is required for this format of the JOBN entity.

- The JOBN entity used to control actions against output files for a job.

  This JOBN entity has the following format:

  SV.JOBN.*system*.*qualifier*.*jobname*.DDNM.*ddname*.AC.*action*

  ***system***

  Specifies the SMF system ID.

  ***qualifier***

  Specifies the JES subsystem name.

  ***jobname***

  Specifies the job name of the job.

  ***ddname***

  Specifies the ddname for the output file.

  ***action***

  Specifies the action taken against the job output file.

  The actions and access required are the same as the ones listed previously for job names.

## JTYP—Control Job Access Based on Job Type

The JTYP entity controls access to jobs based on job type.

The JTYPE entity has the following format:

SV.JTYP.*system*.*qualifier*.*jobtype*

***system***

Specifies the SMF system ID.

***qualifier***

Specifies the JES subsystem name.

***jobtype***

Specifies the job type of the job.

The following are valid job types and the access requirements:

- ATX indicates an APPC transaction.

  **Access:** Read

- INI indicates an initiator.

  **Access:** Read

- JOB indicates a batch job.

  **Access:** Read

- OTX indicates an OMVS transaction.

  **Access:** Read

- STC indicates a started task.

  **Access:** Read

- SYS indicates a system task.

  **Access:** Read

- TSU indicates a TSO user.

  **Access:** Read

## NTFY—Control Job Access Based on Notify

The NTFY entity controls access to jobs based on the NOTIFY value on the JOB statement for the job.

The NTFY entity has the following format:

```
SV.NTFY.system.qualifier.notify
```

***system***

Specifies the SMF system ID.

***qualifier***

Specifies the JES subsystem name.

***notify***

Specifies the notify value of the job.

## USER—Control Job Access Based on User ID

The USER entity controls access to jobs based on the user ID value for the job.

If the USER entity checks allow access, then all other job name checks are skipped. The USER entity is the first check when a SAF job name (JOBN) call is made.

The USER entity has the following format:

SV.USER.*system.qualifier.userid*

***system***

Specifies the SMF system ID.

***qualifier***

Specifies the JES subsystem name.

***user***

Specifies the user ID for the job.

Optionally, you can include actions with the USER entity.

The USER entity with an action has the following format:

SV.USER.*system.qualifier.userid*.AC.*action*

***action***

Specifies the action taken against the job.

The actions and access required are the same as the ones listed previously for job names.

**Note:** See the section on the CHKA entity (see page 149) for information about including actions with the USER entity.

## WTRN—Control Writer Access

The WTRN entity controls access to jobs based on the name of the writer for the job output.

The WTRN entity has the following format:

```
SV.WTRN.system.qualifier.writer
```

***system***

Specifies the SMF system ID.

***qualifier***

Specifies the JES subsystem name.

***writer***

Specifies the writer for the job output.

Read access is required for the WTRN entity.

## RESN—Control Resource Access

The RESN entity controls access to resources, for example, a printer. The FIELD resource type checks access to fields on the CA SYSVIEW displays and the CMDGROUP resource checks access to security command groups.

The RESN entity has the following format:

```
SV.RESN.system.restype.qualifier.resvalue
```

***system***

Specifies the SMF system ID.

***restype***

Specifies the resource type.

***qualifier***

Specifies the resource qualifier.

***resvalue***

Specifies the resource value.

Read access is required for this format of the RESN entity.

**Note:** For the type of resources, see the Resources Section Detail Display (see page 65) section in the chapter "Security Displays."

Optionally, you can include actions with the RESN entity to control actions taken against resources.

The RESN entity with an action has the following format:

SV.RESN.*system.restype.qualifier.resvalue*.AC.*action*

***action***

Specifies the action the user is taking against the job. The actions and access required are the same as the ones listed previously for job names.

**ACTV**

Activates a resource.

**Access:** Update

**ADDR**

Adds a resource

**Access:** Update

**ADVA**

Advances a resource

**Access:** Update

**ALCR**

Allocates a resource.

**Access:** Update

**ALTR**

Alters a resource.

**Access:** Update

**BACK**

Backspaces a resource.

**Access:** Read

**CANR**

Cancels a resource.

**Access:** Update

**CKPT**

Checkpoints a resource.

**Access:** Update

**CLOS**

Closes a resource.

**Access:** Update

**CLRR**

Clears a resource.

