



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

2.12.2

NOVEMBER 9, 2023

EFFECTIVE DATE

(11-09-2023)

PURPOSE

- (1) SACS Security command codes help guide.
- (2) This is the help guide to all SACS Security Command Codes.

MATERIAL CHANGES

- (1) IRM 2.12.2.1 Updating required Internal Controls. No other changes to the IRM in this version.

EFFECT ON OTHER DOCUMENTS

IRM 2.12.1, dated May 13, 2021, is superceded

AUDIENCE

IDRS Security Officers

Kaschit Pandya
Acting, Chief Information Officer

2.12.2

Security and Communication Services (SACS) Security Command Codes

Table of Contents

2.12.2.1 Program Scope and Objectives

- 2.12.2.1.1 Background
- 2.12.2.1.2 Authority
- 2.12.2.1.3 Roles and Responsibilities
- 2.12.2.1.4 Program Management and Review
- 2.12.2.1.5 Program Controls
- 2.12.2.1.6 Terms/Acronyms/ Definitions
- 2.12.2.1.7 Related Resources

2.12.2.2 ADDEM - Add Employee Security Record File (ESRF)

- 2.12.2.2.1 Format 1 : Add returning IDRS users or Console users to their previous unit
- 2.12.2.2.2 Format 2 : Add new or returning IDRS users or Console users to a different unit
- 2.12.2.2.3 Format 3 : Add new or returning IDRS users or Console users and specify all 10 digits of the Employee Number

2.12.2.3 ADMAF - Add Maximum Profile Authorization File (MPAF)

- 2.12.2.3.1 Format 1 : Create MPAF for a new unit
- 2.12.2.3.2 Format 2 : Delete MPAF for a unit
- 2.12.2.3.3 Format 3 : Create new units by copying command code bitmaps and characteristics from existing unit

2.12.2.4 ADTRM - Add a Terminal

- 2.12.2.4.1 Format 1 : Add a single terminal
- 2.12.2.4.2 Format 2 : Add multiple terminals
- 2.12.2.4.3 Format 3 : Remove a terminal

2.12.2.5 ADUNT - Add Unit Command Code Profile (UCCP)

- 2.12.2.5.1 Format 1 : Add the UCCP for a unit
- 2.12.2.5.2 Format 2: Delete the UCCP entry for a Unit
- 2.12.2.5.3 Format 3: Authorize Universal Access

2.12.2.6 ALLOW - Authorize USRs to input command codes UPEMP, RSTRK, and BYPAS for additional OIs within the same computing center

- 2.12.2.6.1 Format 1: Authorize USR to input command code at additional OI
- 2.12.2.6.2 Format 2: Remove USR ability to input command code at additional OI
- 2.12.2.6.3 Format 3: View USR permissions to input command codes at additional OIs
- 2.12.2.6.4 Format 4: View permissions to input command codes at additional OIs for all USRs

2.12.2.7 ASNPW - Assign Password

- 2.12.2.7.1 Format: Assign a password to an employee

2.12.2.8 ATSID - Display Available Terminal Security IDs

-
- 2.12.2.8.1 Format 1: Display all 2-character TSID prefix assigned to a Campus
 - 2.12.2.8.2 Format 2: Displays all available TSIDs at a Campus that start with a given 2-character TSID prefix
 - 2.12.2.9 BYPAS - Bypass Profile Restriction
 - 2.12.2.9.1 Format 1: Activate a temporary bypass to a restriction on an employee profile at a given campus
 - 2.12.2.9.2 Format 2: Remove a temporary bypass to a restriction on an employee profile at a given campus
 - 2.12.2.9.3 Format 3: Display all employees in a campus Designated User Listing (DUL) with a specific restriction bypass
 - 2.12.2.10 CMODE - Change Mode to a Different Service Center
 - 2.12.2.10.1 Format: Change Mode to a Different Service Center
 - 2.12.2.11 DIPID - Display Terminal PIDS Not Used for Six Months
 - 2.12.2.11.1 Format: Display Terminal PIDS Not Used for Six Months
 - 2.12.2.12 DISCC - Display Command Codes and their Attributes
 - 2.12.2.12.1 Format 1: Display the Command Code attributes of a specific Command Code
 - 2.12.2.12.2 Format 2: Display listing of all the Command Codes and their attributes in the SACS Command Code Table
 - 2.12.2.12.3 Format 3: Display listing of all the Command Codes and their attributes which are processed on the specified host processor
 - 2.12.2.12.4 Format 4: Display a listing of all the Command Codes and their attributes which are processed on the specified host processor
 - 2.12.2.12.5 Format 5: Display a listing of enabled or disabled Command Codes at the specified Campus
 - 2.12.2.13 DISGR - Display Command Code Groups
 - 2.12.2.13.1 Format 1: Display a list of all the Command Code Group names
 - 2.12.2.13.2 Format 2: Display a list of all Command Codes within a specific Command Code Group
 - 2.12.2.14 DISNC - Display Network Configuration Information
 - 2.12.2.14.1 Format 1: Display information about single network resources
 - 2.12.2.14.2 Format 2: Display multiple items by Resource or Connection type
 - 2.12.2.15 EXLET - Allow access to high profile TINs
 - 2.12.2.16 EXTAB - Add, Delete and Display the encrypted Exception Negative TINs List
 - 2.12.2.17 FIEMP - Find Employee
 - 2.12.2.18 LOKME - Employee Self Lock
 - 2.12.2.18.1 Format 1: Lock employee profile for a number of days
 - 2.12.2.18.2 Format 2: Lock employee profile until a specific date
 - 2.12.2.18.3 Format 3: Cancel employee lock request
 - 2.12.2.19 MDPCC - Modify Prohibited Command Code Table
 - 2.12.2.19.1 Format 1: Add command codes to/from the Prohibited Command Code Table (PCC)
 - 2.12.2.19.2 Format 2: Delete command codes to/from the Prohibited Command Code Table (PCC)
 - 2.12.2.20 MRINQ - Master Register Inquiry
 - 2.12.2.20.1 Format 1: Display employee history information using a Social Security Number key

-
- 2.12.2.20.2 Format 2: Display employee history information using an Employee Number key
 - 2.12.2.20.3 Format 3: Display employee history information using a Standard Employee Identifier (SEID) key
 - 2.12.2.20.4 Format 4: Display limited information for an employee when using the Social Security Number key
 - 2.12.2.20.5 Format 5: Display the next available Employee Number
 - 2.12.2.20.6 Format 6: Display a list of all Employee Numbers for a given Office Identifier and Sequence Number
 - 2.12.2.21 MRUPD - Master Register Update
 - 2.12.2.21.1 Format 1: Update a user's Social Security Number
 - 2.12.2.21.2 Format 2: Update a user's Investigation status and date
 - 2.12.2.21.3 Format 3: Update a user's Assignment or Origin dates
 - 2.12.2.21.4 Format 4: Display, update and delete workload management
 - 2.12.2.22 PIDTM - Display PID Usage
 - 2.12.2.22.1 Format 1: Display available PIDS at a given campus
 - 2.12.2.22.2 Format 2: Display PIDS in use at a given campus
 - 2.12.2.23 PWACT Set Password Management Function
 - 2.12.2.23.1 Format 1: PWACT HELP
 - 2.12.2.23.2 Format 2: PWACT
 - 2.12.2.24 PWMGT - IDRS Password Management
 - 2.12.2.25 REPTS - Authorizes user access to the IORS application
 - 2.12.2.26 RMODE - Research mode
 - 2.12.2.27 ROUTE - Display Campus Code, Number, Office Identifier, and Routing Status
 - 2.12.2.28 RSTRK - Restrict Profile
 - 2.12.2.28.1 Format 1: Add restrictions against a employee's profile for a given campus
 - 2.12.2.28.2 Format 2: Delete restrictions against a employee's profile for a given campus
 - 2.12.2.28.3 Format 3: Display the Command Codes that are restricted for a user role
 - 2.12.2.28.4 Format 4: Display all employees in a campus Designated User Listing (DUL) with a specific restriction
 - 2.12.2.28.5 Format 5: Display all employees (any or no restriction) in a campus DUL
 - 2.12.2.28.6 Format 6: Display the restriction and bypass history for a specific employee
 - 2.12.2.28.7 Format 7: Change an employee name in the DUL
 - 2.12.2.29 SECOP - Security Operation, Unlock a Terminal
 - 2.12.2.30 SETPW - Set Password Expiration Range for a Unit
 - 2.12.2.31 SFDIS - Display User Profile
 - 2.12.2.32 SFINQ
 - 2.12.2.32.1 Format 1: Display employee information
 - 2.12.2.32.2 Format 2: Display the employee's Production or Training Command Code Profiles
 - 2.12.2.32.3 Format 3: Display all employees in a Unit

-
- 2.12.2.32.4 Format 4: Display all Command Codes allowed in a Unit
 - 2.12.2.32.5 Format 5: Display for one or more Units a list of all employees' names, Employee Numbers, NULL Status, and authorized Foreign Locations Office Identifiers (OIDs)
 - 2.12.2.32.6 Format 6: Display, by terminal TSID, the employee number for any user signed on, or the allowed Time On/Off for that terminal
 - 2.12.2.32.7 Format 7: Display a list of the last usage dates for all Command Codes in a particular Unit
 - 2.12.2.32.8 Format 8: Display authorized Multiple Access (CMODE) locations
 - 2.12.2.32.9 Format 9: Display Password Management Status for a unit
 - 2.12.2.33 SINOFF - Sign off of IDRS
 - 2.12.2.34 SINON - Sign on to IDRS
 - 2.12.2.34.1 Format 1: SINON with Template
 - 2.12.2.34.2 Format 2: SINON with CASL macro
 - 2.12.2.35 SOMMSG - SINON Message Maintenance
 - 2.12.2.36 STATS - Display Terminal Statistics
 - 2.12.2.37 SWTCH - Update the Campus Domain Indicator
 - 2.12.2.37.1 Format 1: Query the Campus Domain Indicator Status
 - 2.12.2.37.2 Format 2: Set the status of the Campus Domain Indicator
 - 2.12.2.38 UNLEM - Unlock System Locked Employee
 - 2.12.2.39 UPCON - Add, Delete OR Display Restriction Record
 - 2.12.2.39.1 Format 1: Add or Delete a Restriction
 - 2.12.2.39.2 Format 2: Display Restrictions Record
 - 2.12.2.40 UPEMP - Update Employee
 - 2.12.2.40.1 Format 1: Change an employee (user) name, their Unit Number, their SAT or Programmer type (in Test only), their TRDB status, their Standard Employee Identifier (SEID), or their telephone number
 - 2.12.2.40.2 Format 2: Add / delete Command Code(s) to / from the user's Profile. This option also displays and changes their IMF - BMF status
 - 2.12.2.40.3 Format 3: Lock or unlock a user's Profile (unlocks system lock, security lock, or self lock) or delete a user
 - 2.12.2.40.4 Format 4: Delete an authorized Foreign Location
 - 2.12.2.40.5 Format 5: Perform workload maintenance functions
 - 2.12.2.40.6 Format 6: Delete an employee's profile
 - 2.12.2.40.7 Format 7: Employees' access to multiple databases is controlled by using UPEMP to add Foreign (secondary) Locations
 - 2.12.2.40.8 Format 8: Multi-Access employees can have their Command Code Profile set to NULL at their Home Campus
 - 2.12.2.41 UPHST - Update / Display Host Profile
 - 2.12.2.41.1 Format 1: Display the current list of Command Codes authorized for a given host
 - 2.12.2.41.2 Format 2: Add or delete up to a full screen of Command Codes from the host profile

-
- 2.12.2.41.3 Format 3: Update all ten IDRS hosts with the inputting of 1 transaction
 - 2.12.2.42 UPMAF - Update the Maximum Profile Authorization File (see also ADMAF)
 - 2.12.2.42.1 Format 1: Add Command Code(s) to or delete Command Code(s) from the Maximum Profile Authorization File (MPAF) for a Unit
 - 2.12.2.42.2 Format 2: Lock and unlock of up to 5 units
 - 2.12.2.43 UPTRM - Update a Terminal
 - 2.12.2.44 UPUNT - Update the Unit Command Code Profile (see also ADUNT)
 - 2.12.2.44.1 Format 1: Update the Command Codes in a Unit
 - 2.12.2.44.2 Format 2: Turn workload management on or off for a Unit
 - 2.12.2.44.3 Format 3: Allow or disallow rerouting also known as Universal Access for a Unit
 - 2.12.2.44.4 Format 4: Enable or disable TRDB dual SINON for a Unit

Exhibits

- 2.12.2-1 Appendix A: Operator Type Codes and units (for ADDEM)

2.12.2.1
(11-09-2023)
Program Scope and Objectives

- (1) This IRM serves as the help guide for all SACS Security command codes.
- (2) **Purpose:** These sections provides information of the formats, variables and related description of SACS Security command codes.
- (3) **Audience:** IDRS Security Officers.
- (4) **Policy Owner:** IT Cybersecurity.
- (5) **Program Owner:** IT Cybersecurity, IDRS Security/IORS.
- (6) **Primary Stakeholders:** IT Cybersecurity, IDRS Security/IORS and Enterprise Operations (EOPS).
- (7) **Program Goals:** Provide information of the formats, variables and related description of SACS Security command codes.
- (8) **Program Management and Review:** SACS maintains the contents of this help guide with information and concurrence from Cybersecurity.
- (9) **Program Controls:** The help guide is updated whenever there are new updates to the existing command code formats or when new command codes are added.

2.12.2.1.1
(11-09-2023)
Background

- (1) This IRM provides information of the formats, variables and related description of SACS Security command codes. It is a replacement of the old guide that was running on a platform that was deprecated in 2009.

2.12.2.1.2
(11-09-2023)
Authority

- (1) Internal securities and communications code governs access and authority of command codes to IRS employees, based on their role and expected job functions.

2.12.2.1.3
(11-09-2023)
Roles and Responsibilities

- (1) IDRS security officers and unit managers are main users of the activities provided in this IRM and responsible for the access and control of these activities for the IDRS agents/users.

2.12.2.1.4
(11-09-2023)
Program Management and Review

- (1) Program Reports: There are no reports generated in association with this IRM.
- (2) Program Effectiveness: This IRM serves as a user guide for some IDRS security command codes.

2.12.2.1.5
(11-09-2023)
Program Controls

- (1) All access to the activity and command codes listed in this IRM are controlled via various BEARS entitlements.