**Access:** Update

**CLSD**

Closes a destination.

**Access:** Update

**DEAC**

Deactivates a resource.

**Access:** Update

**DEFR**

Defines a resource.

**Access:** Update

**DELR**

Deletes a resource.

**Access:** Update

**DEQU**

Dequeues a resource.

**Access:** Update

**DISA**

Disables a resource.

**Access:** Update

**DRNR**

Drains a resource.

**Access:** Update

**DUMP**

Dumps a resource.

**Access:** Update

**ENAB**

Enables a resource.

**Access:** Update

**EXCL**

Restricts a resource.

**Access:** Update

**FORR**

Forces a resource.

**Access:** Update

**FORW**

Forwards a resource.

**Access:** Update

**FREE**

Frees a resource.

**Access:** Update

**FRMT**

Formats a resource.

**Access:** Update

**HALT**

Halts a resource.

**Access:** Update

**HOLD**

Holds a resource.

**Access:** Update

**IDBD**

Issues an IMS DBD command.

**Access:** Update

**IDBR**

Issues an IMS DBR command.

**Access:** Update

**IDLE**

Idles a resource.

**Access:** Update

**IERE**

Issues an IMS ERE command.

**Access:** Update

**INIT**

Initializes a resource.

**Access:** Update

**INRE**

Issues an IMS NRE command.

**Access:** Update

**INTR**

Interrupts a resource.

**Access:** Update

**IOVF**

Issues the IMS command:

```
DISPLAY AREA areaname IOVF
```

**Access:** Update

**KILR**

Kills a resource.

**Access:** Update

**LOCK**

Locks a resource.

**Access:** Update

**MAST**

Assigns master status to a resource.

**Access:** Update

**MNT**

Mounts a resource.

**Access:** Update

**NEWR**

Loads a new copy of a resource.

**Access:** Update

**OPEN**

Opens a resource.

**Access:** Update

**PURG**

Purges a resource.

**Access:** Update

**RELR**

Releases a resource.

**Access:** Update

**REPT**

Repeats a resource.

**Access:** Update

**REQR**

Requeues a resource.

**Access:** Update

**REST**

Restarts a resource.

**Access:** Update

**RESU**

Resumes a resource.

**Access:** Update

**SCFW**

Issues a SETCACHE CACHEFASTWRITE for the resource.

**Access:** Update

**SDEV**

Issues a SETCACHE DEVICE for the resource.

**Access:** Update

**SDFW**

Issues a SETCACHE DASDFASTWRITE for the resource.

**Access:** Update

**SEND**

Sends a resource.

**Access:** Update

**SHUT**

Shuts a resource.

**Access:** Update

**SNVS**

Issues a SETCACHE NVS for the resource.

**Access:** Update

**SSUB**

Issues a SETCACHE SUBSYSTEM for the resource.

**Access:** Update

**STOP**

Stops a resource.

**Access:** Update

**STRT**

Starts a resource.

**Access:** Update

**SWIT**

Switches a resource.

**Access:** Update

**TERM**

Terminates a resource.

**Access:** Update

**TROF**

Turns off a trace.

**Access:** Update

**TRON**

Turns on a trace.

**Access:** Update

**UNL**

Unloads a resource.

**Access:** Update

**UNLK**

Unlocks a resource.

**Access:** Update

**VOFF**

Varies a resource offline.

**Access:** Update

**VON**

Varies a resource online.

**Access:** Update

**XSCN**

Creates a cross-system connection to the resource.

**Access:** Update

In addition to the resources listed in Chapter 4, the FIELD resource type is used to verify access to fields on CA SYSVIEW displays.

The RESN entity that is used to control display fields has the following format:

`SV.RESN.`*`system`*`.FIELD.`*`command`*`.`*`fieldname`*

***system***

Specifies the SMF system ID.

***command***

Specifies the command that is displaying the field.

***fieldname***

Specifies the field name.

Read access is required to display the field.

For information about bypassing field name checking, see the CHKF entity.

CMDGROUP is another resource used to verify access to security command groups.

The RESN entity that is used to control command groups has the following format:

SV.RESN.*system*.CMDGROUP.*groupname*

***system***

Specifies the SMF system ID.

***groupname***

Specifies the security group name.

If read access is granted to this entity, the command group is allowed.

## JQUE—Control Job Queue Access

The JQUE entity controls access to jobs based on job queue.

The JQUE entity has the following format:

SV.JQUE.*system*.*qualifier*.*jobqueue*

***system***

Specifies the SMF system ID.

***qualifier***

Specifies the JES subsystem name.

***jobqueue***

Specifies the job queue for the job.

The following are valid job queues and access requirements:

- CONV indicates a conversion queue.

  **Access:** Read

- EXEC indicates an execution queue.

  **Access:** Read

- OUTP indicates an output queue.

  **Access:** Read

- PURG indicates a purge queue.

  **Access:** Read

- RECV indicates a receiver queue.

  **Access:** Read

- RDR indicates a reader queue.

  **Access:** Read

- XMIT indicates a transmitter queue.

  **Access:** Read

## CHKA—Check Actions

The CHKA entity controls whether actions are included on USER entities.

If the USER entity checks allow access

If read access is granted to this entity, an action is included when performing USER entities check.

The CHKA entity has the following format:

```
SV.CHKA.system
```

***system***

Specifies the SMF system ID.

**Note:** See the USER Entity section for the format of the USER entity when an action is included.

## CHKF—Check Display Fields

The CHKF entity controls whether to perform field checks on the displays.

If read access is granted to this entity, an action is included when performing USER entities checks.

If read access is granted to this entity, display field checks are performed for all CA SYSVIEW formatted displays. To control the display fields, use the RESN entity with a resource type of FIELD.

The CHKF entity has the following format:

```
SV.CHKF.system
```

***system***

Specifies the SMF system ID.

## CHKU—Control Job Name Checks

The CHKU entity controls whether job name checks are bypassed when USER, NOTIFY, or the job name match the user ID of the user. The following job name checks are bypassed: job class, output class, destination, writer name, job type, job queue, output file DD names and actions.

If read access is granted to this entity, the previously listed job name checks are bypassed if the USER, NOTIFY, or the job name of the job match the user ID of the user.

The CHKU entity has the following format:

```
SV.CHKU.system
```

***system***

Specifies the SMF system ID.

## NQDQ—Control Interface Access

The NQDQ entity controls whether to allow simultaneous access to CA SYSVIEW from multiple interfaces. If read access is granted to this entity, the user can only log on to CA SYSVIEW from one interface at a time.

The NQDQ entity has the following format:

```
SV.NQDQ.system
```

***system***

Specifies the SMF system ID.

## WARN—Control Warn Mode

The WARN entity controls whether warn mode is in effect for the user or for a specific entity type.

If warn mode is on for the user, the results from all SAF calls are recorded in the job log of the user. If warn mode is on for a specific entity, then only calls for that entity are recorded in the job log. When warn mode is in effect, the results are recorded in the job log and access to the entity is always allowed. Warn mode is convenient for displaying which entities had a security check without failing access to the entities. Warn mode is also helpful for debugging purposes.

The WARN entity has the following format:

SV.WARN.*system.userid*

***system***

Specifies the SMF system ID.

***userid***

Specifies the user ID of the user.

If read access is granted to this entity, all SAF calls are recorded in the job log and access to all entities is allowed.

The WARN entity for a specific entity has the following format:

SV.WARN.*system.entitytype*

***system***

Specifies the SMF system ID.

***entitytype***

Specifies the type of entity.

When read access is granted to this entity:

- The SAF calls for the entity are recorded in the job log
- The access to the entity is allowed

**Note:** See HELP GSV4204I for a description of the trace message format.

## SUSP—Control Suspend Mode

The SUSP entity controls whether suspend mode is in effect for the user or for a specific entity type.

If suspend mode is on for the user, no SAF checks are made and access to all entities is allowed. If suspend mode is on for a specific entity, then only calls for that entity are skipped and access to the entity is allowed.

The SUSP entity for user suspend mode has the following format:

```
SV.SUSP.system.userid
```

***system***

Specifies the SMF system ID.

***userid***

Specifies the user ID of the user.

If read access is granted to this entity, all SAF calls are skipped and access to all entities is allowed.

The SUSP entity for a specific entity has the following format:

```
SV.SUSP.system.entitytype
```

***system***

Specifies the SMF system ID.

***entitytype***

Specifies the type of entity.

If read access is granted to this entity, SAF calls for the entity are skipped and the access to the entity is allowed.