2.12.2.1.6
(11-09-2023)
Terms/Acronyms/ Definitions

- (1) Refer to Exhibit 2.12.2-1

2.12.2.1.7
(11-09-2023)

Related Resources

- (1) IRS employees must submit appropriate BEARS entitlement requests to get access to command codes listed in this guide. Managers and USRs will be their point of contact for this determination.
- (2) The formats provided in this guide as generated internally from related programs for each command code.

2.12.2.2
(11-09-2023)

ADDEM - Add Employee Security Record File (ESRF)

- (1) ADDEM adds a user's ESRF to the SACS system. There are three different ways to add an employee to the system:
- (2) Format 1 adds returning IDRS users or Console users to their previous unit.
- (3) Format 2 adds new IDRS users or new Console users or returning users to a different unit.
- (4) Format 3 adds new IDRS users or Console users or returning users and specifies all 10 digits of the Employee Number.
- (5) In all three options, definer N establishes a Production Profile which may only be used when the employee has changed mode to a Foreign Location (CMODE) -- they have NO Profile at their Home Location.

2.12.2.2.1
(11-09-2023)

Format 1 : Add returning IDRS users or Console users to their previous unit

- (1) Add returning IDRS users or Console users to their previous unit

Format: ADDEMdsss-ss-ssss ttt pppppp
 lllll fff
 S aaaaa
 T nnn-nnn-nnnn [xNNNNN] [MGR]
 i mm/dd/yyyy
 ccode ccode

Where: d is definer P (Production), N (Production but NULL at home), T (Training), I (IMF only), B (BMF only), or blank.

sss-ss-ssss is Social Security Number.

ttt is Employee Type (SAT, PRG (Programmer), or TRB (TRDB user)) {optional}.

pppppp is Operator Type (see Exhibit 2.12.2-1 for restrictions).

lllll is last name (min of 2 characters - max of 20). Can not use hyphens, spaces, apostrophes, or suffixes (Jr., Sr. III, etc).

fff is first name (min of 1 character - max of 15)

S is SEID Indicator Literal - mandatory.

aaaaa is SEID digit (the SEID is 5 alpha-numeric characters, no vowels).

T is Telephone Number Indicator Literal {optional}.

nnn-nnn-nnnn is telephone number digit (area code and dashes mandatory).

xNNNNN is literal x + 1-5 digit extension {optional}.

MGR is manager literal {optional}.

i is Investigation Indicator: I (Investigation initiated), C (Investigation Completed); E (Enter on Duty).

mm/dd/yyyy is "Investigation date" or "Enter-On-Duty date".

ccode is Command Code to be added {optional}.

Note: Format 1 is used for returning IDRS users or Console users that have been deleted from the system and want to remain in the same Unit. They will receive the same Employee Number they had when they were deleted from the system.

Note: The Telephone Number is optional.

Note: The Command Code(s) are optional. One, two or all can be entered.

Note: Operator Type is only valid for Console users.

2.12.2.2.2
(11-09-2023)

Format 2 : Add new or returning IDRS users or Console users to a different unit

(1) Add new or returning IDRS users or Console users to a different unit

Format: ADDEMdsss-ss-ssss uuuuu ttt pppppp
lllll fff
S aaaaa
T nnn-nnn-nnnn [xNNNNN] [MGR]
i mm/dd/yyyy
ccode ccode

Where: d is definer P (Production), N (Production but NULL at home), T (Training), I (IMF only), B (BMF only), or blank.
sss-ss-ssss is Social Security Number.
uuuuu is Unit Number.
ttt is Employee Type (SAT, PRG (Programmer), or TRB (TRDB user)) {optional}.
pppppp is the Operator Type (see Exhibit 2.12.2-1 for restrictions).

IIII is last name (min of 2 characters - max of 20). Can not use hyphens, spaces, apostrophes, or suffixes (Jr., Sr. III, etc).

fff is first name (min of 1 character - max of 15).

S is SEID Indicator Literal - mandatory.

aaaaa is SEID digit (the SEID is 5 alpha-numeric characters, no vowels).

T is Telephone Number Indicator Literal {optional}.

nnn-nnn-nnnn is telephone number digit (area code and dashes mandatory).

xNNNNN is literal x + 1-5 digit extension {optional}.

MGR is manager literal {optional}.

i is Investigation Indicator: I (Investigation initiated), C (Investigation Completed); E (Enter on Duty).

mm/dd/yyyy is "Investigation date" or "Enter-On-Duty date".

ccode is Command Code to be added {optional}.

Note: Format 2 is used with a new IDRS user or Console user. It is also used when a returning user wants to be added to the system under a different Unit Number. The last five digits of the Unit Number (Sequence Number) will normally be the same as the user had when deleted, if it is available

Note: The Telephone Number is optional.

Note: The Command Code(s) are optional. One, two or all can be entered.

Note: Operator Type is only valid for Console users.

2.12.2.2.3
(11-09-2023)
Format 3 : Add new or returning IDRS users or Console users and specify all 10 digits of the Employee Number

(1) Add new or returning IDRS users or Console users and specify all 10 digits of the Employee Number

Format: ADDEMdsss-ss-ssss uuuuunnnnn ttt pppppp
IIII fff
S aaaaa
T nnn-nnn-nnnn [xNNNNN] [MGR]
i mm/dd/yyyy
ccode ccode

Where: d is definer P (Production), N (Production but NULL at home), T (Training), I (IMF only), B (BMF only), or blank.

sss-ss-ssss is Social Security Number.

uuuuu is Unit Number.

nnnnn is Sequence Number.

ttt is Employee Type (SAT, PRG (Programmer), or TRB (TRDB user)) {optional}.

pppppp is the Operator Type (see Exhibit 2.12.2-1 for restrictions).

lllll is last name (min of 2 characters - max of 20). Can not use hyphens, spaces, apostrophes, or suffixes (Jr., Sr. III, etc).

fff is first name (min of 1 character - max of 15).

S is SEID Indicator Literal - mandatory.

aaaaa is SEID digit (the SEID is 5 alpha-numeric characters, no vowels).

T is Telephone Number Indicator Literal {optional}.

nnn-nnn-nnnn is telephone number digit (area code and dashes mandatory).

xNNNNN is literal x + 1-5 digit extension {optional}.

MGR is manager literal {optional}.

i is Investigation Indicator: I (Investigation initiated), C (Investigation Completed); E (Enter on Duty).

mm/dd/yyyy is "Investigation date" or "Enter-On-Duty date".

cocode is Command Code to be added {optional}.

Note: Format 3 is used for the rare occasion when you want to assign a specific 10 digit Employee Number to an IDRS user or Console user. If you specify the entire 10 digit number, the system will give that number to the user (if it is available).

Note: The Telephone Number is optional.

Note: The Command Code(s) are optional. One, two or all can be entered.

Note: Operator Type is only valid for Console users.

2.12.2.3
(11-09-2023)

**ADMAF - Add Maximum
Profile Authorization File
(MPAF)**

- (1) ADMAF can create the MPAF for a new Unit. The MPAF determines what Command Codes can be given optionally to users within the Unit.
- (2) ADMAF can delete the MPAF for a Unit.
- (3) ADMAF with a definer of 'Z' creates up to ten (10) new Units, copies the Command Code bitmaps and characteristics of the existing Unit to the new Units, moves all active employees from the existing Unit to the first new Unit, thus allowing the employees to keep their Production Command Code bitmaps, then deletes the existing Unit. If the first unit is in a different campus (within the same Computing Center), the restrictions and bypasses for the employees in the old campus are copied over to the new campus. The Revenue Agent and 809 Receipt Book User restrictions and bypasses are deleted for the employees at the old campus.
- (4) ADMAF with a definer of 'U' creates up to ten (10) new Units, and copies the Command Code bitmaps and characteristics of an existing Unit to the new Units.

2.12.2.3.1
(11-09-2023)

**Format 1 : Create MPAF
for a new unit**

- (1) Create MPAF for a new unit

Format: ADMAF uuuuu
ccode ccode ccode ccode ccode ccode

Where: uuuuu is Unit Number
ccode is Command Codes to be added to the MPAF

Note: The first two numeric characters of the Unit Number are the Office Identifier/ Location Code for the Campus/Field Office, followed by three Organization Code numeric characters.

Note: A screen of Command Codes can be entered with the ADMAF command. If it is necessary for there to be more Command Codes in the MPAF, you can use UPMF to add as many as desired. If the Unit number starts with 98 or 99, then the command codes must be Console command codes.

2.12.2.3.2
(11-09-2023)

**Format 2 : Delete MPAF
for a unit**

- (1) Delete MPAF for a unit

Format: ADMAF uuuuu
DELE MAF

Where: uuuuu is Unit Number
DELE MAF is delete this MPAF

Note: The UCCP must be deleted with ADUNT prior to deleting the MPAF for a Unit.

2.12.2.3.3

(11-09-2023)

Format 3 : Create new units by copying command code bitmaps and characteristics from existing unit

- (1) Create new units by copying command code bitmaps and characteristics from existing unit

Format: ADMAFduuuuu nnnnn nnnnn nnnnn nnnnn

Where: d is Z or U.

uuuuu is Old Unit Number.

nnnnn is New Unit Number (from 1 to 10 unit numbers delimited by a space).

Note: The old Unit MUST exist. The new Unit MUST NOT exist. The new Units will have the same MPAF, UCCP, REROUTE and TRDB as the old Unit. With a definer of 'Z', all active employees will automatically be moved to the new Unit and will keep their Production Command Code Profiles (see Note 2), and the old Unit will be deleted.

Note: Definer 'Z' is used to move a unit to a different unit number. The unit command code profile will remain the same. The employees within the unit will also retain the same profile. There are restrictions in place whereby some units cannot ever be moved.

Note: All users must be signed off at the time of implementation.

2.12.2.4

(11-09-2023)

ADTRM - Add a Terminal

- (1) ADTRM can authorize a single terminal or multiple terminals for addition to the SACS network and to set a specific time frame during which a terminal/ terminals can be used to access the network.
- (2) ADTRM can remove a terminal's authorization from the network.

2.12.2.4.1

(11-09-2023)

Format 1 : Add a single terminal

- (1) Add a single terminal

Format: ADTRM tttt ffff nnnn

Where: tttt is Terminal Security ID (TSID).

ffff is time off.

nnnn is time on.

Note: Format 1 authorizes a terminal's access to the SACS network. The time On/ Off fields are expressed in military time (0001 - 2400). A TMADD entry must be entered on the TPF machine to establish network configuration.

2.12.2.4.2
(11-09-2023)

Format 2 : Add multiple terminals

(1) Add multiple terminals

Format: ADTRMMtttt tttt ... tttt
 tttt tttt tttt ... tttt
 ...
 tttt tttt ... ffff nnnn

Where: M is definer for multiple terminals.
 tttt is Terminal Security ID (TSID).
 ffff is time off.
 nnnn is time on.

Note: Format 2 authorizes multiple terminal's access to the SACS network.

Note: Up to 6 full lines (including time off and time on) of TSIDs may be input.

Note: If one or more of the TSIDs cannot be processed, the screen response will display each TSID followed by an error type in parenthesis. Here is the key for the five error types:

1. ADDING OR DELETING OWN TERMINAL NOT ALLOWED
2. INVALID TSID - NOT IN SDI
3. THE TERMINAL ID IS ALREADY IN THE AUTHORIZATION FILE
4. UNABLE TO PROCESS - MAX TERMINALS LIMIT EXCEEDED
5. THE TERMINAL ID IS CURRENTLY IN THE TERMINAL FILE

2.12.2.4.3
(11-09-2023)

Format 3 : Remove a terminal

(1) Remove a terminal

Format: ADTRM tttt DELE TRM

Where: tttt is Terminal Security ID (TSID).
 DELE TERM is delete terminal literal.

Note: Format 3 deletes a terminal from the security file.

2.12.2.5
(11-09-2023)

ADUNT - Add Unit Command Code Profile (UCCP)

- (1) Format 1 adds the UCCP for a unit. The Command Codes in the UCCP are inserted into all user profiles in the Unit. This format also lets workload management to be turned ON or OFF for a unit.
- (2) Format 2 deletes a UCCP for a unit.
- (3) Format 3 sets a unit's Universal Access Switch.

2.12.2.5.1
(11-09-2023)

**Format 1 : Add the
UCCP for a unit**

(1) Add the UCCP for a unit

Format: ADUNT uuuuu [YES/NO]
ccode ccode ccode ccode ccode ccode

Where: uuuuu is Unit Number.
[YES/NO] is Optional workload parameter. Default is NO.
YES will Set all employees in the unit to have access limited to those tax accounts entered on their positive accounts list.
NO is to Setup employees not limited access to tax accounts on their positive accounts list.
ccode is Command Code

Note: A screen of Command Codes can be entered with the ADUNT command. If it is necessary for there to be more Command Codes in the UCCP, you can use UPUNT to add as many as desired. The MPAF must be established prior to adding the UCCP.

Note: If the optional YES/NO parameter is not used when adding a Unit, the Unit will default to 'no'. Later, the Unit can be reset to 'yes' with UPUNT (with definer W).

2.12.2.5.2
(11-09-2023)

**Format 2: Delete the
UCCP entry for a Unit**

(1) Delete the UCCP entry for a Unit

Format: ADUNT uuuuu
DELE UNT

Where: uuuuu is Unit Number.
DELE UNT is for Delete this UCCP.

2.12.2.5.3
(11-09-2023)

**Format 3: Authorize
Universal Access**

(1) Authorize Universal Access

Format: ADUNTRuuuuu YES/NO

Where: R is Definer to change a Unit's access to another Service Center's IDRS database.
uuuuu is the Unit Number.

YES/NO is a Required Parameter.

YES for This Unit may access another Campus' IDRS database.

NO is for This Unit may NOT access another Campus' IDRS database.

Note: Format 3 authorizes Universal Access. If Format 3 is not used when adding a Unit, the Unit will default to 'yes'. Later, the Unit can be reset to 'no' with UPUNT (with definer R).

- 2.12.2.6
(11-09-2023)
**ALLOW - Authorize
USRs to input command
codes UPEMP, RSTRK,
and BYPAS for
additional OIs within the
same computing center**
- (1) Authorize USR to input command code at additional OI.

(2) Remove USR ability to input command code at additional OI.

(3) View USR permissions to input command codes at additional OIs.