If the entity type is RESN, then SAF calls may also be suspended for a particular resource type by granting read access to:

```
SV.SUSP.system.RESN.resourcetype
```

Where *resourcetype* is one of the resource types listed in the Resources Section Detail display. For example, CATALOG,CPU, DEST, MVSCMD, and so on.

# Chapter 7: Preparing the SAFSAMPX Sample Exit

This section contains the following topics:

## Purpose of the Exit

Using the sample exit is optional. The sample SAFSAMPX exit point is provided to let you examine and modify the SAF entity and class name before being passed to SAF for authentication. CA SYSVIEW calls the exit:

- Before calling SAF.
- When a user terminates their session.

**Note:** No SAF entity name is associated with the termination call.

## Define an Exit Using the Sample Exit

Define an exit for your site by customizing the sample exit.

**Follow these steps:**

1. Locate the sample exit shell provided in *sysview*.CNM4BSAM(SAFSAMPX) and customize it to suit the needs of your site.
2. Modify the SAF Exit Name field of the user External Security Section of their internal security group.
3. If you use the same exit for all users, define it in the GLOBAL group.

The exit is defined.

# Exit Specifications

The exit will not be called authorized. If you plan on using any privileged instructions, place the exit into an APF authorized library. The exit is called in 31-bit AMODE.

- Registers on Entry

```
R0 - Entry code (decimal)

     00 - SAF entity is for an initialization call

     04 - SAF entity is for a command validation call

     08 - SAF entity is for a job name validation call

     12 - SAF entity is for a resource validation call

     16 – Termination call (No SAF entity passed)

R1 - Security parameter area address,
     mapped by DSECT SECC#### in macro ZSECC

R2/12 - Work registers

R13 - Save area

R14 - Return address

R15 - Entry address
```

- Registers on Exit

```
R0 - N/A

R1 - N/A

R2/12 - Contents on entry

R13 - Save area

R14 - Return address

R15 - Return code

     00 - Use SAF to decide

     04 - Bypass SAF, allow request

     08 - Bypass SAF, fail request
```