(4) View permissions to input command codes at additional OIs for all USRs.

- 2.12.2.6.1
(11-09-2023)
**Format 1: Authorize USR
to input command code
at additional OI**
- (1) Authorize USR to input command code at additional OI

Format: ALLOWASSS-SS-SSSS NNNNNNNNNN OI OI....
CCCCC CCCCC
OR
ALLOWAaaaaa NNNNNNNNNN OI OI....
CCCCC CCCCC

Where: A is Add identifier.

SSS-SS-SSSS is USR social security number.

NNNNNNNNNN is USR employee ID number.

OI is Office Identifier (up to 12).

CCCCC is command code (up to 8).

aaaaa is the SEID

- 2.12.2.6.2
(11-09-2023)
**Format 2: Remove USR
ability to input command
code at additional OI**
- (1) Format 2a: Remove command codes permission for USR for a set of campuses.

(2) Format 2b: Remove command codes permission for USR for all campuses.

(3) Format 2c: Remove permission for USR for all campuses and all command codes.

Format 2a: ALLOWDSSSS-SS-SSSS NNNNNNNNNN OI OI....
 CCCCC CCCCC

OR

 ALLOWDaaaaa NNNNNNNNNN OI OI....
 CCCCC CCCCC

Format 2b: ALLOWDSSSS-SS-SSSS NNNNNNNNNN DELETE OFFICE IDS
 CCCCC CCCCC

OR

 ALLOWDaaaaa NNNNNNNNNN DELETE OFFICE IDS
 CCCCC CCCCC

Format 2c: ALLOWDSSSS-SS-SSSS NNNNNNNNNN DELETE ALL COMMAND CODES AND ALL
 OFFICE IDS

OR

 ALLOWDaaaaa NNNNNNNNNN DELETE ALL COMMAND CODES AND ALL OFFICE
 IDS

Where: D is Delete identifier.

 SSS-SS-SSSS is USR social security number.

 aaaaa is the SEID

 NNNNNNNNNN is USR employee ID number.

 OI is Office Identifier (up to 5).

 CCCCC is command code (up to 8).

 DELETE OFFICE IDS is fixed identifier to delete all OIs.

 DELETE ALL COMMAND CODES AND ALL OFFICE IDS is fixed identifier to delete all
 OIs and all command codes.

2.12.2.6.3
(11-09-2023)

**Format 3: View USR
permissions to input
command codes at
additional OIs**

(1) View USR permissions to input command codes at additional OIs

Format: ALLOWVSSSS-SS-SSSS VIEW

OR

 ALLOWVSSSS-SS-SSSS NNNNNNNNNN VIEW

OR

ALLOWVaaaaa VIEW
OR
ALLOWVaaaaa NNNNNNNNNN VIEW

Where: V is fixed identifier for view/display.
SSS-SS-SSSS is USR social security number.
aaaaa is the SEID
NNNNNNNNNN is USR employee ID number.
VIEW is optional parameter for display request.

2.12.2.6.4
(11-09-2023)
Format 4: View permissions to input command codes at additional OIs for all USRs

- (1) View permissions to input command codes at additional OIs for all USRs
- Format: ALLOWQ ALL
- Where: Q is fixed identifier for view all.
ALL is fixed identifier for view all.

2.12.2.7
(11-09-2023)
ASNPW - Assign Password

- (1) ASNPW assigns a password to an employee. This is necessary when a user's password is forgotten or is compromised.

2.12.2.7.1
(11-09-2023)
Format: Assign a password to an employee

- (1) Assign a password to an employee
- Format: ASNPW sss-ss-ssss nnnnnnnnnn
- Where: sss-ss-ssss is Social Security Number.
nnnnnnnnnn is Employee Number.

2.12.2.8
(11-09-2023)
ATSID - Display Available Terminal Security IDs

- (1) ATSID displays all 2-character TSID prefixes assigned to a Campus.
- (2) ATSID displays all available TSIDs at a Campus that start with a given 2-character TSID prefix.

2.12.2.8.1

(11-09-2023)

Format 1: Display all 2-character TSID prefix assigned to a Campus

- (1) Display all 2-character TSID prefix assigned to a Campus

Format: ATSID sc

Where: sc is Campus ID, Campus number, or Office Identifier.

Note: Format 1 displays a list of the first 2 characters of possible TSID(s) at the Campus with Campus ID, Campus number, or Office Identifier 'sc'.

2.12.2.8.2

(11-09-2023)

Format 2: Displays all available TSIDs at a Campus that start with a given 2-character TSID prefix

- (1) Displays all available TSIDs at a Campus that start with a given 2-character TSID prefix

Format: ATSID sc/xx

OR ATSID sc xx

Where: sc is Campus ID, Campus number, or Office Identifier.

space or / is Delimited.

xx is a valid first-2-character TSID combination for the given SC.

Note: Format 2 displays a list of the available TSID(s) that start with the 2 characters from the input. (It was necessary to restrict the display to only those TSID(s) that start with a given 2-character combination in order to keep the display from being too long.)

Note: See DISCC for a list of the SC IDs/numbers and Office IDs.

2.12.2.9

(11-09-2023)

BYPAS - Bypass Profile Restriction

- (1) BYPAS can activate a temporary bypass to a restriction on an employee profile at a given campus.
- (2) BYPAS can remove a temporary bypass to a restriction on an employee profile at a given campus.
- (3) BYPAS can display all employees in a campus Designated User Listing (DUL) with a specific restriction bypass.

2.12.2.9.1

(11-09-2023)

Format 1: Activate a temporary bypass to a restriction on an employee profile at a given campus

- (1) Activate a temporary bypass to a restriction on an employee profile at a given campus

Format 1a: BYPASdsss-ss-ssss oi nn

ACTIVATE

Format 1b: BYPASdsss-ss-ssss oi nn mm/dd/yyyy

ACTIVATE

Where: d is Definer A (user role Revenue Agent), M (user role Manual Refund. Authorizer), R (user role 809 Receipt Book User), or U (user role Remittance Perfection Technicians).

sss-ss-ssss is Social Security Number.

oi is Office Identifier (01 through 10).

nn is Number of days the bypass is effective (01 to 14).

mm/dd/yyyy is Calendar date the bypass will be removed (Note: the bypass is removed the morning of this date).

ACTIVATE is Literal for activate bypass option.

Note: Bypasses can only be added if the user role is restricted for the specified campus.

Note: If Format 1a is used, the date of input counts as the first day.

Note: If Format 1b is used, the calendar date input cannot be later than 14 days from today.

Note: Bypasses remain active if an employee changes units within the same campus during the effective period.

Note: An employee can have up to 5 bypasses at a time per campus (equal to the maximum allowable number of restrictions).

Note: If the employee is signed on when Format 1 is input, he/she must sign off then sign on again before the changes take effect.

2.12.2.9.2
(11-09-2023)

Format 2: Remove a temporary bypass to a restriction on an employee profile at a given campus

(1) Remove a temporary bypass to a restriction on an employee profile at a given campus

Format 2: BYPASdsss-ss-ssss oi
 Remove

Where: d is Definer A (user role Revenue Agent), M (user role Manual Refund Authorizer), R (user role 809 Receipt Book User), or U (user role Remittance Perfection Technicians).

 sss-ss-ssss is Social Security Number.

 oi is Office Identifier (01 through 10).

 REMOVE is Literal for remove bypass option.

Note: If Format 2 is not input, the bypass will be removed automatically by SACS on the scheduled removal date.

Note: If the employee is signed on when Format 2 is input, he/she must sign off then sign on again before the changes take effect.

2.12.2.9.3
(11-09-2023)

(1) Display all employees in a campus Designated User Listing (DUL) with a specific restriction bypass

Format 3: Display all employees in a campus Designated User Listing (DUL) with a specific restriction bypass

Format 3a: BYPASd EMPLOYEE oi
 VIEW

Format 3b: BYPASd EMPLOYEE oi uuuuu TO uuuuu
 VIEW

Where: d is Definer A (user role Revenue Agent), M (user role Manual Refund Authorizer), R (user role 809 Receipt Book User), or U (user role Remittance Perfection Technicians).

 EMPLOYEE is Literal for view Prohibited Command Code Table (PCC).

 oi is Office Identifier (01 through 10).

 uuuuu is 5 digit unit number .

 TO is Literal included with a preceding and following unit number, for limiting the display to only members in the range of units.

 VIEW is Literal for display.

Note: For both formats, the list displayed will be in alphabetical order by employee name.

Note: For Format 3b, the range of units only apply to the input Office Identifier.

2.12.2.10
(11-09-2023)

CMODE - Change Mode to a Different Service Center

- (1) CMODE allows authorized users to switch from their Home Location to an authorized Foreign Location. At the same time, it changes their terminal association to the corresponding location and their default IDRS Command Code routing to that location. The routing of CFOL commands is not affected.
- (2) CMODE is also used to change back to the Home Location or to a different Foreign Location.
- (3) Employees cannot execute security Command Codes from a Foreign Location, except for CMODE, SFDIS, SINOF and STATS. If an employee signs off (SINOF) from a terminal while using their foreign number, their employee status and terminal status will be reset to the Home Location.

2.12.2.10.1
(11-09-2023)

Format: Change Mode to a Different Service Center

- (1) Change Mode to a Different Service Center

Format: CMODEaaa

Where: aaa = acronym of the destination location code -- 2 or 3 characters (see SFDIS).

Note: Employees cannot change mode to a Campus or Field Office until they have been given access to that location (see UPEMP with identifier 'S').

2.12.2.11
(11-09-2023)

DIPID - Display Terminal PIDS Not Used for Six Months

- (1) DIPID displays a list of terminals in a specified Campus that have not been used for six months or more.

2.12.2.11.1
(11-09-2023)

Format: Display Terminal PIDS Not Used for Six Months

- (1) Display Terminal PIDS Not Used for Six Months

Format: DIPID sc

Where: sc is Campus ID, Campus number, or Office Identifier **

Note: This entry displays a list of all the terminals that have not been used in the last 6 months.

Note: The terminal PID is in nnn/nnn format. The number to the left of the slash is the PID's decimal number; to the right of the slash is the same PID's hexadecimal number.

Note: ** See DISCC for a list of the Campus IDs/numbers and Office IDs.

2.12.2.12
(11-09-2023)
**DISCC - Display
Command Codes and
their Attributes**

(1) DISCC displays the attribute settings of Command Codes on the Security Command Code Table (CCT) in SACS. It is a Command Code which provides IDRS users with the same functionality as the SACS Operator Command CCDIS.

(2)

- Display the Command Code attributes of a specific command code.
- Displays a listing of all the command codes and their attributes in the SACS Command Code Table.
- Displays a listing of all the Command Codes and their attributes which are processed on the specified host processor.
- Displays a listing of those Command Codes which match ALL of the specified attributes.
- Displays a listing of enabled or disabled Command Codes at the specified Campus.

2.12.2.12.1
(11-09-2023)
**Format 1: Display the
Command Code
attributes of a specific
Command Code**

(1) Display the Command Code attributes of a specific Command Code

Format 1a: DISCC aaaaa

Where: aaaaa is alpha command code.

Format 1b: DISCC nnn

Where: nnn is Command Code number found in the SACS Command Code Table.

Note: Format 1a displays the Command Code attributes of a specific Command Code. The input format is alpha Command Code.

Note: Format 1b displays the Command Code attributes of a specific Command Code. The input format is Command Code number. Leading zeroes are not required for the command code number.

2.12.2.12.2 (1) Display listing of all the Command Codes and their attributes in the SACS
(11-09-2023) Command Code Table

**Format 2: Display listing
of all the Command
Codes and their
attributes in the SACS
Command Code Table**

Format 2a: DISCC ALPHA

Where: ALPHA is the Literal ALPHA.

Format 2b: DISCC NUMERIC

Where: NUMERIC is the Literal NUMERIC.

Note: Format 2a displays an alpha-order listing of all the Command Codes and their attributes in the SACS Command Code Table.

Note: Format 2b displays a numeric-order listing of all the Command Codes and their attributes in the SACS Command Code Table.

2.12.2.12.3 (1) Display listing of all the Command Codes and their attributes which are
(11-09-2023) processed on the specified host processor

**Format 3: Display listing
of all the Command
Codes and their
attributes which are
processed on the
specified host processor**

Format 3a: DISCC ALPHA host

Where: ALPHA is the Literal ALPHA.
host is specified host type of the Command Code.

Format 3b: DISCC NUMERIC host

Where: NUMERIC is the Literal NUMERIC.
host is specified host type of the Command Code.

(2) Valid host types:

TPFT - TPF (SACS)	BRH1 - UNISYS for Brookhaven
IDRS - UNISYS host of user's Campus	CIH1 - UNISYS for Cincinnati
MCCN - Martinsburg CFOL	FRH1 - UNISYS for Fresno
DCCN - Detroit CFOL	KCH1 - UNISYS for Kansas City
EFTP - EFTPS	MEH1 - UNISYS for Memphis
ANH1 - UNISYS for Andover	OGH1 - UNISYS for Ogden
ATH1 - UNISYS for Atlanta	PHH1 - UNISYS for Philadelphia
AUH1 - UNISYS for Austin	

Note: Format 3a displays an alpha-order listing of all the Command Codes and their attributes which are processed on the specified host processor.

Note: Format 3b displays a numeric-order listing of all the Command Codes and their attributes which are processed on the specified host processor.

Note: See Appendix 2 for a list of valid host types. ***** REMOVE *****

2.12.2.12.4
(11-09-2023)

Format 4: Display a listing of all the Command Codes and their attributes which are processed on the specified host processor

(1) Display a listing of all the Command Codes and their attributes which are processed on the specified host processor

Format 4a: DISCC ALPHA arg1 arg2 arg3....argx

Format 4b: DISCC NUMERIC arg1 arg2 arg3....argx

Where: ALPHA is the Literal ALPHA.
NUMERIC is the Literal NUMERIC.

arg1....argx are specified attributes of Command Code.