# What Register 1 Points To

Register 1 points to the data passed to the security exit, formatted as shown in the following example. This data is mapped by the ZSECC macro in the *sysview*.CNM4BMAC data set.

```
                      MACRO
                      ZSECC ,
SECC####              DSECT ,
*
SECC_Access           DS    XL1             Access flag
Access_Prompt         EQU   X'80'               Prompt for password
Access_Fail           EQU   X'08'               Fail command
Access_Msg            EQU   X'04'               Display msg on console
Access_Allow          EQU   X'01'               Allow command
*
SECCFLAG              DS    XL1             Control flag
SECRACT               EQU   X'80'               Security is active
NLOGCALL              EQU   X'40'               NO-LOG call
USESYST               EQU   X'20'               Use resource system
USEQUAL               EQU   X'10'               Use resource qualifier
SECCFCIM              EQU   X'08'            Fail cmd in mult grps
SECCJSPL              EQU   X'04             Use JESSPOOL for JOBV
*
SECCCODE              DS    XL1             Command code
SUBCMND               EQU   X'10'               Subcommand
PRIMCMND              EQU   X'08'               Primary command
*
SECCENV               DS    XL1             Environment flag
TSOENV                EQU   X'80'               TSO
CICSENV               EQU   X'40'               CICS
VTAMENV               EQU   X'20'               VTAM
SPFENV                EQU   X'08'               ISPF
BATENV                EQU   X'04'               BATCH
ETSOENV               EQU   X'02'               Roscoe/etso
APIENV                EQU   X'01'               Api
*
SECCGRPN              DS    CL8             Group name
SECCUSER              DS    CL8             User
SECCACTV              DS    CL8             Active command
SECCCMDA              DS    F               Pointer to command
SECCCMDL              DS    H               Length of command entered
SECCPRML              DS    H               Parameter length
SECCPRMA              DS    F               Pointer to parameters
*
SECCJESN              DS    CL4             JES subsystem name
SECCJCTA              DS    F               Pointer to JCT
SECCSYST              DS    CL4             SMF system ID
SECCRESQ              DS    CL8             Resource qualifier
```

```
SECCREST              DS    CL8             Resource type
SECCRESV              DS    CL48            Resource value
SECCDSNM              EQU   SECCRESV,44     Output file dsname
SECCPASS              EQU   SECCRESV,17     Not used
SECCJOBN              DS    CL8             Jobname
SECCWTRN              DS    CL8             Writer name for output
SECCNTFY              DS    CL8             NOTIFY from JOB card
SECCJTYP              DS    CL3             Type (STC,TSU,JOB,INI,ATX)
SECCJNUM              DS    CL7             Job number
SECCDDNM              DS    CL8             DDname of output file
SECCSUSR              DS    CL8             Security user id for job
SECCSLBL              DS    CL8             Security label for job
SECCNODN              DS    CL8             JES node name
SECCOGRP              DS    CL8             Output group name
*
SECCJQUE              DS    XL1             Job queue
*
         AIF   (D'JQUEOUTP).SKPJQUE
*
JQUEOUTP              EQU   X'80'               Output
JQUEEXEC              EQU   X'40'               Executing
JQUEINP               EQU   X'20'               Input
JQUERDR               EQU   X'10'               Reader
JQUECONV              EQU   X'08'               Converter
JQUEXMIT              EQU   X'04'               Transmit
JQUERECV              EQU   X'02'               Receive
JQUEPURG              EQU   X'01'               Purge
.SKPJQUE              ANOP  ,
*
SECCACTC              DS    XL1             Action code
*
SECCMSGT              DS    XL1             Message type
SECCMSGA              EQU   X'80'               Action
SECCMSGE              EQU   X'40'               Error
SECCMSGW              EQU   X'20'               Warning
SECCMSGI              EQU   X'10'               Info
*
SECCMSG               DS    CL79            Message to be displayed
*
SECCFLG2              DS    X               Flag byte
SEC2DPRM              EQU   X'80'           Don't prompt for password
*
SECCINTC              DS    XL1             Interface code
INTCAPI               EQU   001                API
INTCBATC              EQU   002                Batch
INTCCICS              EQU   003                CICS
INTCISPF              EQU   005                ISPF
INTCLCLD              EQU   006                LCL3270D
INTCTSO               EQU   007                TSO
```

```
INTCVTAM              EQU   008                VTAM
INTCCAPT              EQU   009                Capture
INTCXSSI              EQU   010                Cross system
INTCXSXI              EQU   INTCXSSI           Cross system
*
SECC_Access_Intent    DS    XL1             Access intent for entity
SECC_READ             EQU   X'02'           READ access
SECC_UPDATE           EQU   X'04'           UPDATE access
SECC_CONTROL          EQU   X'08'           CONTROL access
SECC_ALTER            EQU   X'80'           ALTER access
*
SECC_SAF_EntityLen    DS    H               Length of Entity
SECC_SAF_EntityData   DS    CL255           Entity name
*
SECC_SAFClassLen      DS    AL1             Length of class
SECC_SAFClassName     DS    CL8             Class name
*
SECCRSV1              DS    H               Reserved
SECCEND               DS    0D              Align to doubleword
*
SECCL                 EQU   *-SECC####      SECC length
SECL                  EQU   SECCL           Alias for SECCL
SECC                  EQU   SECC####,SECL   SECC name with len attr
*
USERWORK              DS    XL512           User work area
                      ORG   USERWORK        Reset location counter
                      MEND  ,
```

## SECC_Access Field and Equates

The SECC_Access field contains actions that CA SYSVIEW should take for calls made to the exit.

The SECC_Access field has the following features:

- If internal security sets the Access_Fail bit, and the security exit sets the Access_Allow equate, the Access_Allow equate is ignored. The security exit cannot grant access once internal security has failed the access.
- If security is handled by the security exit, change all the security groups in the internal security to allow use of all commands, job names, and resources.

Equates for the SECC_Access field:

**Access_Prompt**

Valid only during the user verification call. Specifying Access_Prompt causes CA SYSVIEW to reprompt for a password and to make another initialization call to the security exit.

For information about passing back a message from the security exit, see the SECCMSGT and SECCMSG fields.

**Access_Fail**

Usage is not authorized.

**Access_Msg**

The security exit causes CA SYSVIEW to write a message to the console. One of the following messages is written:

- GSVX015I - Job was accessed.
- GSVX014I - Command was used.
- GSVX036I - Usage was denied.
- GSVX040I - Resource was altered.
- The message passed back from the security exit, if applicable.

For information about passing back a message from the security exit, see the SECCMSGT and SECCMSG fields.

**Access_Allow**

Usage is authorized. This is always set for an initialization call.

## SECCFLAG Field

The SECCFLAG field contains status information.

Equates in the SECCFLAG field:

**SECRACT**

Internal security has initialized successfully.

**NLOGCALL**

CA SYSVIEW is verifying whether the user can use a command or access a job. NLOGCALL is always set for an initialization call. The security exit checks whether the user has access without actually causing an access violation when the user is not authorized. This method of security checking is typically used to suppress unauthorized commands from menus. The user is not actually using the command; instead, the security exit checks whether the user could even try to use it.

## SECCCODE Field

The SECCCODE field describes the type of command passed by address in SECCCMDA.

The following table explains each equate in the SECCCODE field:

**SUBCMND**

The command passed is a subcommand of the active command.

**PRIMCMND**

The command passed is a primary command.

## SECCENV Field

The SECCENV field describes the environment from which you are accessing CA SYSVIEW.

The following equates are in the SECCENV field:

**TSOENV**

If set, you are running under TSO.

**CICSENV**

If set, you are running under CICS.

**VTAMENV**

If set, you are running through the VTAM interface.

**SPFENV**

If set, you are running under ISPF.

**BATENV**

If set, you are running through the batch interface.

**ETSOENV**

If set, you are running under ROSCOE/ETSO.

**APIENV**

If set, you are running through the API interface.

## SECCGRPN Field

The SECCGRPN field contains the name of the security group to which the user belongs.

The following table explains what the SECCGRPN field is setting:

| If the user | Field is set to |
|---|---|
| Belongs to a security group | Group name |
| Does not belong to a security group | DEFAULT |
| Is a CA SYSVIEW administrator | ADMIN or the security group the user belongs to |

## SECCUSER Field

The SECCUSER field contains the user ID of the user.

The following table explains the SECCUSER field:

| If you are running under | Field is set to |
|---|---|
| TSO or ISPF | The user TSO logon ID. |
| CICS | What the CA SYSVIEW CICS user ID exit routine passes back, or what the user enters on the user ID prompt screen. For a description of this exit, see the *Administration Guide*. |
| VTAM | What the user enters on the user ID prompt screen. |
| Batch interface | The batch jobs user ID. |
| API | The user ID of the user who invoked the API. If it is invoked under TSO, it is the user TSO logon ID. If it is invoked in a batch job, it is the user ID of the batch job. |

## SECCACTV Field

The SECCACTV field contains the command name of the active display command.

## SECCCMDA Field

The SECCCMDA field contains the address of the command entered by the user.

This field is valid only for command validation and initialization calls.

## SECCCMDL Field

The SECCCMDL field contains the length of the command entered by the user.

This field is valid only for command validation and initialization calls.

## SECCPRML Field

The SECCPRML field contains the length of the parameters entered by the user.

This field is valid only for command validation calls.

## SECCPRMA Field

The SECCPRMA field contains the address of the parameters entered by the user.

This field is valid only for command validation calls.

## SECCJESN Field

The SECCJESN field contains the JES subsystem name.

## SECCJCTA Field

The SECCJCTA field contains the address of the JES2 Job Control Table (JCT) control block for the job name being validated.

The following usage notes apply to the SECCJCTA field:

- The address of the JCT is valid only for the duration of the job name validation call.
- The JCT storage is reused for each job name validation call.
- Use the JCTSTART field in the $JCT macro as the base when using the SECCJCTA address.
- This field applies when a job name validation call is made from the APPCOUTQ, JHELDQUE, JJOBQUE, JOBSUM, JOUTQUE, LISTINP, LISTFILE, OUTDES, or OUTPUT command. Job name validation calls by other commands set the field to 0.
- This field is set to 0 unless the following two values are set:
    1. The SAF exit name was specified in the External Security section of the internal security group for the user.
    2. The Pass JES JCT addr to SAF exit value is YES.

## SECCSYST Field

The SECCSYST field contains the SMF system ID.

## SECCRESQ Field

The SECCRESQ field contains the resource qualifier.

## SECCREST Field

The SECCREST field contains one of the resource types listed in the chapter "Security Displays (see page 45)." See that section for more information about the contents of the SECCREST field.

## SECCRESV Field

The SECCRESV field contains the value for the resource type specified in the SECCREST field. The value for the FIELD resource is in uppercase.

## SECCDSNM Field

The SECCDSNM field contains the output file data set name on a job name validation call when the SECCDDNM field is filled in.