(2) Valid arguments are:

PDSY - Displayable at Campus No; (Display ONLY at NCC Yes)	PDSN - Displayable at Campus Yes; (Display ONLY at NCC No)
SVCY - Displayable at Campus Yes	SVCN - Displayable at Campus No
SENY - Sensitive Yes	SENN - Sensitive No
SECY - Security Officer Only Yes	SECN - Security Officer Only No
SUNY - Sunday Available Yes	SUNN - Sunday Available No
SGNY - SINON Required Yes	SGNY - SINON Required Yes
TNGY - Training Database Yes	TNGN - Training Database No
PRIY - Primary Commmand Yes	PRIN - Primary Commmand No
PROY - Profile Required Yes	PRON - Profile Required No
XTTY - Time Exempted Yes	XTTN - Time Exempted No
PPGY - Preserve Pages Yes	PPGN - Preserve Pages No
MFEY - Multi Function Equip Yes	MFEN - Multi Function Equip No
USRY - Unit Security Rep Yes	USRN - Unit Security Rep No
RRTY - Reroutable Yes	RRTN - Reroutable No
TINY - TIN standard position Yes	TINN - TIN standard position No
XDLY - Exempt from Deletion Yes	XDLN - Exempt from Deletion No
TIF1 - TIF Command Code, Group 1	TIFN - TIF Command Code No
TIF2 - TIF Command Code, Group 2	
TIF3 - TIF Command Code, Group 3	

**PDSY - Displayable at
Campus No; (Display
ONLY at NCC Yes)**

**PDSN - Displayable at
Campus Yes; (Display
ONLY at NCC No)**

TIF4 - TIF Command
Code, Group 4

Note: Format 4a displays an alpha-order listing of those Command Codes which match ALL of the specified attributes. Format 4b produces the same list in numeric order.

Note: Attributes which are omitted are ignored, allowing Command Codes with both yes and no settings for that attribute to be on the list.

Note: If conflicting attributes are entered, such as both SENY and SENN, an error message is returned to the user.

2.12.2.12.5
(11-09-2023)

**Format 5: Display a
listing of enabled or
disabled Command
Codes at the specified
Campus**

- (1) Display a listing of enabled or disabled Command Codes at the specified Campus

Format 5a: DISCC ALPHA stat sc

Format 5b: DISCC NUMERIC stat sc

Where: ALPHA is the Literal ALPHA.

NUMERIC is the Literal NUMERIC.

stat is the literal "ENBL" for enabled Command Codes OR "DSBL" for disabled Command Codes.

sc is Campus ID, Campus number, or Office Identifier (OID).

- (2) Valid Campus IDs / SC numbers / OIDs are:

**AN/08/08 - Andover
Campus**

AT/07/07 - Atlanta
Campus

**FR/89/10 - Fresno
Campus**

KC/09/09 - Kansas City
Campus

AN/08/08 - Andover Campus	FR/89/10 - Fresno Campus
AU/18/06 - Austin Campus	ME/49/03 - Memphis Campus
BR/19/01 - Brookhaven Campus	OG/29/04 - Ogden Campus
CI/17/02 - Cincinnati Campus	PH/28/05 - Philadelphia Campus

- (3)
- Note:** Format 5a displays an alpha-order listing of enabled or disabled Command Codes at the specified Campus. Format 5b produces the same list in numeric order.

Note: The Campus can be specified by its ID, by its number, or by its Office Identifier (OID).

Note: For example, DISCC ALPHA ENBL PH and DISCC ALPHA ENBL 28 and DISCC ALPHA ENBL 05 will produce the same results.

2.12.2.13
(11-09-2023)
DISGR - Display Command Code Groups

(1) DISGR can display a list of all the Command Code Group names.

(2) DISGR can display a list of all Command Codes within a specific Command Code Group.

2.12.2.13.1
(11-09-2023)
Format 1: Display a list of all the Command Code Group names

(1) Display a list of all the Command Code Group names

Format 1: DISGR

Note: Format 1 displays a list of the Command Code Groups currently on SACS.

2.12.2.13.2
(11-09-2023)
Format 2: Display a list of all Command Codes within a specific Command Code Group

(1) Display a list of all Command Codes within a specific Command Code Group

Format 2: DISGR gggg

Where: gggg is Command Code Group item to be displayed.

Note: Format 2 displays a list of the Command Codes in the Command Code Group item which is being queried.

- 2.12.2.14
(11-09-2023)
DISNC - Display Network Configuration Information
- (1) DISNC displays network configuration information on SACS terminals, data lines, and sites. DISNC is an IDRS user Command Code which provides the same functionality as the SACS Operator Command NCDIS.
 - (2) Users may display information about **single** network resources using the Terminal Security ID, or the Terminal PID, or the Location ID of a terminal or site.
 - (3) Users may also display **multiple** resources by Resource type (line, site or terminal), or by Connection type.

- 2.12.2.14.1
(11-09-2023)
Format 1: Display information about single network resources
- (1) Display information about single network resources

Format 1a: DISNC tttt

Where: tttt is 4-character Terminal Security ID (TSID).

Format 1b: DISNC 00000

Where: 00000 is 5-digit PID number (leading zeroes not required).

Format 1c: DISNC iiiii(iiii)

Where: iiiii(iiii) is Location ID. (4-6 characters for Sites; 8 characters for Terminals).

Note: Format 1a displays the configuration of the site or device of the queried TSID.

Note: Format 1b display the configuration of the site or device of the queried PID.

Note: Format 1c displays the configuration of the site or the terminal at the queried location.

2.12.2.14.2
(11-09-2023)

(1) Display multiple items by Resource or Connection type

**Format 2: Display
multiple items by
Resource or Connection
type**

Format 2a: DISNC items

Format 2b: DISNC items,sc

Format 2c: DISNC items,zzz,sc

Where: items is Resource or Connection type.

zzz is Status parameter (must begin with comma) {Optional}.

sc is Campus ID, Campus Number of Office ID parameter (must begin with comma) {Optional}.

(2) Valid "Resource" types are:

LINES

SITES

TERMS

(3) Valid "Connection" types are:

TCP - TCP/IP

(4) Valid "Status" parameters are:

OPR - Operational

INP - Not Operational

INS - In Service

OUT - Out of Service

ACT - Active

INA - Inactive

- (5) See Campus Table for valid "Campus ID", "Campus Number", and "Office ID" parameters.

(6)

Note: Format 2 displays the configuration of a group of resources which match all of the input parameters.

2.12.2.15
(11-09-2023)

EXLET - Allow access to high profile TINs

- (1) Access is to this command code is restricted to Cybersecurity IDRS Security staff only.

2.12.2.16
(11-09-2023)

EXTAB - Add, Delete and Display the encrypted Exception Negative TINs List

- (1) Access is to this command code is restricted to Cybersecurity IDRS Security staff only.

2.12.2.17
(11-09-2023)

FIEMP - Find Employee

- (1) FIEMP displays employee case information, using an Employee Number key.

Format: FIEMP nnnnnnnnnn

Where: nnnnnnnnnn is Employee Number.

- (2) FIEMP displays the case owner's name, Standard Employee Identifier (SEID), telephone number, and status (active or inactive).

2.12.2.18
(11-09-2023)

LOKME - Employee Self Lock

- (1) LOKME allows an employee to lock their own profile for a specific number of days or until a specific date. In either format, the employee can lock their profile for up to 45 days. The lock does not take effect until SINOF. An employee may cancel the lock request prior to SINOF.

- (2) Employees who return to duty before the locked period ends must be unlocked by security personnel with the UPEMP Command Code.

2.12.2.18.1
(11-09-2023)

Format 1: Lock employee profile for a number of days

- (1) Lock employee profile for a number of days

Format 1: LOKME nn

Where: nn is number of days (45 maximum).

2.12.2.18.2 (1) Lock employee profile until a specific date
(11-09-2023)

**Format 2: Lock
employee profile until a
specific date**

Format 2: LOKME mm/dd/yyyy

Where: mm/dd/yyyy is date with leading zeroes (not more than 45 days hence)

2.12.2.18.3 (1) Cancel employee lock request
(11-09-2023)

**Format 3: Cancel
employee lock request**

Format 3: LOKME CANCEL

Where: CANCEL is literal "CANCEL".

2.12.2.19 (1) MDPCC adds or deletes command codes to/from the Prohibited Command
(11-09-2023) Code Table (PCC). This command code is only available to Computing Center
Security Officers.

**MDPCC - Modify
Prohibited Command
Code Table**

2.12.2.19.1 (1) Add command codes to/from the Prohibited Command Code Table (PCC)
(11-09-2023)

**Format 1: Add command
codes to/from the
Prohibited Command
Code Table (PCC)**

Format 1: MDPCCd ADD
ccode ccode ccode ccode

Where: d is Definer A (user role Revenue Agent), M (user role Manual Refund Authorizer), or R
(user role 809 Receipt Book User).

ADD is literal for ADD command code.

ccode is command code(s) to be added to the PCC.

Note: 1 to 10 command codes may be input on line 2 of Format 1.

Note: Changes to the PCC will show up in employees' command code profiles on the next day, and only for those employees with restrictions and/or bypasses of the relevant user type.

- 2.12.2.19.2 (1) Delete command codes to/from the Prohibited Command Code Table (PCC)
(11-09-2023)

**Format 2: Delete
command codes to/from
the Prohibited Command
Code Table (PCC)**

Format 1: MDPCCd DEL
ccode ccode ccode ccode

Where: d is Definer A (user role Revenue Agent), M (user role Manual Refund Authorizer), or R (user role 809 Receipt Book User).
DEL is literal for DELETE command code.
ccode is command code(s) to be deleted from the PCC.

Note: 1 to 10 command codes may be input on line 2 of Format 2.

Note: Changes to the PCC will show up in employees' command code profiles on the next day, and only for those employees with restrictions and/or bypasses of the relevant user type.

- 2.12.2.20 (1) MRINQ can display employee history information, using a Social Security
(11-09-2023) Number key, an Employee Number key, or a Standard Employee Identifier
MRINQ - Master Register (SEID) key.
Inquiry (2) MRINQ can display limited information for an employee when using the Social
Security Number key (just the SEID, phone number, and investigation date).
(3) MRINQ can display the next available Employee Number.
(4) MRINQ can display a list of all Employee Numbers for a given Office Identifier
and Sequence Number.

- 2.12.2.20.1 (1) Display employee history information using a Social Security Number key
(11-09-2023)
**Format 1: Display
employee history
information using a
Social Security Number
key**

Format 1: MRINQXsss-ss-ssss

Where: X is definer for Social Security Number key.
sss-ss-ssss is the Social Security Number.

(2)

Note: Format 1 displays a list of Office Identifiers (OIDs) that determine authorized Foreign Locations as well as history information and SEID information for the specified Social Security Number.

2.12.2.20.2
(11-09-2023)

(1) Display employee history information using an Employee Number key

**Format 2: Display
employee history
information using an
Employee Number key**

Format 2: MRINQLnnnnnnnnnn

Where: L is definer for Employee Number key.
nnnnnnnnnn is the Employee Number.

(2)

Note: Format 2 displays a list of Office Identifiers (OIDs) that determine authorized Foreign Locations as well as history information and SEID information for the specified Employee Number.

2.12.2.20.3
(11-09-2023)

(1) Display employee history information using a Standard Employee Identifier (SEID) key

**Format 3: Display
employee history
information using a
Standard Employee
Identifier (SEID) key**

Format 3: MRINQSaaaaa

Where: S is definer for SEID key.
aaaaa is SEID digit (the SEID is 5 alpha-numeric characters, no vowels).

(2)

Note: Format 3 displays a list of Office Identifiers (OIDs) that determine authorized Foreign Locations as well as history information and SEID information for the specified Employee Number.

2.12.2.20.4
(11-09-2023)

(1) Display limited information for an employee when using the Social Security Number key

Format 4: Display limited information for an employee when using the Social Security Number key

Format 4: MRINQPsss-ss-ssss

Where: P is definer for limited Employee Number history.
sss-ss-ssss is the Social Security Number.

Note: Format 4 displays the employee's name, last employee number, SEID, telephone number, and investigation date only.

2.12.2.20.5
(11-09-2023)

(1) Display the next available Employee Number

Format 5: Display the next available Employee Number

Format 5: MRINQN

Where: N is definer for next available Employee Number.

2.12.2.20.6
(11-09-2023)

(1) Display a list of all Employee Numbers for a given Office Identifier and Sequence Number

Format 6: Display a list of all Employee Numbers for a given Office Identifier and Sequence Number

Format 6: MRINQLoi000nnnnn

Where: L is definer for Employee Number history list.
oi is Office Identifier.
000 is the literal "000" (3 zeroes) for a 'wild card' search.
nnnnn is the Employee Sequence Number.

Note: Format 6 displays a list of all Employee Numbers for a given input Office Identifier and Sequence Number. Also included in the display will be the Social Security Number, Employee Name, and dates when the Employee Number was used.

- 2.12.2.21 (11-09-2023)
MRUPD - Master Register Update
- (1) MRUPD can update a user's Social Security Number, their Investigation status and date, or their Assignment or Origin dates.
 - (2) MRUPD can display and update and delete workload management. (See also Workload Management Examples below.)

- 2.12.2.21.1 (11-09-2023)
Format 1: Update a user's Social Security Number
- (1) Update a user's Social Security Number

Format 1: MRUPDUsss-ss-ssss nnn-nn-nnnn

Where: U is definer for update.
sss-ss-ssss is current Social Security Number.
nnn-nn-nnnn is new Social Security Number.

Note: Format 1 changes a user's Social Security Number. SSNs can be changed only if there is no previous MRINQ history.

- 2.12.2.21.2 (11-09-2023)
Format 2: Update a user's Investigation status and date
- (1) Update a user's Investigation status and date

Format 2: MRUPDUsss-ss-ssss d mm/dd/yyyy
OR

MRUPDUaaaaa d mm/dd/yyyy

Where: U is definer for update.
sss-ss-ssss is Social Security Number.
aaaaa is the SEID
d is definer I (Initiated), C (Completed), or E (Enter on Duty).
mm/dd/yyyy is the new date.

Note: Format 2 changes the status and dates of the background investigation required for all IDRS users (Except MCC).

2.12.2.21.3 (1) Update a user's Assignment or Origin dates
(11-09-2023)

**Format 3: Update a
user's Assignment or
Origin dates**

Format 3: MRUPDSsss-ss-ssss d mm/dd/yyyy
OR
MRUPDSaaaaa d mm/dd/yyyy

Where: S is definer for update.
sss-ss-ssss is Social Security Number.
aaaaa is the SEID
d is type of date: A (Assignment) or O (Origin).
mm/dd/yyyy is the new date.

2.12.2.21.4 (1) Display, update and delete workload management
(11-09-2023)

**Format 4: Display,
update and delete
workload management**

Format 4a: MRUPDWsss-ss-ssss
OR
MRUPDWaaaaa

Where: W is definer for workload maintenance.
sss-ss-ssss is Social Security Number of queried employees.
aaaaa is the SEID

Format 4b: MRUPDWsss-ss-ssss (add/update)
TR/nnn-nn-nnnn
TR/nnn-nn-nnnn
TR/nnn-nn-nnnn
TR/nnn-nn-nnnn
TR/nnn-nn-nnnn
OR
MRUPDWaaaaa (add/update)
TR/nnn-nn-nnnn
TR/nnn-nn-nnnn
TR/nnn-nn-nnnn
TR/nnn-nn-nnnn
TR/nnn-nn-nnnn

Where: W is definer for workload maintenance.
sss-ss-ssss is Social Security Number (SSN) of queried employee.
aaaaa is the SEID
T is Negative SSN entry Type; valid Types: S -> Spouse.
R is Range of SSN entry; valid Ranges: S -> 0-4.
nnn-nn-nnnn is Negative SSN to be assigned to employee.
Note: add/update seen by the command above is for information only. It is not part of the entry.

Format 4c: MRUPDWsss-ss-ssss (delete format)
TR/
TR/
TR/
TR/
TR/
OR

MRUPDWaaaaa (delete format)

TR/

TR/

TR/

TR/

TR/

Where: W is definer for workload maintenance.

sss-ss-ssss is Social Security Number (SSN) of queried employee.

aaaaa is the SEID

T is Negative SSN entry Type; valid Types: S -> Spouse.

R is Range of SSN entry; valid Ranges: S -> 0-4.

nnn-nn-nnnn is Negative SSN to be assigned to employee.

Note: delete see by the command above s for information. It is not part of the entry.

Note: Format 4a displays an employee's assigned Negative SSN file.

Note: Format 4b adds or updates a Negative SSN entry on an employee's Negative SSN file.

Note: Format 4c deletes a negative SSN entry on an employee's Negative SSN file.

Note: Format 4b and Format 4c can be combined to do both adds / deletes / updates in a single transaction. Order of entries is not relevant, the only restriction is that each entry is input on a single line.

Example MRUPDWsss-ss-ssss (mixed mode format)
1:

TR/nnn-nn-nnnn

TR/

TR/nnn-nn-nnnn

TR/nnn-nn-nnnn

TR/

Example MRUPDWaaaaa (mixed mode format)
2:

TR/
TR/
TR/nnn-nn-nnnn
TR/
TR/nnn-nn-nnnn

2.12.2.22 (1) PIDTM displays available PIDS or PIDS in use at a given campus.
(11-09-2023)
PIDTM - Display PID Usage

2.12.2.22.1 (1) Display available PIDS at a given campus
(11-09-2023)
Format 1: Display available PIDS at a given campus

Format 1:	PIDTM SVC-sc
-----------	--------------

Where: SVC- is mandatory delimiter.
sc is Campus ID.

Note: Format 1 displays a list of the available PID(s) for use at the Campus ID 'sc'.

2.12.2.22.2 (1) Display PIDS in use at a given campus
(11-09-2023)
Format 2: Display PIDS in use at a given campus

Format 2: PIDTM SVC-sc,U

Where: SVC- is mandatory delimiter.
sc is Campus ID.
, is the mandatory delimiter (comma).
U is the literal "U" for "used" PIDS.

Note: Format 2 displays a list of PID(s) being used by the requested Campus 'sc'.

Note: See DISCC for a list of the Campus IDs.

2.12.2.23

(11-09-2023)

**PWACT Set Password
Management Function**

- (1) PWACT is used by employees to activate their password management function.

2.12.2.23.1

(11-09-2023)

Format 1: PWACT HELP

- (1) PWACT HELP
- (2) . PWACT IS USED TO ACTIVATE, INACTIVATE OR REACTIVATE THE PASSWORD MANAGEMENT CAPABILITY
- (3) . TO ACTIVATE, REACTIVATE OR CHANGE YOUR CURRENT SETTINGS:
- (4) . ENTER: PWACT AFTER SIGNING ON, RESPOND TO ALL THE QUESTIONS. YOUR RESPONSES
- (5) WILL BE USED TO AUTHENTICATE YOU IN CASE YOU FORGET YOUR PASSWORD.
- (6) . INCOMPLETE RESPONSES WILL INACTIVATE THE PASSWORD MANAGEMENT CAPABILITY.
- (7) . FOR SECURITY REASONS, THE RESPONSES TO THE QUESTIONS CANNOT BE REDISPLAYED.
- (8) . TO USE YOUR PASSWORD MANAGEMENT CAPABILITY WHEN YOU FORGET YOUR PASSWORD:
- (9) FROM THE SINON SCREEN OR F1 SCREEN, ENTER ALL REQUIRED FIELDS EXCEPT THE
- (10) PASSWORD. ENTER THE SIGNIFICANT YEAR IN THE SPACE PROVIDED.
- (11) . AN INCORRECT RESPONSE WILL RESULT IN THE TEMPORARY INACTIVATION OF YOUR PSWD.
- (12) MGT. CAPABILITY AND YOU WILL NEED TO SUBMIT AN OL5081 TO GET A NEW PASSWORD.
- (13) . IF THE SIGNIFICANT YEAR IS CORRECT, THE SYSTEM WILL ASK FOR YOUR ANSWER TO
- (14) ONE OF THE THREE QUESTIONS ENTERED WHEN ACTIVATING PASSWORD MANAGEMENT.
- (15) . A NEW TEMPORARY PASSWORD WILL BE DISPLAYED IF YOUR RESPONSE IS CORRECT.
- (16) . A WRONG ANSWER WILL RESULT IN THE TEMPORARY INACTIVATION OF PSWD. MGT.
- (17) . 5 PWMGT REQUESTS IN A 30 DAY PERIOD WILL RESULT IN THE INACTIVATION OF YOUR
- (18) PASSWORD MANAGEMENT CAPABILITY.

2.12.2.23.2 (1)

(11-09-2023)

Format 2: PWACT

The screenshot shows a terminal window with a black background and white text. The text displayed is as follows:

```
PWACT
PROVIDE THE LAST NAME OF A CHILDHOOD FRIEND:
PROVIDE A SIGNIFICANT DATE OTHER THAN YOUR BIRTHDAY(MMDDYYYY):
YOUR FAVORITE COLOR:
SIGNIFICANT YEAR (YYYY):
```

At the bottom of the terminal window, there is a status bar with the text "Pg=1 Row= 2 Col= 47" and "POLL" on the right side.

Figure 2.12.2-1**(2) Instructions - IDRS Password Management Activation**

- (3) 1. While signed onto IDRS, enter the command code "PWACT" and select the transmit key. Note: Command code PWACT is available to all IDRS users and does not need to be in your IDRS profile.

(4) Answer 4 Questions and remember the answers for future use:

1. Provide the last name of a childhood friend
Note: all alpha, between 2-12 characters in length.
2. Provide a significant date – other than your birthday
Note: all numeric, use MMDDYYYY format, date range from 01011800-12312999.
3. Provide a favorite color
Note: all alpha, between 3-12 characters in length.
4. Provide a significant year
Note: all numeric, use YYYY format, year range from 1800-2999.

(5) PWACT Response Messages

(6)

- REQUEST COMPLETED - Password Management has been successfully implemented.
- Any other response - Transaction failed at least one edit check. Try again.

(7) 2. Additional information also is available by entering PWACT HELP <transmit> while signed onto IDRS.

(8) 3. After you have responded to the four inquiries, select the transmit key. Do not send this screen with your responses to a printer.

(9) 4. If you have properly responded to the four inquiries, you will receive a REQUEST COMPLETED message at the bottom of your screen. This message indicates that your Password Management Capability has been successfully activated. We recommend that you perform a SFDISP <transmit> transaction to check your PSWD MGT status. If you have successfully activated this capability, your status will be identified as ACTIVE.

(10) 5. You can change your inquiry responses at any time you are signed-on to IDRS by repeating the steps above. If you change a response, you must respond to all four inquiries again or you will de-activate your capability. IDRS will never show your previous responses but you can re-enter a previous response.

(11) 6. If you do not receive the REQUEST COMPLETED message, you must follow all the above steps and respond to four inquiries. If you continue to have problems, contact your IDRS Unit Security Representative (USR).

2.12.2.24
(11-09-2023)
**PWMGT - IDRS
Password Management**

(1) IDRS Password Management capability that will enable **IDRS users who have forgotten their IDRS password** to get a new temporary IDRS password without having to submit an Online 5081 request. To use this capability, you must activate the IDRS Password Management capability (PWACT) while signed onto IDRS. After the capability has been activated, if you have forgotten your IDRS password you can use this feature to create a new temporary IDRS password which will then let you create a new user password.

Note: PWMGT will not allow IDRS access to a user who has other access impediments, i.e. locked workstation, locked profile, deleted profile.

(2) This field is imbedded in the SINON template.

(3) Possible Errors:

- a. An erroneous 'significant year' is entered in the PWMGT space of the SINON template.
- b. Non-numeric entered in 'significant year' in the PWMGT space of the SINON template.

- 2.12.2.25
(11-09-2023)
REPTS - Authorizes user access to the IORS application
- (1) REPTS authorizes user access to the SACS security reports application IORS via SACS. Users must login to IORS using their SACS login information (SEID, Last Name, First Initial, password). SACS provides user authentication, making sure the user is profiled with REPTS and has an active user account in SACS before allowing them access to IORS. SACS also provides the preliminary security checks to ensure the user access request is issued from an authorized IORS server/terminal. An Audit Trail Record will be produced for all IORS login inputs made using REPTS.
- 2.12.2.26
(11-09-2023)
RMODE - Research mode
- (1) Command code RMODE authorizes an employee to use the command codes contained in their Training Profile in a Research Mode. Employees should contact their USR for instructions on modifying their Training Profile.
 - (2) The Research Mode differs from Production Mode in that production files are accessed but not updated. It differs from Training Mode in that the training files are not accessed.
 - (3) The Research Mode is to be used only by:
 - a. IDRS User Support staff for researching production problems that can be resolved only by accessing production data.
 - b. Application Development staff for addressing issues that can be resolved only by accessing production data. Application Development staff use shall be in compliance with IRM 10.5.8 Sensitive But Unclassified (SBU) Data Policy. Application development staff shall meet all IRM 10.5.8 requirements (including SBU Data Use approval) before RMODE access will be granted.
 - c. Treasury Inspector General for Tax Administration (TIGTA) Strategic Enforcement Division staff.
 - (4) In order to use the research capability, a user shall have command code RMODE in their Production Profile, and input command code SINON with a Production/Training Indicator of R.
 - (5) An Audit Trail Record will be produced for all inputs made in the Research Mode.
 - (6) All Research Mode security violations will be included in IDRS security reports.
- 2.12.2.27
(11-09-2023)
ROUTE - Display Campus Code, Number, Office Identifier, and Routing Status
- (1) ROUTE displays the name, code, number, and Office Identifier (OID) used to identify each Campus' IDRS database. It also displays the current status of the route to that database.
 - (2) Format: ROUTE
- Note:** No definer is required. This command may be issued from a terminal which is not signed on.
- Note:** Martinsburg is used for SAT/PDS Test systems only.

2.12.2.28

(11-09-2023)

RSTRK - Restrict Profile

- (1) RSTRK (meaning restrict) prevents an IDRS user with a certain role type from having specified command codes in their profile. Restrictions added under an Office Identifier can not be removed by security personnel in another Officer Identifier. Restrictions added on a campus in the same computing center will update to the employee profile on the active campus. Restrictions added on a campus on the opposite computing center from the employee's active IDRS account, will need to be manually updated by security personnel. RSTRK can be added to the employee data base for an employee SSN who has no active IDRS account.
- (2) RSTRK can add and delete restrictions against a employee's profile for a given campus.
- (3) RSTRK can display the Command Codes that are restricted for a user role.
- (4) RSTRK can display all employees in a campus Designated User Listing (DUL) with a specific restriction.
- (5) RSTRK can display all employees (any or no restriction) in a campus DUL.
- (6) RSTRK can display the restriction and bypass history for a specific employee.
- (7) RSTRK can change an employee name in the DUL

2.12.2.28.1

(11-09-2023)

Format 1: Add restrictions against a employee's profile for a given campus

- (1) Add restrictions against a employee's profile for a given campus

Format 1: RSTRKdsss-ss-ssss oi
 Iiiii fff
 ADD

Where: d is Definer A (user role Revenue Agent), M (user role Manual Refund Authorizer), R (user role 809 Receipt Book User), or U (user role Remittance Perfection Technicians).
 s is Social Security Number.
 oi is Office Identifier (01 through 10).
 l is Last name (min of 2 characters, max of 20).
 f is First name (min of 1 character, max of 15).
 Add is Literal for add restriction action.

Note: One must input an employee to the correct campus DUL to restrict an employee's Command Code profile. An employee with IDRS access whose unit is in Philadelphia will not be restricted if he/she is has been added to the Brookhaven DUL.

Note: Restrictions remain active if an employee changes units within the same campus.

Note: An employee can have up to 5 restrictions at a time per campus.

Note: If the employee is signed on when Format 1 is input, he/she must sign off then sign on again before the changes take effect.

2.12.2.28.2
(11-09-2023)

(1) Delete restrictions against a employee's profile for a given campus

**Format 2: Delete
restrictions against a
employee's profile for a
given campus**

Format 2: RSTRKdsss-ss-ssss oi
DELETE

Where: d is Definer A (user role Revenue Agent), M (user role Manual Refund Authorizer), R (user role 809 Receipt Book User), or U (user role Remittance Perfection Technicians).
s is Social Security Number.
oi is Office Identifier (01 through 10).
DELETE is Literal for add restriction action.

Note: If Format 2 has not been input, an employee who is deleted from IDRS will still remain on the DUL. So if the employee is later readded to IDRS (in the same campus), the restrictions will again be in effect.

Note: If the employee is signed on when Format 2 is input, he/she must sign off then sign on again before the changes take effect.

2.12.2.28.3
(11-09-2023)

(1) Display the Command Codes that are restricted for a user role

**Format 3: Display the
Command Codes that
are restricted for a user
role**

Format 3: RSTRKd COMMAND CODE
VIEW [HISTORY]

Where: d is Definer A (user role Revenue Agent), M (user role Manual Refund Authorizer), R (user role 809 Receipt Book User), or U (user role Remittance Perfection Technicians).