You should check the SECCDDNM field before this field. If the SECCDDNM field contains a ddname, then this field contains the output file data set name.

## SECCJOBN Field

The SECCJOBN field contains the name of the job to validate on a job name validation call.

If the user enters a line command that affects the job, the field is set to the job name of the job the user is trying to affect.

## SECCWTRN Field

The SECCWTRN field contains the writer name for the job being validated. This field contains hexadecimal zeros when it does not apply.

## SECCNTFY Field

The SECCNTFY field contains the contents of the NOTIFY field from the JOB statement. This field contains hexadecimal zeros when it does not apply.

## SECCJTYP Field

The SECCJTYP field contains the type of job.

Valid values for the SECCJTYP field are shown in the following table:

| Job Type | Field Setting |
|---|---|
| Batch | JOB |
| Started task | STC |
| TSO user | TSU |
| Initiator | INI |
| System task | SYS |
| APPC transaction | ATX |

## SECCJNUM Field

The SECCJNUM field contains the job number for the job in character format.

## SECCDDNM Field

The SECCDDNM field contains the ddname of the output file when the LISTFILES command makes job name validation calls. The SECCDDNM field is also used when a line command is used on an output file from the Output Files display.

This field contains hexadecimal zeros when it does not apply.

## SECCSUSR Field

The SECCSUSR field contains the security user ID for the job or output for a job name validation call.

## SECCSLBL Field

The SECCSLBL field contains the security label for the job or output for a job name validation call.

## SECCNODN Field

The SECCNODN field contains the JES node name for the current system.

## SECCOGRP Field

The SECCOGRP field contains the output group name for a selected output file when you use the following commands:

- JJOBQUE
- JHELDQUE
- JOUTQUE

This field contains hexadecimal zeros when it does not apply.

## SECCJQUE Field and Equates

The SECCJQUE field describes the job queue for the job.

The following table explains the SECCJQUE field equates:

| Equate is Set | If the Job Is on the |
|---|---|
| JQUEOUTP | Output queue |
| JQUEEXEC | Execution queue |
| JQUEINP | Input queue |
| JQUERDR | Reader |
| JQUECONV | Converter queue |
| JQUEXMIT | Transmit queue |
| JQUERECV | Sysout receiver |
| JQUEPURG | Purge queue |

## SECCACTC Field

The SECCACTC field contains the hexadecimal code equivalent of the action performed by the user. For job name validation calls, the SECCJOBN field contains the job name.

For resource validation calls:

- The SECCREST field contains the resource type.
- The SECCRESQ field contains the resource qualifier.
- The SECCRESV field contains the resource value.

Equates for the hexadecimal codes are supplied in the ZACTC member of the *sysview*.CNM4BMAC data set.

## SECCMSGT Field and Equates

The SECCMSGT field contains the type of message being passed back from the security exit.

The following table explains the message-type equates in the SECCMSGT field.

| Equate | Message Type |
|---|---|
| SECCMSGA | Action. Some type of action is required from the user. |
| SECCMSGE | Error |
| SECCMSGW | Warning |
| SECCMSGI | Informational |

If the SECCMSGT field contains hexadecimal zeros, no message is passed back.

## SECCMSG Field

The SECCMSG field contains the message text being passed back from the security exit.

## SECCFLG2 Field

The SECCFLG2 field is a flag byte that contains the SEC2DPRM flag. If the SEC2DPRM flag is set, the security exit does not check or prompt the user for a password. This flag is set in cases in which it is not possible to prompt the user for a password; for example, the security report program.

## SECC_Acess_Intent

The SECC_Access_Intent field is a flag byte that contains the access intent of the security request; READ, UPDATE, CONTROL, or ALTER.

## SECC_SAF_EntityLen

The SECC_SAF_EntityLen field contains the half-word length of the entity name being passed to SAF.

## SECC_SAF_EntityData

The SECC_SAF_EntityData field contains the entity name being passed to SAF.

## SECC_SAFClassLen

The SECC_SAFClassLen field contains the 1-byte length of the class name being passed to SAF.

## SECC_SAFClassName

The SECC_SAFClassName field contains the 8-byte name of the class name being passed to SAF.

## USERWORK Field

The USERWORK field is the start of a 512-byte work area used to store data for the duration of the user session.

The field is cleared to hexadecimal zeros before the first call is made to the security exit.

# Index