COMMAND CODE is Literal for view Prohibited Command Code Table (PCC).

VIEW is Literal for display.

HISTORY is Literal for display history for the PCC {optional}.

Note: The VIEW option shows only those Command Codes which are active in the Prohibited Command Code Table (PCC). 2 columns of data will be presented: the Command Code name and the date the Command Code was last added to the PCC.

Note: The VIEW HISTORY option shows all active and inactive Command Codes in the PCC. 4 columns of data will be presented: the Command Code name, the date the Command Code was last added to the PCC, the date the Command Code was last removed from the PCC (if applicable), and the Command Code status (ACTIVE or INACTIVE).

2.12.2.28.4
(11-09-2023)

- (1) Display all employees in a campus Designated User Listing (DUL) with a specific restriction

Format 4: Display all employees in a campus Designated User Listing (DUL) with a specific restriction

Format 4a: RSTRKd EMPLOYEE oi [NOT ACTIVE] [SSN] [SEID] [SSN SEID]
VIEW

Format 4b: RSTRKd EMPLOYEE oi uuuuu TO uuuuu [SSN] [SEID] [SSN SEID]
VIEW

Where: d is Definer A (user role Revenue Agent), M (user role Manual Refund Authorizer), R (user role 809 Receipt Book User), or U (user role Remittance Perfection Technicians).

EMPLOYEE is View Designated User List (DUL).

oi is Office Identifier (01 through 10).

NOT ACTIVE is to Show only inactive accounts on IDRS {optional}.

SSN is to Show the SSN in the display {optional}.

SEID is to Show the SEID in the display {optional}.

SSN SEID is to Show both the SSN and the SEID {optional}.

VIEW is Literal for display.

uuuuu is 5 digit Unit Number.

TO is Literal included with a preceding and following unit number, for limiting the display to only members in the range of units.

Note: For both formats, the list displayed will be in alphabetical order by employee name.

Note: For Format 4a, if the NOT ACTIVE literal is omitted, the display will show both employees with and without active IDRS accounts.

Note: For both formats, if more than one optional item is input, they must be input in the order shown.

Note: For Format 4b, the range of units only apply to the input Office Identifier.

2.12.2.28.5
(11-09-2023)

(1) Display all employees (any or no restriction) in a campus DUL

Format 5: Display all employees (any or no restriction) in a campus DUL

Format 5a: RSTRKX EMPLOYEE oi [NOT ACTIVE] [SSN] [SEID] [SSN SEID]
VIEW [DELETED]

Format 5b: RSTRKX EMPLOYEE oi uuuuu TO uuuuu [SSN] [SEID] [SSN SEID]
VIEW [DELETED]

Where: X is the Literal for Display.
EMPLOYEE is View Designated User List (DUL).
oi is Office Identifier (01 through 10).
NOT ACTIVE is to Show only inactive accounts on IDRS {optional}.
SSN is to Show the SSN in the display {optional}.
SEID is to Show the SEID in the display {optional}.
SSN SEID is to Show both the SSN and the SEID {optional}.
VIEW is Literal for display.
uuuuu is 5 digit Unit Number.
DELETED is to Show only employees with no restrictions {optional}.
TO is Literal included with a preceding and following unit number, for limiting the display to only members in the range of units.

Note: For both formats, the list displayed will be in alphabetical order by employee name.

Note: For Format 5a, if the NOT ACTIVE literal is omitted, the display will show both employees with and without active IDRS accounts.

Note: For both formats, if more than one optional item is input, they must be input in the order shown.

Note: For Format 5b, the range of units only apply to the input Office Identifier.

2.12.2.28.6
(11-09-2023)

(1) Display the restriction and bypass history for a specific employee

Format 6: Display the restriction and bypass history for a specific employee

Format 6: RSTRKXsss-ss-ssss [oi]
VIEW HISTORY

Where: X is the Literal for Display.
sss-ss-ssss is the Social Security Number.
oi is Office Identifier (01 through 10) [optional].
VIEW HISTORY is the Literal for view history.

Note: If the office identifier is omitted, the display will show all restriction and bypass history items existing for the 5 campuses within the user's Computing Center.

Note: Format 6 will also show the employee's name, as shown in the DUL, as well as his/her employee number (if the employee has an active IDRS account).

2.12.2.28.7
(11-09-2023)

(1) Change an employee name in the DUL

Format 7: Change an employee name in the DUL

Format 7: RSTRKCsss-ss-ssss

IIIII fff

Where: C is the Literal for Change.
 sss-ss-ssss is the Social Security Number.
 IIIII is the Last name (min of 2 characters, max of 20).
 fff is First name (min of 1 character, max of 15).

Note: The name will only be changed in the Designated User List (DUL) of the input user's home campus.

2.12.2.29
 (11-09-2023)
**SECOP - Security
 Operation, Unlock a
 Terminal**

- (1) SECOP unlocks a terminal that has received a security lock as a result of three consecutive security violations.

Format: SECOP tttt

Where: tttt is the Terminal ID.

Note: The Terminal ID (TSID) consists of four alpha/numeric characters.

2.12.2.30
 (11-09-2023)
**SETPW - Set Password
 Expiration Range for a
 Unit**

- (1) SETPW allows Security Officers and Unit Security Representatives to change the number of days users in a Unit have until their passwords automatically expire. The range must be in increments of 30 days.
- (2) The default for a Unit is 120 days. Security Officers may set the range lower than the default or reset it higher, but may never exceed 120 days. Unit Security Representatives may set the range lower or reset it higher, but never higher than the Security Officer's setting.

Format: SETPWduuuuu nn

Where: d is definer S (Security Officer) or definer U (Unit Security Rep.).

uuuuu is Unit Number.

nn is 30 or 60 or 90 or 120 (must be one of these four exactly as shown).

Note: If a Unit Security Rep. enters definer 'S', an error will be returned.

2.12.2.31
(11-09-2023)
**SFDIS - Display User
Profile**

- (1) SFDIS allows users to display their own Profiles. The response to this command will include the user's current (signed on) profile, the Info-connect ID, the user's active restriction/bypasses, password management activation status and availability, individual Command Code profile and authorized Foreign Locations for CMODE. User must be signed on in "T" mode to view his/her training profile.

Format: SFDISd

Where: d is definer, either P or T will display the user's current (signed on) profile, the three options being Production, Training, or Research.

Note: SFDIS displays the user's Command Code Profile for either Training or Production. Command Codes followed by a dollar sign (\$) are exempt from automatic deletion for non-use.

Note: If definer 'P' is selected, the display will also include the File Access Restriction ("IMF only", "BMF only", or "IMF and BMF"). There is no File Access Restriction for training.

2.12.2.32
(11-09-2023)
SFINQ

- (1) SFINQ can display employee information such as name, Employee Number, SEID, user type, locked or unlocked status, active/inactive restrictions and bypasses, authorized foreign access, NULL status and password management status.
- (2) SFINQ can display the employee's Production or Training Command Code Profiles.
- (3) SFINQ can display all employees in a Unit in Employee Number order or name order, show their SEID, Operator Type, whether signed on or off, the TSID of the terminal if signed on, and their locked or unlocked status.
- (4) SFINQ can display all Command Codes allowed in a Unit plus the Unit's Universal Access (reroute) status.
- (5) SFINQ can display for one or more Units a list of all employees' names, Employee Numbers, NULL Status, and authorized Foreign Locations Office Identifiers (OIDs).
- (6) SFINQ can display, by terminal TSID, the employee number for any user signed on, or the allowed Time On/Off for that terminal.
- (7) SFINQ can display a list of the last usage dates for all Command Codes in a particular Unit, plus indicate which Command Codes have been turned off for non-use.
- (8) SFINQ can display authorized Multiple Access (CMODE) locations.
- (9) Finally, this SFINQ displays Command Codes turned off for a Unit. This option has six different options:

- (10) Display LAST 30 days for BOTH System and Security Officer turn-offs.
- (11) Display LAST 30 days for EITHER System or Security Officer turn-offs.
- (12) Display ALL dates for BOTH System and Security Officer turn-offs.
- (13) Display ALL dates for EITHER System or Security Officer turn-offs.
- (14) Display SPECIFIED NUMBER of days for BOTH System and Security Officer turn-offs.
- (15) Display SPECIFIED NUMBER of days for EITHER System or Security Officer turn-offs.
- (16) Display Password Management Status for a unit - SFINQW.

2.12.2.32.1
(11-09-2023)

**Format 1: Display
employee information**

- (1) Display employee information such as name, Employee Number, SEID, user type, locked or unlocked status, active/inactive restrictions and bypasses, authorized foreign access, NULL status and password management status

Format 1: SFINQ sss-ss-ssss
 OR
 SFINQ aaaaa

Where: sss-ss-ssss is the Social Security Number.
 aaaaa is the SEID

Note: Format 1 displays employee name, Number, SEID, user type (SAT or PRG and/or *TRDB*), File Access Restriction ("IMF only", "BMF only", or "IMF and BMF") the profile status (locked or unlocked), date of last logon, password management status, a list of Office Identifiers (OIDs) that determines authorized Foreign access, NULL status, and active inactive restriction and bypasses.

2.12.2.32.2
(11-09-2023)

**Format 2: Display the
employee's Production
or Training Command
Code Profiles**

- (1) Display the employee's Production or Training Command Code Profiles

Format 2: SFINQpsss-ss-ssss
 OR
 SFINQpaaaaa

Where: p is Profile P (Production) or T (Training).

sss-ss-ssss is the Social Security Number.

aaaaa is the SEID

Note: Format 2 displays the Command Code Profile for either Training or Production as well as SEID information and all of the information displayed with Format 1.

2.12.2.32.3
(11-09-2023)

Format 3: Display all employees in a Unit

- (1) Display all employees in a Unit in Employee Number order or name order, show their SEID, Operator Type, whether signed on or off, the TSID of the terminal if signed on, and their locked or unlocked status

Format 3: SFINQduuuuu-LOCK

Where: d is sort definer A (Alphabetically) or X (Numerically).

uuuuu is the Unit Number.

-LOCK is display only locked employees {optional}.

Note: Format 3 displays all employees in a Unit (or optionally just the locked employees in a Unit) either by name (Alphabetically) or Employee Number (Numerically).

2.12.2.32.4
(11-09-2023)

Format 4: Display all Command Codes allowed in a Unit

- (1) Display all Command Codes allowed in a Unit plus the Unit's Universal Access (reroute) status

Format 4: SFINQduuuuu

Where: d is definer M (MPAF) or U (UCCP).

uuuuu is the Unit Number.

Note: Format 4 displays the Command Codes in the MPAF or the UCCP. It will also show the Unit's reroute setting (REROUTE = YES/NO) and the 'lock' status (LOCKED=YES/NO) With definer 'M', Command Codes followed by an asterisk (*) are not present in the UCCP. With either definer 'M' or 'U', Command Codes followed by a dollar-sign (\$) are exempt from automatic deletion for non-use.

2.12.2.32.5
(11-09-2023)

(1) Display for one or more Units a list of all employees' names, Employee Numbers, NULL Status, and authorized Foreign Locations Office Identifiers (OIDs)

Format 5: Display for one or more Units a list of all employees' names, Employee Numbers, NULL Status, and authorized Foreign Locations Office Identifiers (OIDs)

Format 5a: SFINQduuuuu

Where: d is definer E for displaying a single Unit information.
 uuuuu is the Unit Number.

Format 5b: SFINQduuuuu uuuuu uuuuu ... uuuuu

Where: d is definer R for displaying information for multiple units.
 uuuuu is the Unit Number (max of 10 units).

Note: Format 5a displays an alphabetical list of all employees in the Unit, plus their NULL Status and Foreign Location permissions.

Note: Format 5b displays the same information as Format 5a, but for up to ten Units.

2.12.2.32.6
(11-09-2023)

(1) Display, by terminal TSID, the employee number for any user signed on, or the allowed Time On/Off for that terminal

Format 6: Display, by terminal TSID, the employee number for any user signed on, or the allowed Time On/Off for that terminal

Format 6: SFINQdtttt

Where: d is definer S (Signed on) or blank (Time On/Off).
 tttt is Terminal Security ID (TSID).

Note: Format 6 displays the Employee Number of the user currently signed on for the specified terminal when the 'S' definer is used. It displays the authorized Time On/Off for a terminal when the definer field is left blank.

2.12.2.32.7
(11-09-2023)

- (1) Display a list of the last usage dates for all Command Codes in a particular Unit, plus indicate which Command Codes have been turned off for non-use

Format 7: Display a list of the last usage dates for all Command Codes in a particular Unit

Format 7: SFINQduuuuu (Last usage date of Command Codes in a Particular Unit)

Where: d is definer C (MPAF Aged-Delete-Record Command Code use date).
uuuuu is the Unit Number.

Note: Format 7 displays the last usage date of Command Codes in a particular Unit. Display is of Command Codes active in the Unit's MPAF.

Note: In the display, an asterisk (*) denotes the Command Code has been turned off in Employee Profiles due to 90 days of non-use. A pound sign (#) denotes the Command Code has been turned off in the Unit due to 360 days of non-use.

2.12.2.32.8
(11-09-2023)

(1)

Format 8: Display authorized Multiple Access (CMODE) locations

Format 8a: SFINQduuuuu

Where: d is definer D (MPAF Aged-Delete-Record).
uuuuu is the Unit Number.

Note: Format 8a displays the Command Codes turned off for a particular Unit during the previous 30 days (the default if time is not specified). This is a request for display of both System (90 days and 360 days non-use) and Security Officer Command Code turn-offs (the default if type SYS or SEC is not specified).

Note: In the display, an asterisk (*) denotes the Command Code has been turned off in Employee Profiles due to 90 days of non-use. A pound sign (#) denotes the Command Code has been turned off in the Unit due to 360 days of non-use.

(2)

Format 8b: SFINQduuuuuttt

Where: d is definer D (MPAF Aged-Delete-Record).
uuuuu is the Unit Number.
ttt is SYS (System) or SEC (Security Officer).

Note: Format 8b displays the Command Codes turned off for a particular Unit during the previous 30 days (the default if time is not specified). This is a request for display of only System (90 days and 360 days non-use) or only Security Officer Command Code turn-offs.

(3)

Format 8c: SFINQduuuuu*

Where: d is definer D (MPAF Aged-Delete-Record).
uuuuu is the Unit Number.
* is for "display all dates" option.

Note: Format 8c displays the Command Codes turned off for a particular Unit regardless of date of turn off. (List all Dates Turnoff(s) option.) This is a request for display of both System (90 days and 360 days non-use) and Security Officer Command Code turn-offs (the default if type SYS or SEC is not specified).

(4)

Format 8d: SFINQduuuuuttt*

Where: d is definer D (MPAF Aged-Delete-Record).
uuuuu is the Unit Number.
ttt is SYS (System) or SEC (Security Officer).
* is for "display all dates" option.

Note: Format 8d displays the Command Codes turned off for a particular Unit regardless of date of turn off. (List all Dates Turnoff(s) option.) This is a request for display of only System (90 days and 360 days non-use) or only Security Officer Command Code turn-offs.

(5)

Format 8e: SFINQduuuuunnn (Specified Time Period Option)

Where: d is definer D (MPAF Aged-Delete-Record).
uuuuu is the Unit Number.
nnn is number of days previous to today's date.

Note: Format 8e displays the Command Codes turned off for a particular Unit during the time period specified by the user. This is a request for display of both System (90 days and 360 days non-use) and Security Officer Command Code turn-offs (the default if type SYS or SEC is not specified).

(6)

Format 8f: SFINQduuuuutttnnn (Specified Time Period Option)

Where: d is definer D (MPAF Aged-Delete-Record).
uuuuu is the Unit Number.
ttt is SYS (System) or SEC (Security Officer).
nnn is number of days previous to today's date.

Note: Format 8f displays the Command Codes turned off for a particular Unit during the time period specified by the user. This is a request for display of only System (90 days and 360 days non-use) or only Security Officer Command Code turn-offs.

2.12.2.32.9
(11-09-2023)

(1) Display Password Management Status for a unit

Format 9: Display Password Management Status for a unit

Format 9: SFINQduuuuu (Specified Time Period Option)

Where: d is definer W (Shows the Password Management activity status).
uuuuu is the Unit Number.

Note: Format 9 displays the Password Management status for the unit in alphabetical order.

2.12.2.33 (1) SINOF is used to deactivate your session with IDRS.

(11-09-2023)

SINOF - Sign off of IDRS (2) Format: SINOF

Note: All IDRS users are required to sign off of the system upon completion of their work. The user may also "X-out" of the IDRS session to effectively sign off.

2.12.2.34 (1) SINON is used to access the IDRS system. SINON is used to retrieve the template or to actually sign on using the CASL macro.

(11-09-2023)

SINON - Sign on to IDRS

2.12.2.34.1 (1) SINON

(11-09-2023)

Format 1: SINON with Template (2)

```

SINON      PTI:  P  SSN OR SEID:
LAST NAME:
FIRST INITIAL:
PASSWORD:          PWMGT (SIGNIF. YEAR):
  TO CHANGE PASSWORD, ENTER ALL REQUIRED FIELDS ABOVE, THEN ENTER NEW
  PASSWORD AND CONFIRM NEW PASSWORD BELOW.  PASSWORDS MUST BE 8 TO 12
  CHARACTERS.  PASSWORDS MUST HAVE AT LEAST 1 NUMBER, 1 UPPER CASE AND
  1 LOWER CASE LETTER.  NO LETTER OR NUMBER MAY BE REPEATED MORE THAN
  THREE TIMES IN A ROW.  FOR EXAMPLE:  AA@1bbb2  OR  111@222Bcd
  PASSWORDS MUST CONTAIN AT LEAST ONE SPECIAL CHARACTER:  - $ _ @ *
NEW PASSWORD:
CONFIRM NEW PASSWORD:
      *****      INTEGRATED DATA RETRIEVAL SYSTEM      *****

WILLFUL UNAUTHORIZED ACCESS OR INSPECTION OF ANY TAXPAYER INFORMATION
--REFERRED TO AS UNAX--IS EXPRESSLY PROHIBITED.  ACCESS TO THIS SYSTEM IS
RESTRICTED TO THOSE EMPLOYEES AND CONTRACTORS WHO HAVE AN AUTHORIZED,
WORK-RELATED REASON TO ACCESS AND INSPECT TAXPAYER INFORMATION.  WILLFUL
UNAUTHORIZED ACCESS OR INSPECTION OF THE TAXPAYER INFORMATION CONTAINED
IN THIS SYSTEM MAY SUBJECT THE OFFENDER TO CRIMINAL PROSECUTION UNDER
18 U.S.C. 1030 OR 26 U.S.C. 7213, AND ADMINISTRATIVE ACTION.

      *****      REMEMBER - STOP UNAX IN ITS TRACKS      *****

Pq=1 Row= 1 Col= 17      POLL

```

Figure 2.12.2-2

Note: This option will retrieve the SINON template to the user's screen.

Note: When the template is retrieved, the cursor is positioned in the PTI: field with a default value of P. The user may overtype this field with one of the other values or use the TAB key to jump to the beginning of the next field. The TAB key will jump to the beginning of each subsequent field.

Note: TRDB users who have dual-SINON capability will receive additional warnings when they sign on to their second terminal. TRDB users must sign off of both terminals individually.

Note: TRDB users who try to sign on a third terminal without signing off of one of the other two terminals, will automatically be signed off of every terminal and have their Employee Profile locked.

Note: TRDB users may change their password from either session.

Note: If the Multi-Access NULL Status of the user's Home Location is 'ON' and the user has only one authorized Foreign Location then the user mode will automatically change to the Foreign Location. Refer to Command Codes UPEMP with definer S and CMODE for related information.

2.12.2.34.2

(11-09-2023)

Format 2: SINON with CASL macro

(1) Press F1 Key to bring up the macro.

(2)

SINON ver. 16.6

5 Character SEID:

Last Name:

First Name Initial:

Password:

PTI
☒ P ☐ R ☐ T

PWMGT - Enter Significant Year (4 numeric characters):

OK Cancel

Change Password
 To change your Password, enter all required fields, then enter the New Password and Confirm Password in the boxes below.
 Passwords must be 8 to 12 characters long, must have at least one number, must be mixed case (upper and lower letters) with at least one of these special characters: - @ _ \$ *. No character may be repeated more than three times in a row.
 Valid examples: AA@1bbb2 or 111\$222Bcd

New Password:

Confirm Password:

 THIS U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!

 Use of this system constitutes consent to monitoring, interception, recording, reading, copying, or capturing by authorized personnel of all information stored within the system. There is no right to privacy in this system.
 ***** INTEGRATED DATA RETRIEVAL SYSTEM *****
 WILLFUL UNAUTHORIZED ACCESS OR INSPECTION OF ANY TAXPAYER INFORMATION IN THIS SYSTEM IS EXPRESSLY PROHIBITED. ANY UNAUTHORIZED ACCESS OR INSPECTION MAY SUBJECT THE OFFENDER TO CRIMINAL PROSECUTION UNDER 18 U.S.C. 1030 OR 26 U.S.C. 7213, AND TO ADMINISTRATIVE ACTION.

Figure 2.12.2-3

(3) Possible SINON errors:

(4)

- Both password and significant year entered.
- Wrong significant year.
- Non numeric entered instead of a significant year.

2.12.2.35
(11-09-2023)

SOMSG - SINON
Message Maintenance

- (1) SOMSG updates the message that appears when a user signs on to IDRS. It also can be displayed with the STATS Command Code.

Format: SOMSG

text line 1

text line 2

text line 3

text line 4

text line 5

text line 6

text line 7

text line 8

text line 9

text line 10

text line 11

text line 12

text line 13

text line 14

Note: Any number of lines, from 1 to 14 may be entered.

Note: SOMSG always replaces the *entire* message, no prior items are saved.

Note: The SINON message for a SACS test system should always contain the phrase "Test System".

2.12.2.36
(11-09-2023)

STATS - Display
Terminal Statistics

- (1) STATS displays general information relative to the session such as TSID, PID number, InfoConnect ID, date, time, and whether IDRS is up.

- (2) Format: STATS

- (3)

Note: STATS does not require being signed on.

2.12.2.37
(11-09-2023)

SWTCH - Update the
Campus Domain
Indicator

- (1) SWTCH queries the status setting of the Campus Domain Indicator (@APSW1 global) or TURNON/TURNOFF status for the Campus Domain Indicator. Security Officers can query the Campus Domain Indicator Status, or set the status of the Campus Domain Indicator.

2.12.2.37.1 (1) Query the Campus Domain Indicator Status
(11-09-2023)

**Format 1: Query the
Campus Domain
Indicator Status**

Format 1: SWTCH

Note: Format 1 queries status setting of the campus domain indicator.

2.12.2.37.2 (1) Set the status of the Campus Domain Indicator
(11-09-2023)

**Format 2: Set the status
of the Campus Domain
Indicator**

Format 2: SWTCHvvv

Where: vvv is ON or OFF.

ON will set campus domain indicator global to "ON" status (campus domain is "open").

OFF will set campus domain indicator global to "OFF" status (campus domain is "closed").

Note: Format 2 sets the campus domain global status ON and OFF.

2.12.2.38 (1) UNLEM unlocks an employee who has been locked by the system after a 17-
(11-09-2023) day period of inactivity. This allows Terminal Security Administrator (TSAs) to
UNLEM - Unlock System unlock system-locked employees without needing to have UPEMP in their
Locked Employee profiles.

Format: UNLEMPsss-ss-ssss nnnnnnnnnn
OR
UNLEMPaaaaa nnnnnnnnnn

Where: P is Definer.
sss-ss-ssss is the Social Security Number.
aaaaa is the SEID
nnnnnnnnnn is the Employee Number.

- 2.12.2.39 (1) Add or Delete Restriction.
(11-09-2023)
UPCON - Add, Delete OR Display Restriction Record (2) Display Restriction Record.

- 2.12.2.39.1 (1) Add or Delete a Restriction
(11-09-2023)
Format 1: Add or Delete a Restriction
- Format: UPCONPSSSSS CCCCC PARM

Where: P is R (Add a restriction), X (Delete a restriction).
SSSSS is SEID.
CCCCC is Command code.
PARM is Parameter of command code restriction.

- 2.12.2.39.2 (1) Display Restrictions Record
(11-09-2023)
Format 2: Display Restrictions Record
- Format: UPCONDSSSSS

Where: D is Display parameter.
SSSSS is SEID.

- 2.12.2.40 (1) UPEMP can change an employee (user) name, their Unit Number, their SAT or Programmer type (in Test only), their TRDB status, their Standard Employee Identifier (SEID), or their telephone number.
(11-09-2023)
UPEMP - Update Employee
- (2) UPEMP can add / delete Command Code(s) to / from the user's Profile. This option also displays and changes their IMF - BMF status.
- (3) UPEMP can lock or unlock a user's Profile (unlocks system lock, security lock, or self lock) or delete a user.
- (4) UPEMP can delete an authorized Foreign Location.
- (5) UPEMP can perform workload maintenance functions.
- (6) UPEMP can delete an employee's profile.
- (7) Employees' access to multiple databases is controlled by using UPEMP to add Foreign (secondary) Locations.
- (8) Multi-Access employees can have their Command Code Profile set to NULL at their Home Campus.

2.12.2.40.1
(11-09-2023)

- (1) Change an employee (user) name, their Unit Number, their SAT or Programmer type (in Test only), their TRDB status, their Standard Employee Identifier (SEID), or their telephone number

Format 1: Change an employee (user) name, their Unit Number, their SAT or Programmer type (in Test only), their TRDB status, their Standard Employee Identifier (SEID), or their telephone number

Format 1a: UPEMPdsss-ss-ssss lllll ffff
OR
UPEMPdaaaaa lllll ffff

Where: d is definer C (Name Change).
sss-ss-ssss is the Social Security Number.
aaaaa is the SEID
lllll is the last name (min of 2 characters and max of 20).
ffff is the first name (min of 1 character and max of 15).

Note: Format 1a changes the user's name. Use of UPEMPC is restricted to Security Officers in units 930 and 931.

(2)

Format 1b: UPEMPdsss-ss-ssss uuuuu
OR
UPEMPdaaaaa uuuuu

Where: d is definer P (Production), T (Training) or blank.
sss-ss-ssss is the Social Security Number.
aaaaa is the SEID
uuuuu is the Unit Number.

Note: Format 1b changes the employee's Unit Number. The Command Codes in the UCCP of the new Unit are inserted into the user's Profile as designated by the definer. (If left blank, no Command Codes will be in the user's Profile.)

Note: If a Home Location change is made on an employee who has active assigned Foreign Locations, the Foreign Locations associated with the employee's previous Home Location will be automatically deleted with the employee's assignment to a new Unit.

(3)

Format 1c: UPEMP sss-ss-ssss
 ttt
 OR
 UPEMP aaaaa
 ttt

Where: sss-ss-ssss is the Social Security Number.
 aaaaa is the SEID
 ttt is type SAT (System Tester) or PRG (Programmer) or TRB (TRDB=YES) or TRX (TRDB=NO).

Note: Format 1c changes a user's access type.

Note: Access types SAT and PRG are restricted to the SACS Test systems.

Note: Before you can set an employee's access type to TRB, you must first set their Unit to TRDB=YES. (UPUNT with definer 'T'.)

Note: When employees are moved to non-TRDB units, their access type is automatically set to TRX.

(4)

Format 1d: UPEMPEsss-ss-ssss aaaaa
 OR
 UPEMP nnnnn aaaaa

Where: E is definer E (SEID change).
 sss-ss-ssss is the Social Security Number.
 nnnnn is the current SEID
 aaaaa is new SEID digit (the SEID is 5 alpha-numeric characters, no vowels).

Note: Format 1d changes the Standard Employee Identifier (SEID) for the owner of the input Social Security Number.

(5)

Format 1e: UPEMPFsss-ss-ssss ttt-ttt-tttt [xNNNNNN] [MGR]
OR
UPEMPFaaaaa ttt-ttt-tttt [xNNNNNN] [MGR]

Where: F is definer F (telephone number change).
sss-ss-ssss is the Social Security Number.
aaaaa is the SEID
ttt-ttt-tttt is telephone number (must include area code and dashes).
xNNNNNN is literal x + 1-5 digit extension {optional}.
MGR is manager literal {optional}.

Note: Format 1e changes the telephone number for the owner of the input Social Security Number.

2.12.2.40.2
(11-09-2023)

(1) Add / delete Command Code(s) to / from the user's Profile. This option also displays and changes their IMF - BMF status

**Format 2: Add / delete
Command Code(s) to /
from the user's Profile.
This option also
displays and changes
their IMF - BMF status**

Format 2a: UPEMPdsss-ss-ssss
(blank line)
ccode 1 ccode 0
OR
UPEMPdaaaaa
(blank line)
ccode 1 ccode 0

Format 2b: UPEMPdsss-ss-ssss
(blank line)
OR
UPEMPdaaaaa

(blank line)

Where: d is definer P (Production), T (Training), I (IMF only), or B (BMF only).

sss-ss-ssss is the Social Security Number.

aaaaa is the SEID

ccode is Command Code.

0 is to delete command code.

1 is to add command code.

Note: Format 2a adds or deletes Command Code(s) from the user's Training or Production Profile.

Note: Format 2a changes the user's File Access Restriction between IMF only (I), BMF only (B), or unrestricted (P) while adding/deleting Command Codes.

Note: Format 2b changes the user's File Access Restriction between IMF only (I), BMF only (B), or unrestricted (P) with no changes to Command Codes.

2.12.2.40.3
(11-09-2023)

(1) Lock or unlock a user's Profile (unlocks system lock, security lock, or self lock) or delete a user

Format 3: Lock or unlock a user's Profile (unlocks system lock, security lock, or self lock) or delete a user

Format 3: UPEMP sss-ss-ssss nnnnnnnnnn
action
OR
UPEMP aaaaaa nnnnnnnnnn
action

Where: sss-ss-ssss is the Social Security Number.
aaaaa is the SEID
nnnnnnnnnn is the Employee Number.
action is literal LOCK, UNLOCK, or DELE EMP (delete employee).

Note: Format 3 locks or unlocks a user's Profile. The lock feature sets the "security lock". The unlock feature cancels all lock types (system lock, security lock, or self lock). The delete feature removes a user from the system.

2.12.2.40.4 (1) Delete an authorized Foreign Location
(11-09-2023)

**Format 4: Delete an
authorized Foreign
Location**

Format 4: UPEMP sss-ss-ssss sc
DELE OID
OR
UPEMP aaaaa sc
DELE OID

Where: sss-ss-ssss is the Social Security Number.
aaaaa is the SEID
sc is Office Identifier (OID).
DELE OID is delete employee identifier literal.

Note: Format 4 removes an authorized Foreign Location.

2.12.2.40.5 (1) Perform workload maintenance functions
(11-09-2023)

**Format 5: Perform
workload maintenance
functions**

Format 5a: UPEMPWsss-ss-ssss
OR
UPEMPWaaaaa

Format 5b: UPEMPWsss-ss-ssss
n/sss-ss-ssss
OR
n/

Format 5c: UPEMPWaaaaa
n/sss-ss-ssss
OR

n/

Where: W is Definer W (Workload Maintenance).

sss-ss-ssss is the Social Security Number.

aaaaa is the SEID

n indicates which slot number to be used for the Positive SSN. This number can be one or two digits between 1 - 15 followed by a slash(/); ex. 1/ or 01/ or 15/ not 015/.

Note: Format 5a displays the Positive Workload Maintenance List for the employee whose SSN is listed.

Note: Formats 5b and 5c permits change of the information in the employee's Positive Workload Maintenance List. The change may be from nothing to something (an add), something to something else, or something to nothing (a delete). To add or change, type the slot number and a slash followed by the SSN to be added or changed. To delete, type the slot number and a slash. Any slot number not listed will remain unchanged.

2.12.2.40.6
(11-09-2023)

(1) Delete an employee's profile

Format 6: Delete an employee's profile

Format 6: UPEMP sss-ss-ssss nnnnnnnnnn
DELE EMP
OR
UPEMP aaaaa nnnnnnnnnn
DELE EMP

Where: sss-ss-ssss is the Social Security Number.

aaaaa is the SEID

nnnnnnnnnn is the Employee Number.

DELE EMP is delete employee profile literal.

Note: Format 6 removes an employee profile. User can not be deleted if in an active (signed on) IDRS session. .

2.12.2.40.7
(11-09-2023)

- (1) Employees' access to multiple databases is controlled by using UPEMP to add Foreign (secondary) Locations

Format 7: Employees' access to multiple databases is controlled by using UPEMP to add Foreign (secondary) Locations

Format 7: UPEMPSsss-ss-ssss oi oi ... oi
 OR
 UPEMPSaaaaa oi oi ... oi

Where: S is Definer S (Secondary/Foreign location).
 sss-ss-ssss is the Social Security Number.
 aaaaa is the SEID
 oi is Office ID of the desired location (1 to 15 may be entered).

Note: Format 8 authorizes access to Foreign Locations for the owner of the input Social Security Number. Up to 15 Foreign Locations can be added. The Office Identifier (OID) entered must not be the same as the SSN owner's Home Location OID, and no duplicate Foreign Location OIDs can be installed.

Note: Employee Command Code Profiles at Foreign Locations are always exactly the same as at their Home Location. Definer 'S' cannot be used to change employee Command Code Profiles.

Note: If the employee is signed on during this transaction, the employee will immediately be able to determine the authorization via the SFDIS command. However, the employee will not be able to change mode (CMODE) until the next SINON. The employee should be advised to SINOF and then SINON if this activity is required immediately.

2.12.2.40.8
(11-09-2023)

- (1) Multi-Access employees can have their Command Code Profile set to NULL at their Home Campus

Format 8: Multi-Access employees can have their Command Code Profile set to NULL at their Home Campus

Format 8: UPEMPNsss-ss-ssss ppp
OR
UPEMPNaaaaa ppp

Where: N is Definer N (NULL).
sss-ss-ssss is the Social Security Number.
aaaaa is the SEID
p is Literal ON/OFF.

Note: Format 8 changes the NULL Status of the employee's Home Command Code Profile to ON or OFF. ON prevents employees from using their Command Codes at their Home Location, so that they may only access Foreign Locations. An employee with a NULL Profile can still use SINON, SINO, STATS, and CMODE at their Home Location.

2.12.2.41
(11-09-2023)
**UPHST - Update /
Display Host Profile**

(1) UPHST displays or changes the list of Command Codes in a host profile. This feature controls the cross-routing of Command Codes from host to host. A host may only forward Command Codes which are on its authorized list. There is an additional feature that allows the updating of all ten IDRS hosts with the inputting of 1 transaction.

2.12.2.41.1
(11-09-2023)
**Format 1: Display the
current list of Command
Codes authorized for a
given host**

(1) Display the current list of Command Codes authorized for a given host

Format 1: UPHSTDnnnn

Where: D is definer for display.
n is the host name **

Note: Format 1 displays the current list of Command Codes authorized for a given host. If a host has more than one screen's worth of Command Codes, the output is automatically paginated with an embedded PAGE command added to the bottom of each screen.

Note: ** The host name is the same name used for Command Code routing (i.e.: Austin 2200 would be AUH3 or the Fresno Document Input System would be FRD1).

2.12.2.41.2 (1) Add or delete up to a full screen of Command Codes from the host profile
(11-09-2023)

**Format 2: Add or delete
up to a full screen of
Command Codes from
the host profile**

Format 2: UPHST nnnn
ccode 1 ccode 0

Where: nnnn is the host name **
ccode is the command code.
0 is to delete Command Code.
1 is to add a Command Code.

Note: Format 2 adds or deletes up to a full screen of Command Codes from the host profile. If a host needs more than a screen full of Command Codes, a subsequent UPHST entry is used.

Note: Hosts have Production profiles only; there are no Training profiles for hosts.

Note: ** The host name is the same name used for Command Code routing (i.e.: Austin 2200 would be AUH3 or the Fresno Document Input System would be FRD1).

2.12.2.41.3 (1) Update all ten IDRS hosts with the inputting of 1 transaction
(11-09-2023)

**Format 3: Update all ten
IDRS hosts with the
inputting of 1
transaction**

Format 3: UPHST IDRS
ccode 1 ccode 0

Where: IDRS is the literal that allows the updating of all 10 IDRS hosts at once.
ccode is the command code.
0 is to delete Command Code.
1 is to add a Command Code.

- 2.12.2.42 (11-09-2023) **UPMAF - Update the Maximum Profile Authorization File (see also ADMAF)**
- (1) UPMAF adds Command Code(s) to or deletes Command Code(s) from the Maximum Profile Authorization File (MPAF) for a Unit.
 - (2) UPMAF also allows for the locking and unlocking of up to 5 units.

- 2.12.2.42.1 (11-09-2023) **Format 1: Add Command Code(s) to or delete Command Code(s) from the Maximum Profile Authorization File (MPAF) for a Unit**
- (1) Add Command Code(s) to or delete Command Code(s) from the Maximum Profile Authorization File (MPAF) for a Unit

Format 1: UPMAF uuuuu
ccode 1 ccode 1 ccode 0 ccode 0 ccode 1

Where: uuuuu is the Unit Number.
ccode is the command code.
0 is to delete Command Code.
1 is to add a Command Code.

Note: If Command Code(s) are deleted from the MPAF, the Command Code(s) will immediately be removed from the associated UCCP. The Command Code(s) will be removed from all of the user's Profiles in the Unit at the end of day during record maintenance.

- 2.12.2.42.2 (11-09-2023) **Format 2: Lock and unlock of up to 5 units**
- (1) Lock and unlock of up to 5 units

Format 2: UPMAFLuuuuu x uuuuu x uuuuu x uuuuu x uuuuu x

Where: uuuuu is the Unit Number (up to 5 units).
L is Definer.
x is L for lock or U for Unlock.

Note: This format allows for the locking and unlocking of up to 5 units. The purpose of locking a unit is that no employees can be added to the unit, moved in or from the unit. Employees may be deleted from a locked unit.

The SFINQM and SFINQU screens now include information on the current lock status. The literal LOCKED =YES or LOCKED = NO appears on the second line. The default is "No".

Note: The following error: UNITS WITH # ARE INVALID OR IN ERROR - NO UNITS WERE PROCESSED will result for these conditions.

2.12.2.43
(11-09-2023)
**UPTRM - Update a
Terminal**

- (1) UPTRM changes the permanent or temporary Time On/Off parameters for a terminal.

Format: UPTRM tttt ffffnnnn

Where: tttt is Terminal Security ID (TSID).

ffff is Time Off.

I is Indicator. blank = Permanent; * = Temporary.

nnnn is Time On.

Note: Temporary changes can only be made to the Time Off parameter. (The temporary Time Off expires at 2400 Midnight). The asterisk must follow the Time Off for temporary entries.

2.12.2.44
(11-09-2023)
**UPUNT - Update the Unit
Command Code Profile
(see also ADUNT)**

- (1) UPUNT is used to maintain a Unit's Minimum Command Code Profile (UCCP).
(2) Update the Command Codes in a Unit.
(3) Turn workload management on or off for a Unit
(4) Allow or disallow rerouting also known as Universal Access for a Unit
(5) Enable or disable TRDB dual SINON for a Unit

2.12.2.44.1
(11-09-2023)
**Format 1: Update the
Command Codes in a
Unit**

- (1) Update the Command Codes in a Unit

Format: UPUNT uuuuu
ccode 1 ccode 1 ccode 0 ccode 0 ccode 1

Where: uuuuu is the Unit Number.

ccode is the command code.

0 is to delete Command Code.

1 is to add a Command Code.

Note: When adding Command Code(s) to the UCCP, the MPAF is updated with the Command Code(s) immediately. The added Command Codes will be added to all of the user's Profiles for that Unit at the end of day during record maintenance.

2.12.2.44.2
(11-09-2023)

Format 2: Turn workload management on or off for a Unit

(1) Turn workload management on or off for a Unit

Format: UPUNTWuuuuu YES/NO

Where: W is definer to turn a Unit's workload Management on or off.

uuuuu is the Unit Number.

[YES/NO] is required parameter.

YES = all employees in the Unit will have their access limited to tax accounts on their Positive Accounts List.

NO = employees not limited to tax accounts on their Positive Accounts List.

Note: Format 2 turns on/off Workload Management for a Unit.

Note: The workload parameter may be set to "Yes" or to "No" at any time without regard to its current setting. If, for example, it is set to "YES" for a Unit which is already "YES", the entry will be accepted with no error reported.

2.12.2.44.3
(11-09-2023)

Format 3: Allow or disallow rerouting also known as Universal Access for a Unit

(1) Allow or disallow rerouting also known as Universal Access for a Unit

Format: UPUNTRuuuuu YES/NO

Where: R is definer to change a Unit's re-routing privileges or access to another Campus' IDRS database.

uuuuu is the Unit Number.

[YES/NO] is required parameter.

YES = this Unit may access another Campus' IDRS database.

NO = this Unit may NOT access another Service Center's IDRS database.

Note: Format 3 turns on/off Universal Access for a Unit.

2.12.2.44.4
(11-09-2023)

(1) Enable or disable TRDB dual SINON for a Unit

**Format 4: Enable or
disable TRDB dual
SINON for a Unit**

Format: UPUNTTuuuuu YES/NO

Where: T is definer to allow employees in this Unit to be given
TRDB dual SINON capability.

uuuuu is the Unit Number.

[YES/NO] is required parameter.

YES = employees in this Unit may be given dual SINON.

NO = employees in this Unit may not have dual SINON.

Note: Employees are not automatically enabled for dual SINON when this
parameter is set to YES, but the Unit must be enabled first before UPEMP
will allow this access to be given to individual employees in the Unit.

This Page Intentionally Left Blank

Security and Communication Services (SACS)

Security Command Codes 2.12.2

page 71

Exhibit 2.12.2-1 (11-09-2023)

Appendix A: Operator Type Codes and units (for ADDEM)

Each Operator Type Code is only valid for the corresponding listed designated units associated to location code/Office Identifier (OI) of 98 and 99 ONLY.

Note: 5 digit Unit number is made up of 2 digit location code/Office Identifier and 3 digit Organization number.

Note: nn below can be 98 or 99 only.

Operator Type Code	Unit	Operator Type Description
IRSOPR	nn940	COMPUTER OPERATOR
IRSCOM	nn941	COMMUNICATIONS
IRSCSA	nn942	COMPUTER SYSTEMS ANALYST
IRSAPL	nn944	APPLICATIONS
IRSSYS	nn945	SYSTEMS
IRSAUD	nn946	AUDITOR
IRSFTP	nn947	FTP OPERATOR
IRSOCC	nn948	OCC OPERATOR
IRSAUT	nn949	AUT OPERATOR

